UDC 004.056
DOI: https://doi.org/10.17721/ISTS.2024.7.39-44

Volodymyr KHOROSHKO, DSc (Engin.), Prof.
ORCID ID: 0000-0001-6213-7086
e-mail: professor_va@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Mykola BRAILOVSKYI, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0002-3148-1148
e-mail: bk1972@ukr.net
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Ivan PARKHOMENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-6889-9284
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Taras KYRYCHUK, Student
ORCID ID: 0000-0003-0013-2989
e-mail: taraskiricuk@gmail.com
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

MODEL OF IMPLEMENTATION OF MANAGEMENT OF ACCESS TO INFORMATION ASSETS IN THE CONCEPT OF ZERO TRUST

Background. *Controlling access to information assets is one of the key functions of information security. This task in one form or another must be solved both as a whole at the level of the entire information technology (IT) infrastructure of a company or organization, and in each local information system.*

Methods. Methods *on existing approaches, the article develops a model for providing access to information assets, which allows implementing access control processes in a distributed IT infrastructure. A special feature of the model is an algorithm for dynamically determining the necessary security policies, taking into account the access of users with different privileges.*

Results. *The model takes into account remote access at several conventional "levels" – access of the organization's clients, organization employees, as well as partners and contractors. Since modern information infrastructures of organizations have become complex and distributed, the model assumes the presence of a significant number of access points, including automated workstations in the infrastructure, remote automated workstations, various user and mobile access devices, as well as specific devices, such as effective access control should ensure centralized access of all users to information assets.*

Conclusions. *The model provides for the implementation of a single access point, built on the basis of access models from the zero trust concept, for users and for "robots" – technical accounts used for inter-system interaction. The results of the study will make it possible to develop an architecture for remote user access to distributed information assets and organize access control and management processes based on dynamic determination of the level of trust in access subjects, which generally increases the security of organizations.*

Ключові слова: *zero Trust, multifactor authentication, single Sign-On, security Policies, fast IDentity Online.*

Background

The Zero Trust security model addresses the needs of applications, users, and devices for fast and secure data access in distributed architectures. Using this concept, it is possible to create fail-safe and continuous protection of users and information assets in cases where it is not possible to be reliable in the security of the network. This concept requires that each individual user, device, or session access each specific request to an information asset without initially verifying and verifying security. The concept of zero trust is a set of ideas designed to increase reliability in the decision to grant access for each request on an untrusted network. Its main goal is the prevention of unauthorized access and the most detailed access management, with this concept, an approach is proposed, rather than specific algorithms and models of access control implementation (Chapman, & Chapman, 2021).

In fact, the concept of zero trust is a set of concepts designed to minimize the level of uncertainty when making decisions about providing access to an information resource in discovered insecure networks that meet the requirements of least privilege. It should be emphasized that the planning of bringing the infrastructure into compliance with the principles of zero trust cannot be carried out partially or within the framework of updating information systems. Restructuring of the information infrastructure as a whole, as well as integration into all aspects of the organization's activities, is required in order for the principles of zero trust to show their effectiveness (Lambert et al., 2023).

At the same time, the greatest efficiency is achieved by investing sufficient funds and increasing investments in the processes of supporting zero-trust infrastructure (Lambert et al., 2023).

The basis of the concept is laid in the special publication NIST 800-207 207 (NIST CSWP, 2023. https://www.ibm.com/topics/zerotrust), which can be used as a guide for the development and implementation of ZTA (ZeroTrustAccess) in organizations. This publication also provides an abstract logical model of the zero-trust architecture (Fig. 1), which was the basis of the developed access control implementation model.

