Algorithm for Assessing the Degree of Information Security Risk of a Cyber Physical System for Controlling Underground Metal Constructions

Volodymyr Yuzevych [1,2], Anatoliy Obshta [2] , Ivan Opirskyy [2] and Oleh Harasymchuk [2]

[1] *Lviv Karpenko Physico-mechanical Institute of the NAS of Ukraine, 5 Naukova str., Lviv, 79060, Ukraine*
[2] *Lviv Polytechnic National University, 12 Stepana Bandery str., Lviv, 79013, Ukraine*

Abstract

A procedure for monitoring the functioning of the "underground metal structure (UMC) - aggressive environment (AE)" system has been developed, taking into account the methods of monitoring information on the detection and localisation of product leaks, methods for assessing the life of the corresponding cyber-physical system, as well as optimisation criteria related to the life of metal structural elements, risk assessment units and cryptographic information security system.

A system for assessing the value of information for the procedure of integral diagnosis of the CPS cyber-physical system has been developed, taking into account the division of the components of the value of the diagnosis D into two parts, where one part corresponds to incidents and the other to vulnerabilities, taking into account the Vaadin, Spring, AnyLogic, OptQuest frameworks

A compromise function has been developed that can be used to ensure the functioning of a cyber-physical system with given values of risk, the value of information about incidents, the value of information related to CPS vulnerabilities, as well as the strength of structural elements and parameters characterizing the quality of the cryptography algorithm.

The proposed approach uses elements of graph theory and takes into account the interdependencies of vulnerabilities. The result obtained with the help of criterion ratios makes it possible to: propose a new methodology for assessing the degree of risk of information security of CFS, taking into account the index of probability of a successful attack on the system and the index of adjustment, which provides feedback Some results have been obtained: modelling of the main processes and links in the CFS; a procedure for identifying vulnerabilities in the physical space (at the sensor level), in cyberspace, and in the communication environment; an algorithm for calculating the degree of information security risk for the CFS using the neural network method and taking into account the quality functionality and quality criterion.

Keywords

Underground metal structures (UMC), cyber-physical system (CFS), optimization algorithm, quality criterion, neural networks, risk level, information security, protection system, sensors, communication environment.

1. Introduction

In the process of a comprehensive analysis of the functioning of the underground metal structures (UMC) system, it is necessary to take into account modern technologies for selecting, storing and processing information obtained by the cyber-physical system (CFS) in the process of control and the corresponding information security risks related to corrosion defects. In this context, the research subject is the procedure for assessing the level of information security risk of a cyber-physical system (CFS) for underground metal structures (UMC), which is implemented in the form of an approach that considers the interdependence of vulnerabilities.

This work aims to develop a methodology for assessing the functioning of the underground metal structures system and the degree of information security risk of the Cyber Physical System (CFS), which would ensure the reliability, confidentiality, completeness, value, and authenticity

CMIS-2024: Seventh International Workshop on Computer Modeling and Intelligent Systems, May 3, 2024, Zaporizhzhia, Ukraine

yuzevych@ukr.net (V. Yuzevych); obshta2002@gmail.com (A. Obshta); iopirsky@gmail.com (I. Opirskyy), garasymchuk@ukr.net (O. Harasymchuk),

0000-0001-5244-1850 (V. Yuzevych); 0000-0001-5151-312X (A. Obshta); 0000-0002-8461-8996 (J. X. Ceur), 0000-0002-8742-8872 (O. Harasymchuk),

of information, as well as reduce the ambiguity of determining informative parameters. By the goal, the following tasks need to be performed:

1a) to develop an approach to the design of a monitoring complex for the underground metal structure (UMC) - aggressive environment (AE) system, taking into account information monitoring methods, methods for assessing the life of the relevant cyber-physical system, and optimisation criteria;

2b) to develop a system for assessing the value of information for the procedure of integral diagnosis of the CPS cyber-physical system, taking into account the division of the components of the value of the diagnosis D into two parts, where one part C_Inz (D) corresponds to incidents, and the second C_Vnz (D) - to vulnerabilities:

3c) to develop a compromise function that can be used to ensure the functioning of a cyber-physical system with the specified values of risk, the value of information about incidents, the value of information about vulnerabilities related to CPS vulnerabilities, as well as the strength of structural elements and a high-quality cryptography algorithm.

UMCs are often subject to terrorist attacks and vandalism [1], which can lead to environmental problems of environmental pollution, hydrocarbon decomposition, and significant economic losses. It is necessary to control (monitor) UMCs, but the relevant process requires significant material costs and is also often dangerous. Therefore, it is advisable to use remote wireless monitoring of the UMC, taking into account the threshold values of informative parameters, in particular: temperature, relative humidity pressure around the UMC, dew point of the environment, carbon monoxide volume, number of liquefied petroleum gas leaks, human movement around the facility, fire and smoke [2]. There are safety regulations and documents, safety guidelines, and industry standards and regulations, compliance with which increases the likelihood of preventing system security failures, the ability to protect the engineering facility from an incident, and ensures the integrity of UMC structural elements [3].

Wireless sensor networks, together with microcontrollers, sensor devices, and communication interfaces, allow users to measure and select the necessary information, as well as respond to phenomena in the monitored UMC environment [4].

The relevance of UMC system risk research is related to the issues of hardware and software information protection. In this context, two important factors should be noted. Firstly, the risks of CFS hardware components are related to the fact that these components are not always certified and this affects the energy consumption and performance in the final version [5]. Secondly, fuzzy logic and neural networks (NNs) are applied to the risks of UMC software, as the combination of these two methods provides the highest efficiency and adaptability to non-numerical data [6]. It should be noted that the relevance of this type of research is also because IT risk may also be the risk of loss that originates from computer software malfunction, such as a manufacturer's software license expiration or glitches, and the ways it affects corporate activities [7, 8].

2. A model for diagnosing underground metal constructions concerning the quality criterion

We will build a diagram of the process of diagnosing an underground metal structure taking into account the quality criterion in the BPWin Process Modeller program using the IDEF0 module. Information about BPWin Process Modeller and the IDEF0 module is given in [9, 10]. The corresponding model diagram is shown in Fig. 1, which displays information for monitoring underground metal structures.

The input to the monitoring system (Fig. 1) is the information denoted by the set of parameters M(P) and obtained using sensors for UMC [11-16]: electric current density, voltage, polarisation potential, soil moisture, and temperature. To verify the reliability of the input parameters, we use regulatory documents (standards, regulations, instructions). To organise the information on M(P) for UMC, we use databases, knowledge bases, and appropriate algorithms (Fig. 1).

