International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307 (Online), Volume-15 Issue-4, September 2025

Algorithm for Conducting Information Security Audit in Organizations Based on a Multilevel Model Based on Graph Theory

Kholimtayeva Ikbol, Shamshieva Barno Makhmudjanovna, Muminova Sunbula Shakhzodovna

Abstract. This paper presents a multi-level topological model for auditing information security of critical information infrastructure (CII) objects, developed using graph theory. The model accounts for resource costs, technical impacts (ITE), vulnerability levels, potential damage, and object elements. The proposed framework enables the identification of optimal testing scenarios based on an "efficiency/cost" criterion, supporting the formation of comprehensive test sets for thorough audit coverage. An algorithm was developed to implement the model, which includes graph construction across hierarchical layers and application of Dijkstra's shortest path algorithm to determine the most cost-effective information-technical effects. Additionally, a software tool was created using C# to visualize the graph, manage input data, and dynamically calculate optimal audit paths and damage estimates. A comparative analysis highlights the strengths and limitations of the graph-based model in comparison to traditional audit methods, including compliance audits, risk assessments, penetration tests, and automated monitoring. The graph-based approach stands out for its flexibility, scientific foundation, and ability to prioritise critical vulnerabilities and efficiently audit resources in constrained environments.

Keywords*: Graph Theory, Critical Information Infrastructure, Audit, IT Impacts, Penetration Testing, Damage, Vulnerabilities, Resource, IT Counter Test, Audit Resource Volume, Resource Level, Vulnerability Level

Abbreviations:
ITE: Information-Technical Effects
CII: Critical Information Infrastructure

I. INTRODUCTION

Currently, there is no clear definition of the audit used to analyze the level of information security. You can find different definitions in different sources. Some of them are mentioned below.

Audit- this is a form of independent, neutral control of any sphere of the organization's activity [1]

Audit- is a set of special techniques (methods) used to process primary data to achieve set goals. Various methods of audits are usually combined into four groups: determination of the actual state of objects, analysis, evaluation, and production of technical proposals [1].

Audit - This is a systematic, independent, and documented process of obtaining documents, recording facts, or other relevant information, and objectively evaluating them to determine the extent to which the specified requirements have been met [1].

Audit of information systems- checking the compliance of the information systems, security systems, and communication systems with the external environment, the corporate network used by the company, with the business processes taking place in the company, as well as compliance with international standards, assessing the risk of malfunctions in their operation [1].

Information security audit - an organisation aimed at assessing the state of information security in the automated information system and ensuring the protection of the information resources of the system from information security threats. The audit develops recommendations on the use of a set of measures and software and hardware tools [1].

Information security audit - this is a systematic process of obtaining objective, qualitative, and quantitative assessments of the company's current information security state, evaluated against specific security criteria and indicators [1].

Information security audit - this is a set of organisational and technical measures carried out by independent experts to assess the state of information security of the audited object and its level of compliance with audit criteria [2].

As a result of analysing the definitions given above, the following definition was derived. This definition is the most general and detailed definition of the audit process. This definition is also consistent with the ISO 19011:2011 standards.

Definition 1. An information security audit is a systematic, independent, and documented process of objective analysis that assesses the information security status of the audited object and determines the level of compliance with the audit criteria.

Based on the above definitions, it is possible to conclude that the audit has both general and specific objectives.

Manuscript Received on 25 July 2025 | First Revised Manuscript Received on 04 August 2025 | Second Revised Manuscript Received on 10 August 2025 | Manuscript Accepted on 15 September 2025 | Manuscript published on 30 September 2025.

*Correspondence Author(s)

Kholimtayeva Ikbol Ubaydullayevna*, Senior Lecturer, Department of Information Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. Email ID: iqbola.ubaydullayevna@gmail.com, ORCID ID: 0009-0004-1160-0519

Shamshieva Barno Makhmudjanovna, Senior Lecturer, Department of Information Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. Email ID: bshamsiyeva@gmail.com

Muminova Sunbula Shakhzodovna, Senior Lecturer, Department of Information Security, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. Email ID: sunbulaaxmedova@gmail.com

The primary purpose of the audit is to verify and assess the compliance of the information system with the criteria that determine the requirements for the level of information security.

The procedure and frequency of internal audits of information security for the organisation (or its structural units) are determined by the organisation's management based on the needs for such activities. Independent auditors conduct an external audit of information security [3].

Specific objectives of the audit [2]:

– analysis of risks associated with the possibility of implementing security threats;

– assessment of the current level of security;

– identify vulnerabilities in the security subsystem and obstacles in the system;

– assessment of the compliance of the system with the current standards in the field of information security, as well as with the security policy;

– formulation of recommendations on a set of measures aimed at increasing the effectiveness of the existing protection system.

The objectives of the audit can be divided into the following [2]:

– prevention - aimed at actively identifying threats and vulnerabilities, as well as developing measures to prevent information security incidents;

– detection - aimed at identifying new threats and weaknesses or existing features of the protection system during or after information security incidents;

– corrective - aimed at developing a set of measures to increase the effectiveness of the existing protection system after information security incidents, considering newly identified threats and vulnerabilities.

Currently, the information security audit is carried out on the following objects:

– organizations;

– business processes;

– management systems (management);

– information systems;

– technical systems.

Audit forms are as follows:

– organizational-normative - when analyzing organizational measures to ensure information security and regulatory documents in this field;

– technical - when analyzing the technical means and methods of ensuring information security.

An audit is the most general form of assessing the state of information security of an audited object. The audit is conducted to ensure compliance with requirements developed by stakeholders and regulatory documents.