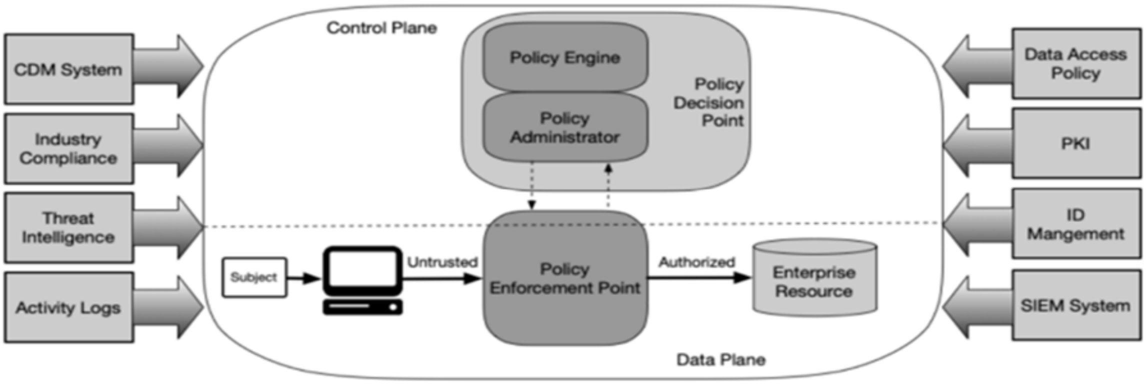

Fig. 1. Basic Logical Components of the Zero Trust Model NIST

The main elements of this model are TechRadar, 2023 (https://www.techradar.com/opinion/whyzero-/trust-cybersecurity-relies-on-people-as-much-as-tech):

- Policy Engine (PE) – the core of ZTA implementation, components on which access possibilities within requests are evaluated, usually based on data from various sources (monitoring systems and logs, threat detection systems at endpoints, etc.);
- Policy Administrator (PA) – a component that implements the policies set on the PE and ensures the establishment, maintenance and termination of access sessions through the control plane (a set of channels between all model elements);
- Policy Enforcement Point (PEP) – a component with which subjects interact by sending requests for access to information assets, collecting information about access subjects and checking them for compliance with policies received from the PA;
- information flows (Policy Information Points, PIPs) – flows that are not the main functional components of the zero trust model, but are used to support the functioning of the PE by providing data for making decisions about access requests.

The basis of providing access to an information resource are the principles outlined in the same concept, which can be briefly formulated as follows:

1) authentication and authorization of all access subjects is dynamic and mandatory;

2) all data sources and services are pre-considered resources;

3) the state of security and integrity of all information resources is constantly monitored;

4) all interactions are protected regardless of network membership;

5) access to specific information resources is provided within the session corresponding to such access;

6) the decision to grant access is made on the basis of dynamic policies that take into account the data received from the PIP;

7) collection of the maximum possible amount of data on the state of security of information assets, network infrastructure and access subjects is ensured.

The listed principles are basic and must be followed when implementing the concept of zero trust in the organization. However, the study does not consider the abstract situation of providing access to a certain subject, but to specific groups of users with their own specificity, that is, subjects with different powers in information assets – user and administrative, as well as specific subjects – external services.

For objects that require greater authority or administrative access, this implies the use of specialized methods and tools to ensure access security for such objects. Thus, in addition to the basic principles of the concept of zero trust, the following two principles were also defined:

1) stricter policies are required to grant broader privileges in an access session;

2) the formation of PP policies should be carried out taking into account the maximum possible degree of security and integrity of access subjects.

The first additional principle is based on the specifics of granting access to entities performing management functions, as these functions require the provision of excess powers that go beyond the minimum necessary. The access of such subjects is usually carried out during the implementation of additional measures to check the devices from which the access is made, to control such access and to monitor.

The second additional principle is based on the likely limitations that may be present when requesting access to technical services, as the various technologies used to implement access may not objectively meet the requirements of the main PE policies. They should be formed taking into account each specific technical service and ensure access to the minimum necessary information resources.

Methods

Methods on existing approaches, the article develops a model for providing access to information assets, which allows implementing access control processes in a distributed IT infrastructure. A special feature of the model is an algorithm for dynamically determining the necessary security policies, taking into account the access of users with different privileges.

