Платформа VIII

Диджиталізація фінансового сектору економіки

УДК 336.77:330.567.22(477)

Veremiiets M.D.,
Fifth-year student,
"Financial Management and Controlling" program
Academic Advisor:
Ph.D., Kovbasa V.A.,
Associate Professor of the Department of Corporate Finance and Controlling
Kyiv National Economic University named after Vadym Hetman

THE ROLE OF ZERO TRUST APPROACH IN ENTERPRISE MANAGEMENT AND INFORMATION SECURITY

The rapid digitalization of the financial sector has revolutionized enterprise operations and expanded service accessibility, yet it has also heightened the need for advanced security models to protect sensitive data and assets. With financial services increasingly reliant on interconnected systems and digital platforms, traditional perimeter-based security models are no longer sufficient to address complex cyber threats. As a result, the Zero Trust approach with its "never trust, always verify" philosophy has become essential, reshaping how financial institutions manage security in a digital environment where both internal and external threats are prevalent. The principles of Zero Trust represent a security concept emphasizing the need for stringent access control and continuous monitoring of all users – from employees to vendors and clients – regardless of their location or network [1].

The Zero Trust model significantly impacts enterprise management within the financial sector by emphasizing continuous verification of identity, strict access controls, and granular monitoring. As organizations move away from perimeter-based assumptions of trust, management must actively oversee and integrate Zero Trust principles into every layer of enterprise operations.

The need for a Zero Trust model is underscored by incidents such as the December 2023 cyberattack on Kyivstar JSC, which incurred significant financial and

reputational damage. This incident is recognized as the largest hacker attack, occurring amid the ongoing russian invasion of Ukraine. The parent company estimated the damages due to this cyberattack at 3.6 billion UAH [2].

Moreover, adopting a Zero Trust model allows management to enhance organizational oversight. By implementing granular access policies based on user identity, device health, and location, managers gain a higher level of control over network access and user behavior. By implementing Zero Trust principles, enterprises can better protect their sensitive data and critical assets from unauthorized access and lateral movement by cyber attackers [3, p. 9].

The model also enables enterprises to maintain consistent security controls across hybrid and multi-cloud environments, ensuring that security policies are enforced uniformly whether resources are accessed on-premises or in the cloud. Additionally, Zero Trust architecture helps organizations meet regulatory compliance requirements by providing detailed audit trails and granular access controls, while its advanced security measures prevent threats from spreading across the network [4, p. 38].

The implementation of a Zero Trust approach presents organizations with distinct challenges while emphasizing the critical role of management involvement (see Figure 1). The challenges can be categorized into three primary dimensions: cultural, requiring a shift from traditional perimeter-based security to a Zero Trust mindset; organizational, demanding cross-departmental coordination; and technical.

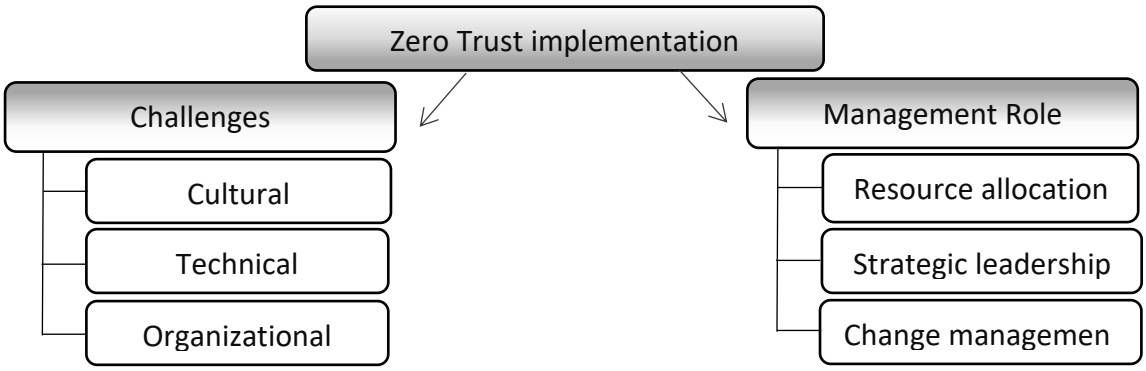

Figure 1 – Key Components of Zero trust implementation

Reference: developed by the author based on [4, p. 49]

Implementing Zero Trust is particularly critical in the financial sector for securing payment systems and protecting clients' personal data. Banks and financial institutions process millions of transactions daily, each of which must be safeguarded according to Zero Trust principles. A potential trend in the development of Zero Trust within the financial sector may integrate with artificial intelligence and machine learning technologies to detect anomalous behavior and potential threats in real-time, enabling financial institutions to respond to suspicious activities automatically.

In conclusion, the Zero Trust approach is indispensable in the digitalization of the financial sector, empowering institutions to achieve a higher level of security while supporting operational resilience. As management navigates this shift, embracing Zero Trust can lead to a more secure and compliant enterprise that is resilient in the face of evolving digital threats under the current conditions of uncertainty.

References:

1. Kiteworks. Zero Trust Architecture. URL: https://www.kiteworks.com/cybersecurity-risk-management/zero-trust-architecture-never-trust-always-verify/ (Date of access: 14.11.2024)
2. Forbes Ukraine magazine: Cyber attack on Kyivstar. January 20, 2024 URL: https://forbes.ua/innovations/finansoviy-stan-kyivstar-20012024-18652 (Date of access: 14.11.2024p)
3. Rose, S. (2022, May 6). Planning for a Zero Trust Architecture. URL: https://doi.org/10.6028/nist.cswp.20 (Date of access: 14.11.2024)
4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020, August 11). Zero Trust Architecture. URL: https://doi.org/10.6028/nist.sp.800-207 (Date of access: 14.11.2024).