Methods and means of ensuring the functional stability of information systems of critical infrastructures

Oleksandr Dodonov[1], Olena Gorbachyk[1], Maryna Kuznietsova[1]

[1]*Institute for Information Recording of the National Academy of Sciences of Ukraine, Kyiv, 03113, Ukraine*

Abstract

The dependence of critical infrastructure (CI) on the functional stability and cybersecurity of information systems (IS) is well established. The growing complexity of hybrid threats and the associated security risks underscore the urgent need to strengthen CI's resilience to incidents arising from adverse information impacts. In addition to protecting the physical components of CI and preventing harmful influences, it is crucial to maintain high standards of management, monitoring, and the execution of both technological and administrative processes – all of which rely on information systems that are integral to nearly every critical infrastructure. This paper examines the characteristics of modern information systems within critical infrastructure and identifies the requirements for ensuring their functional stability. It also reviews international practices, approaches, and standards, and proposes strategies, measures, and tools to support the functional stability of information systems in CI.

Keywords

Critical infrastructure, functional stability of information systems, cybersecurity

1. Introduction

Critical infrastructures (CI) are complexly structured entities characterized by hierarchy, functional and resource distribution (service, software and hardware, telecommunications), a large number of interacting elements, blocks, subsystems, and a complex management system [1]. Information systems (IS) are components of any CI. IS tools collect, process, transmit, store, display, document, and reproduce information to ensure management functions, support resilience, restore, and develop CI.

CI IS must have high readiness, stability, mobility, the necessary communication network bandwidth, availability, security, manageability and ensure compliance with the requirements for timeliness, reliability and security of information exchange [2].

The requirements for the resilience of critical infrastructure (CI), the strategies for managing and sustaining its operation in the face of environmental complexity, chaos, and potential instability, as well as the demands for the functional stability of CI information systems, are becoming increasingly stringent amid a growing number of complex and hybrid threats and related security risks. According to the IT Ukraine Association, Ukraine's infrastructure experienced 2,194 cyberattacks in 2022, 2,544 in 2023, and 4,315 in 2024.

Incidents associated with negative impacts on the IS of CI lead to the destruction of information resources, violation of interaction process regulations, failures in standard information procedures, production stoppages at CI facilities, disruption of logistics chains, distortion of management decisions, i.e. they pose a threat to the stability of the CI functioning as a whole.

Incidents in IS of CI are difficult to predict; they usually occur unexpectedly. The probability of a risk associated with physical phenomena (for example, equipment failure) can be determined based on accumulated statistical data, while predicting the implementation of cyber threats in IS is much more difficult. Cyberattacks are diverse, occurring in different time periods, on different components of the IS, and with different periodicity. According to IBM's latest "Cost of a Data Breach Report,"

ITS-2024: Information Technologies and Security, December 19, 2024, Kyiv, Ukraine

dodonovua@gmail.com (O. Dodonov); bges@ukr.net (O. Gorbachyk); marglekuz@gmail.com (M. Kuznietsova)

0000-0001-7569-9360 (O. Dodonov); 0000-0001-8492-4478 (O. Gorbachyk); 0000-0001-6054-418X (M.Kuznietsova)

the average time it takes to detect and contain a cyberattack is over 200 days, making it difficult to respond in a timely manner and minimize damage.

One of the components of increasing the resilience of CI, accelerating the response and restoration of CI functioning after the implementation of threats, reducing the duration of service interruptions and minimizing recovery time is ensuring the functional stability of CI IS - the main information and communication asset of CI.

2. The features of critical infrastructure's IS

CI *information systems* are complex systems with a distributed multi-level structure that are in constant interaction with each other and with the external environment. The functionality, reliability, and security of critical facilities and infrastructures depend on the quality of IS functioning. The CI include IS of the operational level of CI objects, IS of the knowledge level, IS of the management level, and information and analytical systems of the strategic level.

Operational-level IS provides operational data processing and management of production processes at CI facilities. Knowledge-level and management-level systems (middle-level management IS) are focused on monitoring the status of critical infrastructure and individual objects, control, development and adoption of management decisions, administration, etc. The tools of these IS allow you to track and compare current infrastructure performance indicators with past ones, archive and provide access to archived information, create reports for a certain period of time, etc. Strategic-level IS are involved in long-term planning, analysis and forecasting of changes in the operating environment of CI objects, identification of resources for changes in the functioning of CI as a whole, etc.

The functional stability of IS is defined as its ability to maintain its control structure and continue performing its primary intended functions despite the influence of failures, malfunctions, or disruptions [3]. Functional stability implies that the IS have a certain level of reliability, fault tolerance, survivability, and security and characterizes the system's ability to resist change and be stable. A functionally stable IS is guaranteed to perform the main functions of its intended purpose, does not have a negative impact on the environment and does not pose a threat to its existence.

The operation of a CI IS results in a complex set of control actions of various physical natures – direct or indirect, differing in intensity, duration, and frequency – applied to the controlled objects. In the event of adverse impacts, the CI IS provides:

- monitoring, which continuously processes real-time data from CI objects and generates alerts when specific parameters exceed permissible limits;
- diagnostics**,** aimed at identifying and localizing areas of malfunction or error;
- prediction of the potential consequences of events or phenomena based on the analysis of data from diverse sources;
- planning of actions and allocation of resources to prevent incidents and mitigate threats;
- adjustment of management decisions when incidents, errors, or failures are detected;
- control of CI objects and the entire CI system, including the establishment of appropriate operating modes for the information system itself;
- information exchange within the CI.