Results

Figure 2 presents the model of the enclave gateway, on the basis of which the model of providing access to information assets in potentially unprotected networks will be organized.

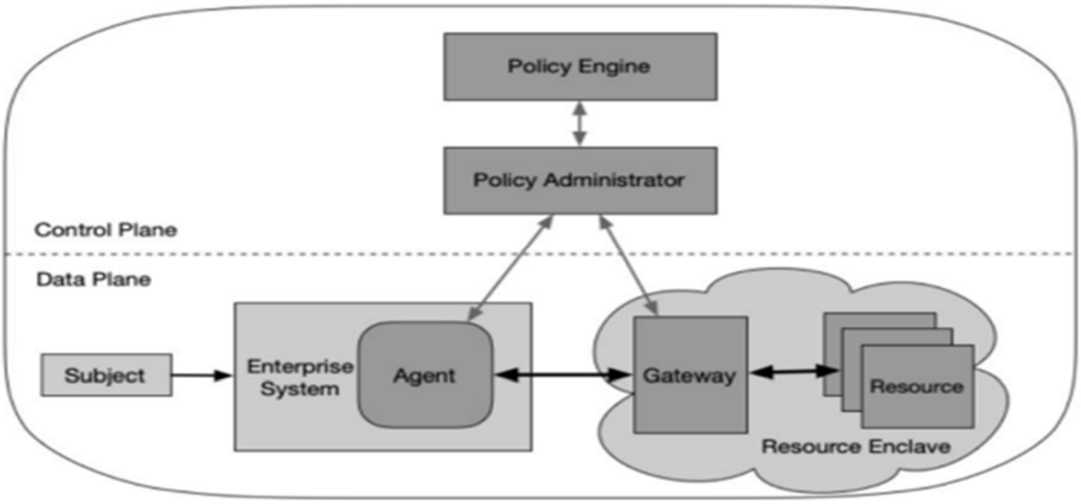

Fig. 2. Model of the enclave gateway

It involves the use of the following logical components:

- an agent located on a resource from which
- access request;
- gateway, which is the entry point of access to information resources.

Information resources located behind the gateway are not unified (like, for example, a web service), but represent an "enclave" – a set of information assets located on the same computing resources.

In this model, the access subject has an agent that is used to connect to the "enclave" gateway and can be an agent of a specific information protection system, which will allow, for example, to provide control of privileged access. With the help of an agent, you can ensure the implementation of targeted access policies to a specific resource, and with the help of a gateway, you can control access directly to a list of information resources, which makes it possible to implement policies for users with different privileges Wagenseil, 2010 (https://www.scmagazine.com/resource/identity-/andaccess/how-identity-and-access-management-fits-/into-zero-trust).

A disadvantage of this model is that the gateway secures the resources of the enclave as a whole and may fail to secure individual ones, thus giving access subjects the potential to discover resources within the enclave to which they do not have legitimate access. The model developed as part of the study (Fig. 3) is a complex version of the "enclave gateway model", which is characterized by more complex mechanisms for providing access through the gateway to all the above-mentioned groups of access subjects.

