A model of a secure information system for cognitive data processing in IoT sensor networks for laboratory climatic testing[⋆]

Yaroslav Tarasenko[1,*,†], Oleh Chervotoka[1,†], Serhii Orlov[1,†], Nataliia Lada[1,†], Volodymyr Shapoval[2,†] and Andrian Piskozub[3,†]

[1] *State Scientific Research Institute of Armament and Military Equipment Testing and Certification, 18000 Cherkasy, Ukraine*
[2] *Cherkasy State Technological University, 18000 Cherkasy, Ukraine*
[3] *Lviv Polytechnic National University, 12 Stepana Bandery str., 79000 Lviv, Ukraine*

Abstract

Information protection during data transmission in IoT-based sensor networks used in laboratory testing is an important task in the context of growing demand for laboratory climatic tests. The use of cognitive artificial intelligence in the process of managing laboratory climatic tests requires taking into account not only factors affecting the test object, but also factors of possible network-based attacks on the cyber-physical system. That is why the paper presents a model of a secure information system for cognitive data processing in IoT sensor networks. When cognitive information processing is performed, situational factors of the first kind (data on climatic conditions) and the second kind (potential network-based attacks) are taken into account. Data protection is implemented through cryptographic information transformation based on the generation of two-operand asymmetric CET-operations with an accuracy of up to the permutation of the second operand when transmitting information from sensors to the cognitive data processing unit (Algorithm I). To protect the information transmitted from the database to the cognitive processing unit, a synthesis of direct and inverse operations is used based on the generation of two-operand asymmetric CET-operations with an accuracy of up to the permutation of the first operand (Algorithm II). To protect the information transmitted from the cognitive data processing unit to the actuators, a synthesis of direct and inverse operations is used based on the generation of two-operand asymmetric CET-operations with an accuracy of up to the permutation of the transformation result (Algorithm III). Situational factors of the first kind affect the information, due to which encryption is performed according to algorithm I. The presence of algorithms II and III is due to situational factors of the second kind. A graphical and tabular representation of the information system model was formed, which determined the role and place of protection algorithms in the functional structure of an IoT-based sensor network. The analysis of the development in modeling managerial decision-making based on cognitive data processing, taking into account situational factors of the first and second kind under conditions of network-based attack simulation, showed improved efficiency. The development is 7% more efficient compared to the results of managerial decision-making by a person and 49% more efficient compared to the use of the LIMS considered in the work.

Keywords

cryptographic information protection, wireless sensor networks, network-based attacks, cognitive intelligence, cognitive map, CET-operations, IoT based climatic testing, laboratory information management systems

1. Introduction

Applying new technologies in production development and globalization processes impose high requirements on the quality of any product, its safety and compliance with regulatory documents. This situation leads to the search for ways to improve and expand the procedures for confirmingthe quality of manufactured products. Determining the characteristics to confirm reliability and quality is the task of research laboratories. Today, the problem of reproducing the impact of environmental conditions on manufactured products in the laboratory by using secure

[⋆] *CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine*

[*] Corresponding author.
[†] These authors contributed equally.

yaroslav.tarasenko93@gmail.com (Ya. Tarasenko); ron1978@ukr.net (O. Chervotoka); w7nner@gmail.com (S. Orlov); ladanatali256@gmail.com (N. Lada); vsh60909@gmail.com (V. Shapoval); andriian.z.piskozub@lpnu.ua (A. Piskozub)
0000-0002-5902-8628 (Ya. Tarasenko); 0000-0002-1083-4178 (O. Chervotoka); 0000-0003-3840-4089 (S. Orlov); 0000-0002-7682-2970 (N. Lada); 0009-0000-5334-4841 (V. Shapoval); 0000-0002-3582-2835 (A. Piskozub)

information systems is extremely relevant. According to a Value Market Report [1], the market for climatic test chambers is expanding rapidly. The report provides data on the market size starting from 2024 (USD 1.46 billion) and forecasts growth until 2033 (USD 1.79 billion) in increments of 2.33% (Figure 1).

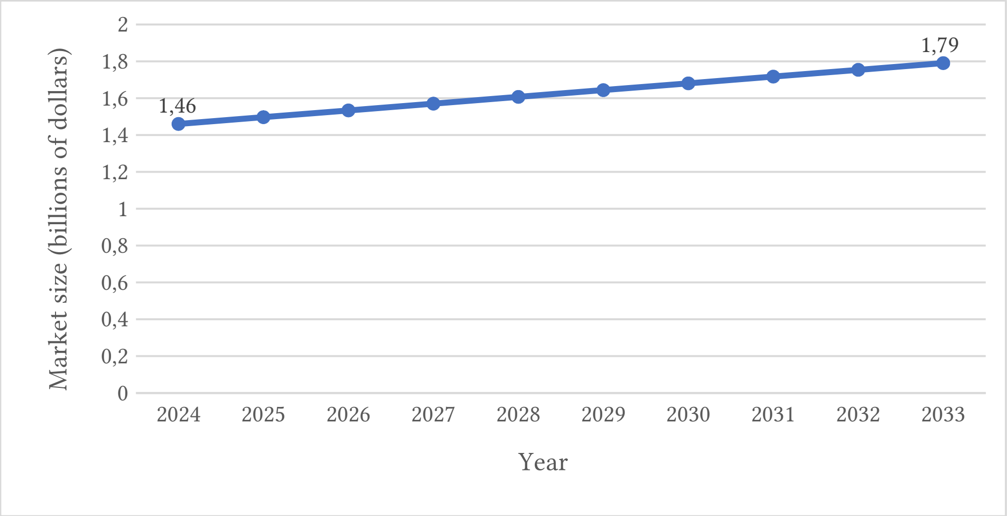

Figure 1: Climate test chambers market growth forecast to 2033

Presented data proves the relevance of laboratory testing for the impact of external climatic factors. This report also identifies the prospects for the use and development of laboratory climate testing technologies aimed at improving the accuracy and efficiency of testing processes. These areas include automation of testing processes and data processing. It is noted that automation integrated with the Internet of Things (IoT) technology in climate testing chambers has high potential and can rapidly change the market. The analytical report proves that IoT technology implemented in climate chambers enables automated real-time data processing, remote monitoring, and test prediction approaches. This is confirmed by a review of the findings of the National Institute of Standards and Technology (NIST), which confirms the high potential of IoT technology to support product quality improvement processes.