An audit may involve various methods of testing the subsystems and processes of the audited facility, including analysing documents and other sources of information, as well as interviewing experts.

Audit stages. When conducting an information security audit, it is usually carried out in the following sequence of steps [1]:

1) preparatory stage:

– selection of audit object;

– selection of audit criteria and methods;

– selection of audit tools and methods;

– forming a team of auditors;

– determining the size and scope of the audit, setting the deadlines for its implementation.

2) IIIn stage:

– analysis of the information security status of the inspected object;

– registration, collection and verification of statistical data and results of instrumental measurement of vulnerabilities and threats;

– assessment of inspection results;

– creating a report on the audit results of individual elements of the audit object and various aspects of information security.

3) final stage:

– preparation of the final report;

– formulation of recommendations on a set of measures aimed at increasing the effectiveness of the existing protection system;

– development of a plan of measures to eliminate weaknesses and deficiencies in information security.

The sequence of the audit, especially the approaches based on the analysis of information security standards and conformity assessment [4], has been described in detail in many literatures; therefore, it was not discussed in this work.

II. LITERATURE REVIEW

In most cases, the audit of critical information infrastructure objects is conducted through a comparative analysis or risk analysis in conjunction with regulatory documents governing information security. At the same time, studies in this direction [6] demonstrate the need for a new practical approach to auditing, namely, an audit based on experimental studies of the system or its prototype. This type of audit is carried out by exposing the system to various means or methods of information exposure to practically check the effectiveness of technical or organisational protection measures, as well as to identify new vulnerabilities in the system. However, to ensure the reliability of the audit, the exposures used should be similar to those used by both non-professional and professional violators. In some works, for example [7], the term "penetration test" (in the English literature - "penetration test", "pen-testing") is used to denote this approach, as well as other terms: "active audit", "instrumental audit" and others also represent an approach to auditing, but the essence of the approach to auditing does not change.

Thus, we can say that one of the promising directions of practical information security audits of critical information infrastructure objects is to conduct penetration tests against them, specifically testing data and information-technical effects (ITE) on objects with a high exposure probability. Although such a test is a reasonably adequate and highly reliable approach to safety assessment, it is not widely used. The IIIn reasons for this are the lack of a single generally accepted scientific and methodological basis for conducting this type of audit.

In international practice, conducting a security audit of a facility typically involves

using penetration tests, OSSTMM, ISSAF, OWASP, PTES, NIST SP 800-115, BSI, and other standards, such as those regulated by PETA. A reasonably comprehensive analysis of these standards is presented in. At the same time, the study reveals that these standards are not grounded in any systematic or general theoretical approaches.

S.I. Makarenko [8] is devoted to the practical issues of evaluating the information security status of objects through testing. E.K. Baranova, A.N. Begaeva and others [9], M.Yu. Umnitsyna [10], M.K. Borodina, P.Yu. Borodina [11], M.A. Poltavtseva, A.I. Pechenkina [12], A.M. Kadana, A.K. Doronina [13], N.N. Eremenko, A.N. Kokoulina [14] considered practical methods of information system security testing, such as “penetration testing”. In some works, this type of test is indicated under the name "instrumental audit".

Analysis of the above cases showed the following. In the works devoted to the experimental testing of real information systems, such methods and scenarios are considered only as “penetration testing” or “instrumental audit”. At the same time, there is no universal recognition of conducting this type of audit in practice. Not regulated by the established guidelines or test method regulations. In some work on penetration testing, it is recommended to focus on identifying the most critical vulnerabilities, those that, when eliminated, will yield the most significant economic benefit to the company performing the audit.

Thus, it can be concluded that a promising direction for the development of traditional theory and practice in penetration testing should be based primarily on the already established methods and standards of this type of testing that have been developed abroad.

The studies of authors such as C.P. Pfleeger et al., J.P. McDermott, S.I. Makarenko [5], P. Ami, A. Hasan, F. Holik, and P. Herzog are devoted to providing a scientific basis for testing with special information and technical measures (ITE). In his article, J.P. McDermott presented a test model in the formalism of Petri net theory. In his work, S.I. Makarenko [6] attempted to systematise the possibilities of utilising test information and technical measures to assess the security of critical information infrastructure (III) objects and provide a scientific basis. C.P. Pfleeger et al., F. Alisherov, F. Sattarova, P. Ami, and P. Herzog presented various options for testing methods in their articles. However, none of these works considered the issues of forming a basic audit model, based on which it would be possible to base test ITE sets for various audit tasks on the security of the III object.

One of the goals of this research work is to develop a model for auditing the security of the III facility through technical information activities that can be used to produce test sets for various audit tasks in a scientific manner.

III. METHODOLOGY

To achieve the purpose of the work, the official description of the testing process for the III object is based on the effectiveness of individual ITEs, identified and preventable damage, and their focus on checking a set of vulnerabilities in specific aspects of the III object, mainly in terms of quantity. $i\{z\}\{e\}\{u\}\eta_i$ A Multi-level topological model, taking into account the interrelationship of the cost spent in the process of testing the resource (in this case, the abstract resource can be understood as spending the auditor's time, paying for his labour, the cost of computer time, the cost of specialized equipment, etc.), should be formed in the form of

The following notations are introduced to represent the model:

p/p_n – the absolute/relative value of the totality of the identified and preventable damage;

$E = \{e\}$ - a set of elements that make up a vital information infrastructure object;

e_j –an element of a vital information infrastructure object;j

$g(e_j, e_m, \sigma_n)$ – element – a value describing the destabilizing effect of the element on the component when information security is violated;$e_j \sigma_n e_j e_m$