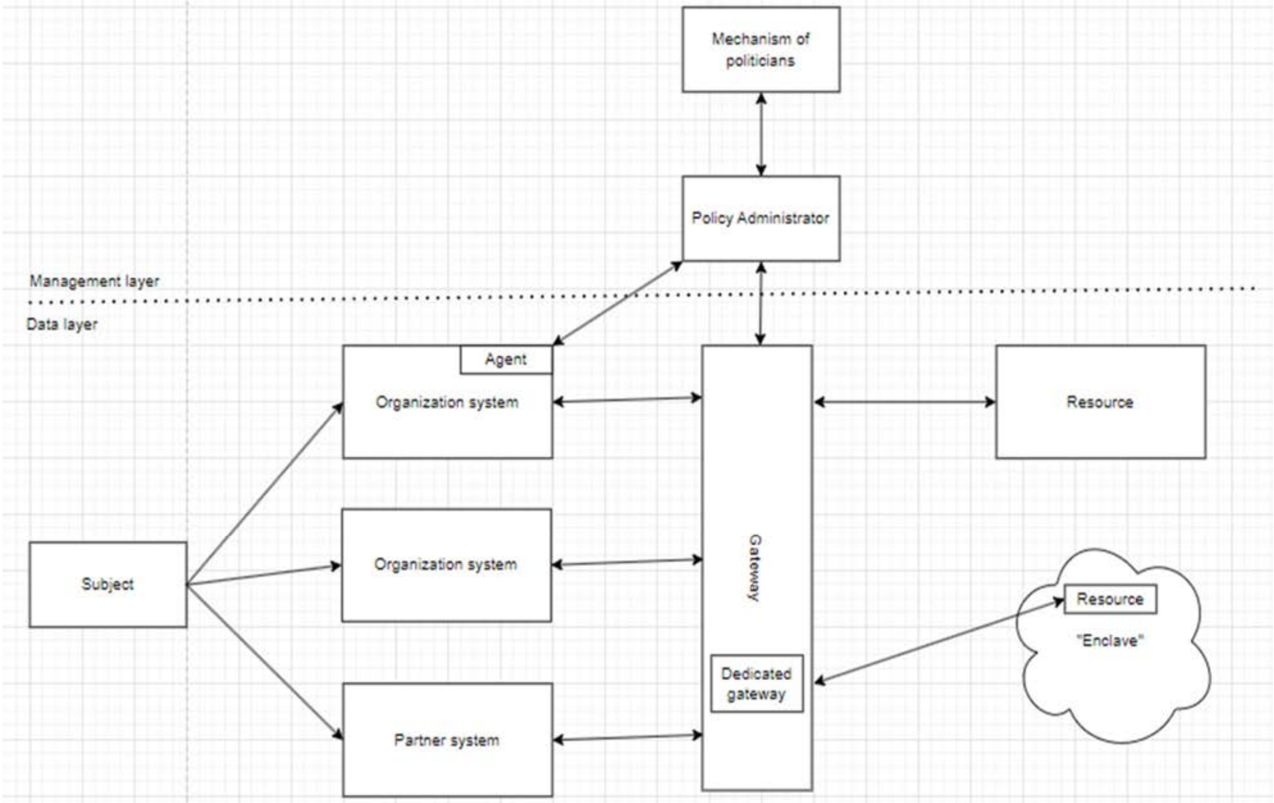

Fig. 3. The developed model of access control implementation

The access subject can make access requests from the corporate system with or without an installed agent, as well as from conditionally external partner systems. Each access request is processed at the gateway, which is the point of policy enforcement, while requests from partner systems are processed at a dedicated part of the gateway for which the policy engine applies different policies.

Figure 4 shows the access request routing scheme through the gateway. The access request comes through the load balancer because the gateway is a composite object in the model. For each request, based on the security status data coming from the PIP, the source of the request and the subsequent processing path are determined – which gateway component will receive it for processing. Next, based on the access policies, identification and authentication is performed, and if successful, an authorization request is generated.