Automation of laboratory tests is an important component of improving the accuracy, objectivity and reproducibility of the results obtained. Automation processes are researched, improved and implemented to research laboratories in a wide range of areas. Paper [2] investigates automation in clinical microbiology laboratories. The purpose of automation is to obtain accurate, relevant, and timely results. The author suggests the use of artificial intelligence and specialized information systems to achieve the needed level of automation. It is also appropriate to use artificial intelligence in laboratory climatic testing, provided that the peculiarities of climatic testing processes are taken into account. Such features include: a wide range of climatic impacts on the test object, the importance of adjusting further procedures based on the object's response to external factors, taking into account the results of previous tests, and the use of IoT sensor networks. It is IoT sensor networks that are characterized by the presence of actuators which influence laboratory testing procedures. Such conditions determine the need to use an alternative direction of artificial intelligence in the process of automating laboratory climate tests, which is cognitive artificial intelligence. The cognitive approach allows modelling operator behavior and reactions of a real person when interacting with IoT-based cyber-physical systems in the context of test process automation.

The analysis of modern challenges, current technological solutions and forecast of trends in the development of laboratory testing technologies allows to substantiate the problem of developing and improving mechanisms for automated data processing in IoT-based cyber-physical systems through the introduction of information systems using cognitive artificial intelligence.

2. Background and related work

Laboratory Information Management Systems (LIMS) are now widely used in automating data processing in laboratory testing. Such systems provide functionality for managing laboratory tests. Paper [3] analyses such systems from the side of data management in testing research laboratories. The authors note that the main task of LIMS is to automate the processes of storing data from research experiments. The authors refer to other areas, such as communication, scheduling, etc., as another class of software that is not related to LIMS. It can be agreed with this statement from the point of view of the conceptual process in laboratory test data processing, in terms of data storage mechanisms. Automated information systems of research laboratories are not limited to the automatic storage of the results obtained, but also perform their processing. Thus, work [4] describes the actual implementation of a specially developed LIMS in the National Health Laboratory (Timor-Leste) in order to overcome the challenges of automating the work at research laboratories, which include data processing. It is proposed to overcome such challenges with the help of LIMS also in [5]. A significant advantage of the approach proposed by the authors is the integration of LIMS with the IoT system and wireless sensor network to automate repetitive tasks in laboratories. Automation of repetitive tasks does not allow for the implementation of a full-fledged control system taking into account situational factors.

In order to improve data processing, attempts are being made to use artificial intelligence as an additional tool for automating management and decision-making processes. Paper [6] describes the use of artificial intelligence in information management for robotic systems during laboratory research. The approach is conceptually appropriate for an IoT-based system of automated laboratory testing, but requires significant constructive adaptation.

As already mentioned, the IoT-based approach of the automated laboratory testing system involves the use of wireless sensor networks. Information from the sensors is transmitted via wireless channels for processing by the information system, which in turn transmits the data to the actuators in order to influence the testing processes depending on the situational decisions made. This poses a threat to the integrity and confidentiality of the transmitted data. In order to protect the information system and ensure the objectivity and reliability of information, it is important to integrate security modules into the overall system model. Paper [7] discusses various approaches to organizing the protection of online LIMS and provides a classification of threats, according to which there are network-based, access-based and device-based attacks. In the case of considering an IoT-based sensor network, network-based attacks are the most important. The approaches to protecting the integrity and confidentiality of information from network-based attacks, including those that exploit the vulnerabilities of wireless networks, include encryption. The work in the field of strategies for securing IoT devices [8] proves the need to take into account the limited memory resources of IoT devices for the implementation of encryption algorithms. Lightweight cryptographic algorithms [9] are being developed and can be integrated into the laboratory test information management system, but need to be improved to solve the problem of taking into account situational factors. Work in the field of cybersecurity using information-driven operations [10] allows encryption based on data obtained in a particular situation.

An analysis of the functionality of existing LIMS has revealed their insufficiency for the full automation of research laboratories that use IoT technologies due to the lack of implementation of modern artificial intelligence approaches, in particular cognitive intelligence, in the systems. The insufficiency of current LIMS developments in the field of laboratory climatic testing has been identified. LIMS models do not take into account the situational factor and do not have an adequate level of integrated information security tools.

There is a need to develop a model of an information system for managing the process of laboratory testing for the impact of external climatic factors through the use of an IoT-based sensor network. A significant contribution to the development of information technologies for automating the assessment of climatic impact parameters was made in [11]. The authors proposed an approach based on operational monitoring data, which should be used in the process of processing information obtained during the monitoring of IoT-based laboratory testing systems for the impact of external climatic factors.

Existing scientific works determine the need to develop a model of an information system for data processing in IoT-based sensor networks for laboratory climatic testing, which takes into account situational factors caused by both the impact of external climatic factors on the test object and potential security threats to the sensor network.

The aim of the work is to improve the efficiency of automated control in climatic laboratory testing processes based on cognitive artificial intelligence through situational control of testing processes taking into account the probable network-based attacks.

To achieve this goal, the following tasks were set:

- To form a psychological basis of human decision-making for cognitive modelling of automated managerial decision-making processes.
- To model the processes of automated managerial decision-making by building a cognitive map.
- To form a tabular and graphical representation of the information system model.
- To perform modelling of climatic laboratory testing processes management based on situational factors.
- To build algorithms for cryptographic transformation of information in transmitting over wireless channels of the sensor network.

3. Modelling of the information system

System modelling consists of several interrelated components. These include a psychological basis with a formalized representation of concept formation in the form of an ontology. The cognitive map, which is formed by the concepts' set of the ontology is the basis for modelling the information system using a directed graph. Situational management model and cryptographic protection unit are integral components of the system. In situational modelling, it is mandatory to take into account situational factors of environmental conditions and the results of the impact on the test object measured by sensors (situational factors of the first kind) and factors of potential network-based attacks on data transmission channels in an IoT-based wireless sensor network (situational factors of the second kind). A schematic diagram of the components' interaction in the IoT-based sensor network with an information system of cognitive data processing, taking into account situational factors of the first and second kind, is shown in Figure 2.