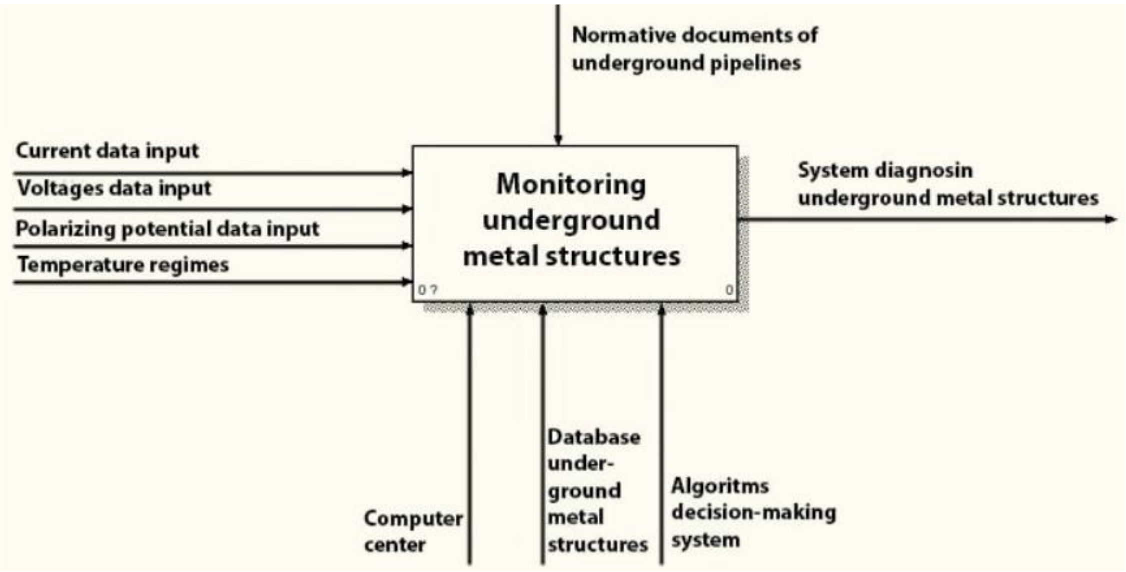
Normative documents of underground pipelines
Current data input
Voltages data input
Polarizing potential data input
Temperature regimes
Monitoring underground metal structures
0 ?
0
System diagnosin underground metal structures
Computer center
Database under-ground metal structures
Algoritms decision-making system

Figure 1: Monitoring system for underground metal constructions

The decomposition scheme of the model presented in Fig. 1 is shown in Fig. 2. To implement the model decomposition procedure, we used the relevant principles similarly to those in [11, 12, 17].

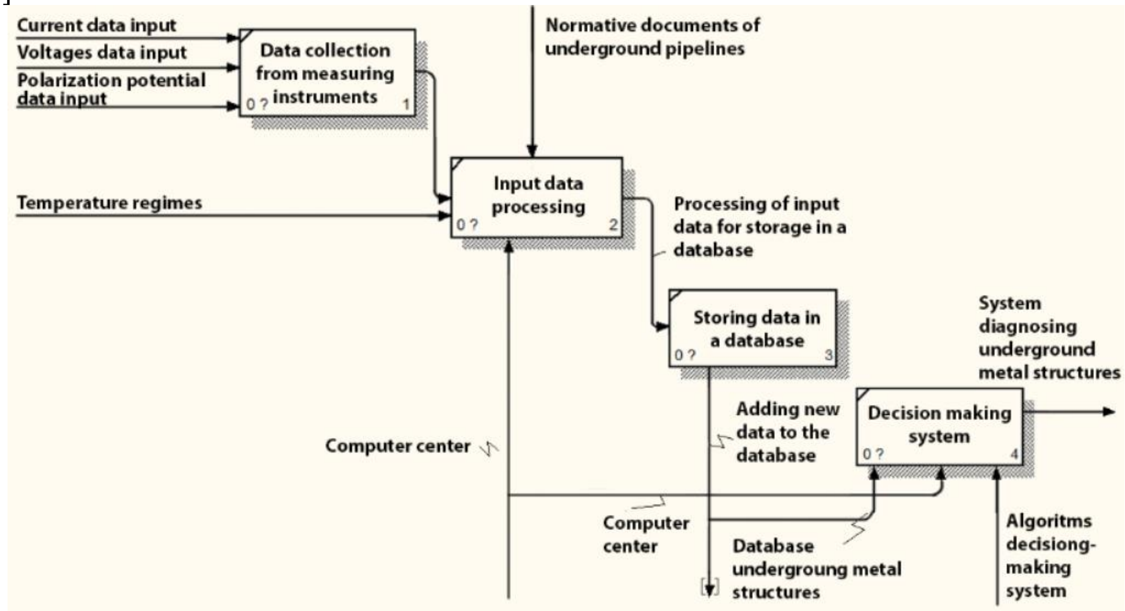
Current data input
Voltages data input
Polarization potential data input
Data collection from measuring instruments
0 ?
1
Normative documents of underground pipelines
Input data processing
0 ?
2
Temperature regimes
Processing of input data for storage in a database
Storing data in a database
0 ?
3
System diagnosing underground metal structures
Adding new data to the database
Decision making system
0 ?
4
Computer center
Computer center
Database undergroung metal structures
Algoritms decisiong-making system

Figure 2: Decomposition monitoring model for underground metal constructions

Decomposition is a scientific method that uses the structure of a problem and allows replacing the solution of one large problem with a series of smaller problems, taking into account data availability, clarity, and the level of model complexity [17]. To organize the information about M(P) for UMC in the decomposition process, we use databases, knowledge bases, as well as strength and quality criteria for each individual task. The complexity and categoricality of decomposition tasks are assessed by seven indicators of the component tasks similarly to [17]. This allows us to specify the quantitative description of the model, taking into account clear criteria and the peculiarities of the fact that structures are located underground. Such specification reduces the uncertainty and ambiguity of qualitative judgments, facilitating the assessment of the tasks of the model elements. The appropriate distribution of the categories of tasks of the UMC monitoring model is based on the experience of the authors of the scientific article [17] and the experience of the authors of this publication.

The block diagram of the new system, which corresponds to the technology of monitoring information on electrophysical parameters for underground metal structures with regard to the aggressive environment, is shown in Fig. 3.

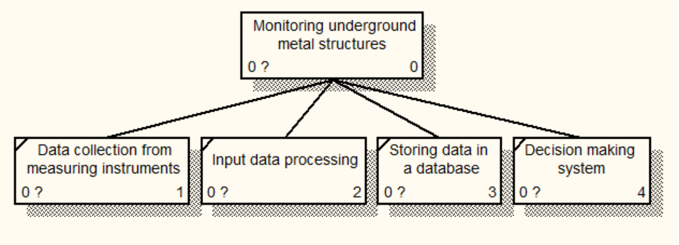
Monitoring underground metal structures
0 ?
0
Data collection from measuring instruments
0 ?
1
Input data processing
0 ?
2
Storing data in a database
0 ?
3
Decision making system
0 ?
4

Figure 3: Block diagram of information monitoring for the system “underground metal construction (UMS) – aggressive environment (AE)”

Monitoring of the "UMC - Aggressive Environment (AE)" system details information on data acquisition from measuring devices (currents, voltages, soil moisture, temperature), processing of input data, data storage in the database, and decision-making in the context of optimizing informative parameters and physical characteristics of contacting media (soil, dielectric coating, metal).

