DOI https://doi.org/10.32782/2078-0877-2026-26-1-7
UDC 004.056.5:004.75

Y. O. Zhyvylo[1], PhD ORCID: 0000-0003-4077-7853
A. S. Yanko[1], PhD ORCID: 0000-0003-2876-9316
E. Y. Rubin[2], PhD ORCID: 0009-0005-4447-4413
V. V. Magaletska[2], PhD ORCID: 0009-0000-5562-699X
[1] *National University "Yuri Kondratyuk Poltava Polytechnic"*
[2] *University of Modern Technologies*
e-mail: zhivilka@i.ua

ADAPTIVE TRUST ASSESSMENT MODEL FOR CROSS-DOMAIN SECURITY SYSTEMS BASED ON ZERO TRUST ARCHITECTURE

Summary. In modern distributed information systems, there is a significant increase in the complexity of interaction between different security domains, creating new challenges for ensuring high-reliability access control and effective protection of information resources. Traditional security models based on static access policies and fixed trust levels demonstrate limited effectiveness in the context of dynamic, heterogeneous, and cross-domain environments where diverse organizational, technological, and network domains interact. This paper proposes an adaptive trust assessment model for cross-domain security systems implemented based on the principles of Zero Trust architecture. The proposed approach involves the dynamic determination of the trust level for an access subject, considering a comprehensive set of parameters, including user behavioral characteristics, endpoint trust, domain reputation, access request context, and the history of previous interactions. To formalize the proposed approach, a mathematical trust assessment model has been developed, which allows for the real-time calculation of an integral trust metric and its use in decision-making regarding granting or restricting access. Based on the model, an adaptive trust assessment algorithm has been formulated, ensuring continuous verification of users and devices in a cross-domain environment. Furthermore, a system architecture is proposed, which includes modules for contextual information collection, behavioral analysis using artificial intelligence methods, a Trust Engine computational mechanism, and a decision-making system for access management. To evaluate the effectiveness of the model, an experimental simulation of a cross-domain environment was conducted with various user behavior scenarios and potential attacks, demonstrating improved trust assessment accuracy and a reduced probability of unauthorized access compared to traditional access control approaches. The proposed model can be applied to enhance the cybersecurity level of distributed information systems, cloud environments, and other complex infrastructures where ensuring adaptive access control between different security domains is critically important.

Keywords: cybersecurity, cross-domain security, trust assessment, adaptive trust model, Zero Trust architecture, access control, behavioral analysis.

Statement of the problem. Modern distributed information systems are characterized by a significant increase in the complexity of cross-domain interaction. This is driven by the scaling of organizational, technological, and network infrastructures. Additionally, the integration of heterogeneous hardware and software components further impacts this complexity.

The growing complexity of systems creates new technical challenges. Primarily, there is a need for effective access management for users and devices. Ensuring the confidentiality, integrity, and availability of information resources is also critical. Furthermore, systems must possess a high level of cyber resilience and the capability to counter dynamic threats in real time.

Traditional access control models based on static policies and predefined trust levels demonstrate limited effectiveness in such dynamic and heterogeneous environments. They do not provide an adaptive response to changes in user behavior, device state, or access request context. This is particularly

critical for cross-domain systems where diverse technologies, platforms, and organizational policies interact simultaneously. Consequently, there is an urgent need to develop adaptive trust assessment mechanisms. These mechanisms should dynamically determine the access level of users and devices in real time, accounting for behavioral characteristics, request context, and interaction history.

It is essential to emphasize that the primary problem of modern cross-domain security systems is the lack of universal trust assessment mechanisms. Existing models do not integrate a comprehensive set of factors influencing the trust level, specifically user behavioral patterns, endpoint status, domain reputation, request context, and previous interaction history.

Accordingly, the insufficient adaptability of traditional access control models increases the likelihood of unauthorized access. It also reduces the efficiency of cross-domain access rights management. Therefore, the lack of adaptability in traditional access control models leads to the limited applicability of static Zero Trust architectures and creates a requirement for implementing dynamic trust assessment mechanisms supported by contextual and behavioral analytics. Thus, it is critically important to implement mechanisms for dynamic trust assessment and continuous verification of users and devices. Subsequently, such mechanisms will ensure improved access control accuracy, a significant reduction in the probability of compromise, and reliable coordination of interaction between different domains of the information infrastructure.

Analysis of recent research. Current developments in the concept of cybersecurity demonstrate significant attention to Zero Trust Architecture (ZTA) as the primary paradigm of minimal trust and continuous verification of users, devices, and transactions. At the international level, systematic literature reviews confirm that ZTA has become a fundamental model for protecting complex digital ecosystems, as classical perimeter defense models are unable to function effectively in heterogeneous and cross-domain environments [1, p. 2].

In particular, literature reviews from recent years [2–6] indicate a broad field of research aimed at applying ZTA in cloud infrastructures, IoT, corporate networks, industrial systems, and distributed services. It should be emphasized that almost all modern sources point to the loss of effectiveness of static policies, thereby necessitating a transition to adaptive access control models.

Certain scientific circles in the USA, notably NIST (National Institute of Standards and Technology), have developed specialized recommendations formalizing Zero Trust components, ranging from elements of continuous authentication to conditional access based on context and risk. These standards actively influence further research and implementation practices of ZTA in government, corporate, and critical infrastructures. Current research papers reflect significant regional specificities where, considering national characteristics, technology development vectors vary considerably. For instance, while the priority in the EU is the implementation of Zero Trust in cross-domain networks in compliance with regulations (GDPR, NIS2), the emphasis in China is shifted towards adapting the architecture to local solutions where flexible access control on a corporate scale is critically important.