Sensors that measure environmental conditions and the condition of the test object encrypt the data and transmit it to the information system where it is processed taking into account information about previous tests from the database. The decision on further actions is sent to the actuators and entered into the database. Potential attacks affect the transmission of data from the sensors to the information system, from the information system to the actuators, and from/to the database.

3.1. Psychological basis for cognitive modelling

Artificial intelligence is required to process the information received from sensors and the information about the results of previous tests from the database. Traditional approaches to implementing a neural network are not sufficient for effective managerial decision-making during laboratory tests on the impact of external climatic factors. A prerequisite is the modelling of human actions. The main tool for meeting this requirement is cognitive artificial intelligence.

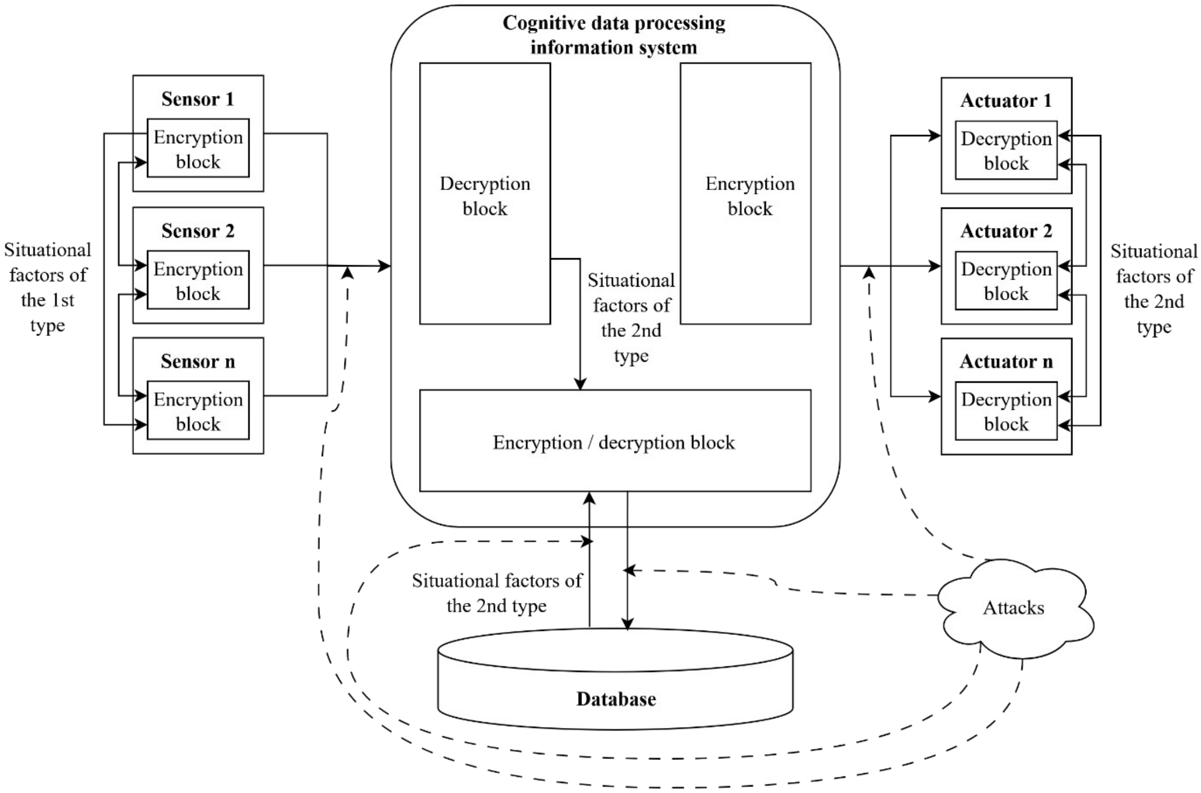
Cognitive data processing information system
Sensor 1
Encryption block
Sensor 2
Encryption block
Sensor n
Encryption block
Situational factors of the 1st type
Decryption block
Encryption block
Situational factors of the 2nd type
Encryption / decryption block
Actuator 1
Decryption block
Actuator 2
Decryption block
Actuator n
Decryption block
Situational factors of the 2nd type
Situational factors of the 2nd type
Attacks
Database

Figure 2: Schematic diagram of the interaction of components of an IoT-based sensor network with an information system of cognitive data processing, taking into account situational factors

The work [12] is of great importance for performing human thought simulation processes. The results can be used in the process of forming a psychological basis for cognitive modelling of managerial decision-making processes. The results should be used not to model the interaction between artificial intelligence and humans, as noted in the paper, but to model human behavior in managing laboratory tests. To model the behavior of objects in a wireless sensor network and enable the system to respond according to the principle of human behavior, the structure of interaction and relationships described in [13] was used.

Paper [13] uses 3 main concepts that are appropriate to use as a psychological basis for modelling human behavior: short-term memory, long-term memory, and integration of memory types. In the context of solving the problem of forming a psychological basis for cognitive modelling, all parameters of current tests are used as the concept of short-term memory. The concept of long-term memory is the most significant ones recorded in the database based on the data of previous tests. Integration is performed by prioritizing and assessing the data's relevance to the relevant psychological functional state based on the method described in [14]. An ontology is a tool for describing concepts. The ontology provides the appropriate concept's formation tools for further cognitive modelling, as well as for situational managerial decision-making. The approach to defining an ontology of typical processing and computer simulation tasks described in [15] can be extended to take into account the basic concepts of the psychological basis for modelling human behavior. The ontology is described by equation:

$$O=\{A=B\cup C,K,K^{*},K'=\left\{\sum_{j=1}^{n}\frac{\mu^{S_j}\left(k^{*},i\right)}{\sum_{i=1}^{N}\mu^{S_j}\left(k^{*},i\right)}\right\},F\{f(.)\}, \tag{1}$$

where A is the set of concepts that make up the terms of ontology; B is the set of possible tasks during laboratory tests; C is the set of terms that reveal the content of possible tasks; K is the set of parameters of current tests; K^{*} is the set of the most important parameters in the test database; K'

is a set that performs memory integration by linking current events with those defined in the test base; *S* is a functional psychological state; k^* is an element from the test base; *N* is total number of parameters of current tests; μ is similarity measure; *n* is number of possible psychological states of interpretation; *F* is a set that contains an interpretation function; *f*(.) is an interpretation function that forms an ontology glossary based on possible tasks.