$I = \{i\}$– a set of information-technical counter tests;

i_j– j - information-technical meter test;

j, l, m, n– accounting variables;

N_I– the number of test ITEs corresponding to the number of set elements;I

N_U– the number of vulnerabilities corresponding to the number of elements of the set of vulnerabilities;U

R– amount of audit resources;

r_j – the amount of the auditor's resources spent on organizing and conducting the ITE test;j

r_n – resource costs of the auditor for conducting the test of ITE;n

$s(x)$– the value of an edge is equal to the number of edges falling on it, meeting certain conditions;x

u – vulnerability of a vital information infrastructure object;

$U = \{u\}$– a set of vulnerabilities of a vital information infrastructure object;

$v(x_1, x_2)$- the weight of the edge connecting the elements of the model;$x_1 x_2$

$z(e_j, s_n)$ – damage caused by a violation of the information security properties of an element;$e_j s_n$

$Z = \{z\}$- general indicator of possible damage to the III object;

σ_n - information security feature: n=1-usability; n=2-integrity; n=3-confidentiality.

The security audit model of the organization's information security object is presented using elements of graph theory and set theory. The model has a linked structure of resources, ITE tests, vulnerabilities, and components of the III object, with damages to each object presented in a hierarchical form (Fig. 1).

Resource level. In the first stage of the model, the resources required to perform the relevant tests of the ITE are ranked in ascending order of "cost". The relationship between the level of resources and the level of ITE tests is established by linking each ITE to a specific element.$i_j r_j$

It is a dependency $v(r_j, i_j)$ is represented by its value, which depends on the cost of conducting the ITE test as follows:i_j.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$v(r_j, i_j) = \frac{r_j}{\sum_{n=1}^{N_I} r_n} \quad \dots \quad (1)$$

The choice of expression (1) depends on the following considerations. First, the resource level from the ITE test level, the set of weights of the edges leading to it, must be normalised to one, i.e.,. $\sum_{j=1}^{N_I} v(r_j, i_j) = 1$ Second, rational testing of ITEs using this model is planned, based on algorithms for finding shortest paths, where lower edge weights correspond to the use of ITEs with less resource consumption. Should have an optimal edge corresponding to the value of Expression (1) that satisfies these conditions.

ITE test level. At the second stage of the model, a set of ITE tests is formed to assess the safety of the III object. $I = \{i\}$

Correlation between the level of ITE tests and the level of vulnerabilities each i_j To achieve ITE {} is defined by identifying a subset of the elements of the vulnerability layer, specifically {} vulnerabilities that the ITE can utilise to cause some amount of damage to the III object. and this correspondence between {} is defined by {} sets of edges, where three is the counter of matching edges. Each $u_m j u_m i_j u_m i_j, u_m m = 1 \dots M_j - i_j v\{i_j, u_m\}$ the weight of an edge {} is proportional to the normalized level of the tip concerning the number of edges leading to elements in the weak level: $u_m i_j$

$$v\{i_j, u_m\} = \frac{1}{N_I \cdot s(i_j | i_j \to u_m)} \quad \dots \quad (2)$$

$s(i_j | i_j \to u_m)$- the value of a vertex is equal to the number of edges that lead to its elements, for example, for the model diagram in Figure1: $i_j\{u\}\ s(i_1) = 2,\ s(i_2) = 3, s(i_1) = 1.$

The same considerations apply to the interpretation of expression (2) as to expression (1). First, the set of edge weights leading from the ITE test level to the vulnerability level should be normalized to unity, that is, . Second, the edge ITE of the best node should match the smaller value of the edge weight when testing more {} vulnerabilities. $\sum_{j,m} v(i_j, u_m) = 1 i u_m$

Vulnerability level. At the third stage of the model, a set of vulnerabilities is formed in the elements of the III object, which have the potential to be used by the ITEacker to destabilize and damage the components of the III object. $U = \{u\}$

Correlation between the level of vulnerabilities and the level of elements of the III object for each vulnerability $u_j\{e_l\}$ Element-level vertices are implemented by connecting to a subset of edges, i.e. elements that can be damaged by exploiting the -th vulnerability. and $j\{e_l\} u_j\{e_l\}$ this match between $\{(u_j e_l)\}$ is represented by the set of edges, where is the counter of the edges corresponding to the end. $l = 1 \dots L_j u_j$

The weight of each edge is inversely proportional to the number of descending edges leading to vertices at the element level: $v(u_j e_l) e_l u_j$

$$v(u_j, e_l) = \frac{1}{N_U \cdot s(u_j | u_j \to e)} \quad \dots \quad (3)$$

$s(u_j | u_j \to e)$ –u_j The value of a vertex is equal to the number of edges leading to it, for example, for a model diagram (see Figure 3.1) $s\{e\}(u_1) = 2, s(u_3) = 3, s(u_4) = 1.$

The same considerations apply to the interpretation of expression (3) as to expression (2). First, the set of weights of the edges leading from the ITE test level to the vulnerability level must be normalized to unity, that is, . Second, the best edge of a node should correspond to a smaller value of edge weight, which is weakly compatible with more tested elements. $\sum_{j,l} v(u_j, e_l) = 1 u e_l u$

Level of elements of critical information infrastructure objects. In the fourth stage of the model, the III object can be harmed by exploiting specific vulnerabilities. $E = \{e\}$ a set of elements is formed.