In the context of trust models, global experience suggests integrating risk assessment, behavioral analysis, and access management into the decision-making process. Under these conditions, Risk-based access control becomes an integral component of modern solutions, combining American experience in optimizing real-time trust assessment algorithms with European approaches to standardizing model interaction in distributed networks. Additionally, to ensure security in large-scale device networks without centralized control, the field of trust computation in IoT environments, based on the integration of ZTA architecture and decentralized learning, is actively developing [7, p. 42].

Methods of behavioral analysis, included in modern solutions based on machine learning and anomaly detection, are highlighted separately. These methods allow for a significant increase in the accuracy and adaptability of trust assessment. Specifically, studies in the USA and the EU show that such approaches significantly reduce the number of false positives and increase the response speed

to anomalous events. This is particularly important for distributed and cross-domain systems where traditional access rules cannot adapt in time to changes in the behavior of access subjects.

Scientific circles pay special attention to cross-domain security issues, as the integration of heterogeneous policies, protocols, and access structures significantly complicates the creation of a consistent trust verification mechanism. Therefore, international standards and modern research emphasize the interoperability of Zero Trust components in complex infrastructures where traditional models prove ineffective due to the gap between domains and the heterogeneity of access rules.

Ukrainian researchers also make a significant contribution to the development of the field, with works dedicated to adapting security architectures and policies based on the Zero Trust concept to the specifics of the national infocommunication space. For example, access management models based on the dynamic determination of security policies developed in [8, p. 84] demonstrate the adaptation of ZTA approaches for distributed IT infrastructures, considering different classes of users and devices. Other Ukrainian works, including projects on the application of Zero Trust in IoT environments [5, p. 173], explore the possibilities of integrating behavioral analysis and micro-segmentation for modern dynamic systems. Specific examples of ZTA application for Ukraine's critical infrastructures show the importance of adaptive access models in the context of increased threats and the need to comply with international security standards [9, p. 94].

Despite significant achievements, several substantial gaps are still observed in the scientific environment. First, there is a lack of adaptive trust models that comprehensively integrate behavioral, contextual, and historical parameters for real-time access management. Second, there is insufficient use of behavioral analysis and ML algorithms for cross-domain trust assessment, which limits the accuracy and speed of decision-making. Third, there is the absence of a universal cross-domain access architecture capable of ensuring the interoperability of diverse security policies and dynamic trust assessment across complex hybrid environments.

Thus, a review of current literature and analytical reports from international and national scientific centers confirms the presence of significant gaps in the field of cross-domain security. This underscores the urgent need to develop adaptive trust assessment mechanisms capable of dynamically determining the access level of users and devices in real time, accounting for behavioral characteristics, contextual parameters, and the history of previous interactions. It is this justified need that forms the basis for developing the research methodology and constructing the mathematical model, algorithm, and experimental simulation presented in the following sections.

The objective of this paper is to develop an adaptive trust assessment model for cross-domain security systems based on the principles of Zero Trust architecture, which allows for improving access control accuracy, ensuring dynamic verification of users and devices, reducing the risks of unauthorized access, and optimizing interaction between heterogeneous domains of the information infrastructure.

To achieve the stated objective, the following research tasks have been identified:

– analysis of existing access control and trust assessment models in international and national research, including Zero Trust architectures, risk-based access control, and behavioral models;

– development of a mathematical trust assessment model that integrates user behavioral characteristics, device state, domain reputation, request context, and the history of previous interactions;

– creation of an adaptive access management algorithm that implements dynamic trust level determination and decision-making regarding granting or restricting access to resources in cross-domain environments;

– designing a system architecture that includes modules for contextual information collection, behavioral analysis, a trust computation mechanism, and an access decision-making system;

– conducting an experimental simulation of a cross-domain environment to verify the effectiveness of the proposed model, algorithm, and trust assessment mechanisms under various user behavior scenarios and potential attacks.

The implementation of these tasks enables a comprehensive approach to adaptive access management in distributed and heterogeneous systems by integrating Zero Trust principles and modern behavioral analysis methods.

Consequently, achieving the outlined objective of this paper will facilitate the fulfillment of the defined tasks and establish a scientifically grounded foundation for developing adaptive trust assessment mechanisms in cross-domain security systems. Furthermore, the developed model will create the necessary conditions for building modern intelligent systems capable of self-learning, preemptive response to anomalous events, and continuous monitoring of trust levels in dynamic environments.

Development of an adaptive trust assessment model for cross-domain systems. Modern information systems are characterized by high complexity of cross-domain interaction and the integration of heterogeneous technological components. This necessitates the implementation of access control and trust assessment models capable of providing dynamic verification of users and devices, as well as real-time access management. To systematize the research, existing approaches can be classified into three main groups:

1. Traditional access control models (DAC, RBAC). Traditional access control models, such as DAC and RBAC, are characterized by relative simplicity of implementation and a clear policy structure, ensuring effective integration into existing corporate systems. At the same time, the centralized structure and static nature of policies limit the ability of such models to dynamically respond to changes in user behavior and endpoint states, while also complicating integration into multi-domain and heterogeneous information environments. Examples of practical implementation of these approaches include Microsoft Active Directory, which uses RBAC for centralized access management, and Oracle Database Security, which supports DAC and RBAC policies for database access control.

2. Risk-Based Access Control (R-BAC). Compared to traditional models, R-BAC approaches evaluate access requests based on the current risk level, integrating contextual parameters such as user geolocation, endpoint device type, and history of previous actions. This ensures dynamic access management, consideration of request context, and the possibility of integration with behavioral analysis mechanisms to improve decision-making accuracy. At the same time, R-BAC approaches have limitations, including increased complexity in policy configuration, significant load on risk assessment computational mechanisms, and partial support for cross-domain interaction in heterogeneous environments. Examples of R-BAC implementation include IBM Security Verify Access, which applies a risk-based approach for access control in corporate and cloud environments, and Cisco Identity Services Engine, which provides dynamic access policies with integrated contextual analysis.