The ontology allows to structure the data of the subject area in the form of concepts for further cognitive processing.

3.2. Cognitive map of information processing for automated managerial decision-making

According to paper [16], structured data formed in the human brain during information processing is based on dynamic memory processes. Such data can be the basis for information processing using cognitive artificial intelligence. Cognitive maps and diagrams are the main tools for representing structured knowledge. In the context of the current task, cognitive maps will be the most useful. According to the mechanisms of abstraction from structure-based models presented in [16], cognitive maps, in contrast to cognitive schemas, represent an association-based mechanism and a graph-based mechanism. Associations make it possible to make decisions as close to human as possible based on the processed data. The graph-based representation allows using data processing in modelling managerial decision-making processes and integrating the data processing into the information system, the model of which is presented in graphical form in 3.3.

In this case, the structure-based model is the ontology, which, according to formula (1), already takes into account dynamic memory processes.

The cognitive map is built using the mechanisms presented in [17]. The cognitive map acts as an oriented symbolic graph. The vertices of the graph are situations, the arcs are relations followed by subsequent situations. The "+" sign reflects an increase in the importance of the resulting situation with an increase in the importance of the situation that caused it, and the "−" sign reflects a decrease in the importance of the resulting situation with an increase in the importance of the situation that caused it. A cognitive map of information processing for automated management decision-making by an information system is shown in Figure 3.

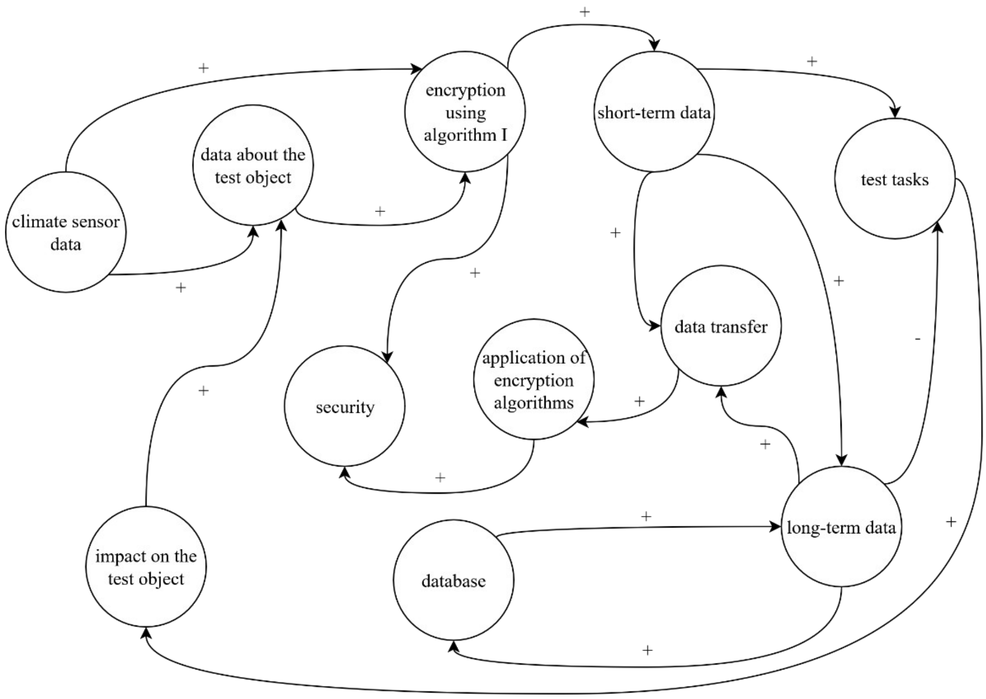
encryption using algorithm I
short-term data
test tasks
data about the test object
climate sensor data
data transfer
application of encryption algorithms
security
impact on the test object
database
long-term data
+
-

Figure 3: Cognitive map of information processing

The path of the concept when making a decision in processing the received data by the system from the moment of receipt to the moment of decision-making is described by analogy of [17] by the formula:

$$a_i \rightarrow b_k \ldots \rightarrow a_j^O, \tag{2}$$

where a_i is an element of the concepts' set in the ontology; b_k is an element of the tasks' set; a_j^O is a concept that represents the situation according to the model of the laboratory tests' ontology; (i, k, ..., j) is a path.

The formed cognitive map is a necessary component for integration into the model of the information system for cognitive processing of laboratory climatic testing data as one of the output data streams responsible for deciding on further actions. The decision is made on the basis of cognitive data processing.

3.3. Presentation of the information system model

The methodological approach for modelling the information system was chosen from [18]. The functional representation of the information system in tabular form as a F-system was used (Table 1).

Table 1
Functional representation of the developed information system model

	y_1	y_2	y_2	y_3	y_3	y_3	y_3	y_3	y_2	y_1	y_1
	z_0	z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8	z_9	z_{10}
x_1	z_{10}	z_2	z_3	z_4	z_8	z_6	z_7	z_9	z_5	z_0	z_1
x_2	z_1	z_3	z_4	z_0	z_7	z_5	z_5	z_8	z_9	z_{10}	z_2

The represented table shows the functional model of a secure information system for cognitive data processing in IoT sensor networks for laboratory climatic testing. The F-system has 11 states: z_0 is a start of tests; z_1 is a measurement of environmental parameters by sensors; z_2 is a measurement of the test object state by sensors; z_3 is a edge calculations in sensors; z_4 is a cryptographic transformation of the information by algorithm I; z_5 is a connection with the database; z_6 is a cryptographic transformation of the information by algorithm II; z_7 is a data analysis; z_8 is a decision-making; z_9 is a cryptographic transformation of the information by algorithm III; z_{10} is a execution of actions by actuators. The F-system has 2 input data streams and 3 output data streams. The input data streams are: x_1 is a transmission of measured parameters; x_2 is a transmission of a control signal. The output data streams are: y_1 is a signal to change the state of the object or climatic conditions; y_2 is a decision on further actions; y_3 is a calculation results.