A block diagram of the cyber-physical system (CPS) and the corresponding decision-making system for the operation of the CPS is shown in Fig. 4.

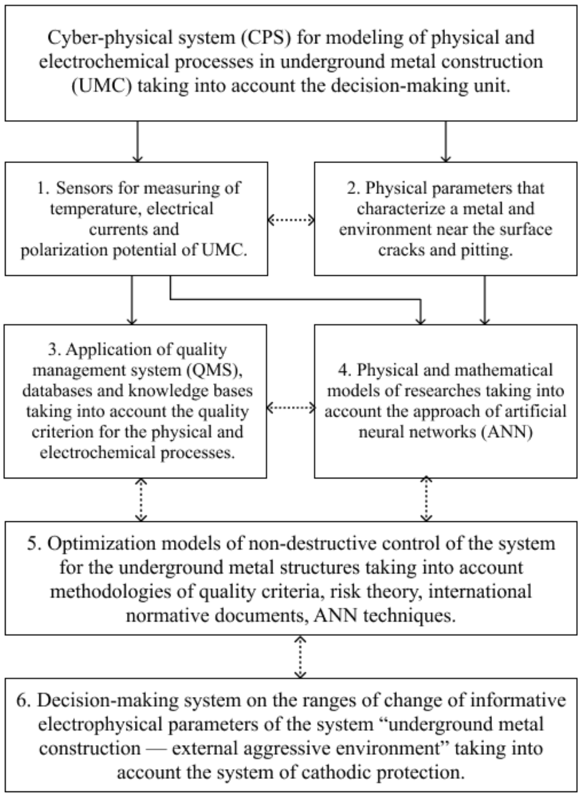
Cyber-physical system (CPS) for modeling of physical and electrochemical processes in underground metal construction (UMC) taking into account the decision-making unit.
1. Sensors for measuring of temperature, electrical currents and polarization potential of UMC.
2. Physical parameters that characterize a metal and environment near the surface cracks and pitting.
3. Application of quality management system (QMS), databases and knowledge bases taking into account the quality criterion for the physical and electrochemical processes.
4. Physical and mathematical models of researches taking into account the approach of artificial neural networks (ANN)
5. Optimization models of non-destructive control of the system for the underground metal structures taking into account methodologies of quality criteria, risk theory, international normative documents, ANN techniques.
6. Decision-making system on the ranges of change of informative electrophysical parameters of the system “underground metal construction — external aggressive environment” taking into account the system of cathodic protection.

Figure 4: Block diagram of a cyber-physical system (CPS) for modelling the electrophysical parameters of the system "underground metal structure – external aggressive environment"

The block diagram in Fig. 4. contains 6 blocks, of which blocks 1-2 characterize the information and measurement system (IMS) for measuring electrophysical parameters. Blocks 3 and 4 are the basis of the information processing system for the CPS, obtained by sensors and non-destructive testing devices. Units 3 and 4 are used to organize and clarify the information received by the information monitoring system (Fig. 3). The methods of functioning of blocks 1-4, taking into account the methods of using neural networks, are described in detail in articles [13-16].

We will introduce an integral indicator of the effectiveness of the ER functioning of the underground pipeline monitoring system similar to [17] with the addition of the parameters of the quality management system (QMS) [15, 16] and the cryptographic information protection system [20, 21]:

$$ER= f(F(R), M(P), F(Z), F(Q), F(It, Pw)) \Rightarrow opt \quad (1)$$

Here $F(R)$ is the effectiveness of the monitoring system and the corresponding algorithm in the context of the risk-based corrosion model R; $F(Z)$ is the effectiveness of the information security structural units; $F(Q)$ is the effectiveness of the algorithm taking into account the QMS; $F(It, Pw)$ is a function of performance and the effectiveness of the algorithm in the context of personnel functioning; It is the index of creativity, qualification and loyalty of employees; Pw is a set of parameters that characterizes the behaviour of personnel, including qualitative and quantitative factors Pwi. ($i = 1, 2, \ldots n_s$; n_s is the total number of parameters of the corresponding model).

To optimize the information flows $J_n(M(P), Pwi)$ in the cyber-physical system monitoring system and improve the corrosion protection system of underground metal structures, we use the quality functionality with feedback similar to [14]:

$$\Psi(J_n(M(P), Pw_i), R, FB(M(P), Pw_i)) = \int_{t_0}^{t_k} f(\overline{y}, \overline{u}, \overline{\xi}) dt \Rightarrow opt \quad (2)$$

where $\overline{y}$ – vector of specified influences ($y_j(t)$ - components of the vector, $j = 1,2,\ldots,n_t$); $\overline{u}$ - vector of controls; $\overline{\xi}$ - vector of uncertain disturbances; $[t_0, t_k]$ - time interval in which the process is considered (formation of optimal values of information and financial flows $J_n(Pw_i)$; $n = 1,2,\ldots,m$; $i = 1,2,\ldots,n_S$; m - total number of parameters); $f(\overline{y}, \overline{u}, \overline{\xi})$ - a function that reflects the quality indicator; $FB(M(P), Pw_i)$ - a function that characterizes the feedback between the flows $J_n(M(P), Pw_i)$, taking into account the regulatory documents on information security and expert opinions. Here, the symbol opt corresponds to the condition of optimality of the functional (2).

It is worth noting that relation (2) is written in the form of a quality criterion for the corresponding cyber-physical system (CPS). It is worth noting that the inverse relationship $FB(M(P), Pw_i)$ is related to the risks R and the conditions of operation of the cryptographic information security system. To optimize the risks, we will take into account the following factors [14, 20, 21]: quality and reliability, information capacity, and risk factors R associated with the software that provides cryptographic encoding.

For the functioning of the algorithm for assessing the degree of risk of CPS information security, i.e., for the control of underground metal structures, we use the structural elements of the Vaadin, Spring, AnyLogic, and OptQuest frameworks, which together provide a reliable database that ensures effective protection of CPS, as well as the cathodic protection system metal structures (CPSMS) [22-25].

Vaadin offers a server-oriented architecture based on Java Enterprise Edition (JEE) [25]. Using JEE allows you to execute the bulk of the program logic in the context of the server, and also allows you to interact with the user, taking into account the capabilities of desktop applications [25]. To display user interface (UI) elements and interact with the server on the client side, Vaadin uses its own set of web components [25]. An important feature of the Vaadin framework is that the interaction between the server and the browser is fully automated, and this connection allows developers to create web interfaces efficiently and quickly without having to manually code HTML (HyperText Markup Language) and CSS (Cascading Style Sheets) elements [24].