In the context of threats, the emergence of an emergency situation (ES) in CI and in the functioning of IS, problems arise that are associated with the high rate of changes in the state of CI objects, the unpredictability of events, the dependence of information flows on the situation, changes in the distribution of functions, the expansion or narrowing of the scope of action, etc. The situation is further complicated by the fact that the reaction of the management object (critical infrastructure) to external control influences and other external and internal excitations, taking into account the ability of the CI, as a system, to self-organize, is a priori known and predictable only to a certain extent. The above-mentioned features of CI and CI IS result in significant uncertainty regarding their state at any given time, the set of characteristics that describe this state, and the completeness of such descriptions. Consequently, both CI and their IS are subject to a high degree of uncertainty in relation to external inputs, control actions, the condition of the control system, and the status of the controlled objects. This uncertainty makes attempts to accurately determine the full vector of their state or to develop a complete functional description of their interactions – both internal and with the external

environment – largely impractical. At the same time, ensuring the functional stability of the IS requires developing a framework (or model) of possible IS states that are critical to maintaining this stability. In other words, it is necessary to create a comprehensive list of threats to the IS's functional stability and provide detailed descriptions of each. Clearly, this list cannot remain static over time; it must be periodically reviewed and updated, which may result in either an increase or a decrease in the number of identified threats. Threats may be independent or exhibit cause-and-effect relationships. In most cases, building threat models involves compiling a list of threats, identifying their sources, methods of realization, affected objects, and destructive properties, as well as assessing the level of danger each threat poses to the specific system. In practice, expert-based methods are most often used to develop such threat lists. A review (or reassessment) of the threat list should be conducted at least in the following cases:

- identification of new system vulnerabilities (internal causes),
- identification (emergence) of new opportunities for "violators" or environmental factors (external causes),
- deepening knowledge about the system (accumulation of operating experience) or its external environment.

When forming a list of threats to the functional stability of the IS and performing their description (in fact, creating models), it is necessary to determine a list of parameters and characteristics of the IS that lead to the emergence of a particular threat. Monitoring these parameters (their indicators) will allow determining the possibility of the emergence, further development, or weakening of the threat. Of course, it is advisable to include in the list of such parameters only those that can be measured (determined) in one way or another (direct or indirect). It is logical to assume that the same parameters, but (in the general case) with different values, will correspond to different threats.

As studies show, a common feature of parameters and factors (environmental influences) that determine the state, operating conditions, and threats to the functional stability of CI IS is their inherent uncertainty of various kinds, which concerns:

• forms of their existence (expression);
• heterogeneity of data requiring joint processing;
• correspondence of indicator values to the actual characteristics of IS and CI;
• ability of indicators in aggregate to reflect the state of IS CI;
• possibility of simultaneous receipt of different values of the same indicators from different sources.

3. The task of ensuring the functional stability critical infrastructure's information systems

Let us consider some information system Ω as a part of the CI, the functional stability of which must be ensured. As already noted, functional stability is a property that determines the ability of a system to perform its functions, adapting to various destructive influences. We will decompose the IS by functional criteria. The result of the decomposition of the IS will be a certain set of relatively independent functional subsystems that have a minimum number of connections between them $\Omega=\{\Theta_i\}, i = \overline{1,n}$. Each such subsystem Θ_i performs some unique function within the system Ω .

It is possible to further decompose subsystems Θ_i in order to determine the list of "standard" functions and typical technical and other means (resources) for their implementation. Among Θ_i there are subsystems Θ_j^* ,that perform a certain integral function, further decomposition of which is impractical for consideration of the system Ω. The isolation of such subsystems separately is important from the point of view of resolving issues of monitoring indicators that characterize the process of functioning of the Ω system. As a rule, subsystems Θ_j^* perform supporting functions that are not included in the target function of the system. Monitoring the performance indicators of such subsystems is advisable to understand the "movement" of the subsystem towards "aging" and cessation of functioning.

For all other functional subsystems $\{\Theta_i\}\backslash\{\Theta_j^*\}$, it is advisable to carry out further decomposition in order to identify groups of homogeneous and unique elements in each subsystem. Homogeneous elements of a subsystem are understood as "microfunctions" that are close (similar) in content, as well as typical technical means and personnel of the same qualification level. Within homogeneous

groups, the issue of redistribution of functionality is resolved most simply, without significant losses in the efficiency of the system as a whole. The presence of reserve elements in such groups allows for redistribution to be carried out virtually “imperceptibly” for the Ω system. As for personnel, instead of reserve elements, it is appropriate to talk about additional labor resources, which can be accumulated not only by attracting additional employees, but also by transitioning the existing staff from standard conditions to a more intense work regime.

It should be noted that homogeneous elements are not necessarily “located” within only one subsystem. Such elements can be in different subsystems simultaneously. And in this case, “free” elements of some functional subsystems can be transferred “for use” to other subsystems that have suffered losses.

Monitoring the performance of homogeneous elements in the simplest case can be reduced to determining the fact of their operability at certain moments (or intervals) of time: "operable" or "inoperable". Such an indicator can in most cases be measured by technical means. In relation to personnel, the performance indicator can also be “measured” by technical means, for example, by systems for controlling arrival and/or presence at the workplace.

Unique elements of subsystems solve a unique (specific) “microfunction”, and therefore the transfer of their function to other elements is practically impossible, and therefore, to ensure the functional stability of the system Ω, it is necessary to have backup unique elements. Provided that there are backup elements, monitoring the indicators of unique elements of the system can also be reduced to determining the fact of their operability at certain points in time.

A special category of unique system elements includes expert, analytical, or diagnostic groups that operate to maintain the operability of the IS and the CI as a whole. Their work produces certain generalized indicators, which, although somewhat subjective, serve as evaluative measures. These interrelated system indicators form the basis for monitoring the state of the system Ω and identifying existing threats to the stability of its functioning.