There are two types of connections at this level:

- connection of elements with each other determined by the probability of destabilizing effect of the element on the element when the information security property of the element is violated; $e_j \sigma_n e_j e_m P_{BT}(e_j, e_m, \sigma_n)$

– connection of the vertices of the element level {} with the vertices of the damage level. $e_j z_l$

The connection of the elements of the same stage to each other is defined by the edges of the view (). The inverse probability of the destabilizing effect determines the weight of each edge: $\{e_j\} e_j, e_m\, g(e_j, e_m, \sigma_n) P_{BT}(e_j, e_m, \sigma_n)$

$$g(e_j, e_m, \sigma_n) = 1 - P_{BT}(e_j, e_m, \sigma_n) \quad \dots \quad (4)$$

In expression (4), under investigation e_m due to the matching of the lower value of the edge weight to the tip with a higher probability of destabilizing effect corresponding to a more complete coverage of the elements. If there is no destabilizing effect, then, i.e., is much smaller than 1 and is topologically "impassable" concerning edge weights, so can be neglected. $P_{BT}(e_j, e_m, \sigma_n) g(e_j, e_m, \sigma_n) =$
$= 1 v(u_j, e_l) v(e_j, z_l) g(e_j, e_m, \sigma_n) = 1$

$\{e_j\}$ Connecting element-level vertices with damage-level vertices is achieved by assigning damage-level vertices to each element based on the information security feature. The correspondence between this and {} is represented by the sets of edges {()}. Each edge $\{z_l\}\{e_j\}\ \sigma_n z_l(e_j, \sigma_n)\{e_j\}\ z_l e_j, z_l$ $v(e_j, z_l)$ weight normalized z_l is inversely proportional to the damage level:

$$v(e_j, z_l) = \frac{\max\limits_{m=1\dots N_E} \{z(e_m \sigma_n)\} - z_l(e_j \sigma_n) + 1}{\sum_{m=1}^{N_E} \sum_{n=1}^{3} z_l(e_m \sigma_n)} \quad \dots \quad (5)$$

where - the number of elements of the III object corresponding to the number of components of the set, - the amount of damage for all aspects of the III object and information security features, - $N_E E \sum_{m=1}^{N_E} \sum_{n=1}^{3} z_l(e_m, \sigma_n) n = 1 \dots 3\sigma_n$ Counter of information security features - maximum damage value between all combinations of information security elements and features. $max\ \dots \{\dots\}$

The following should be explained in expression (5). First, the sum of the set of weights of the edges leading from the level of the elements of the III object to the level of damage must converge, i.e. Second, the best edge with a larger damage value should correspond to a lower weight value. The addition of one in the expression is necessary to make the edge weight corresponding to the maximum damage value non-zero.

$$\sum_{i,l} v(e_i, z_l) \to 1$$

In the fifth stage of the model, the values of damage caused to the III object are sorted in ascending order of "cost". Each specific value is numerically equal to the "cost" of the damage caused to the element of the III object when the -th information security property is violated.$z(e_i, \sigma_n)e_i\sigma_n$

Table- I: Initial Data for Damage Modelling in Specified Units

IS feature	III object elements							
	e_1	e_2	e_3	e_5	e_7	e_8	e_9	e_{10}
σ_1	1	3	6	10	13	9	18	19
σ_2	2	5	8	12	16	15	21	22
σ_3	4	7	11	14	17	20	24	23

$\{u\}$ The values of the edges of the ITE level are determined by the number of edges falling on the elements. Then, using the formula (2), the values of the weights of the edges going from the ends of the {} ITE level to the ends of the vulnerability level are determined (column B of Table 2).$s(i_j|i_j \to \{u\})i_j\{u_m\}v(i_j, u_m)$

$\{e\}$The values of the edges of the vulnerability level are determined by the number of edges that fall into each element. Then, using the formula (3), the values of the weights of the edges going from the ends of the {} edge to the ends of the object element level are determined (Table 2, column C).$s(u_j|u_j \to \{e\})u_j\{e_l\}v(u_j, e_l)$.

Table- II: Calculated Values of the Three and Edge Weights

levels / Node number, j	A.Calculated values of edge weights connecting the resource layer and the ITE test layer $v(r_j, i_j)$	B.The calculated values of the level of ITE tests and the values of edge weights connecting the level of ITE tests and the level of vulnerabilities $s(i_j\|i_j \to \{u\})v(i_j, u_m)$		C.Calculated values of vulnerability level and values of edge weights connecting vulnerability level and elements level of III objects $s(u_j\|u_j \to \{e\})v(u_j, e_l)$	
	$v(r_j, i_j)$ *edge weight*	$s(i_j\|i_j \to \{u\})$ *level*	$v(i_j, u_m)$ *edge weight*	$s(u_j\|u_j \to e\})$ *level*	$v(u_j, e_l)$ *edge weight*
1	0.049	2	0.082	1	0.144
2	0.094	3	0.057	4	0.035
3	0.144	1	0.168	3	0.047
4	0.200	2	0.084	1	0.143
4	0.236	3	0.056	3	0.047
5	0.288	3	0.057	3	0.048
6	0.047	2	0.084	2	0.072
7	-	-	-	1	0.142

When considering the level of elements of the III object, it is initially assumed that one element has no destabilizing effect on another and that all aspects are considered independently., therefore, given that the values of and are much smaller than 1, such a value can be regarded as 'topologically impassable' and is not used in further calculations. $\forall P_{BT}(e_j, e_m, \sigma_n) = 0 \forall g(e_j, e_m, \sigma_n) = = 1 \forall v(u_j, e_l) \forall v(e_j, z_l) \forall g(e_j, e_m, \sigma_n)$

According to expression (5), the values of the edge weights leading from the ends of the element level to the ends of the damage level are determined based on the following initial data. (Table 1). The values of the edge weights are given in Table 3. In general, the safety audit model of the III object is presented in Figure 3.3 with the calculated values of the edge levels and edge weights. Using hierarchical models and graph theory methods, it is possible to analyze the application of certain ITEs by searching for the shortest paths, since the choice of edge weights is formed in such a way that the lower value of the edge weight corresponds to the "best transition option" from one level of the model to another.$\{e_j\}\{z_l\}v(e_j, z_l)v(e_j, z_l)$.