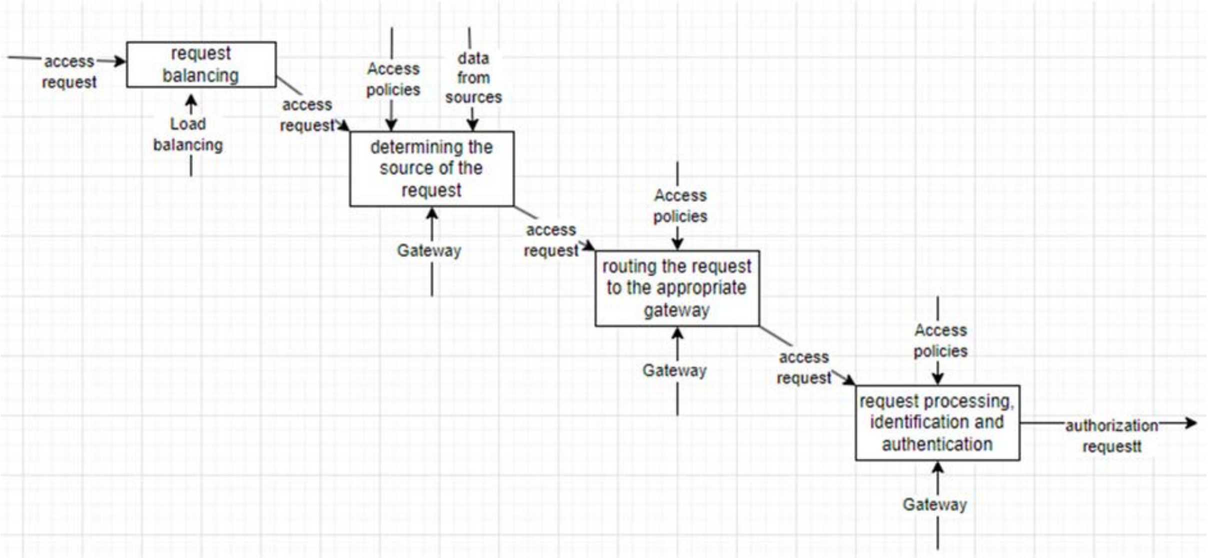

Fig. 4. PEP access request routing diagram

Identification is the first step in providing access and at the same time the basis of the concept of zero trust (Cai, & Zhang, 2019, pp. 46–49). Authentication can be implemented in various ways, and adding a second authentication factor can further reduce the risk of attacks on the access control system (Zeng, 2020, p. 48). After successful authentication, an authorization request is conditionally formed, which is subject to further processing, the scheme of which is presented in Fig. 5.

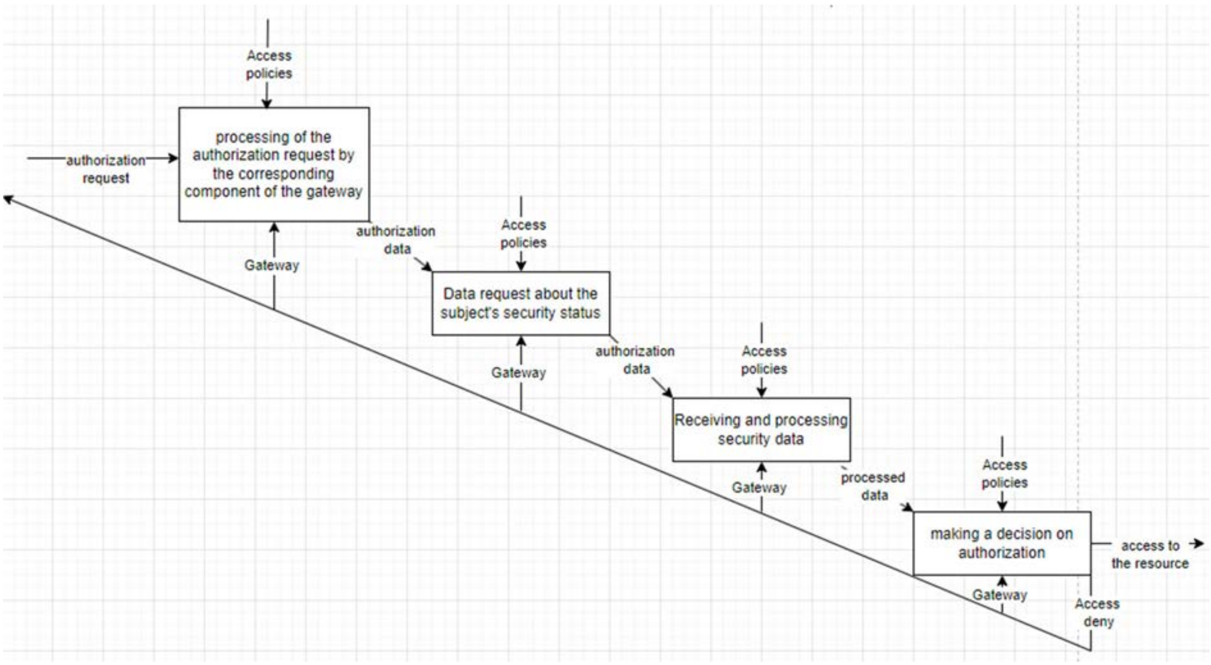
Access policies
authorization request
processing of the authorization request by the corresponding component of the gateway
Gateway
authorization data
Access policies
Data request about the subject's security status
Gateway
authorization data
Access policies
Receiving and processing security data
Gateway
processed data
Access policies
making a decision on authorization
access to the resource
Gateway
Access deny