After the loss of reserve resources of subsystems, the system loses functional stability and its further adaptation to the current operating conditions can be carried out by abandoning some “elementary functions”, the failure of which minimally affects the target function Ω or postpones such an impact for some time. However, it should be noted that a situation is possible when some "elementary function" of one of the subsystems, which has little effect on its functions, can significantly affect the functions of another subsystem with which it interacts. Therefore, it is desirable that the degradation of the functionality of individual subsystems be carried out under a certain "control from above", primarily to avoid the so-called "domino" effect, when the loss of function by an individual subsystem can lead to a cascade of removal from the working state of a large number of other elements or even subsystems of the CI. It is advisable to have pre-developed scenarios for such functional degradation of IS and other components of CI, and various situations of resource shortage.

It is also necessary to have means of monitoring external environmental factors, as this will allow to identify in advance the group/groups of system elements (or connections between them) that may be subject to the destructive influence of an external factor and to respond in a timely manner, and will also simplify the task of determining the list of possible factors that led to this and identifying a specific factor of destructive influence that needs to be neutralized.

CI components may possess their own means for influencing the external environment to improve the conditions of their functioning. Such means are an important – and sometimes fundamental – for ensuring the functional stability of CI components and the overall resilience of the infrastructure.

The task of developing models to detect threats to the functional stability of CI IS can be viewed as a recognition problem. During the monitoring of a CI IS, the degree to which the system’s current state corresponds to the characteristics of a specific threat is assessed. Threat models should therefore be developed and described in advance, and the set of CI IS performance indicators must be evaluated for conformity with the identified threat signatures.

Recognition methods provide high-quality results when the recognition objects are significantly “spaced” in the feature space. When the threat feature space overlaps, i.e., the threat images are similar, the complexity of correctly solving the recognition problem increases.

The complexity of formalizing the dependencies between individual indicators of the functioning

of the CI IS and the possibility of certain threats leads to the fact that it is most appropriate to carry out a fuzzy recognition procedure to identify threats. In addition, the incompleteness of information about threats and data about their characteristics generates various kinds of information uncertainties both regarding the threat itself, the object of recognition, and the "image" of the object obtained by the system for monitoring the state of functioning of the CI IS. Therefore, in a strict sense, the recognition task becomes fuzzy by definition.

The task of recognizing threats to CI IS generally involves two stages:

1) formation of templates (standards, descriptions) of threats;
2) identification ("recognition") of states of the CI IS threatening the functional stability.

At the first stage, it is necessary to determine the set of possible (predictable) threats Z. Threats from the set Z can be in different hierarchical relationships, however, determining such relationships is not important for forming patterns, but is important for solving the problem of attracting and distributing resources to neutralize threats.

For each threat $z_t \in Z$, an exhaustive set of features M_t must be defined, which characterizes it and is a subset of the set of features available for observation by the IS CI status monitoring subsystem.

After that, we divide the set of threats Z into subsets in such a way that the threats of different subsets do not overlap in terms of the list of features that define them, or overlap in such a way that the list of features of threats of one subset is not a subset of the list of features of threats of another. All threats of one subset will be considered to be of the same type. For threats of the same type, typical response and neutralization solutions can be developed. For each subset of threats $Z_j \subset Z$ it is possible to determine the degree of danger to the functioning of the CI IS.

For a subset of threats Z_j, a complete list of features $\mathcal{M}_j$ is formed by the operation of merging the feature sets M_t of all threats of the subset Z_j ,where $j \in [1;\ J]$.Then, the set of possible feature values from the set $\mathcal{M}_j$ is determined for each threat in the subset Z_j. The degree of correspondence of each value to each threat of the subset Z_j (correspondence to its existence, occurrence (actualization)) is determined on the set of possible values. Next, the task of formalizing (creating a model) of the threat itself is solved. In essence, this is the task of aggregating features into an integral indicator (sign) of the emergence (existence) of the threat. Such aggregation, as a rule, is hierarchical.

In fact, the result of all the steps of the first stage of solving the problem of recognizing threats to IS CI is the formation of fuzzy models (templates) of threats based on a set of features that define them and are subject to monitoring. All threats from any subset $Z_j \subset Z$ are described by an identical set of heterogeneous features in the general case.

The first stage should be carried out in advance. In the process of functioning of a specific CI IS, both the list of threats and the threat indicators that define them, and the method of aggregating indicators into a sign of the existence of a threat can be specified.

At the second stage of solving the problem of recognizing threats to the CI IS, the stage of "recognizing" the states of the CI IS that threaten the functional stability, it is checked whether each indicator obtained during monitoring is included in the sets of threat signs $\mathcal{M}_j$. If "yes" – the indicator value is fed as "input" to the subset threat templates Z_j. If "no" - the indicator is ignored. At a predetermined rate, the set of received signs is aggregated according to the template of each threat within the threats of a specific subset, obtaining the value of the sign of the occurrence (existence) of the threat. The dynamics of aggregation of the values of the indicators of the functioning of the CI IS significantly depends on the possible rate of development of management decisions in the system and only for individual groups of threats (or threats in groups) that pose a significant danger to the functioning of the CI IS and have rapid development over time, the maximum possible rate of determining the state of the threat is used.

Let us consider the process of creating fuzzy standards of threats to the stable functioning of CI IS.