The table displays the input data streams horizontally and the output data streams vertically in accordance with the system state. The cells show the values of the system's transitions from one state to another.

Cognitive data processing is used to obtain a data stream that is responsible for deciding on further actions.

The graphical representation of Table 1 is performed using a directed graph (Figure 3). The vertices of the graph represent the states of the system, and the arcs represent the transitions between the states.

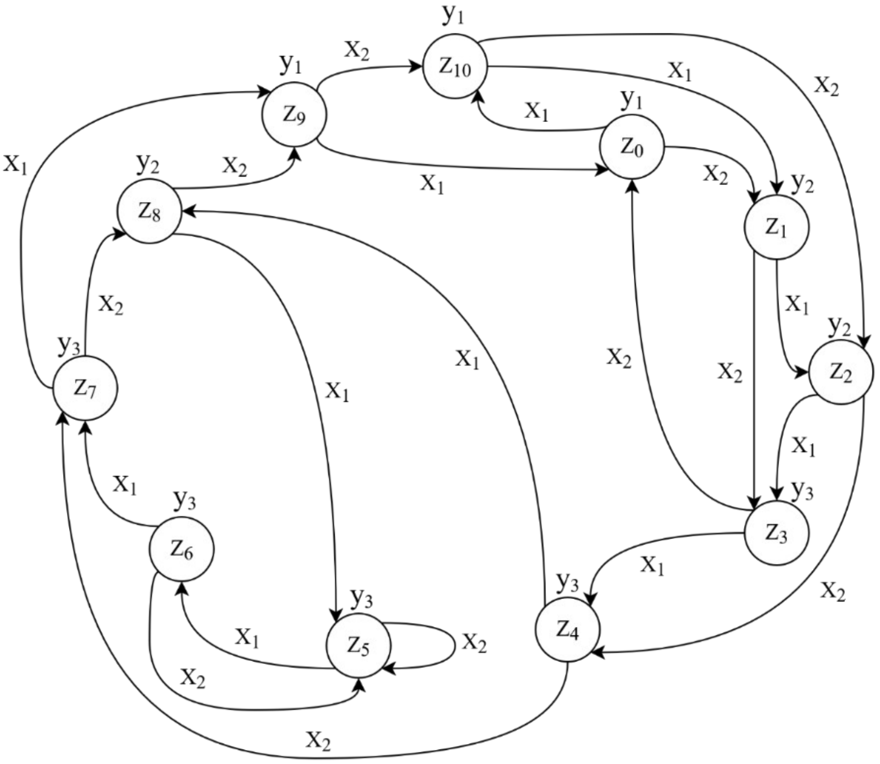

Figure 4: graphical representation of the developed information system model

Modelling of the information system in a formalized form is performed by means of a discrete-deterministic model according to the formula:

$$F = \langle Z, X, Y, \varphi, \vartheta, z_0, y_2, S \rangle, \tag{3}$$

where Z is a set of states; X is a set of input data; Y is a set of output data; φ is a transition function; ϑ is an output function; z_0 is the initial state; y_2 is decision making based on cognitive modelling; S is a set of encryption algorithms.

3.4. Situational model of climatic laboratory testing process management

Managerial decisions made by the cognitive data processing module of the information system are based on the management approach described in [19]. To make a managerial decision, the significance of the situation for achieving the main goals (Table 2) of the information system design, as well as situational goals of the first (Table 3) and second (Table 4) kind, is taken into account according to the formula:

$$S = \bigcup_{r=1}^{14} S_c^{K'} \cup \bigcup_{l=1}^{4} S_{c'}^{K'} \cup \bigcup_{m=1}^{3} S_{c''}^{K'}, \tag{4}$$

where S is a situation; $S_c^{K'}$ reflects the level of achievement of the main goal C in accordance with the evaluation characteristic of combining short-term and long-term memory when building an ontology; $S_{c'}^{K'}$ reflects the level of achievement of the situational goal of the first kind C'; $S_{c''}^{K'}$ reflects the level of achievement of the situational goal of the second kind C''.

Objectives from C_1 to C_4 are functional objectives, from C_5 to C_9 are information objectives, from C_{10} to C_{11} are information security objectives, and from C_{12} to C_{14} are management objectives.

Situational objectives of the second kind are caused by potential attacks on data transmission channels in an IoT-based information system.

Table 2
Main objectives of information system design

Designation	Description
C_1	Automation of laboratory testing processes
C_2	Automatic managerial decision making
C_3	Cognitive modelling of human management processes
C_4	Filling the test database
C_5	Organizing of long-term data storage
C_6	Organizing the stored data processing
C_7	Organizing of processing data received during tests
C_8	Optimization of data collection
C_9	Ensuring data reliability
C_{10}	Ensuring data integrity and confidentiality
C_{11}	Protecting data through information-driven encryption
C_{12}	Improving the efficiency of test management
C_{13}	Improving the accuracy of task execution
C_{14}	Improving the objectivity of results interpretation

The technique of adapting laboratory tests to changes caused by external climatic factors and changes in the test object under the influence of these factors and potential network-based attacks, according to the results of the study [19], is determined by the formula:

$$SA:(C_n \cup C_n^{'} \cup C_n^{''}, a_j^O) \rightarrow K \in K^{'};,. \tag{5}$$

Table 3
Situational goals of the first kind

Designation	Description
C_1	Adaptation of the test process in real time
C_2	Fixing changes in the parameters of the test object
C_3	Taking into account the data of previous tests
C_4	Fixing and changing environmental parameters

Situational objectives of the first kind are caused by external climatic factors in the test object.

Table 4
Situational goals of the second kind

Designation	Description
C_1	Ensuring data integrity
C_2	Ensuring data confidentiality
C_3	Protection against potential threats to data transmission channels

Potential attacks involve the use of encryption algorithms for information transmitted over wireless channels in an IoT-based sensor network for laboratory climate testing.