3. Zero Trust Architecture (ZTA) and adaptive trust assessment models. ZTA models are based on the "never trust, always verify" principle, which entails continuous, real-time verification of users, endpoints, and transactions. An advancement of these approaches lies in adaptive trust assessment models that integrate dynamic trust scoring mechanisms. These models account for user behavioral patterns, access context, domain reputation, and the history of previous interactions, enabling an accurate and flexible assessment of the trust level within complex cross-domain environments.

The implementation of such models provides several key advantages. First, continuous verification of users and devices is implemented, which reduces the probability of unauthorized access. Second, the integration of behavioral analysis and machine learning algorithms allows for dynamic anomaly detection and real-time response to behavioral changes. Third, these approaches demonstrate high efficiency in multi-domain and heterogeneous environments where traditional static access control models prove insufficient.

At the same time, these models have significant limitations that result in the complexity of their practical implementation. Key challenges include the high complexity of constructing trust models and trust scoring algorithms, significant computational costs for processing large volumes of contextual data, and the need for centralized or hybrid data collection for accurate trust level determination.

Examples of practical implementation of ZTA and adaptive trust assessment models include Google BeyondCorp, which applies the principles presented in [10, p. 12], and the Adaptive Trust Models proposed in research [5, p. 171], which demonstrate the effectiveness of integrating behavioral analysis and dynamic trust scoring in cross-domain systems.

Given the advantages and limitations of the discussed access control and trust assessment models, a systematic comparison of their key characteristics is appropriate. Such an analysis allows for determining the effectiveness of each model under various conditions, evaluating the level of dynamism, the integration of contextual and behavioral analysis, and the capability for application in multi-domain environments. Table 1 below presents a comparison of access control models, summarizing key parameters, advantages, and practical implementation examples.

Table 1

Comparative table of access control models

Model	Dynamism	Contextual Analysis	Behavioral Analysis	Support for Cross-domain Systems
DAC	Low	No	No	No
RBAC	Low	No	No	No
Risk-Based AC	Medium	Yes	No	Partial
Zero Trust	High	Yes	Partial	Yes
Adaptive Trust	High	Yes	Yes	Yes

Thus, the conducted comparative analysis indicates that traditional DAC and RBAC models remain effective in centralized environments due to their simplicity of implementation and clear policy structure. However, their application in heterogeneous and multi-domain systems is limited by the static nature of policies and the lack of dynamic response to changes in user behavior and endpoint status.

Meanwhile, R-BAC models provide more flexible access control by integrating contextual factors such as geolocation, device type, and user activity history. Nonetheless, their effectiveness in cross-domain environments remains partially limited, as they only partially integrate behavioral analysis and cross-domain interaction, while policy configuration and risk assessment require significant computational resources.

In contrast, ZTA ensures continuous real-time verification of users and devices, which improves access control accuracy and reduces the probability of unauthorized access [11, p. 74]. At the same time, the application of ZTA requires centralized contextual data collection and high computational costs, which may complicate implementation in large-scale multi-domain systems.

In contrast to traditional and risk-oriented models, adaptive trust assessment models integrate Zero Trust principles, behavioral analysis, and contextual information, providing dynamic and high-precision access management in real time. Therefore, this approach demonstrates high efficiency in complex cross-domain environments and allows for the application of ML mechanisms to enhance system resilience against anomalies, unauthorized actions, and potential attacks.

Thus, the conducted analysis underscores the necessity of developing a proprietary adaptive trust assessment model that combines Zero Trust principles, behavioral, and contextual analysis, ensuring high-precision access control, dynamic verification of users and devices, and effective interaction in multi-domain information environments.

In cross-domain information security systems, effective access management requires a dynamic and comprehensive approach to trust assessment. To this end, a mathematical model is proposed that integrates key factors influencing the trust level of an access subject. The model formalizes the integral trust indicator T_s, which enables real-time decision-making regarding the granting or restriction of access.

$$T_s = \sum_{i \in \{u,d,r,c,h\}} w_i \cdot T_i, \tag{1}$$

where $T_s \in [0, 1]$ – the integral indicator of trust in a user or device. A value of 0 corresponds to complete distrust, while 1 represents the maximum level of trust; T_i – the assessment of a specific trust component; $w_i \in [0, 1]$ – the weight coefficient reflecting the significance of each factor; $\sum w_i = 1$ ensures the normalization and consistency of the integral indicator; indices $i \in \{u, d, r, c, h\}$ correspond to the following components:

u – user behavioral characteristics (T_u),
d – endpoint state (T_d),
r – domain reputation (T_r),
c – request context (T_c),
h – history of previous interactions (T_h).

Component T_u represents the probability of normal user behavior, estimated based on the analysis of their actions within the system:

$$T_u = 1 - P(A_u), \tag{2}$$

where $P(A_u) \in [0, 1]$ – the probability of user behavior anomaly, determined by machine learning methods and statistical detection of deviations.

High values of T_u indicate stable, predictable user behavior, while low values suggest a potential risk of unauthorized access.

To calculate A_u, activity pattern clustering, anomaly detection, or autoencoders can be applied to predict the risk of anomalous activity.

Component T_d assesses the technical security of the device used to access the system:

$$T_d = \alpha_s \cdot S_{OS} + \alpha_p \cdot P_{patch} + \alpha_v \cdot V_{antivirus}, \quad \alpha_s + \alpha_p + \alpha_v = 1, \tag{3}$$

Where $S_{OS} \in [0, 1]$ – assessment of the operating system state (configuration, absence of vulnerabilities); $P_{patch} \in [0, 1]$ – relevance of installed patches and updates; $V_{antivirus} \in [0, 1]$ – anti-virus protection status; α_s, α_p, α_v – weight coefficients reflecting the criticality of each sub-factor for device security; $\alpha_s + \alpha_p + \alpha_v = 1$ ensures the normalization of the assessment T_d.