After determining the list of characteristic features of the threat, they are described in the form of fuzzy sets $\{x, \mu(x)\}$, whose carriers are distinct sets of possible sign values $x \in X$. The membership function $\mu(x)$ of each fuzzy set should reflect the degree of correspondence of each value of the feature x of the crisp set X to the threat for which the template (reference description) is being formed. The next step is to determine the weights of each feature from the point of view of

identifying (detecting) this particular threat. It is necessary to choose the modality by which these features should be aggregated (convolved), that is, the "transformation" of the set of features into one integral feature of the threat. For example, if a threat can be identified by any of the specified features, the convolution modality should be close to a logical “OR”, if the fact of detecting a threat requires taking into account all features – a logical “AND”. In all other cases, the convolution modality is between these extremes.

The proposed reference description of the threat is two-level (obtaining the values of the features from the set of their possible values and “obtaining” the threat feature from the set of features). That is, at the first level, the values of the features are determined, and at the second, their convolution is performed. In the general case, the description of the threat can be multi-level:

• at the lower level – sets of values of individual threat features are determined, which will be convolved with their specific values;

• at the second level – individual features are convolved into complex features of a higher level.

• at subsequent levels – complex features are convolved into more complex features and so on until an integral threat feature is obtained.

At each level, the same fuzzy integral is used for convolution, but with a different modal shade of convolution. At the lowest level, where fuzzy sets of features are convolved by a measure that describes a reference representation of these features, the “possibility” modality (logical “OR”) is usually used. Using the fuzzy integral, the following convolution modalities are implemented (the modalities are ordered by their amplification) [4]: “possibility”, “likelihood”, “probability”, “trust”, “necessity”. Such a wide range of modalities allows us to bring the content of integral assessments closer to human intuitive expectations.

An important question is the degree to which the set of detected features corresponds to the reference description of a certain threat, allowing us to claim that it has been detected. The decision on the adequacy of the level of correspondence of the set of features of the statement about the recognition of a certain type of threat depends on the quality (accuracy, completeness) of the reference description, the quality of monitoring data, the similarity (closeness in description) of the threats and, finally, the cost of incorrectly attributing or not attributing the “current image” to known threat images. And therefore, the task of deciding whether the level of correspondence of the set of observed threat features to the object of recognition is sufficient for its "recognition" rests with the person (their experience and knowledge). However, it should be noted that in the practical use of the approach, provided that a sufficient amount of statistical data is accumulated, it is possible to define a clear or "blurred" scale for automatically solving this problem or to use the capabilities of artificial intelligence.

At the second stage of recognizing threats to the CI IS, the stage of identifying the states of the CI IS that are threatening to the functional stability, it is necessary to clearly determine whether the state of the CI IS is threatening according to its characteristics (parameters). For identification, an identification method based on a step-by-step analysis of the features (parameters) of the system state can be applied. The system state can be considered as some information object (IO) in the state space. Each IO has an image - a set of features that characterize this object to a certain extent. The IO identification procedure is reduced to a simple comparison of the IO features with those specified in the identification request. If the characteristics of the IO coincide to a necessary and sufficient extent with the image specified in the query (and it is possible to use semantic queries or fuzzy proximity measures), it is considered that the IO is identified, that is, there is a set of information objects θ ,that determines the threatening states of the CI IS $\theta = \{IO_1, IO_2, \dots, IO_m\}$,each of which is characterized by a set of features $(P_1, P_2, \dots, P_n)$. Each of IO_i are characterized by the same number of features. However, there are possible cases when IO_i may lack the values of some features, which is due to the fact that the parameters by which these features are formed are not available to monitoring tools. Each IO of the set of states is unique, there are no absolutely identical IOs.

Currently, there is no universal technology for constructing a comprehensive set of CI states that pose a threat to the system’s functional stability. Each solution is tailored to a specific field of activity and to particular software and hardware platforms. However, several common factors are always

considered: the established division of CI information systems into subsystems; the multi-level hierarchical architecture that combines principles of centralization and decentralization; and the principle of necessary diversity, which holds that a system complex in its functions cannot possess a simple structure or consist of uniform elements.

4. Formalization of the task of assessing the functional stability of information infrastructure in the context of computer attacks

Predictions of the scale of possible damage to CI objects when various threats are implemented are usually based on a priori assessments of the threat potential. The risk to critical infrastructure is higher, the greater the potential of the threat. Numerous computer attacks on CI IS are a significant factor in disruptions in CI functioning. The task of ensuring cybersecurity for CI as protection against cyberattacks and ensuring the functional stability of CI IS in the face of cyberattacks has become urgent.

The information and communication infrastructure of CI is a set of interconnected components, among which there are those that are susceptible to cyberattacks, such as CI IS. At the design stage of the information and communication infrastructure of the CI, special means are laid down for each component that ensure its protection from negative influences. Moreover, the requirements for CI resilience require the presence of a functional recovery system within the CI information and communication infrastructure, which has some, albeit limited, resource. The recovery system responds to damage to any component of the information and communication infrastructure and, using the available resource, restores the affected component, thereby restoring the overall functionality of the information and communication infrastructure of the CI.

Suppose:

ΔT – the period of time from the beginning to the end of a negative impact, in particular a cyberattack.

$\Delta T = (0, T]$, where T – the point in time when the cyberattack ended.

$\mathfrak{h} = \{F, N, T\}$ – characteristics of a cyberattack.

$F = \{F_i(t)\}$, where $F_i(t)$ – distribution function of random η_i time interval before the start of $i-$ cyberattack, $i = \overline{1, N}, N$ – number of cyberattacks.

$\mu = \{T_{rec}, S\}$ – an indicator of the functional stability of a certain j - component information and communication infrastructure CI, which characterizes the ability to restore the broken functionality of the component through the implemented i - cyberattack.