3.5. Constructing the algorithms for cryptographic transformation of information

In the context of low resources in the presented system and the need to ensure the encoding and decoding of information at three transmission directions (when transmitting information from sensors to the cognitive data processing unit, which includes the encryption-decryption component of information, from the database to the cognitive data processing unit and from the cognitive data processing unit to the actuators), the use of traditional cryptographic algorithms is a difficult task to implement. In represented information system model, it is necessary to ensure the speed of operations as close to real-time as possible. In this case, it is advisable to use low-resource CET-encryption [9]. The peculiarity of the CET-encryption is that it is streaming, provides a high speed of cryptographic transformation of information and guarantees bidirectional transmission between the components of the IoT-based sensor network [20–25].

In this information system, it is advisable to use asymmetric network operations to ensure the encryption of the same information using the same key sequences but with the construction of different ciphers.

Among the CET-operations, it is advisable to distinguish strict cryptographic transformation operations that provide maximum uncertainty of encryption results [26]. These CET-operations guarantee the transformation of each bit of the operation with a probability of 0,5. Each one-operand CET-operation implements one substitution table. Two-operand CET-operations implement several substitution tables. The choice of the substitution table for converting the first operand is determined by the value of the second operand in which the pseudo-random sequence is entered. The group of two-bit two-operand CET-operations of strict cryptographic encoding is shown in Table 5.

When constructing cryptographic systems, it is advisable to use not one two-operand CET-operation, but a group of operations with specified properties.

Constructing a group of modified two-operand CET-operations with permutation accuracy is possible on the basis of three synthesis options:

- Up to permutation of the first operand

$$C_i(x,y)=C\left(C_i(x),y\right). \tag{6}$$

- Up to permutation of the second operand

$$C_i(x,y)=C\left(x,C_i(y)\right)., \tag{7}$$

- With permutation accuracy of the transformation result

$$C_i(x,y)=C_i\left(C(x,y)\right)., \tag{8}$$

Generating a group of two-operand operations is possible by using the method of synthesis of two-operand two-bit operations with permutation accuracy.

On the basis of (6)–(8), it is possible to implement a pseudo-random sequence generator that will select the encoding operation based on the information received from the sensors. It should be noted that, for example, when using (7), the entire group of operations presented in Table 5 will be implemented in a pseudo-random sequence. When using (6) and (8), operations that are not included in the specified mathematical group will be generated. This may increase the uncertainty of choosing a CET-operation to be used in the cryptographic transformation. However, not all generated operations will meet the requirements of strict cryptographic encoding.

Table 5
A group of two-bit two-operand CET operations of strict cryptographic encoding

$C_3=C_6^{'}=\begin{bmatrix} x_1\cdot(\overline{\gamma_1\oplus\gamma_2})\oplus x_2\cdot(\gamma_1\oplus\gamma_2) \\ x_1\cdot(\gamma_1\oplus\gamma_2)\oplus x_2\cdot(\overline{\gamma_1\oplus\gamma_2}) \end{bmatrix}\oplus\begin{bmatrix} \gamma_1 \\ \overline{\gamma_1} \end{bmatrix}$	$C_6=C_3^{'}=\begin{bmatrix} x_1\cdot(\overline{\gamma_1\oplus\gamma_2})\oplus x_2\cdot(\gamma_1\oplus\gamma_2) \\ x_1\cdot(\gamma_1\oplus\gamma_2)\oplus x_2\cdot(\overline{\gamma_1\oplus\gamma_2}) \end{bmatrix}\oplus\begin{bmatrix} \gamma_2 \\ \overline{\gamma_2} \end{bmatrix}$
$C_{12}=C_9^{'}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1} \\ k_1 \end{bmatrix}$	$C_9=C_{12}^{'}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \overline{k_2} \end{bmatrix}$
$C_{16}=C_{23}^{'}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \overline{k_1} \end{bmatrix}$	$C_{23}=C_{16}^{'}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \overline{k_2} \end{bmatrix}$
$C_{20}=C_{13}^{'}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1} \\ k_1 \end{bmatrix}$	$C_{13}=C_{20}^{'}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \overline{k_2} \\ k_2 \end{bmatrix}$
$C_1=C_2^{'}=\begin{bmatrix} x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \overline{k_2} \end{bmatrix}$	$C_2=C_1^{'}=\begin{bmatrix} x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
$C_8=C_7^{'}=\begin{bmatrix} x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \end{bmatrix}\oplus\begin{bmatrix} \overline{k_2} \\ k_2 \end{bmatrix}$	$C_7=C_8^{'}=\begin{bmatrix} x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
$C_{18}=C_{21}^{'}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \\ x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \overline{k_2} \end{bmatrix}$	$C_{21}=C_{18}^{'}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \\ x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
$C_{22}=C_{17}^{'}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \\ x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_2} \\ k_2 \end{bmatrix}$	$C_{17}=C_{22}^{'}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\overline{k_1} \\ x_1\cdot\overline{k_1}\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
$C_4=C_5^{'}=\begin{bmatrix} x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \overline{k_1} \end{bmatrix}$	$C_5=C_4^{'}=\begin{bmatrix} x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
$C_{15}=C_{24}^{'}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \\ x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \overline{k_1} \end{bmatrix}$	$C_{24}=C_{15}^{'}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \\ x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
$C_{14}=C_{19}^{'}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \\ x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \overline{k_2} \end{bmatrix}$	$C_{19}=C_{14}^{'}=\begin{bmatrix} x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \overline{k_1} \end{bmatrix}$
$C_{10}=C_{11}^{'}=\begin{bmatrix} x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \end{bmatrix}\oplus\begin{bmatrix} \overline{k_2} \\ k_2 \end{bmatrix}$	$C_{11}=C_{10}^{'}=\begin{bmatrix} x_1\cdot\overline{k_2}\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\overline{k_2} \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1} \\ k_1 \end{bmatrix}$

Synthesizing groups of CET-operations with permutation accuracy based on (6)–(8) will allow to build generators of pseudo-random sequences of CET-operations with the same properties to ensure the construction of cryptographic algorithms for stream encryption.