Domain reputation is modeled as an exponential smoothing of the security incident history:

$$T_r(t) = \beta \cdot T_r(t-1) + (1 - \beta) \cdot (1 - R_{incident}(t)), \tag{4}$$

where $T_r(t) \in [0, 1]$ – domain reputation at time t;

$R_{incident} \in [0, 1]$ – risk assessment of the current incident in the domain;

$\beta \in [0, 1]$ – smoothing coefficient that prioritizes previous events or emphasizes recent incidents.

Consequently, a high domain reputation reduces the risk of unauthorized access and increases the overall trust level.

The contextual assessment accounts for external conditions that influence access security:

$$T_c = \sum_{j=1}^{m} \gamma_j \times C_j, \quad \sum_{j=1}^{m} \gamma_j = 1, \tag{5}$$

where $C_j \in [0, 1]$ – normalized context indicators, such as user geolocation, device type, access time, and resource criticality level;

γ_j – weight coefficients of each contextual parameter;

m – the number of contextual factors.

User interaction history is formed through a cognitive trust accumulation function:

$$T_h = \frac{\sum_{k=1}^{n} \delta^{n-k} \cdot S_k}{\sum_{k=1}^{n} \delta^{n-k}}, \quad \delta \in (0,1), \tag{6}$$

where $S_k \in [0, 1]$ – assessment of the k-th previous interaction;

δ – discount factor highlighting the relevance of recent events;

n – the number of recent interactions considered when calculating the integral indicator.

To implement model adaptivity, weight coefficients may vary depending on the current context:

$$w_i = w_i^0 \cdot f\left(C_{context}(t), R_{risk}(t)\right), \tag{7}$$

where w_i^0 – the baseline value of the weight coefficient; $f(\cdot)$ – an adaptation function that increases or decreases the significance of a component in the event of threats or anomalies.

This approach ensures dynamic balancing of trust factors in real time. The proposed model integrates behavioral, technical, and contextual analysis, along with historical interactions of users and devices, providing a complete integral trust indicator T_s. The model formalizes adaptive trust scoring, which serves as the foundation for the decision-making algorithm in cross-domain security systems [12, p. 3], enabling dynamic access management, enhanced risk assessment accuracy, and a lower probability of unauthorized actions.

Following the principles of the modern Zero Trust concept, access to information system resources must be determined through continuous assessment of the trust level of the access subject as well as an analysis of the potential risk associated with request execution [13, p. 1].

In view of the above, an adaptive access management algorithm is presented below for dynamic trust evaluation and flexible regulation of user rights within the system. Primarily, it is necessary to formalize a set of parameters characterizing the state of the access subject and the context of the request. To achieve this, a vector of contextual characteristics is introduced:

$$X(t) = \begin{bmatrix} B(t) \\ D(t) \\ R(t) \\ C(t) \\ H(t) \end{bmatrix}, \tag{8}$$

where $X(t)$ – vector of trust parameters at time t; $B(t)$ – indicator of user behavioral characteristics; $D(t)$ – trust level of the access device; $R(t)$ – reputation of the domain environment; $C(t)$ – request context (time, geolocation, network type); $H(t)$ – history of previous interactions with the system.

Comparing the vector representation of parameters with traditional trust assessment approaches, it can be noted that such an approach enables the application of linear algebra and statistical analysis methods for information processing.

Since various factors have different levels of significance for assessing access security, it is appropriate to utilize a system of weight coefficients. To this end, we introduce a weight vector:

$$\mathbf{W} = [w_1\ w_2\ w_3\ w_4\ w_5], \tag{9}$$

where w_i – the weight coefficients of the corresponding trust parameters.

Then the integral trust level is defined as the dot product of the weight vector and the parameter vector:

$$T(t) = \mathbf{W} \cdot X(t), \tag{10}$$

specifying:

$$T(t) = w_1B(t) + w_2D(t) + w_3R(t) + w_4C(t) + w_5H(t), \tag{11}$$

where $T(t)$ – the integral trust indicator at time t; w_i – the weight coefficients of the factors, $\sum_{i}^{5} w_i = 1$.

Thus, the integral trust assessment is formed as a weighted aggregation of factors, enabling the model to adapt to various levels of information resource criticality.

However, relying solely on the trust level is insufficient for making an informed access decision. Therefore, an access risk assessment function is introduced based on the principle of balancing trust and risk:

$$R_{risk}(t) = \sum_{i=1}^{n} \lambda_i F_i(t), \tag{12}$$

where $R_{risk}(t)$ – the integral risk indicator; $F_i(t)$ – the i-th risk factor; λ_i– the weight coefficient of the risk factor; n – the number of risk factors.

Risk factors may include:

– anomalous user behavior;
– use of a new or untrusted device;
– access from an atypical geolocation;
– use of an unsecured network;
– low reputation of the domain environment.

Thus, risk assessment allows for accounting for potential threats that may arise during the execution of an access request.

To combine the trust level and the risk level, a generalized security indicator is introduced:

$$S(t) = \beta T(t) - \gamma R_{risk}(t), \tag{13}$$

where $S(t)$ – integral access security indicator; $T(t)$ – trust level; $R_{risk}(t)$ – risk level; β, γ – weight coefficients of the influence of trust and risk.

Therefore, based on this relationship, even a high level of trust can be compensated for by an increased level of risk, which fully corresponds to the concept of dynamic access management in a Zero Trust environment.