$T_{rec} = \{\tau_i^{low}, \tau_i^{up}\}$ – set of lower τ_i^{low} and upper τ_i^{up} value of time intervals for restoring functionality j - component (estimates τ_i^{low} and τ_i^{up} obtained either through the use of expert methods or by conducting special studies).

$S = \{S_i(t)\}, i = \overline{1, N}, -$ the set of distribution functions of random time intervals of recovery of the component functional after i - cyberattack.

$\wp$ – set of indicators of functional stability of components φ, which characterizes the ability of a component to maintain its functionality after repelling a cyberattack.

$\wp = \{p_i\}, i = \overline{1, N}, N-$ number of cyberattacks, p_i- the probability of damage to a component during the i-cyberattack (obtained either through the use of expert methods or as a result of statistical modeling).

$K_{or}(u, t) = K_r(u)P(t, \Delta T)$ – non-stationary operational readiness coefficient of a component, which is determined by the probability of failure-free operation of the component during the implementation of a cyberattack and elimination of consequences.

u – indicator of reliability and recoverability of the component of the information infrastructure of the CI under normal operating conditions.

$K_r(u)$ – component availability factor calculated for standard conditions.

$P(t, \Delta T)$ – probability of failure-free operation of a component over a period of time ΔT. $\Delta T = (0, T]$.

The functional stability of the component of the information and communication infrastructure of the CI in the conditions of cyberattacks can be characterized by the function $\varphi(t, \mathfrak{h}, \mu, \wp)$,whose

average value on the interval ΔT:

$$\varphi_{\text{c}} = \frac{1}{T}\int_{0}^{T} \varphi(\ t, \mathfrak{h}, \mu, \wp) dt.$$

To assess the functional stability of a component of the information and communication infrastructure of the CI, an indicator can be used that characterizes the probability of the component being in a state of full functionality at any point in time $t \in (0, T]$:

$$\kappa_{\varphi} = \lim_{\substack{t \to T \\ n \to N}} \varphi(t, \mathfrak{h}, \mu, \wp)$$

T and N – the maximum possible moment of implementation of a set of cyberattacks and the maximum predicted number of cyberattacks in the set are determined, respectively, through the use of expert methods.

Regarding the practical application of the proposed functional stability assessment, we note that the calculation of the κ_{φ} indicators using statistic modeling methods requires a lot of time, and therefore it is possible to obtain an assessment of functional stability untimely, when it becomes irrelevant. In addition, the question of the reliability of such an assessment remains open [5].

5. Means of ensuring functional stability of systems available in IS of critical infrastructures

The functional stability of the information and communication infrastructure of a CI is significantly affected by the information technology implemented in the CI. The reliability and security of information technology largely depends on the technology for processing user requests (officials and staff), the availability of the necessary resources for this, and their compliance with the tasks being performed, the flow of which can be considered external to the IS. Failures in servicing user requests can occur not only due to failures and malfunctions of technical equipment, but also due to overload, insufficient IS resources, and this can lead to loss of requests or delay in service beyond acceptable time limits. Failure to fulfill a user request within a specified time can be considered a failure of the information and communication infrastructure or its components, and therefore taking into account critical service delays is important when assessing the functional stability of critical infrastructure IS. It is worth noting that since critical infrastructure IS usually operate in real time, which does not allow delays in the execution of functions beyond maximum permissible values, the possibilities of repeating the execution of the function after failures and errors are limited, and even more so the possibilities of performing recovery procedures.

Functional stability of IS implies the ability of the system to withstand incidents without loss of functionality, limiting the duration of interruption in processing user requests and minimizing recovery time. Recovery does not necessarily mean returning to the state in which the incident occurred; it may involve adaptation to new operating conditions with possible improvement of system functionality in the future.

The task of ensuring the functional stability of the IS and, accordingly, the information and communication infrastructure of the CI should be formulated as a system-wide one during design, when a certain redundancy (structural, programmatic, time, resource) is traditionally introduced, built-in control systems and protection circuits are being formed, and components with an increased level of security and reliability are being selected. All of these solutions contribute to increasing the functional stability of the IS regardless of the negative impact on the system, and take into account the known states and reactions of system elements, but they have limitations. Additional redundancy leads to a deterioration in technical and economic characteristics. Control systems monitor certain parameters, but not always, or at all, can provide an adequate response to an emergency situation and do not affect the probability of these situations occurring. The protection circuit can minimize the impact of predicted external factors, but does not completely eliminate them. Choosing an element base with an increased level of security and reliability increases the fault tolerance of the IC, but does not ensure functional stability when a failure has already occurred.

The quality and security of the functioning of the information and communication infrastructure of the CI are definitely influenced by the technologies being implemented – data management technologies, cloud services, artificial intelligence technologies.

Analysis of incidents in CI IS shows that in most cases, initial unauthorized access to IS resources is obtained in advance, through the use of compromised VPN accounts or through configuration flaws and/or software vulnerabilities. In the first quarter of 2024, 15 incidents were recorded in Ukraine, during which five types of malware were used: Remcos Rat, QuasarRat, Venom Rat, Remote Utilities, Lummastealer. Given the massive number of attacks and the use of programs that rely on stolen authentication data, it can be assumed that these data are a prerequisite for unauthorized access to CI IS. Therefore, special attention is clearly paid to the protection of CI IS data, their reliability, integrity, and confidentiality at all stages of processing – from collection and transmission to analysis and placement in storage, using encryption, data masking throughout their migration, and strict regulation of data work.