The Vaadin Framework simplifies the process of creating and maintaining high-quality web user interfaces and is structured as a server API, a client API, a set of UI components on both sides, a theme engine for designing the interface, and a data model that allows you to link server components directly to data [25].

The server part of the Vaadin application runs on any servlet or portlet container, accepts HTTP requests from the user and interprets them as events of a specific session [25]. Events associated with client interface components are delivered to those event listeners that appear in the application and the corresponding UI logic is accompanied by changes to the UI components on the server side, this procedure provides the process of obtaining an image with a model response for display in a web browser [25].

The Vaadin Framework corresponds to two models of web application development: for the client (browser) and the server side, respectively, and the client layer of the Vaadin interface includes two types of components: basic UI components and application components [25].

The UI component library of the Vaadin framework contains a set of pre-built, tested, and well-documented user interface (UI) components that can be easily reused in the UI of a product [25]. This ensures that the final product has a user-friendly appearance, promotes efficiency and scalability in its operation, and allows users to perform actions and monitor processes and events [25]. The noted components of the Vaadin interface are quite general and can be introduced into various programs since they do not violate the logic of the computer program and can be successfully used to control R risks.

The purpose of the Spring Boot project is to simplify the creation of Spring-based programs and to create web applications with minimal effort from designers in terms of configuration and code writing [23]. The Spring framework provides comprehensive support for web application infrastructure for developing Java programs [23].

Spring Boot is focused on extending the Spring environment with Spring, Spring Boot, and Spring Cloud components, eliminates some of the template configurations required to set up a Spring application, and provides a fairly fast and efficient system for developing various partial tasks that are useful for cybersecurity [23].

Spring Framework is a universal, widespread application framework that focuses on the corporate development of complex programs in the Java environment and provides a modular approach, as well as allows for the implementation of aspect-oriented programming (AOP) dependencies and rational data access [23].

Aspect-oriented programming (AOP) complements object-oriented programming (OOP) by specifying information about the program structure [23]. The key unit of modularity in OOP is the class, while in AOP the unit of modularity is the aspect, and the set of aspects and classes makes it possible to implement modules in procedures such as transaction management that combine several types and objects [23]. In the literature, problems such as transaction management with AOP are related to the structure of AOP and are often called cross-cutting problems [23].

That is, AOP can be a kind of tool for solving problems that are not directly related to Spring logic but allows you to modify the behaviour of existing Spring code without changing its functionality [23]. Spring has its own AOP framework that complements OOP by introducing a new technique for achieving modularity and greater code cleanliness that is conceptually easy to understand and allows you to effectively solve most practical problems in enterprise Java applications [23].

Since Spring AOP is implemented in the object-oriented Java programming language, there is no need for a special compilation procedure. When using Spring AOP, there is no need to manage the class loader hierarchy, because Spring AOP creates the conditions for use in a Servlet container or application server [23].

Spring AOP primarily supports method composition points and in this case, provides recommendations for method execution on Spring components [23]. Field capture operations (sensitive information) are often not implemented, although support for field capture can be added without breaking the core Spring AOP APIs [23]. If the user needs to advise access to the field and update the connection points, then it is worth considering an additional task in the AspectJ programming language [23].

Spring AOP's approach to AOP differs from most other AOP frameworks [23]. The goal in this context is not to provide the complete AOP implementation (although Spring AOP is quite capable of doing so); rather, it is to ensure tight integration between the AOP implementation and Spring IoC to help provide effective algorithms for solving typical cybersecurity problems in enterprise applications [23].

The functionality of the AOP Spring Framework is usually used in conjunction with the Spring IoC (Inversion of Control) container, and the characteristics of the corresponding implementation of the cybersecurity program are configured using the bean-component definition syntax, and the corresponding approach allows to implement effective "auto proxy" capabilities and this technique provides a significant difference from other AOP implementations [23]. The experience of the conducted research shows that Spring AOP provides a rational and successful solution to most of the tasks in enterprise Java programs that are subject to AOP. However, the Spring IoC container is independent of AOP, that is, the user does not need to use AOP if he does not want to [23]. AOP does not compete with AspectJ to provide comprehensive problem-solving with AOP, and at the same time complements Spring IoC to provide sufficiently efficient solutions to applied cybersecurity problems with middleware [23].

It is known that proxy-based frameworks such as Spring AOP and full-scale frameworks such as AspectJ are valuable and that they complement each other rather than compete [23]. Spring seamlessly integrates Spring AOP and IoC with AspectJ to provide the full capabilities of AOP in a coherent Spring-based application architecture [23]. This integration does not affect Spring AOP: that is, Spring AOP remains backwards compatible [23].

Spring Boot is built on top of the traditional Spring Framework, which is widely used to develop REST APIs and is characterized by standalone applications with a built-in server, standalone productivity applications, simplified configuration, and selective defaults [23].

The Spring Framework Inversion of Control (IoC) components codify formalized design patterns as first-class objects that users can integrate into their applications, provide a formalized means of combining different components, and build on this basis fully working applications that are ready to use [23]. The Spring Framework always offers choices and the user has the freedom to make an informed decision about which option is best suited for their particular use case or scenario, and modifies formalized design patterns as separate cybersecurity objects that the user can integrate into their applications [23].

AnyLogic integrates the leading OptQuest optimizer and is based on sophisticated analytical algorithms that allow finding optimal parameter values when solving cybersecurity problems using modeling tools and help users make informed decisions [24].

The system for protecting a metal structure element in an aggressive soil environment, taking into account the Vaadin, Spring, AnyLogic, and OptQuest frameworks, will be linked to the $R_S(R)$ resource for the safe operation of a material with a damaged insulating coating in a corrosive environment, and the corresponding ratios will be written in a form similar to that in [25]:

$$R_S(R) = R_w \cdot w(R); \quad R_w(R) = K_w \cdot R_P(R). \tag{3}$$

Here, $R_P(R)$, and w(R) are the design and relative service life of the metal structure material in the air, respectively; $K_W=K_W(N_P, N_S)$ is the coefficient of influence of the aggressive environment on the durability of the metal structure material; N_P, N_S is the durability of the metal structure material in the air and aggressive environment; $R_w= R_w(M(P), Pw_i)$ is the service life of the metal structure material with a damaged insulation coating underground under the condition of contact with the soil. The influence of an aggressive environment on the parameters characterizing the service life of a metal structure is characterized using the methods given in [26, 27]. The effect of an aggressive environment on the service life and protection system of a metal structure is characterized using the methods given in [21, 28].