To ensure a more flexible decision-making mechanism, it is appropriate to apply a logistic function, which allows for estimating the probability of granting access:

$$P_{access} = \frac{1}{1 + e^{-k(S(t)-\theta)}}, \tag{14}$$

where P_{access} – probability of granting access; $S(t)$ – integral security indicator; k – steepness coefficient of the logistic function; θ – security threshold value; e – base of the natural logarithm.

By comparing the obtained value P_{access} with established thresholds, the system determines the required level of access to the resource.

The access decision can be represented by the following function:

$$Decision = \begin{cases} Allow, & P_{access} \geq 0.75 \\ Challenge, & 0.4 \leq P_{access} < 0.75, \\ Deny, & P_{access} < 0.4 \end{cases} \quad (15)$$

where *Allow* – granting full access to the resource; *Challenge* – necessity of additional authentication; *Deny* – denial of access.

Thus, an adaptive access control mechanism is implemented, which takes into account not only the static attributes of the user but also the interaction context, behavioral history, and potential risks.

In general, the adaptive access management algorithm in a cross-domain environment is implemented as a sequence of the following stages:

1. Receiving an access request to the information resource.
2. Forming a vector of contextual access parameters.
3. Calculating the integral trust level.
4. Assessing the access risk level.
5. Forming a generalized security indicator.
6. Calculating the access probability using the logistic function.
7. Making a decision regarding granting, restricting, or denying access.
8. Updating interaction history and trust parameters.

Thus, the proposed algorithm provides dynamic and context-oriented access management in cross-domain information environments. Comparing this approach with traditional access control models, it can be argued that the use of integral indicators of trust, risk, and probabilistic decision-making methods significantly enhances the security level of information systems.

At the same time, the practical application of the proposed algorithm requires its implementation in the form of a cohesive information system. Therefore, given the necessity of processing a significant number of contextual parameters and ensuring prompt access decision-making, it is appropriate to develop a modular system architecture.

In this process, each system component fulfills a specific functional load. Specifically, the contextual information collection module ensures the retrieval of data regarding the user, device, and network environment. The behavioral analysis module processes the obtained data and detects deviations from typical behavior. Based on this data, the trust calculation mechanism implements the mathematical model for evaluating the trust level, while the decision-making system forms the final decision regarding granting or restricting access.

Thus, the logical continuation of the developed algorithm is the design of the system architecture, which ensures the coordinated operation of the specified modules. Consequently, the next stage of the research involves designing the system architecture, including modules for contextual information collection, behavioral analysis, a trust calculation mechanism, and an access decision-making system.

The Fig. 1 illustrates the component architecture of the adaptive access control system, reflecting the interaction structure of the primary functional modules and the data flows between them.

This architecture can be represented as a set of functional modules:

$$S = \{M_c, M_b, M_r, M_t, M_d\}, \quad (16)$$

where M_c – context collection module; M_b – behavior analysis module; M_r – risk assessment module; M_t – trust evaluation module; M_d – decision module.

The interaction of the components of the proposed architecture can be represented as a graph