The main approaches to organizing universal data management platforms have been the use of multi-model systems and integrated data management platforms. A large number of SQL, NoSQL, and NewSQL class systems are offered for both operational and analytical data processing based on data warehouses, data lakes, and data clouds [7]. Modern applications work with large volumes of diverse data and require high performance, scalability, and security, and systems of each class have different approaches to protecting structured, loosely structured, and unstructured data. SQL data management systems built on the basis of the relational data model are most often used for online transaction processing (OLTP) and analytical data processing systems (OLAP) based on classic data warehouses. These systems work well with a fixed schema and maintain data integrity through constraints and triggers, executing transactions in full compliance with the ACID principles (Atomicity, Consistency, Isolation, Durability). Procedures that perform calculations within the database itself help minimize data transfer. High availability is achieved through data replication and partitioning between disk systems, and increased performance is achieved through vertical scaling.

SQL systems have a limited range of applications, in particular due to the rigidity of the schemas, unacceptably high query execution latency, inconvenience in working with unstructured data, and difficulty in horizontal scaling. It is possible to overcome the limitations of SQL systems by using NoSQL systems, which are distributed non-transactional data management systems. They, like SQL systems, are divided into operational and analytical systems. NoSQL systems enable horizontal data scaling by using thousands of identical servers, support variable schemas and specific data types, and have high performance when processing large amounts of unstructured information coming from the network in real time.

Almost all NoSQL technologies were created to solve the problem of partitioning, that is, to work effectively on clusters.

NoSQL repositories can be easily divided into clusters due to their specific data storage structure.

This provides horizontal scaling of the system and a high level of performance in the cluster, simplifies the methods of storing and accessing data.

Internal connections between disparate heterogeneous information sources are established by creating metadata and storing it in a NoSQL system. The main method of searching the database is to search the metadata by keywords.

NoSQL DBMSs may not comply with ACID standards, using instead the less stringent BASE requirements (basic availability, soft state, eventual consistency) and are capable of using different data models [7], including:

- "key-value" – Redis, MemcacheDB, Riak, DinamoDB DBMS;
- column-oriented – Cassandra, HBase DBMS;
- document-oriented – MongoDB, Couchbase, MarkLogic DBMS;
- graph – OrientDB, Neo4J, Titan DBMS;
- XML-based – BaseX, TeraText Database System, Sedna, eXistdb DBMS;
- object-oriented – db4o, GemStone, ObjectDB, Objectivity DBMS.

In 2011, NewSQL appeared - a class of modern relational DBMSs (Clustrix, VoltDB, MemSQL, NuoDB, MySQL Cluster, TokuDB, Spanner), which combine the advantages of NoSQL and classic SQL systems for OLTP processing of structured and unstructured data, offer partial access to many tools of traditional SQL systems, and support the SQL language as the main mechanism for interaction.

They support transactions, segmentation, replication, and the use of MapReduce methods.Many NewSQL systems offer the use of SQL clusters with a significant number of physical nodes for storing and processing large amounts of data. High processing speed is ensured by the use of RAM and new types of disks (flash memory/SSD), which are the primary data storage. Some of this class of systems support several data models, but the relational one prevails.

The rapid evolution of the functionality of NoSQL systems led to the merger of NoSQL and NewSQL systems and the emergence of multi-model DBMSs. The functions of key-value, document-oriented and graph databases with support for SQL are simultaneously performed in one system. The use of multi-model DBMSs allows solving problems related to security, reconciliation and data transformation of different DBMSs.

Multi-model DBMSs have given impetus to the development of cloud databases provided as a service (DBaaS – Data Base as a Service). Currently, there is a smooth migration of data management systems to the cloud, where there is easy scalability, high fault tolerance, availability of servers from all over the world, and easy cloning and deployment of data. Disadvantages of clouds: the required level of security is not guaranteed, since it is impossible to physically control the data, as it is under the control of the cloud provider, i.e. important data is stored on an uncontrolled site.

Today, it is possible to use an integrated data management platform, which consists of an infrastructure platform, a structured and unstructured data storage platform, and a data processing platform. This provides the ability to select a variety of data processing tools for different tasks based on a single platform. Examples include software packages for deploying, monitoring, and managing an Enterprise Hadoop cluster, such as Hortonworks Data Platform (HDP), IBM BigInsight, Arenadata Hadoop (ADH). The integrated platform includes current stable versions of all the most popular tools, such as Apache Hive, Apache Spark, and Apache Atlas, and tools to ensure correct integration of the tools with each other. It is possible to exchange metadata with other tools and processes inside and outside the Hadoop stack. The integrated platform provides tools for efficient data transfer between Apache Hadoop and structured data stores such as relational databases, data warehouses (EDW).

Another example of an integrated data management platform is Oracle's large stack of data management and analytics solutions, including the Oracle Cloud Database Services platform.

The main problem for creating integrated platforms is the lack of generally accepted standards for programming interfaces and languages for different classes of systems [7]. Universal data management systems store data of different types, different levels of structure and value. There is integration on a single platform of data warehouses of different types, including cloud ones, with different storage media. The concept of perimeter security is becoming blurred, and there is a need to shift the emphasis from protecting applications and infrastructure elements to protecting data. It becomes advisable to use an *information-centric security model (Data-Centric Security Model-DCS*), which allows you to build a security system taking into account the value of the data, that is, protection measures are determined depending on the value of the data. The use of data analysis tools, machine learning methods for data classification, and detection of suspicious user actions allows us to guarantee a certain level of data protection when working with heterogeneous devices and data, depending on their value at a certain point in time.

Data value analysis should be conducted periodically, as the value of data changes over time. DCS is focused on protecting critical data at all stages of its processing – from collection and transmission to analysis and placement in storage. The DCS model involves encryption, data masking throughout its migration path, and strict regulation of data work for authorized users.