The effectiveness of UMC protection depends on the intensity of corrosion processes on the surface. Relevant engineering objects are protected by coatings and cathodic protection equipment (CPE). The UMC surface is covered with defects such as cracks and pittings. The corrosion inhibition coefficient and information security risks of the relevant cyber-physical system (CPS) depend on the state of the defects [29, 30].

Let us consider the diagnostic value of information $C_{Di}(k_j)$ for the CPS system, which includes UMC, CPE, and the sensor system [13-16, 29]. The diagnostic value $C_{Di}(k_j)$ for a feature k_j for a state (diagnosis) D_i is the amount of information about incidents and vulnerabilities (including frameworks) (incidents (In) and vulnerabilities (Vn)) contributed by all variants of the corresponding feature implementation in establishing the corresponding state [29]. We propose to write the expression $C_{Di}(k_j)$ for the m -bit feature in the same way as in [29]:

$$C_{Di}\left(k_j, D_i\right) = \sum_{s=1}^{m} P\left(k_{js} / D_i\right) \log \frac{P\left(k_{js} / D_i\right)}{\sum_{i=1}^{n} P\left(D_i\right) \cdot P\left(k_{js} / D_i\right)} = C_{In}(D_i) + C_{Vn}(D_i). \tag{4}$$

Here, in (4), the feature k_j has several values k_{js} for a given object, and these values together form the realization of the feature k_j; $P(k_{js}/D_i)$ is the probability of the state (diagnosis) D_i, provided that the feature $\mathrm{k_j}$ has received the value k_{js}; $P(D_i)$ is the a priori probability of the diagnostic state.

Let us write down the ratio of the integral value of information $C_D(D,CPS)$ for the procedure of integral diagnosis $D=D(R)$ of the CPS system, taking into account the division into two components $C_{Inz}(D)$, $C_{Vnz}(D)$, where the $C_{Inz}(D)$ component corresponds to incidents and $C_{Vnz}(D)$ to vulnerabilities:

$$C_D\left(D,\ CPS\right)=C_{Inz}(D,R)+C_{Vnz}(D,R). \tag{5}$$

To ensure a high level of security of a cyber-physical system (CPS), we use a cryptography algorithm (ACR), which is characterized by quality, stability, and reliability. It is formed using elements of the AES and RSA algorithms, as well as a system for testing, encrypting, and decrypting information using software that operates with the NetBeans program [31]. The proposed approach (5) takes into account the interdependencies of vulnerabilities and uses elements of graph theory. The method of randomization and encryption based on the method of matrix operations (MORE) was used to train neural networks using encrypted data [32]. It was found that the use of a neural network approach, as well as training a neural network using MORE, improves the accuracy, running time, and performance of CPS, as well as the appropriate level of privacy compared to other state-of-the-art methods [32, 33]. The quality of a cryptography algorithm $Q_{Cz}(R_A,T_C,S_C,A_R)$ is characterized by four parameters [31, 32]: reliability R_A, time complexity T_C, spatial complexity S_C, accuracy A_R, i.e., the level of ensuring the correct result.

Let's write down the criterion relations for the functional dependencies $\mathrm{C_{Inz}(D)}$, $\mathrm{C_{Vnz}(D)}$, $\mathrm{Q_{Cz}(R_A,\ T_C,\ S_C,\ A_R)}$, as well as for the structural strength S_S:

$$\begin{gathered} C_{Inz}(D,R)\Rightarrow \min;\ \ C_{Vnz}(D,R)\Rightarrow \min;\ Q_{Cz}(R_A,T_C,S_C,A_R,R)\Rightarrow \max; \\ S_{Sz}(*)=S_{Sz}(W_S,\sigma_S,K_{CV},W_{PL},K_{1C},R)\Rightarrow \max. \end{gathered} \tag{6}$$

Here, W_S, σ_S are the surface energy and tension of the structural material, respectively; K_{CV} is the impact toughness of the material; W_{PL} is the surface plastic strain energy of the material; K_{1C} is the fracture toughness of the material [33].

Let us convert the functional dependencies $C_{Inz}(D)$, $C_{Vnz}(D)$, $Q_{Cz}(R_A,T_C,S_C,A_R)$, $S_{Cz}(*)$ to a dimensionless form, in particular:

$$C_{In}(D)=C_{Inz}(D)/(C_{Inz}(D))_{CP};\ \ C_{Vn}(D)=C_{Vnz}(D)/(C_{Vnz}(D))_{CP}; \tag{7}$$

$$Q_C(*,D)=Q_C(R_A,T_C,S_C,A_R)=Q_{Cz}(R_A,T_C,S_C,A_R)/(Q_{Cz}(R_A,T_C,S_C,A_R))_{CP}; \tag{8}$$

$$\begin{gathered} S_S(*,D)=S_S(W_S,\sigma_S,K_{CV},W_{PL},K_{1C}), \\ S_S(*,D)=S_{Sz}(W_S,\sigma_S,K_{CV},W_{PL},K_{1C})/(S_{Sz}(W_S,\sigma_S,K_{CV},W_{PL},K_{1C}))_{CP}. \end{gathered} \tag{9}$$

Here $(C_{Inz}(D))_{CP}$, $(C_{Vnz}(D))_{CP}$, $(Q_{Cz}(R_A,T_C,S_C,A_R))_{CP}$, $(S_{Sz}(W_S,\sigma_S,K_{CV},W_{PL},K_{1C}))_{CP}$ – values of the relevant functions at critical (special) points. These can be, for example, the maximum possible values of the relevant factors.

Since the factors (functions) $C_{In}(D)$, $C_{Vn}(D)$, $Q_C(*,D)$, $S_S(*,D)$ in relations (7)-(9) are dimensionless, then they can be used to formulate a trade-off function $F_Q(D,R)$ (Trade-off function) and, with its help, the optimization criterion, since the first two of them should tend to decrease in terms of safety, and the third and fourth in absolute value should increase:

$$F_Q(D,R)=\alpha\cdot C_{In}(D)+\beta\cdot C_{Vn}(D)+\gamma\cdot Q_C(*,D)+\delta\cdot S_S(*,D)\Rightarrow opt, \tag{10}$$

where $C_{In}(D)$, $C_{Vn}(D)$, $Q_C(*,D)$, $S_S(*,D)$ – functional dependencies that we establish based on the experiment; α, β, γ, δ – weighting coefficients, which are determined on the basis of a computational experiment, taking into account information of the type presented in Fig. 4, as well as criteria (1), (2), (5). The result obtained using (10) makes it possible to: propose a new methodology for assessing the degree of risk of CFS information security, taking into account the index of the probability of a successful attack on the system and the index of adjustment, which provides feedback.

As a result, taking into account the quality criteria (2), (5), parameters characterizing the resource (3), and the corresponding optimization algorithm based on the trade-off function (10), it is possible to assess the risk degree R of the metal structure and increase the efficiency of the CPS protection system against unauthorized influences and threats.