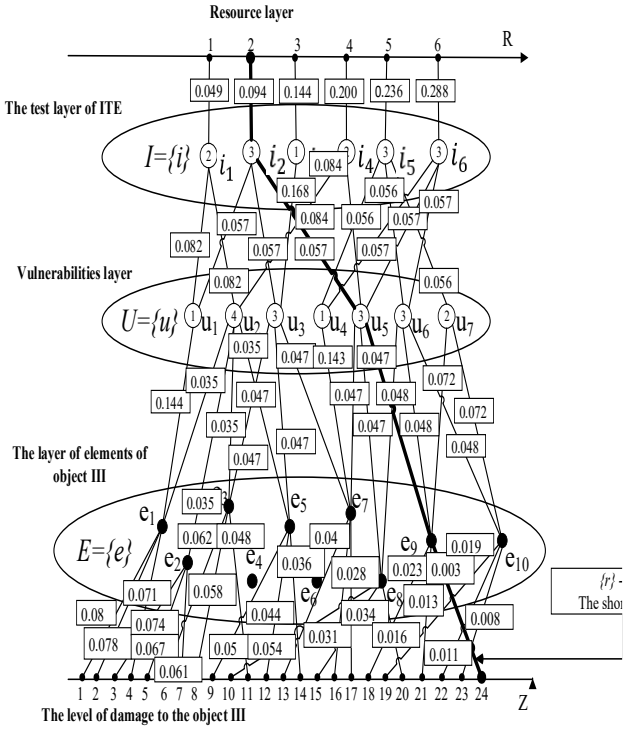
Table- III: σ_n Values of Edge Weights v (E_J, Z_l) by Properties

Property of IS	III Object Elements							
	e_1	e_2	e_3	e_5	e_7	e_8	e_9	e_{10}
σ_1	0.08	0.074	0.062	0.05	0.04	0.054	0.023	0.019
σ_2	0.078	0.067	0.058	0.044	0.031	0.034	0.013	0.011
σ_3	0.071	0.061	0.048	0.036	0.028	0.016	0.003	0.008

For example, in the topological model, using Dijkstra's shortest path search algorithm, the shortest path between a set of nodes in the source layer and nodes in the damage layer passes through the nodes, and its length can be determined to be 0.201. Based on this, it can be concluded that it is preferable to use the III object for testing (indicated by a thick black line in Figure 1). Analysis of the possibilities of using this ITE shows that its elements have weaknesses $\{r\}\{z\}(r_2, i_2, u_5, e_9, z_{24})i_2\{u_1, u_3, u_5\}\{e_1, e_3, e_5, e_7, e_8, e_9\}$ can be used for testing (test paths shown by thick grey lines in Figure 1). In this case, a conditional resource cost will be incurred for testing. For all information security features of the above elements, the absolute value of the potentially preventable damage is a conditional unit. This value is

equal to the relative value of detected and potentially preventable damage = 73%, taking into account that the total damage for all vulnerabilities and elements of the III object is equal to 300 conditional units. $r = 2p = 221p_n$

This model represents the process of testing the III object in the form of a multi-level topological model consisting of individual levels such as resource costs for conducting ITE, ITE test, vulnerabilities, elements of the III object and damage levels. The application of search methods will help identify the "better" ITE based on the "effectiveness/cost" criterion, as well as the ITE test kits that ensure the completeness of the III audit. Allows creation. In further work, this model will be utilised as part of the methodology to establish a set of test ITVs for the reasonable completeness of CII facility safety assessments under limited resource conditions.



[Fig.1: Security Audit Model for III Facility]

The novelty of the III object security audit model presented in this section is that, unlike the formal approaches presented in other works [6], the formal form of the model considers the interdependence:

- the effectiveness of individual ITE trials in terms of identified and potentially preventable harm;
- focusing on testing a particular set of vulnerabilities of some aspects of the III object of individual ITEs;
- consumption of a certain amount of the auditor's resources during the test.

Model learning using graph theory approaches enables the creation of ITE test sets that ensure the completeness of the security audit for the III object.

IV. RESULT AND DISCUSSION

An algorithm and software tool have been developed based on the information security assessment model used in organisations.