Transforming a set of disparate data into a single array is also possible through "data virtualization" – organizing access to them through logical data windows. A logical data warehouse (data mart, dashboard, or dashboard) is an integrated system architecture in which all data does not change its physical location in the original systems and repositories. The showcase has access to each source, is "aware" of its structure, is able to request information from source systems and transform it according to a single structure, automatically combine data received from different sources, and provide access to it. This concept is used to organize work with data lakes, using semantic technologies and ontological data models [7].

Oracle has released Oracle Autonomous Database and Oracle Autonomous Data Warehouse DBMS options with self-management, self-protection, and self-healing capabilities that allow for automatic detection and remediation of threats while the DBMS is running. The DBMS security

system automatically recognizes threats, such as the possibility of data theft, and configures the DBMS accordingly. All routine and preventive data operations are performed automatically without intervention by the DB administrator.

It should be noted that for new generation data management systems (NoSQL, NewSQL), security issues are considered within the framework of individual implementations. Research on the security of such data management systems has not kept up with the dynamic development of the market for database technologies and cloud computing, and the practice of solutions for integrating data of various types.

The implementation of cloud computing models – infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) – into the information and communication infrastructure of CI requires the implementation of adequate and appropriate security protection measures. In cloud service environments, management of various levels is distributed between the cloud service provider and the cloud service subscriber depending on the cloud service model. The different layers in the cloud services architectural stack are based on certain differences from the model proposed by the Cloud Services Security Alliance. While there is a general consensus on the threats and security objectives for each layer, there remain nuances associated with varying degrees of control over the layers in different cloud service models or environments. This affects the set of protection measures that can be implemented and determines their effectiveness in specific conditions.

The main data protection measures when using cloud technologies are data encryption, backup, access control with additional layers of protection, security auditing and monitoring to identify suspicious actions and potential threats, implementation of an intrusion detection and threat analysis system, and application of international standards and regulatory requirements [8-10].

Insufficient attention to cloud service providers' security practices, failure to comply with government regulations and industry standards, and unclear division of responsibilities between the provider and the consumer create gaps in information protection. In particular, failure to implement proper security measures by a cloud service provider can result in cloud misconfiguration and lead to numerous cyber threats, such as data leaks, ransomware attacks, malware, phishing, etc.

Integrating data from external sources creates third-party risks, as vendors can generate varying levels of threats to the information and communication infrastructure of CIs whose data is stored in the cloud. Data supply chain attacks occur when attackers penetrate CI IS through external users or cloud service providers who are granted access to CI IS and data.

Unknown software vulnerabilities (zero-day vulnerabilities) can certainly also be exploited to negatively impact CI IS. This realization led to the emergence of a “roadmap” of recommendations for software manufacturers to create programs that are secure by design and by default, update development programs, with transparency and accountability, and facilitate configuration automation, monitoring, and regular updates (Cybersecurity and Infrastructure Security Agency (USA) and 13 other countries and organizations).

The following measures can effectively reduce security risks to the information and communication infrastructure of CI and, in particular, the IS of CI when using cloud technologies and avoid data loss and modification:

- implementation of mechanisms for protecting data-centric cloud services;
- assessment of attack vectors on data assets from both the external and internal information interaction contours existing between CI IS;
- identification of risks of data-centric service sources, also from third and fourth parties;
- developing a response plan for potential incidents;
- permanently assessing the security status of data-centric cloud service providers;
- providing staff training;
- regularly assessing compliance of measures with all necessary regulatory requirements.

In most CI, the information and communication infrastructure operates on the principle of centralized management, when full control over the system is exercised through the main server, which increases the risk of compromising the entire system and increases the number of vulnerabilities and threats.

Current innovation trends indicate that decentralized systems and autonomous mechanisms will gradually replace centralized networks with automated management and control. The use of distributed decentralized systems and networks in CIs will reduce the vulnerability of their

information and communication infrastructure. But the cyberthreat landscape continues to evolve towards more effective, more damaging, and larger-scale attacks. Thus, the development of generative artificial intelligence (GenAI) has led to a growth in the number of phishing attacks by a whopping 4151% since ChatGPT's public debut in late 2022 [6]. According to SlashNext's "State of Phishing in 2024" report, the Anti-Phishing Working Group (APWG) recorded 932,923 phishing attacks in the third quarter of 2024 alone [6]. The World Economic Forum's Global Risks 2024 report predicts that the average annual cost of attacks on technological assets and services, including financial systems and communications infrastructure, owned by any country's CIs will reach over $23 trillion in 2027, up from $8.4 trillion in 2022 [6].

Given the use of artificial intelligence (AI) technologies to create cyberthreats, the integration of AI into cyber defense systems becomes understandable. Organizations of all sizes are already experiencing an overall increase in ransomware attacks compared to previous years. GenAI makes phishing more dangerous by making it easier for attackers to create expressive bait to lure potential victims GenAI has numerous security risks that began to emerge in 2023, including sensitive data leaks and data poisoning. GenAI has become a growing cybersecurity concern. At the same time, AI is a critically important tool in the cybersecurity strategy, and experts expect that with the development of AI technology, cybersecurity will be strengthened [11]. Threat detection and blocking are among five key areas where artificial intelligence (AI) – including machine learning (ML) and generative AI (GenAI) – is helping to improve operational efficiency. The other four areas where AI is useful are analyzing user behavior, automating routine tasks, monitoring network traffic to detect malware, and predicting potential vulnerabilities where breaches may occur [11].

According to Spherical Insights, in 2022 the global market for AI solutions for cybersecurity was estimated at $15.25 billion, and it is predicted that by 2032 it should grow to $96.81 billion.