$$G = (V, E), \quad (17)$$

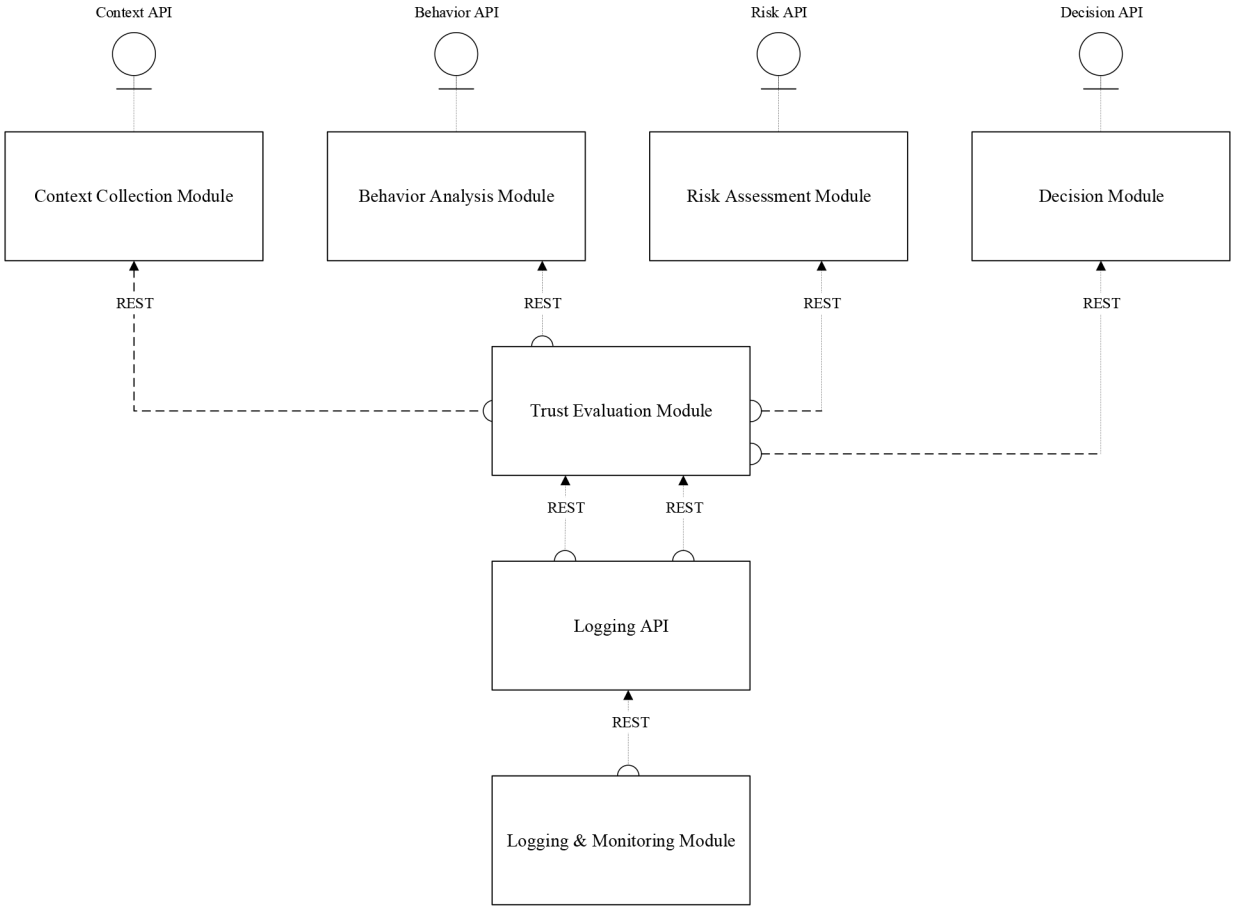

Fig. 1. Access control system architecture

where $V = \{M_c, M_b, M_r, M_t, M_d\}$ – the set of vertices corresponding to the functional modules of the system; E – the set of edges defining the information data flows between the modules.

The set of edges is defined as

$$E = \{(M_c, M_b), (M_c, M_r), (M_b, M_t), (M_r, M_t), (M_t, M_d)\}. \quad (18)$$

The flow logic is implemented through the following set of processes:

(M_c, M_b) – contextual data is transmitted to form a behavioral profile;

(M_c, M_r) – the same data is transmitted to assess the risk of potential compromise;

(M_b, M_t) – behavioral analysis results are used to form an integral trust indicator;

(M_r, M_t) – risk assessment is also integrated into the trust scoring formula;

(M_t, M_d) – the final trust indicator is transmitted for access decision-making.

This means that the contextual information collection module transmits data both to the behavior analysis module and directly to the trust evaluation module, while the behavioral analysis results are used for further assessment of the trust level. After calculating the integral trust indicator, the relevant data is transmitted to the decision-making module.

Taking into account the specified structure, the functioning of the adaptive access control system can be described by a generalized function

$$A = F(U, C, B, P), \quad (19)$$

where U – user attributes; C – contextual parameters of the access environment; B – behavioral analysis results; P – information system security policies; A – access decision result.

The function $F(\cdot)$ implements the adaptive access control algorithm and includes the stages of contextual information collection, behavioral analysis, trust level calculation, and forming the final access decision.

In the general case, the access decision is defined as

$$A = Decision(T, P), \tag{20}$$

where T – integral trust indicator; P – set of security policies.

Thus, the proposed formalization allows for describing the access control system architecture as an interconnected set of functional modules between which contextual and analytical data is transmitted. The use of a graph model provides a clear visual representation of component interaction, while the mathematical description of the decision-making function formalizes the process of adaptive access control in a cross-domain information environment [14, p. 4].

The experimental research simulation was implemented to evaluate the effectiveness of the proposed adaptive trust assessment model and access management algorithm in multi-domain heterogeneous information systems. The primary objective of the study was to determine the extent to which the integration of behavioral analysis, the risk assessment module, and contextual data improves access control accuracy compared to traditional approaches such as DAC, RBAC, and R-BAC. In this regard, the experiment was comprehensive in nature and included modeling dynamic user behavior scenarios and various resource access conditions.

The purpose of the simulation was to evaluate the accuracy of the integral trust indicator T, the adaptability of the decision-making algorithm A, and the system's effectiveness in reducing the risk of unauthorized access. Additionally, the experiment allowed for determining the contribution of behavioral analysis and the risk assessment module to the system's dynamism and its ability to respond to anomalous or attacking user actions.

To achieve the goal, three domains with different access policies (D_1, D_2, D_3) were simulated, and 5000 user requests with varying behavior were generated. The simulation included three scenarios: normal, anomalous, and potentially attacking behavior, which provided the conditions for testing the model's adaptability. The results were compared with DAC, RBAC, and R-BAC models to evaluate the advantages of the proposed approach.

The following simulation parameters were determined: three domains, 150 users, 50 resources, and 5000 requests. The distribution of behavior scenarios consisted of 70 % normal, 20 % anomalous, and 10 % attacking. Trust threshold values were set at $T_{hight} = 0.8$ and $T_{low} = 0.5$ to ensure a balance between security and resource accessibility.

Consequently, the experimental configuration reproduced a realistic multi-domain environment and provided a reliable basis for further analysis regarding the accuracy, adaptability, and efficiency of the proposed trust evaluation model.

The effectiveness of the proposed system was evaluated using three key metrics: decision-making accuracy (Accuracy), the false positive rate (FPR), and risk mitigation efficiency (Risk Mitigation). These are defined in the following way:

$$\text{Accurace}(\%) = \frac{N_{correct}}{N_{total}} \cdot 100, \quad \text{False Positive Rate}(\%) = \frac{N_{false}}{N_{total}} \cdot 100;$$

$$\text{Risk Mitigation}(\%) = \left(1 - \frac{N_{breaches}}{N_{total}}\right) \cdot 100,$$

where $N_{correct}$ is the number of correctly processed requests, N_{false} is the number of false positives, $N_{breaches}$ is the number of recorded unauthorized accesses, and N_{total} is the total number of requests.

The simulation results are presented in Table 2.

Table 2

Comparison of Access Control Models Effectiveness

Model	Accuracy (%)	FPR (%)	Risk Mitigation (%)
DAC	85.2	8.4	76.5
RBAC	87.5	7.2	78.3
R-BAC	92.1	5.6	84.7
Adaptive Trust (proposed)	97.3	2.4	93.8

The analysis of the results confirmed that traditional DAC and RBAC models are effective in centralized environments, but they exhibit limited adaptability in multi-domain scenarios. While R-BAC models provide dynamic context-aware access control, the integration of behavioral analysis and cross-domain interaction remains partial. The proposed adaptive model demonstrates the highest accuracy, significantly reduces the false positive rate, and increases risk mitigation efficiency.