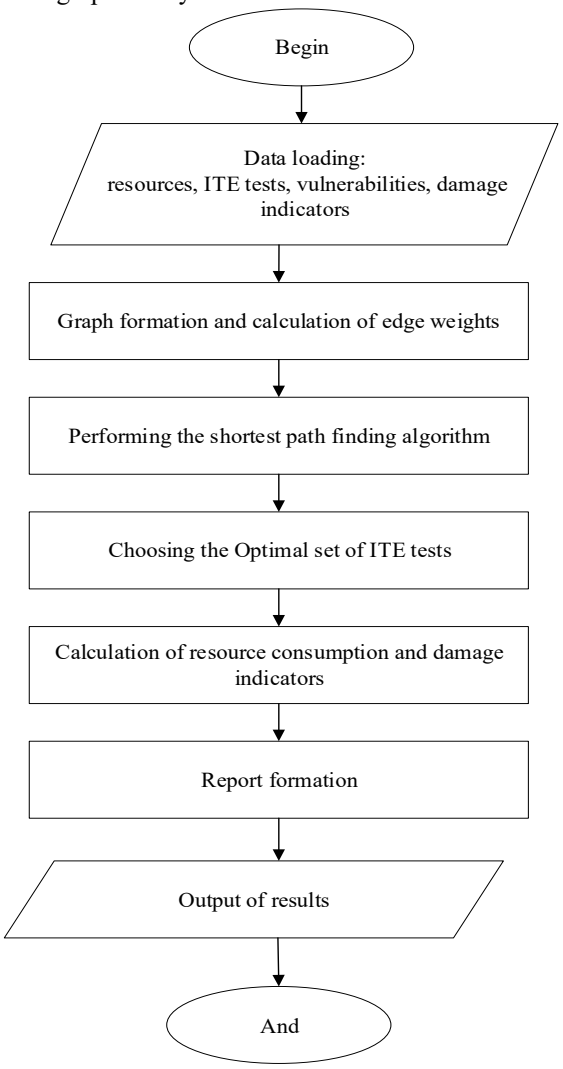
The three steps of the algorithm for conducting an information security audit in organizations based on a multi-level model based on graph theory

The algorithm is expressed as follows (Fig. 2):

1. Enter: Resources, ITE tests, vulnerabilities, and damage indicators.
2. Exit: Optimal ITE test suite and total damage/cost estimation.
3. Algorithm:

1. Upload data: Resources, ITE tests, vulnerabilities, damage indicators.
2. Forming graphs and calculating edge weights.
3. Executing the shortest path algorithm.
4. Choosing the optimal ITE test set.
5. Calculation of resource consumption and damage indicators.
6. Forming a report.

Overview of the algorithm for conducting information security audits in organizations based on a multi-level model based on graph theory:



[Fig.2: An Algorithm for Auditing Information Security in Organizations Based on a Multi-Level Model Based on Graph Theory]

Step 1. Data formation

- Identifying and loading resources: Identify and allocate resources (eg time, cost) required for each ITE;
- ITE tests: Identify vulnerabilities and associated damage metrics corresponding to each test, and define ITE test names, vulnerability compatibility, and resource requirements.
- Weaknesses: Create a list describing the vulnerabilities in the III object and enter the information related to the vulnerability names and their risk indicators (risk factor).
- Damage indicators: Load damage values to set damage probability for each vulnerability or ITE test.

Step 2. Forming a graph

- Create a graph showing the relationship between the III object, ITE tests, vulnerabilities, and damage levels.
- Calculating edge weights at each level. For example, showing relationships between resource consumption, ITE test performance, and vulnerability levels.

Step 3. Shortest path algorithm

- Determining the shortest path from resources to damage level using Dijkstra's algorithm. This algorithm is used to find the optimal path between different layers.
- When calculating edge weights, it is necessary to consider each edge and its weight to choose the least expensive paths.

Step 4. Analyze and produce results:

- Analyzing the selected ITE tests and data, forming an optimal set of tests.
- Resources and costs are evaluated based on the effectiveness and harm reduction rate of each test.

Step 5. Optimization and Decision Making:

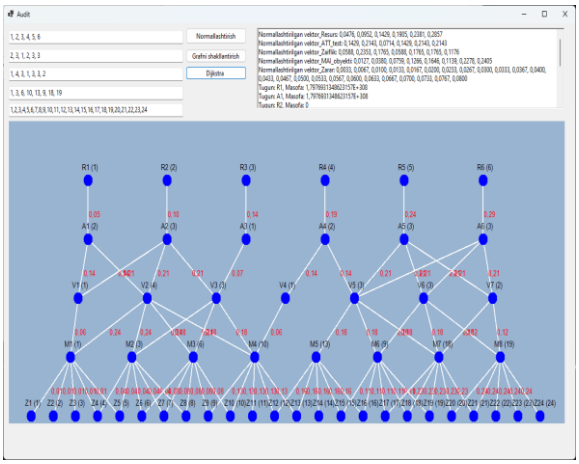
- Coordination of resource consumption and damage indicators.
- Choosing the optimal solution based on the total weights of different paths.

When creating the program code of the algorithm, the following steps must be performed in C#:

- Data Entry: Creating an interface for inputting resources, ITE tests, and vulnerabilities.
- Calculating Graphs and Weights: Calculating edge weights based on input data.
- Extracting audit results: Finding the optimal path and calculating total damage indicators.

In the process of developing a software tool (Fig. 3) created based on an algorithm for conducting an information security audit in organizations, the following steps were performed:

1. Create a graph:
   - Node (Node)and Edge classes were created. The Node class stores the name, position, and value of each node, while the Edge class defines the connection between the start and end nodes, as well as the weight of the edge.
   - Graph class is used to organize nodes and edges. This class has an AddEdge method for adding edges, which specifies the start node, the distance between the nodes, and the weight.
2. Normalization function
   - NormalizeL1function was created, which uses the L1 normalization method. This normalises vectors by dividing each element by the sum of the absolute values of the vector elements.
   - NormalizeDistancefunction is used to normalize distances, where the minimum and maximum values normalize the distance.
3. Dijkstra's algorithm
   - Dijkstra's algorithm is used to find the shortest distance between each node in the graph.
   - PriorityQueue: using the node with the smallest distance is selected, and the distances are updated. For each node, the distance is updated, and the node with the minimum distance is selected.
4. Creating a graph and adding edges
   - Resources level (R) and created a user interface that can enter values for nodes in other levels (eg ITE Tests, Vulnerabilities, III Object).
   - After the user entered vectors through the textBox, the vectors were normalized and their values were used as weights.
   - Create Edges and Create Edges for Resurs ToITE to create links between nodes, Create Edges ForITE to Weakness such methods were developed. These methods make the closest links between nodes.
5. Draw a graph
   - Windows Formspanel was used to visualize the graph.
   - EdgesWhite was drawn using the Pen object, and the nodes were drawn using Brushes. Blue.
   - The weight of each edge, i.e. the distance, is shown in red at the centre of the edge.
6. Finding a path in a graph
   - Dijkstra's algorithm. Dijkstra's method was used to determine the shortest path. This method calculates the distances from each node to all other nodes and outputs the results to the console.
7. Dynamically update the graph
   - panel1.Invalidate() The graph was updated when the draw graph button was clicked through the function. With this, the graph is automatically updated when the user adds new nodes or edges.
   - User Interface (UI)
   - Windows Forms created a user interface using Vectors. User input is entered through Text Box components, and graph drawing and shortest path finding functions are used using Button components.
   - Rich Text Box normalized vectors using the component and the results are displayed to the user.



[Fig.3: View of the Software Tool Developed Based on the Algorithm for Conducting Information Security Audits in Organizations]

The results of comparing the advantages and disadvantages of the graph theory-based model of conducting an information security audit in organizations, which represents the object verification process in the form of a multi-level topological model, and the algorithm-based method of performing an information security audit in organizations with other methods are presented in Tables 4 and 5.

Table- IV: The III_n Advantages and Disadvantages of Information Security Audit Methods in Organizations

No	method/ Algorithm	The basis	Achievements	Disadvantages
1.	Compliance audit	Based on industry and legal standards such as GDPR, PCI-DSS, and ISO 27001	Ensures compliance with legal requirements; increases the confidence of stakeholders	May ignore internal threats [15]
2.	Internal audit	It is based on the organization's internal policies, procedures and management systems.	Provides an opportunity to understand the processes of the organization deeply; provides constant monitoring	Lack of objectivity; limitation of internal vision [16]
3.	External audit	Independent third-party experts carry it out	Provides external and objective assessment; identifies deficiencies that the internal team may not notice	High prices; may disrupt operational activity [16]
4.	Risk assessment	Analyzes potential vulnerabilities in the system and the risks that may arise due to them	Helps prioritize security and allocate resources appropriately	A complex process requires high qualifications [15]
5.	General control audit	Focuses on assessing IT infrastructure, applications and physical security	Creates an overview of IT and physical security	Requires significant resources for full coverage [15]
6.	Application control audit	Checks input, process and output security for applications	Identifies application-level vulnerabilities	Limited to applications, does not cover infrastructure [15]
7.	Automated auditing	Continuous security monitoring using Nmap, Metasploit and SIEM systems	Real-time analysis reduces manual intervention	Risk of misconfiguration; excessive dependence on equipment [15]
8.	Penetration test	Detects vulnerabilities by simulating ITEacks	Identify exploitable vulnerabilities; increases readiness for real ITEacks	Does not cover active risks; does not integrate with other processes [15]
9.	Based on the graph-based model	When ITE tests are performed against resources, vulnerability is determined by the amount of damage to the information object	Helps prioritise security and allocate resources effectively; identifies exploitable vulnerabilities. increases readiness for real ITEacks	Does not cover active risks;

Table-V: Comparative Analysis of the Achievements of Information Security Audit Methods in Organizations

	Compliance audit	Internal audit	External audit	Risk assessment	General control audit	Application control audit	Automated auditing	Penetration test	Based on the graph-based model
Ensures compliance with legal requirements;	+	-	+	+	+	+	-	-	+
Increases stakeholder confidence	+	-	+	+	-	-	+	+	+
Provides a deep understanding of organizational processes	-	+	+	+	-	-	-	-	+
Provides constant monitoring	-	+	-	-	-	-	+	-	-
Gives an external and objective assessment	-	-	+	-	-	-	-	+	+
The internal team will identify the shortcomings that were not noticed	-	-	+	-	-	-	+	+	+
Creates an overview of IT and physical security	+	+	+	+	+	-	-	-	+
Identifies application-level vulnerabilities	-	+	+	+	-	+	+	+	+
Real-time analysis	-	-	-	-	-	-	+	+	+
Reduces manual intervention	-	-	-	-	-	-	+	+	+
Helps prioritize security and allocate resources appropriately;	-	+	+	+	-	-	+	+	+
Identify exploitable vulnerabilities	-	-	+	+	-	-	+	+	+
Increases readiness for real ITEacks	-	-	-	+	-	-	+	+	+