Attackers are actively using AI technologies in preparing cyberattacks to automate hacking processes (searching for vulnerabilities, overcoming protections); simplifying and automating targeted phishing to steal personal data; creating deepfakes for fraud and social engineering; "data poisoning" to disable AI models for any tasks; simplifying the development of malicious software. This is forcing the cybersecurity industry to quickly adapt and widely implement appropriate AI algorithms to monitor suspicious activity, search for vulnerabilities in systems, assess risks, recognize AI-generated materials, and respond to attacks. Cybersecurity experts consider AI as an algorithm that can find patterns in input data or evaluate it in order to further use the results obtained for independent decision-making [12]. AI is used for automatic processing and analysis of security reports, detection of system intrusions, monitoring and analysis of traffic, combating "false alarms", and predicting threats.

AI tools can help with assessment and optimization during large-scale updates to the information and communication infrastructure of the CI, in particular when implementing a new system over a local environment, when moving to the cloud, when implementing new technologies or integrating different systems, etc. AI algorithms simplify configuration analysis and setup, and significantly improve the quality of testing to verify compatibility, performance, and security of IS, allowing you to detect most conflicts, errors, and vulnerabilities that may arise when upgrading or changing the operating environment.

Today, we can already say that the application of cognitive technologies and AI in the field of information security has opened up new opportunities for creating automated, "smart" security tools for data management systems. Such systems have the inherent ability to self-analyze and configure themselves taking into account existing conditions and events based on defined criteria and knowledge of previous states of the system. AI can take into account a significant number of different parameters to detect behavioral anomalies and minimize the risks associated with the human factor. Machine learning technologies are able to identify weaknesses in security systems and predict the directions of future attacks. Cognitive technologies allow the use of various AI methods to enhance the capabilities of security services. But it should always be borne in mind that the tools present in cyberspace can be used to protect systems and improve the quality of infrastructure, and on the other hand, they can be turned against those who are being protected and used to harm the same systems and their users.

Ukraine has been at war for three years, and the country's information and communication infrastructures, intelligence and intelligence systems have been repeatedly hit by specially designed cyberweapons. This type of weapon is used by cybercriminals and state-sponsored groups, but most

of what is used as cyber warfare tools are actually functional pieces of infrastructure or tools that can be used for innovation [7].

6. Conclusions

Given the complexity, interdependence and interconnectedness of CI and their information and communication infrastructures, to ensure the resilience of CI, and in particular the functional stability of CI IS, it is necessary to rely on a systemic approach and apply both solutions to generally increase the reliability and fault tolerance of computer resources, as well as solutions to counteract the expected negative impacts. An essential factor in ensuring the functional stability of CI IS is the analysis of uncertainties and risk assessment for CI IS, which allows maintaining the ability of IS to counteract unforeseen negative impacts through the timely development and application of appropriate adequate means and measures.

Declaration on Generative AI

During the preparation of this work, the authors used ChatGPT-4 in order to Grammar and spelling check. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the publication's content.

References

[1] Dodonov, O., Gorbachyk, O., Kuznietsova, M. Automated Organizational Management Systems of Critical Infrastructure: Security and Functional Stability. In: XXI International Scientific and Practical Conference «Information Technologies and Security» (ITS 2021). CEUR Workshop Proceedings 2021, 3241, pp.1-12. URL: http://ceur-ws.org/Vol-3241/paper1.pdf

[2] Structural synthesis models for managing parameters of infocommunication networks of critical infrastructure systems: monograph / V. V. Kosenko, I. Sh. Nevlyudov. Kh.: Kharkiv National University of Radioelectronics, 2019. 163 p. (Ukr.)

[3] Dodonov, O., Gorbachyk, O., Kuznietsova, M. Critical Infrastructure Resilience and Cybersecurity of Information Management Systems,p.1-10//Selected Papers of the XXIII International Scientific and Practical Conference "Information Technologies and Security" (ITS 2023) Kyiv, Ukraine, November 30, 2023. URL: http://ceur-ws.org/Vol-3887/ paper1.pdf

[4] Bocharnikov V.P. Fuzzy Technology: modality and decision-making in marketing communications. 2002. K.: Nika-Center, Elga. 224p. (Ukr.)

[5] Voevodin V.A. Monte Carlo method for predicting the stability of functioning of the informatization object in conditions of massive computer attacks. International Conference "MSR-2021" Journal of Physics: Conference Series. V.2099, 2021.

[6] Cybersecurity statistics to lose sleep over in 2025. URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020.

[7] Spasitelyeva S.O., Zhdanova Yu. D., Chichkan I. V. Security problems of universal data management platforms // Cybersecurity: education, science, technology, vol. 2, No. 6, p.122-133, 2019. URL: https://csecurity.kubg.edu.ua/index.php/journal/issue/view/9.

[8] ENISA: Compendium of risk management frameworks with potential interoperability. Technical report, European Union Agency for Cybersecurity (2022).

[9] 10. Freund, J., Jones, J.: Measuring and Managing Information Risk. Butterworth-Heinemann, Waltham (2015). URL: https://doi.org/10.1016/C2013-0-09966-5.

[10] Law M. Top 10 data security risks faced by businesses in 2023 // Cybermagazine. [Electronic resource].URL:https://cybermagazine.com/top10/top-10-data-security-risks-faced-by-businesses-in-2023.

[11] How AI could change threat detection. URL:https://www.techtarget.com/searchsecurity/tip/How-AI-could-change-threat-detection.

[12] Application of AI in cybersecurity: role and benefits. (Ukr.) URL: https://wezom.com.ua/ua/blog/zastosuvannya-shi-u-kiberbezpetsi-rol-ta-perevagi.