Visualization of the results in Fig. 2 and 3 demonstrates a clear advantage of the adaptive model across all experiment scenarios. The accuracy graph shows that the integration of behavioral analysis and risk assessment allows for achieving 97.3 % Accuracy, which exceeds the performance of traditional models. The risk mitigation level graph reflects 93.8 % for the adaptive model, confirming its ability to minimize unauthorized access threats.

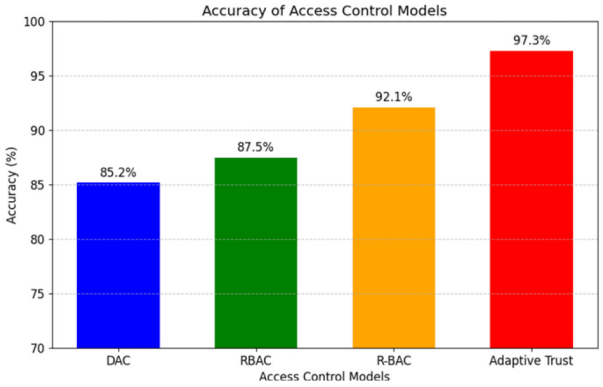

Fig. 2. Accuracy graph

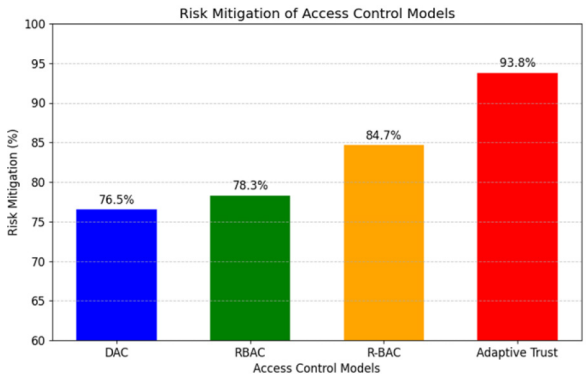

Fig. 3. Risk mitigation level graph

The experimental simulation confirmed that the integration of behavioral analysis and the risk assessment module significantly increases the accuracy of trust evaluation in multi-domain information environments. The use of the proposed adaptive access management algorithm ensures a reduction in the number of false positives and unauthorized access incidents compared to traditional DAC, RBAC, and R-BAC models, which indicates an increase in system reliability. Overall, the application of trust threshold values allows for achieving an optimal balance between security and resource accessibility while ensuring dynamic and context-oriented verification of users and devices [15, p. 42]. Thus, the simulation results confirm the high effectiveness of the proposed adaptive trust evaluation model and justify its further integration into real-world cross-domain information systems where ensuring precise access control and resilience against potential threats is critically important.

Research Results. As a result of the study, a comprehensive evaluation was conducted on the effectiveness of the proposed adaptive trust evaluation model for cross-domain security systems, built on Zero Trust Architecture principles. The developed approach involves the integration of user behavioral analysis, device state assessment, domain reputation, request contextual parameters, and the history of previous interactions to form a dynamic integral trust indicator. This integration

ensures context-oriented and adaptive verification of access subjects within cross-domain information environments.

The obtained results confirm that the combination of adaptive access management algorithms, behavioral analysis, and risk assessment mechanisms allows for a significant increase in access decision-making accuracy, reduces the probability of unauthorized actions, and ensures more effective detection of anomalous activity. The application of the proposed model contributes to the increased reliability, adaptability, and resilience of cross-domain information systems against potential cyber threats.

Overall, the research results confirm the feasibility of utilizing adaptive trust evaluation mechanisms in next-generation access control systems and justify the practical suitability of the proposed model for implementation in complex multi-domain information infrastructures.

Conclusion. The study successfully achieves its stated objective through the development of an adaptive trust assessment model specifically designed for cross-domain security systems operating on Zero Trust principles. A primary outcome of this research is the establishment of a robust mathematical and algorithmic framework that integrates a diverse range of parameters such as user behavioral patterns, endpoint device states, domain reputation, and the history of previous interactions. This framework is supported by a newly proposed adaptive algorithm that enables the real-time calculation of an integral trust score, effectively shifting access control from rigid static policies to a model of dynamic and continuous verification.

Furthermore, the research provides a detailed design for a modular system architecture which incorporates specialized engines for contextual data collection and behavioral analysis alongside a centralized Trust Engine for automated decision-making. The effectiveness of this approach was confirmed through experimental validation involving the simulation of a cross-domain environment subjected to various attack scenarios and behavioral fluctuations. These results demonstrate a significant improvement in trust assessment accuracy and a measurable reduction in the probability of unauthorized access when compared to traditional perimeter-based security models. Ultimately, the implementation of these findings establishes a scientifically grounded foundation for enhancing the cybersecurity and resilience of distributed heterogeneous information infrastructures.

Future studies should be directed toward the integration of machine learning and deep learning methods to enhance the precision of user behavioral analysis and ensure the early detection of anomalies and potential threats.

Another critical aspect involves expanding risk assessment mechanisms by incorporating additional contextual parameters, such as the temporal characteristics of user activity, endpoint device status, and the specific security policies of individual domains. Looking ahead, these advancements will increase system adaptability and the accuracy of the integral trust indicator.

Special attention should also be paid to optimizing the performance and scalability of algorithms as the number of users, resources, and domains increases, alongside exploring the integration of the proposed model into hybrid and cloud environments characterized by heterogeneous security policies.