V. CONCLUSION

In this research work, an information security audit in organisations is represented by resource costs, test data, and technical effects, as well as vulnerabilities and damage. The audit process is divided into levels of object elements, forming a multi-level topological model. A model of transfer based on graph theory was developed. The use of this model in audit practice enables the justification of the most effective effects according to the "efficiency/cost" criterion, as well as creating test sets that ensure the completeness of the audit of a critical infrastructure object. Additionally, an algorithm for conducting an information security audit in organisations based on a graph theory model was developed. This model represents the object verification process in a multi-level topological framework, facilitating the audit process.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. Макаренко С.И.. Аудит безопасности критической инфраструктуры специальными информационными воздействиями. Монография. – СПб.: Наукоемкие технологии, 2018. – 122 с. https://www.researchgate.net/publication/340862431
2. Астахов А. Введение в аудит информационной безопасности [Доклад] // GlobalTrust Solutions [Электронный ресурс]. 2018. – URL: https://globaltrust.ru/ (дата обращения: 29.01.2018).
3. Irgasheva Durdona Yakubdjanovna, Nasrullayev Nurbek Bakhtiyarovich, Xolimtayeva Iqbol Ubaydullayevna. Implementation of intercorporate correlation of information security messages and audits.https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9351470
4. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с. https://www.researchgate.net/publication/340871849_Informacionnoe_protivoborstvo_i_radioelektronnaa_borba_v_setecentriceskih_vojnah_nacala_XXI_veka_Information_warfare_and_electronic_warfare_to_network-centric_wars_of_the_early_XXI_century
5. Makarenko S.I. Audit of Information Security - the Main Stages, Conceptual Framework, Classification of Types. Systems of Control, Communication and Security. 2018; 1:1-29 (in Russ.). DOI: https://doi.org/10.24411/2410-9916-2018-10101
6. Makarenko, S.I. Security Audit of Critical Infrastructure with Special Information Impacts. Monograph. Saint Petersburg: Naukoemkie tehnologii Publ.; 2018. 122 p. (in Russ.) https://www.researchgate.net/publication/340862431_Audit_bezopasnosti_kriticeskoj_infrastruktury_specialnymi_informacionnymi_vozdejstviami_Security_audit_of_critical_infrastructure_with_special_information_impacts
7. Skabtsov N. Security Audit of Information Systems. Saint Petersburg: Piter Publ.; 2018. 272 p. (in Russ.)https://itsecforu.ru/wp-content/uploads/2017/11/%D0%90%D1%83%D0%B4%D0%B8%D1%82_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%B8.pdf
8. Makarenko S.I., Smirnov G.E. Analysis of Penetration Testing Standards and Methodologies. Systems of Control, Communication and Security. 2020;4:44–72. (in Russ.). DOI: https://doi.org/10.24411/2410-9916-2020-10402
9. Begaev A.N., Begaev S.N., Fedotov V.A. Penetration testing. Saint Petersburg: Saint Petersburg National Research University of Information Technologies, Mechanics and Optics Publ.; 2018. 45 p. (in Russ.) https://www.researchgate.net/profile/Sergey-Makarenko-5/publication/350758773_Model_audita_zasisennosti_obekta_kriticeskoj_informacionnoj_infrastruktury_testovymi_informacionno-tehniceskimi_vozdejstviami_Model_of_Security_Audit_of_a_Critical_Information_Infrastructure_Object_wi/links/63087bff5eed5e4bd11dfbd3/Model-audita-zasisennosti-obekta-kriticeskoj-informacionnoj-infrastruktury-testovymi-informacionno-tehniceskimi-vozdejstviami-Model-of-Security-Audit-o

f-a-Critical-Information-Infrastructure-Object-wi.pdf
10. Umnitsyn M.Y. Approach to semi-natural security evaluation of information system. Izvestia VSTU. 2018;218(8): 112–116 (in Russ.) https://www.researchgate.net/publication/350758773_Model_audita_zasisennosti_obekta_kriticeskoj_informacionnoj_infrastruktury_testovymi_informacionno-tehniceskimi_vozdejstviami_Model_of_Security_Audit_of_a_Critical_Information_Infrastructure_Object_wi
11. Borodin M.K., Borodina P.Ju. VGATE R2 Information Security Penetration Testing. Regional'naja informatika I informacionnaja bezopasnost [Regional Informatics and information security]. Saint Petersburg, 2017. p.264–268 (in Russ.) https://cyberleninka.ru/article/n/analiz-standartov-i-metodik-testirovaniya-na-proniknovenie
12. Poltavtseva M.A., Pechenkin A.I. Data mining methods in penetration tests decision support system. Information Security Problems. Computer Systems. 2017; 3:62 69. (in Russ.). DOI: https://doi.org/10.3103/S014641161708017X
13. Kadan A.M., Doronin A.K. Cloud infrastructure solutions for penetration testing. Uchenye zapiski ISGZ. 2016;14(1): 296–302. (in Russ.) https://cyberleninka.ru/article/n/model-analiza-zaschischennosti-obekta-informatizatsii-zheleznodorozhnogo-transporta-i-metodika-obosnovaniya-nabora-testovyh/pdf
14. Eremenko N.N., Kokoulin A.N. Research of methods of penetration testing in information systems. Master's Journal. 2016; 2:181–186 (in Russ.)
15. IT Security Audit Methodology – A Complete Guide. https://www.getastra.com/blog/security-audit/it-security-audit-methodology/
16. Information Security Audits: An Overview of Different Types. Johanson Group, LLP Audit Cybersecurity and IT, Oct 17 2024. https://www.johansonllp.com/blog/information-security-audits.

AUTHOR'S PROFILE

Kholimtayeva Ikbol Ubaýdullaevna has worked at the Department of Information Security at the Tashkent University of Information Technologies, named after Muhammad al-Khwarizmi, since 2016. She conducts research on security audits in institutions. To date, she has published over 20 scientific articles on the subject.

Shamshieva Barno Makhmudjanovna. As a senior lecturer in the Department of Information Security at the Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Shamshieva Barno Makhmudjanovna teaches students a range of subjects in the field of security, including network security, malware, and the basics of cybersecurity. She is currently conducting her research on the scientific topic of "detecting network security anomalies".

Muminova Sunbula Shakhzodovna has worked at the Department of Information Security at Muhammad al-Khwarizmi Tashkent University of Information Technologies since 2017. Her research focuses on the security of electronic document management systems, and she has published numerous scientific articles on this topic.