Fig. 5. Processing of access request through PEP

A feature of the proposed processing scheme is repeated access to PIPs information streams, which provide available data on the current security status of the access subject at the time of authorization. Thus, it is implied that the decision to grant access is made with two stages of verification of the subject - during the processing of the request for identification and authentication, and also after successful authentication, which will increase the confidence that this access request is legitimate and will not create risks for information security.

Dual subject checking as part of access request processing provides flexibility in decision-making on the PEP side and allows for different policies that may be more or less strict depending on the type of access subject. Weak or insufficient control policies, according to a Verizon study (Zuo., 2018, pp. 50–51), lead to the majority of incidents involving compromised accounts, and according to a report by XMCyber (Liu, 2018, pp. 80–87), 73% of the most common attack methods involve poor access control mechanisms or compromised accounts. By using complex dynamic policies, access control can be implemented, minimizing the risk of security breaches.

Zero trust generally reduces the possible attack surface and reduces the level of damage and consequences of cyber attacks by reducing the time and cost of managing security threats. A high degree of transparency during the provision of access simplifies administration processes and reduces the risks of unauthorized access, since it can be obtained only by those subjects who, based on a series of checks, have confirmed their level of security (Columbus, 2022). In addition, the unification of access policies between applications and servers, which are critical parts of the IT infrastructure, is the key to unifying IAM into a single secure and manageable place for on-premises and cloud IT departments.

Discussion and conclusions

The proposed model of access provision has not lost the shortcomings of the prototype model, but on demand, it provides the possibility of access to individual information resources through the gateway, as well as to resources in the enclave, which ensures the implementation of more complex and universal policies on the PP, which will be built into the administrative policy. Thanks to this, it is possible to build secure real architectures that will create different access paths to target information resources. This creates difficulties for administration and policy development, but this fact cannot be considered an insufficient model, after the concept of zero trust, it implies constant revision of policies and changes in the information infrastructure. This is a complex process in itself that requires a zero-trust architecture and the ability to adapt to changes. As part of further research, a detailed study of the process of granting access and the development of an access policy based on dynamic data on the security status of access subjects is possible.

Authors' contribution: Volodymyr Khoroshko – conceptualization; methodology; analysis of sources; Mykola Brailovsky – preparation of the literature review; Ivan Parkhomenko – preparation of the theoretical foundations of the research; Taras Kyrychuk – collection of empirical data and their validation; empirical research.

REFERENCES

Cai, R., & Zhang, X. (2019). Zero Trust Based Identity Security Solution. *Information Technology & Standardization*, 9, 46–49.

Chapman, G., & Chapman, J. (2021). *Zero Trust Security: An Enterprise Guide*. Springer.

Columbus, L. (2022). *How zero trust can help battle identities under siege*. VentureBeat. https://venturebeat.com/security/how-zero-trust-can-help-battleidentities-under-siege/.

Lambert, M., Surhone, M., Tennoe, M., & Henssonow, S. (2023). *NIST Enterprise Architecture Model. What is a Zero Trust Architecture.* Palo Alto (2023). https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trustarchitecture.