In the presented information system, it is advisable to implement cryptographic protection of information based on the generation of two-operand asymmetric CET-operations with an accuracy up to permutation of the second operand when transmitting information from sensors to the cognitive data processing unit (algorithm I). The generated direct and reverse asymmetric two-operand CET-operations will belong to the synthesized group with the accuracy up to permutation of the second operand and will have the same cryptographic properties.

To implement the cryptographic protection of information from the database to the cognitive data processing unit, it is advisable to use the synthesis of direct and inverse operations based on the generation of two-operand asymmetric CET-operations with an accuracy up to permutation of the first operand (algorithm II).

To implement the cryptographic protection of information from the cognitive data processing unit to the actuators, it is advisable to use the synthesis of direct and inverse operations based on the generation of two-operand asymmetric CET-operations with an accuracy up to the permutation of the transformation result (algorithm III).

The situational factors of the first kind affect the information used for encryption by algorithm I. The presence of algorithms II and III is due to situational factors of the second kind (potential attacks) to increase the reliability of information protection during transmission over wireless channels of a sensor network and protect from network-based attacks.

3.6. Efficiency of the information system model

Evaluation of the effectiveness of an information system requires taking into account the level of achievement of situational factors, such as those determined by the research objectives and the need to protect the information system. The level's value of situational goals achievement for proposed development can be compared with similar solutions. This can determine the effectiveness of proposed development. According to the approach described in work [27], to obtain level's value of situational goals achievement, it is necessary to determine the implementation level of the situational strategy by the formula:

$$\hat{R}_i = \frac{\sum_{j=1}^{n} R_{ik}^{j} \cdot R_{a_j^O}^{j}}{S_n}, , \tag{9}$$

where R_{ik}^{j} are the relevant solutions; $R_{a_j^O}^{j}$ is a solution of the final stage according to the cognitive map; S_n is the total number of situational decisions.

B is the set of possible tasks during laboratory tests;

For each strategy, the achievement's level of situational goals is calculated using the formula:

$$E_i = \sum E_j^{'} \hat{R}_i . \tag{10}$$

To obtain the value of the development efficiency, the modelling of testing a personal computer motherboard with a network-based attack situation was performed. As the data of previous tests, an information sample of 15 similar boards of different technical condition and manufacturers was used.

Calculating the achievement level of situational strategies based on the modelling results proved the increased efficiency of the proposed development by 7% compared to the results of human decision-making and by 49% compared to the use of LIMS discussed in Section 2.

Conclusions

The paper develops a model of a secure information system for cognitive data processing in IoT-based sensor networks for laboratory testing tasks based on cognitive artificial intelligence through situational management of laboratory testing processes, which makes it possible to automate the process of making managerial decisions taking into account protection against network-based attacks.

According to the modelling results, the proposed development demonstrates an efficiency that is 7% higher than human decision-making and 49% higher than the use of classical LIMS, taking into account the risks of network-based attacks.

At the work it was obtained following scientific results:

1. A psychological basis for decision-making by cognitive artificial intelligence based on ontological modelling was formed by using the concepts of short-term, long-term, and integrated memory through assessing functional psychological states, which made it possible to perform cognitive modelling of automated managerial decision-making processes.
2. A cognitive map of data processing in IoT-based sensor networks based on cognitive modelling was built by forming a directed graph using the transitions of concepts in the ontology of laboratory climatic tests, which allowed to perform modelling of automated managerial decision-making processes in the information system of cognitive data processing
3. A model of the information system for laboratory test management based on a cognitive data processing map was formed by means of tabular, graphical and formalized representation through the F-system and directed graph, which made it possible to integrate the cognitive approach of automatic decision-making into an IoT-based sensor network of laboratory climatic tests, taking into account network-based attacks.
4. Modelling the management of climatic laboratory testing processes depending on the main situational factors, situational factors of the first (external influences and the object's reaction) and the second (potential network-based attacks) kind was carried out by taking into account the importance of the situation for achieving the goals through the use of an ontological model of situational management with regard to risks, which allowed to form a model of managerial decision-making by the information system of cognitive information processing.
5. The choice of a stream encryption algorithm based on the generation of pseudo-random sequence of modified CET-operations with an accuracy up to permutation is determined by the requirements for cryptographic stability and available information resources. Algorithm I provides a change in the order of one-operand CET-operations when modifying a two-operand CET-operation. Therefore, when using it, it is possible to determine the requirements for converting a block of information. Algorithms II and III, in the process of modifying a two-operand CET-operation, modify one-operand CET-operations, and therefore change the lookup tables. An increase in the number of lookup tables provides an increase in cryptographic stability. However, the implementation of the requirements for converting a block of information is significantly complicated.

The practical value lies in the possibility of implementing the protected information management systems with the ability to automate the management of testing processes according to the developed model for real implementation in IoT-based research laboratories for climatic testing.

The prospect of further research is to expand the scope of secure data processing to the field of mechanical laboratory testing. A promising direction is to predict the behavior of the test object during climatic laboratory tests, taking into account cyber threats and automated formation of a digital twin model in IoT-based laboratory tests.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication’s content.

References

[1] Global Environmental Test Chambers Market Report, Environmental Test Chambers Market Size, Share, Growth, and Industry analysis Report Segmented by Type (Temperature and

Humidity Chamber, Thermal Shock, Corrosion Test Chamber, Xenon Test Chamber, Others), Application and Regions (North America, Europe, Asia-Pacific, Latin America, Middle East and Africa), 2025-2033. Value Market Report, 2025. https://www.valuemarketresearch.com/report/environmental-test-chambers-market

[2] A. Mencacci, G. V. De Socio, E. Pirelli, P. Bondi, E. Cenci, Laboratory Automation, Informatics, and Artificial Intelligence: Current and Future Perspectives in Clinical Microbiology, Frontiers in Cellular Infection Microbiology 13 (2023). doi:10.3389/fcimb.2023.1188684

[3] M. A. M. Alamer, et al., Impact of Implementing Laboratory Information Management Systems (LIMS) on Improving Data Management and Reporting, Chelonian Conservation and Biology 17.2 (2022). doi:10.18011/2022.04(1)1783.1792