Example. The results of testing the leak detection system (LDS) on the linear part of the main oil pipeline "section 43" station "5C" - station "1K" from 0 km to 231 km were used [1]. The tests were carried out with full verification of the system operation algorithms, by the design decisions, by organising oil product discharges from the pipeline according to the approved programme and testing methodology of the IHS [1]. A partial result of a series of tests conducted using pressure sensors according to the methodology [1] is shown in Table 2. To check the performance of the IED, oil product discharges were organised at 2-3 points of the protected section of the oil pipeline "section 43", 0-231 km, with different intensity, leakage development time and for different modes of operation of the pipeline [1].

In the course of the work, the following were performed [1]: verification of functional requirements for the IED; verification of the IED characteristics; checking the system for stability; and checking the accuracy and reliability of leakage detection within the protected area.

At the time of testing, the complete set of software and hardware was provided, as well as the completeness of permits and technical documentation following norms and standards for all supplied equipment [1]. Before the start of the tests, the readiness of the material, technical and metrological support facilities was checked to ensure that the conditions and test modes were created under the programme [1]. The tests were carried out to determine the appropriate size of the minimum recorded leakage for a given oil pipeline in the following modes of operation [1]: maximum, minimum, and one of the intermediate modes.

The tests were carried out at each of the modes of operation of the oil pipeline with the following leakage development time [1]: up to 1 s, - from 1 to 10 s, more than 10 s.

The tests were carried out in series of 2-3 showers for each leak, taking into account the following conditions [1]: 4 series of experiments were carried out; the first - three experiments, the second - three, the third - two, the fourth - three experiments. The mean values and standard deviations for each series of experiments were calculated.

Table 1
Abbreviated table of system test results [1]

Tests Results	Date and Time	The duration of the leak ΔT, s	The size of the leak Q, l	The magnitude of the leak ΔP, mPa (out/in)	The fact of detecting a leak	Actual coordinate of selection, km	System leakage coordinate, km	Error_k, m
	1	2	3	4	5	6	7	8
1	12.02 12:00	1	1	0.02/*	Yes	23.4	23.55	150
2	12.02 12:10	1	2	0.03/*	Yes	23.4	23.15	250
3	12.02 12:20	1	2	0.03/*	Yes	23.4	23.2	200
4	12.02 13:30	10	15	0.07/0.024	Yes	56.1	56.4	300
5	12.02 13:40	10	15	0.07/0.024	Yes	56.1	56.35	250

6	12. 02 13:50	10	15	0.07/0.024	Yes	56.1	56.4	300
7	12. 02 14:00	60	80	0.12/0.04	Yes	120.7	120.3	400
8	12. 02 14:10	60	90	0.12/0.04	Yes	120.7	120.2	500
9	15. 02 12:00	1	1	0.02/*	Yes	140.4	140.1	300
10	15.02 12:10	1	2	0.03/*	Yes	140.4	140	400
11	15. 02 12:20	1	1.5	0.03/*	Yes	140.4	140.2	200

Average (mean) value of Error= 295,45 m.

So, if we sum all errors in determining the leak coordinate and divide them by the total number of tests, we should get an average (mean) value, which should be less than ±300m (k = 1,2,...11).

A refined leakage test was carried out using the BVS-K non-contact current meter and the VPP-M polarisation potential meter for non-destructive testing of metal surfaces according to the methodology presented in [13-16,34]. As a result, the average error value Errors2= 2 m was obtained. The relative value of Errors3= 2/300 = 0.007. It is irrational to control leaks only with the help of BVS-K and VPP-M devices. It is more rational to conduct leakage control based on pressure sensors at the first stage and obtain results similar to those in Table 1, and at the second stage, it is possible to clarify the locations of leaks (depressurisation) using remote monitoring devices BVS-K and VPP-M.

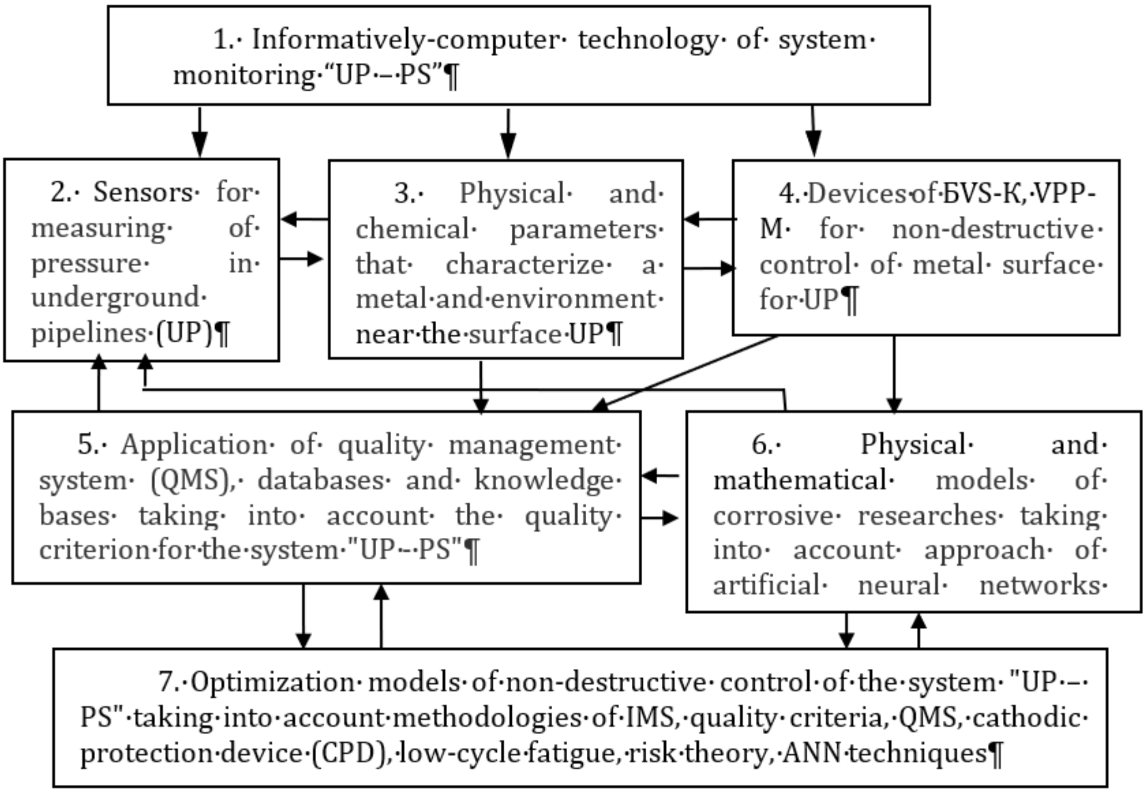
1.· Informatively-computer· technology· of· system· monitoring·"UP·–·PS"¶
2.· Sensors· for· measuring· of· pressure· in· underground· pipelines·(UP)¶
3.· Physical· and· chemical· parameters· that· characterize· a· metal·and·environment· near·the·surface·UP¶
4.·Devices·of·БВС-К,·VPP-M· for· non-destructive· control· of· metal· surface· for·UP¶
5.· Application· of· quality· management· system· (QMS),· databases· and· knowledge· bases· taking· into· account· the· quality· criterion·for·the·system·"UP·–·PS"¶
6.· Physical· and· mathematical· models· of· corrosive· researches· taking· into· account· approach· of· artificial· neural· networks·
7.·Optimization· models·of·non-destructive· control·of·the·system· "UP·–·PS"·taking·into·account·methodologies·of·IMS,·quality·criteria,·QMS,·cathodic· protection·device·(CPD),·low-cycle·fatigue,·risk·theory,·ANN·techniques¶