Bibliography

1. Gambo M. L., Almulhem A. Zero Trust Architecture: A Systematic Literature Review. *Journal of Network and Systems Management*. 2026. Vol. 34, No. 25. DOI: https://doi.org/10.1007/s10922-025-09998-x

2. Mushtaq Sadaf, Mohsin Muhammad, Mushtaq Muhammad Mujahid. A Systematic Literature Review on the Implementation and Challenges of Zero Trust Architecture Across Domains. *Sensors*. 2025. Vol. 25, No. 19. Art. 6118. DOI: https://doi.org/10.3390/s25196118

3. Ma X., Fang F., Wang X. Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks. *arXiv preprint arXiv:2501.03601*. 2025. URL: https://arxiv.org/html/2501.03601v1. (дата звернення: 15.02.2026).

4. Romashko I., Kalashnikova Y. CISCO SECUREX AND ZERO TRUST: MODERN APPROACHES TO CYBER DEFENSE. 2025. URL: http://perspectives.pp.ua/index.php/nts/article/view/29469/29425

5. Zhyvylo Y., Kuchma Y. Mathematical modeling of intellectual and cryptographic protection of authentication keys. *ITS*. 2025. Vol. 13, No. 2. P. 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591

6. Fesenko T., Kalashnikova Y. Mathematical aspects of the combined application of the AES algorithm and steganographic methods in authentication key protection. *Information Technology and Security (ITS)*. 2025. Vol. 13, No. 2. P. 178–191. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344592

7. Хорошко В., Браіловський М., Пархоменко І., Киричук Т. Модель реалізації управління доступом до інформаційних активів в концепції нульової довіри. *Безпека інформаційних систем і технологій*. 2024. Т. 1, № 7. С. 39–44. DOI: https://doi.org/10.17721/ISTS.2024.7.39-44

8. Mankovskyi B., Dovbniak V., Opirskyy I. RESEARCH ON THE FEASIBILITY OF IMPLEMENTING THE ZERO TRUST CONCEPT IN IOT SYSTEMS. *Кібербезпека: освіта, наука, техніка*. 2025. Vol. 1, No. 29. P. 73–91. DOI: https://doi.org/10.28925/2663-4023.2025.29.864

9. Трофімов О. С. Вдосконалення політики безпеки інформаційних систем об'єктів критичної інфраструктури України на основі концепції ZERO TRUST. Телекомунікаційні та інформаційні технології. 2025. № 3. С. 87–102. DOI: https://doi.org/10.31673/2412-4338.2025.038702

10. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology. 2020. DOI: https://doi.org/10.6028/NIST.SP.800-207

11. Zhyvylo Ye., Kuz V. Risk Management of Critical Information Infrastructure: Threats-Vulnerabilities-Consequences. *Theoretical and Applied Cybersecurity*. 2023. Vol. 5, Iss. 2. P. 68–80. DOI: https://doi.org/10.20535/tacs.2664-29132023.2.280377

12. Wang Z., Liu H., Ma R. A Probabilistic Linguistic Large-Group Emergency Decision-Making Method Based on the Louvain Algorithm and Group Pressure Model. *Mathematics*. 2025. Vol. 13, No. 4. Art. 670. DOI: https://doi.org/10.3390/math13040670

13. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024: Predictive Security Intelligence and AI-Driven Threat Analysis. Heraklion: ENISA Publications Office, 2024. URL: https://op.europa.eu/en/publication-detail/-/publication/e71394ea-85f0-11ef-a67d-01aa75ed71a1

14. Wei Z., Lan G., Zhao H., Li Z., Ju Z. Lattice-Based Certificateless Proxy Re-Signature for IoT: A Computation-and-Storage Optimized Post-Quantum Scheme. *Sensors*. 2025. Vol. 25, No. 15. Art. 4848. DOI: https://doi.org/10.3390/s25154848

15. The development of management methods based on bio-inspired algorithms / Kashkevich, Shyshatskyi A. et al. *Information and control systems: modelling and optimizations : collective monograph*. Kharkiv : TECHNOLOGY CENTER PC, 2024. P. 35–69. DOI: http://doi.org/10.15587/978-617-8360-04-7

Дата першого надходження статті до видання: 15.02.2026
Дата прийняття статті до друку після рецензування: 10.03.2026
Дата публікації (оприлюднення) статті: 28.04.2026

Є. Живило[1], А. Янко[1], Е. Рубін[2], В. Магалецька[2]

[1] Національний університет «Полтавська політехніка імені Юрія Кондратюка»

[2] ТОВ ПВНЗ «Університет сучасних технологій»

АДАПТИВНА МОДЕЛЬ ОЦІНЮВАННЯ ДОВІРИ ДЛЯ МІЖДОМЕННИХ СИСТЕМ БЕЗПЕКИ НА ОСНОВІ АРХІТЕКТУРИ ZERO TRUST

Анотація

У статті досліджено проблему ускладнення міждоменної взаємодії в розподілених інформаційних системах, що обмежує ефективність традиційних моделей контролю доступу. Запропоновано адаптивну модель оцінювання довіри, побудовану на принципах архітектури Zero Trust. Наукова новизна полягає у розробці математичного апарату для динамічного обчислення інтегрального показника довіри на основі поведінкових чинників, репутації домену та контексту запиту.

Розроблено алгоритм безперервної верифікації суб'єктів і пристроїв, а також архітектуру системи, що інтегрує механізми штучного інтелекту для аналізу контексту (Trust Engine). Результати експериментальної симуляції підтвердили високу точність моделі у виявленні несанкціонованих дій та стійкість до атак у гетерогенних середовищах. Запропонований підхід є перспективним для посилення кіберзахисту хмарних інфраструктур та складних мережевих систем.

Ключові слова: кібербезпека, міждоменна безпека, оцінювання довіри, адаптивна модель довіри, архітектура Zero Trust, контроль доступу, поведінковий аналіз.