[4] T. Oakley, et al., Implementation of a Laboratory Information Management System (LIMS) for Microbiology in Timor-Leste: Challenges, Mitigation Strategies, and End-User Experiences, BMC Medical Informatics and Decision Making 25.1 (2025). doi:10.1186/s12911-024-02831-6

[5] J. N. Wangere, E. Mwambe, D. Flavian, R. Sinde, Development of Smart Laboratory Information Management System: A Case Study of NMAIST Arusha of Tanzania, Int. J. Adv. Sci. Res. Eng. 08.04 (2022) 01-14. doi:10.31695/ijasre.2022.8.4.1

[6] S. U. Khan, V. K. Moller, R. J. N. Frandsen, M. Mansourver, Real-Time AI-driven Quality Control for Laboratory Automation: A Novel Computer Vision Solution for the Opentrons OT-2 Liquid Handling Robot, Appl. Intell. 55.6 (2025). doi:10.1007/s10489-025-06334-3

[7] A. E. Pena-Molina, M. M. Larrondo-Petrie, Safety and Security Considerations for Online Laboratory Management Systems, J. Cybersecur. Privacy 5.2 (2025) 24. doi:10.3390/jcp5020024

[8] I. Rozlomii, A. Yarmilko, S. Naumenko, Innovative Resource-Saving Security Strategies for IoT Devices, J. Edge Comput. (2025). doi:10.55056/jec.748

[9] V. Rudnytskyi, V. Babenko, S. Rudnytskyi, T. Korotkyi, Generating a Sequence of Asymmetric CET Operations with an Accuracy of up to the Permutation of the Second Operand, Inf. Technol. Society 16.1 (2025). doi:10.32689/maup.it.2025.1.28

[10] V. Babenko, T. Myroniuk, A. Lavdanskyi, Y. Tarasenko, O. Myroniuk, Information-Driven Permutation Operations for Cryptographic Transformation, in: Cybersecurity Providing in Information and Telecommunication Systems, 3654, 2024, 137–149. doi:10.5281/zenodo.10953299

[11] O. Yehorova, O. Mislyuk, O. Khomenko, O. Loboda, Modeling the Distribution of Pollutants in Urban Soils Using GIS Technologies, in: Lecture Notes on Data Engineering and Communications Technologies, Springer Nature Switzerland, Cham, 2024, 486–495. doi:10.1007/978-3-031-71801-4_36

[12] R. Salas-Guerra Cognitive AI Framework: Advances in the Simulation of Human Thought, arXiv, 2025. doi:10.48550/arXiv.2502.04259

[13] W. A. Jasim, R. A. Hussein, B. M. Basheer, H. A. A. Algashamy, O. Turovsky, Advanced Network Analysis Techniques for Social Media Study: Unveiling Patterns and Influences in Digital Communities, J. Ecohumanism 3.5 (2024) 353–364. doi:10.62754/joe.v3i5.3911

[14] V. P. Shapoval, Y. V. Tarasenko, Method of Intelligent Video Monitoring of Primary Signs of Psychological State, Scientific notes of Taurida National V. I. Vernadsky University. Series: Technical Sciences 2.2 (2025) 222-227. doi:10.32782/2663-5941/2025.2.2/30

[15] S. A. Lupenko, O. V. Volianyk, Improved Ontological Model of the Knowledge Base Expert System for Decision Support in the Field of Digital Processing and Computer Simulation of Cyclic Signals, Environmental Safety and Natural Resources 52.4 (2024) 92-98. doi:10.32347/2411-4049.2024.4.92-98

[16] Y. Yu, Y. Yan, Y. Jin, Structural Knowledge: From Brain to Artificial Intelligence, Artificial Intell. Rev. 58.9 (2025). doi:10.1007/s10462-025-11270-2

[17] I. Karpunin, N. Zinchenko, Cognitive Modelling of Intellectual Systems of Analysis of the Financial Condition of the Entity, Cybersecur. Educ. Sci. Tech. 1.21 (2023) 75–85. doi:10.28925/2663-4023.2023.21.7585

[18] A. M. Farid, D. J. Thompson, W. Schoonenberg, A Tensor-based Formulation of Hetero-Functional Graph Theory, Sci. Reports 12.1 (2022). doi:10.1038/s41598-022-19333-y

[19] T. Prokopenko, Y. Lanskykh, V. Prokopenko, O. Pidkuiko, Y. Tarasenko, Development of the Ontological Model of Situation Management of Projects based on SCRUM under Risky Conditions, Eastern-European J. Enterprise Technol. 6.3 (126) (2023) 47-54. doi:10.15587/1729-4061.2023.292526

[20] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 449–457.

[21] A. Novytskyi, V. Sokolov, L. Kriuchkova, P. Skladannyi, Determining the Error Distribution of BLE Beacons at Antenna Near and Far Fields, in: Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), vol. 4024 (2025) 133–143.

[22] O. Mykhaylova, et al., Resistance to Replay Attacks of Remote Control Protocols using the 433 MHz Radio Channel, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 98–110.

[23] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th Int. Conf. on Problems of Infocommunications, Science and Technology (2023) 522–526. doi:10.1109/PICST57299.2022.10238518

[24] O. Bahatskyi, V. Bahatskyi, V. Sokolov, Smart Home Subsystem for Calculating the Quality of Public Utilities, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 168–173.

[25] Y. Sadykov, et al., Technology of Location Hiding by Spoofing the Mobile Operator IP Address, in: IEEE Int. Conf. on Information and Telecommunication Technologies and Radio Electronics (2021) 22–25. doi:10.1109/UkrMiCo52950.2021.9716700

[26] D. Jancarczyk, et al., Two-Operand Operations of Strict Stable Cryptographic Coding with Different Operands' Bits. In: 2020 IEEE Int. Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), IEEE, 2020. doi:10.1109/idaacs-sws50031.2020.9297067

[27] T. Prokopenko, Y. Lanskykh, V. Prokopenko, O. Pidkuiko, Y. Tarasenko, Development of the Comprehensive Method of Situation Management of Project Risks based on Big Data Technology, Eastern-European J. Enterprise Technol. 1.3 (121) (2023) 38-45. doi:10.15587/1729-4061.2023.274473