Liu, Z. (2018). Discussion on the construction of network information security system for digital transformation enterprises under the new normal. *Cyberspace Security*, 9(11), 80–87.

NIST CSWP 20 (2022). *Planning for a Zero Trust Architecture. A Planning Guide for Federal Administrators.* p. 14.

Zeng, H. (2020). Discussion on Network Security Model and Zero-trust Practice. *Computer Products and Circulation*, 7, 48.

Zuo, Y. (2018). Zero-trust architecture: a new paradigm for network security. *Financial Computerizing*, 11, 50–51.

Отримано редакцією журналу / Received: 11.03.24
Прорецензовано / Revised: 15.03.24
Схвалено до друку / Accepted: 13.05.24

Володимир ХОРОШКО, д-р техн. наук, проф.
ORCID ID: 0000-0001-6213-7086
e-mail: professor_va@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

Микола БРАІЛОВСЬКИЙ, канд. техн. наук., доц.
ORCID ID: 0000-0002-3148-1148
e-mail: bk1972@ukr.net
Київський національний університет імені Тараса Шевченка, Київ, Україна

Іван ПАРХОМЕНКО, канд. техн. наук, доц.
ORCID ID: 0000-0001-6889-9284
Київський національний університет імені Тараса Шевченка, Київ, Україна

Тарас КИРИЧУК, студ.
ORCID ID: 0000-0003-0013-2989
e-mail: taraskiricuk@gmail.com
Київський національний університет імені Тараса Шевченка, Київ, Україна

МОДЕЛЬ РЕАЛІЗАЦІЇ УПРАВЛІННЯ ДОСТУПОМ ДО ІНФОРМАЦІЙНИХ АКТИВІВ У КОНЦЕПЦІЇ НУЛЬОВОЇ ДОВІРИ

Вступ. *Контроль доступу до інформаційних активів є однією з ключових функцій забезпечення інформаційної безпеки. Це завдання в тій чи іншій формі має розв'язуватися як загалом на рівні всієї інформаційно-технологічної інфраструктури компанії чи організації, так і в кожній локальній інформаційній системі.*

У статті на основі існуючих підходів розроблено модель забезпечення доступу до інформаційних активів, що дає змогу реалізувати процеси контролю доступу в розподіленій ІТ-інфраструктурі.

Методи. *На основі існуючих підходів у статті розроблено модель забезпечення доступу до інформаційних активів, яка дозволяє реалізувати процеси контролю доступу в розподіленій ІТ-інфраструктурі. Особливістю моделі є алгоритм динамічного визначення необхідних політик безпеки з урахуванням доступу користувачів із різними привілеями.*

Результати. *Результатом є алгоритм динамічного визначення необхідних політик безпеки, який враховує доступ користувачів із різними привілеями. Модель враховує віддалений доступ на кількох умовних "рівнях" – доступ клієнтів організації, співробітників організації, а також партнерів і підрядників. Оскільки сучасні інформаційні інфраструктури організацій стали складними й розподіленими, модель передбачає наявність значної кількості точок доступу, серед яких автоматизовані робочі станції в інфраструктурі, віддалені автоматизовані робочі станції, різноманітні користувацькі та мобільні пристрої доступу, а також специфічні пристрої на зразок торгових терміналів, ефективний контроль доступу має забезпечувати можливість централізованого доступу всіх користувачів до інформаційних активів.*

Висновки. *Модель передбачає реалізацію єдиної точки доступу, побудованої на основі моделей доступу з концепції нульової довіри, для користувачів і для "роботів" – технічних облікових записів, які використовують для міжсистемної взаємодії. Результати дослідження дадуть змогу розробити архітектуру віддаленого доступу користувачів до розподілених інформаційних активів та організувати процеси контролю й управління доступом, які базуються на динамічному визначенні рівня довіри до суб'єктів доступу, що загалом покращує безпеку організацій.*

Ключові слова: *нульова довіра, багатофакторна автентифікація, єдиний вхід, політики безпеки, Fast IDentity Online.*

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.