Figure 5: Block diagram of informatively-computer technology for underground pipelines (UP) taking into account the informatively-measuring system (IMS) (2, 3, 4) for control of corrosive processes [34]

In actual pipeline operation conditions, it is necessary to take into account the possibility of corrosion defects such as pitting, cavities, and cracks, which change their size over time and eventually become fracture sites. We describe their evolution using relations (1)-(10), taking into account the monitoring system, which is based on a cyber-physical system (CPS) for modelling the electrophysical parameters of the system "underground metal structure - external aggressive environment", taking into account the risk assessment unit and the cryptographic information security system (Fig. 4).

To diagnose defects on the surface of the pipe and places of depressurisation (leakage) of the pipeline using: pressure sensors and non-destructive testing devices, which measure potentials and corrosion currents, an information and computer technology has been developed, the structural diagram of which is presented in [34] (Fig. 5) for the underground pipeline (UP) - pumping station (PS) system.

The scheme in Fig. 5 contains 7 blocks, of which blocks 2, 3, 4 correspond to the information and measurement system (IMS) for measurements. Blocks 5, 6, 7 are the basis of the system for processing information received by sensors and non-destructive testing devices (IMS). The methods of operation of units 5, 6, 7 are partially described in articles [13-16, 34].

The scheme in Fig. 5 contains 7 blocks from which blocks 2, 3, 4 answer the informative-measuring system (IMS) for realisation of measurement. Blocks 5, 6, 7 are the basis of the information processing system received by sensors and non-destructive control devices (IMS). Methodologies of functioning of blocks 5, 6, 7 are partially described in articles [13-16, 34].

For the cyber-physical system (CPS) (Fig. 4) and information and computer technology (Fig. 5), we use the Vaadin, Spring, AnyLogic, OptQuest frameworks, as well as the principles of cryptographic encoding and decoding of information

Conclusions

The basics of the method and a variant of the methodology for improving the efficiency of the CPS protection system of an underground metal structure against unauthorized influences and threats, taking into account the corrosive effect on the life and strength of the material, quality criteria (2, 5) and the corresponding optimization algorithm based on the trade-off function and the Vaadin, Spring, AnyLogic, OptQuest frameworks, are presented.

1) An approach to monitoring the system "underground metal structure (UMC) - aggressive environment (AE)" was developed, taking into account information monitoring methods, methods for assessing the life of the corresponding cyber-physical system, as well as optimization criteria related to the life of metal structural elements, risk assessment units, and cryptographic information security system.

2) A system for assessing the value of information for the procedure of integral diagnosis of a cyber-physical system CPS was developed, taking into account the division of the components of the value of the diagnosis D into two parts, where one part $C_{Inz}(D)$ corresponds to incidents, and the second $C_{Vnz}(D)$ - to vulnerabilities, taking into account the Vaadin, Spring, AnyLogic, OptQuest frameworks.

3) A compromise function has been developed that can be used to ensure the functioning of a cyber-physical system with given values of risk, the value of information about incidents, the value of information related to CPS vulnerabilities, as well as the strength of structural elements, and parameters that characterize the quality of the cryptography algorithm.

Using the trade-off function, options for methods of improving the efficiency of the CPS protection system, and the initial values of the parameters M(P), specific partial tasks can be formulated and the corresponding risk values can be determined.

For the functioning of the optimization algorithm for assessing the degree of risk of information security of a cyber-physical system and, in this context, to ensure the conditions for controlling the protection system of underground metal structures, we use the structural elements of the Vaadin, Spring, AnyLogic, OptQuest frameworks, as well as the principles of cryptographic encoding and decoding of information.

References

[1] Anatoliy Obshta, Yurii Biliak, Vladyslav Shugai. Cyber-Physical System for Diagnostic Along the Controlled Section of the Oil Pipeline // Advances in Cyber-Physical Systems Vol. 8, Num. 1, 2023 pp. 66-73 DOI: 10.23939/acps2023.01.066; Language: EN.

[2] Ngonadi I. V., Ajiroghene S. Remote Pipeline Monitoring Security System // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2021. Vol. 7, No. 6. P. 135-145. https://doi.org/10.32628/CSEIT217631.

[3] Pipeline Security and Incident Recovery Protocol Plan / Transportation Security Administration. U. S. Departament of Homeland Security. 2010. 58 p.

[4] Pipeline Infrastructure Vandalism Monitoring using Wireless Sensor Networks Technique / Y. Kefas, A. O. Sunday, A. M. Bashir and A. A. Abraham // International Journal of Computer Science and Telecommunications. Vol. 8, No. 2, 2017. P. 39-42.

[5] Lerner, L. W. Farag, M. M., Patterson, C. D.: Run-time prediction and preemption of configuration attacks on embedded process controllers. In: SecurIT '12: Proceedings of the First International Conference on Security of Internet of Things, August 2012, P. 135–144. (2012). https://doi.org/10.1145/2490428.2490447.

[6] Lee, M.-C.: Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method. International Journal of Computer Science & Information Technology (IJCSIT). 2014. 6(1), P. 29-45. DOI:10.5121/ijcsit.2014.6103.

[7] Biro M., Mashkoor A., Sametinger J., Seker R.: Software Safety and Security Risk Mitigation in Cyber-physical Systems. IEEE Software. 2018. 35(1). P. 24–29.

[8] Hu F.: Cyber-Physical Systems: Integrated Computing and Engineering Design. New York: CRC Press. 2018. 398 p.

[9] Design and validation of a C++ code generator from abstract state machines specifications / S Bonfanti, A Gargantini, A Mashkoor // Journal of Software: Evolution and Process. 2020. 32 (2), e2205.

[10] Bendoly E., Rosenzweig E. D., Stratman J. K. The efficient use of enterprise information for strategic advantage: A data envelopment analysis // Journal of Operations Management, 2009. No. 27. P. 310-323.

[11] Construction Site Monitoring Data Processing Based on Detecting Anomalies and Improved Variational Mode Decomposition / Y. Shaoa, T. Anb, Y. Qic, W. Liu // Proceedings of the 2023 5th International Conference on Structural Seismic and Civil Engineering Research (ICSSER 2023), Atlantic Highlights in Engineering 24. 2023. P. 258-269. https://doi.org/10.2991/978-94-6463-312-2_27.

[12] Ahmed, M., Mahmood, A. N., and Hu, J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 2016. 60: P. 19-31. DOI: 10.1016/j.jnca.2015.11.016.

[13] Yuzevych, L., Skrynkovskyy, R., Yuzevych, V., Lozovan, V., Pawlowski, G., Yasinskyi, M., Ogirko, I.: Improving the diagnostics of underground pipelines at oil-and-gas enterprises based on determining hydrogen exponent (ph) of the soil media applying neural networks. Eastern-European Journal of Enterprise Technologies. 2019. 4(5 (100)), P. 56–64. doi: https://doi.org/10.15587/1729-4061.2019.174488.

[14] Lozovan, V., Skrynkovskyy, R., Yuzevych, V., Yasinskyi, M., Pawlowski, G.: Forming the toolset for development of a system to control quality of operation of underground pipelines by oil and gas enterprises with the use of neural networks. Eastern-European Journal of Enterprise Technologies. 2019. 2(5 (98)), P. 41–48. doi: http://dx.doi.org/10.15587/1729-4061.2019.161484.

[15] Yuzevych, L,, Yankovska, L., Sopilnyk, L., Yuzevych, V., Skrynkovskyy, R., Koman, B., Yasinska-Damri, L., Heorhiadi, N., Dzhala, R., Yasinskyi, M.: Improvement of the toolset for diagnosing underground pipelines of oil and gas enterprises considering changes in internal working pressure. Eastern-European Journal of Enterprise Technologies. 2019. 6(5 (102)), P. 23–29. DOI: 10.15587/1729-4061.2019.184247.

[16] Lozovan V., Dzhala R., Skrynkovskyy R., Yuzevych V.. Detection of specific features in the functioning of a system for the anti-corrosion protection of underground pipelines at oil and gas enterprises using neural networks // Eastern-European Journal of Enterprise Technologies. 2019. Vol. 1, No. 5 (97). P. 20–27. doi: https://doi.org/10.15587/1729-4061.2019.154999.

[17]. Chen Z., Pouliot J., Hubert F. Task decomposition and level of complexity to select the content of underground utility network model // The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLVIII-4/W4-2022 17th 3D GeoInfo Conference, 19–21 October 2022, Sydney, Australia. P. 21-27. https://doi.org/10.5194/isprs-archives-XLVIII-4-W4-2022-21-2022, 2022.

[17] Agmon, N.; Kordova, S.; Shoval, S. Global Quality Management System (G-QMS) in Systems of Systems (SoS)—Aspects of Definition, Structure and Model. Systems 2022, 10, 99. https://doi.org/10.3390/systems10040099.

[18] International Organization of Standardization. ISO 9004:2018 Quality Management–Quality of an Organization–Guidance to Achieve Sustained Success; ISO: Geneva, Switzerland, 2018.

[19] Wicik R., Borowski M. Cryptographic protection of classified information in military radio communication faced with threats from quantum computers // Proc. SPIE 11442, Radioelectronic Systems Conference 2019, 114420Q (11 February 2020); 8 p. doi: 10.1117/12.2565467.

[20] Encryption Technology in Information System Security / S. Suo, W. Xi, T. Cai, G. Jian, H. Yao, J. Li // 3rd International Conference on Mechatronics Engineering and Information Technology (ICMEIT 2019). Advances in Computer Science Research, 2019. Vol. 87. P. 495-499.

[21] Mattila T. Building a complete fullstack software development environment. Turku University of Applied Sciences. 2018. 112 p.

[22] Spring Framework Reference Documentation. https://docs.spring.io/spring-framework/docs/3.2.x/spring-framework-reference/html/index.html.

[23] The official site of the AnyLogic company. Access mode: https: // www.anylogic.com/.

[24] vaadin/docs: Official documentation for Vaadin and Hilla. https://github.com/vaadin/docs.

[25] Wilds N. Corrosion under insulation. In: Energy Trends in Oil and Gas Corrosion Research and Technologies. Duxford, UK: Woodhead Publishing, 2017: P. 409–429.

[26] Eltai E. O., Musharavati F., Mahdi E. Severity of corrosion under insulation (CUI) to structures and strategies to detect it // Corros Rev 2019; 37(6): P. 553–564. https://doi.org/10.1515/corrrev-2018-0102.

[27] Furrer F. J. Safety and Security of Cyber-Physical Systems. Engineering dependable Software using Principle-based Development. Springer Vieweg Wiesbaden. 2022. 537 p. https://doi.org/10.1007/978-3-658-37182-1.

[28] Yuzevych V., Skrynkovskyy R., Koman B. Intelligent analysis of data systems for defects in underground gas pipeline // Proceedings of the 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). Lviv, Ukraine. August 21-25, 2018. P. 134-138. DOI: 10.1109/dsmp.2018.8478560

[29] X. Lyu, Y. Ding, S.-H. Yang, Safety and security risk assessment in cyber-physical systems // IET Cyber-Physical Systems: Theory & Applications. 2019, Vol. 4, No. 3. P. 221-232.

[31]. Pattanavichai S. Program for Simulation and Testing of Apply Cryptography of Advance Encryption Standard (AES) Algorithm with Rivest-Shamir-Adleman (RSA) Algorithm for Good Performance // International Journal of Electronics and Telecommunications, 2022, Vol. 68, No. 3, P. 475-481. Doi: 10.24425/ijet.2022.141263.

[32]. Enhanced Security in Cloud Computing Using Neural Network and Encryption / M. U. Sana, Z. Li, F. Javaid, H. B. Liaqat, and M. U. Ali // IEEE Acces, 2021, Vol. 9, October. P. 145785-145799.

[33]. Yuzevych, V. M., Lozovan, V. P. Influence of Mechanical Stresses on the Propagation of Corrosion Cracks in Pipeline Walls // Materials Science, 2022. Vol. 57, No. 4. P. 539-548; https://doi.org/10.1007/s11003-022-00576-z. DOI 10.1007/s11003-022-00576-z.

[34]. Yuzevych, V., Horbonos, F., Rogalskyi, R., Yemchenko, I., & Yasinskyi, M. (2020). Determination of the Place Depressurization of Underground Pipelines in the Monitoring of Oil and Gas Enterprises. International Journal of Recent Technology and Engineering (IJRTE), 2020. Vol. 9, No. 1. P. 2274–2281. http://doi.org/10.5281/zenodo.3841287.