E CONF SERIES

International Conference on Economics, Finance, Banking and Management
Hosted online from Paris, France
Website: econfseries.com 24th September, 2025

BUSINESS PLATFORM SECURITY ISSUES

Tadjiyeva Malika Murotovna

Annotation:

This thesis provides a scientific analysis of the issues of ensuring the security of business platforms in the process of digital transformation. The main focus is on such key threats as cyberattacks (DDoS, phishing, malware, ransomware), unauthorized data theft, insider threats and technical vulnerabilities. The article covers the main areas of ensuring security, including authentication and authorization (MFA, RBAC), cryptographic protection (AES, RSA, TLS), network security (IDS/IPS, firewall, VPN), monitoring and log analysis (SIEM), and employee training. Artificial intelligence and machine learning (AI/ML) algorithms, the Zero Trust model, and blockchain technologies are also considered as modern security trends. The article emphasizes the need to ensure the security of business platforms by combining technical means, management processes, and the human factor, offering practical recommendations and directions for future research.

Confidentiality, integrity and availability of data (the CIA triad) are among the key criteria for ensuring the secure operation of business platforms. Their violation leads not only to financial losses, but also to damage to the company's reputation. For example, unauthorized theft of data or its storage without encryption leads to a decrease in customer trust, and service interruptions can disrupt production processes.

This thesis is aimed at scientifically analyzing the issues of ensuring the security of business platforms, systematically considering existing threats and proposing effective solutions based on modern approaches.

The main risks encountered in business platforms are:

Cyberattacks. Nowadays, cyberattacks targeting business platforms take many forms. In particular, DDoS (Distributed Denial of Service) attacks disrupt the uninterrupted operation of services, which can disrupt the company's production and customer service processes. Phishing attacks fraudulently obtain confidential information (login, password, bank card details) from users. Also, malware (malicious programs) and ransomware (programs that encrypt a system or files and

demand a ransom in exchange for their decryption) attacks directly damage a company's information resources.

Data theft. One of the most vulnerable points of business platforms is unauthorized data theft. In such cases, there is an illegal distribution of customers' personal data, intellectual property or trade secrets. As a result, the company's competitiveness decreases, and its reputation and credibility in the market are seriously damaged. For example, in international practice, incidents where customers' payment card data was stolen have caused great difficulties for companies in restoring long-standing trust.

Insider threats. Negligence or intentional malicious actions of employees operating within a company can be more dangerous than external threats. This is because internal employees are familiar with the system's architecture, security policies, and vulnerabilities. This allows them to gain unauthorized access, steal, or falsify data. Therefore, "insider threat management" is considered a separate area in modern cybersecurity concepts.

Technical vulnerabilities. Weaknesses in the software or network configuration of business platforms are one of the main factors that hackers exploit. For example, outdated operating systems, poorly configured servers, or web applications that are not patched in a timely manner create favorable conditions for attackers. Therefore, penetration testing, vulnerability scanning, and regular technical audits are essential for protecting business platforms [1,5].

Key areas of security:

Authentication and authorization. Multi-factor authentication (MFA) requires the user to provide additional factors, such as a password, biometric data (fingerprint, facial recognition) or a temporary code, in addition to a password. In addition, role-based access control (RBAC) allows each user to be granted only the rights appropriate to their tasks. This approach significantly reduces the success of internal and external attacks.

Cryptographic protection. Business platforms require extensive use of encryption tools during data transmission and storage. For example, AES (Advanced Encryption Standard) is used for symmetric data encryption, and RSA is used in

public-key cryptography. At the transport layer, the confidentiality and integrity of the transmitted data is ensured through the TLS (Transport Layer Security) protocol. An electronic digital signature guarantees the authenticity of documents.

Network Security. Protecting the network infrastructure is the foundation of business platform security. Systems such as IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) allow you to detect and block unusual activity on the network. Firewalls control incoming and outgoing traffic, and VPN (Virtual Private Network) technologies provide secure remote connections.

Monitoring and log analysis. Modern business platforms use SIEM (Security Information and Event Management) systems to monitor events in real time and detect attacks early. SIEM systems collect log files, automatically analyze them, and send alerts when suspicious activity occurs. This helps the company make quick decisions and mitigate the consequences of an attack [6,8].

Artificial Intelligence-based Security. In recent years, artificial intelligence (AI) and machine learning (ML) algorithms have been playing an important role in ensuring the security of business platforms. AI tools analyze large volumes of network traffic in real time and allow you to detect anomalous activity faster than traditional methods. For example, anomaly detection can detect abnormal transactions, phishing emails, or botnet activity at an early stage. In addition, ML algorithms are effectively used to study the behavior of attacks and predict new types of threats. AI-based automated response mechanisms can quickly respond to security incidents, reducing the need for human intervention.

Table 1 Key risks encountered in business platforms

№	Type of risk	Description	Consequences
1	Cyber attacks (DDoS, phishing, malware, ransomware)	It disables services, steals or encrypts confidential data.	Financial losses, service disruptions.
2	Data theft	Illegal acquisition of customers, intellectual property, and trade secrets.	Loss of reputation and trust, decreased competitiveness.
3	Insider threats	Negligence or malicious conduct of employees.	Data theft, system damage.
4	Technical weaknesses	Software and network flaws (not updated system, incorrect configuration).	Hackers break into the system by exploiting vulnerabilities.

Cloud Security. As the use of cloud services such as SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service) expands, their security mechanisms are also becoming an urgent issue. Traditional perimeter-based security models are no longer sufficient in cloud infrastructure. Therefore, the "Zero Trust Security Model" is being widely implemented. In this model, no user or device is automatically considered trusted, but each access action undergoes strict authentication and authorization.

Blockchain technologies. The main advantage of blockchain is that transactions are stored in a decentralized manner and are virtually impossible to forge. Therefore, blockchain offers great opportunities for preventing data corruption and fraud, as well as for reliably recording electronic documents and financial transactions.

Table 2 Analysis of the main areas of security

№	Direction	Practical methods	Expected result
1	Authentication and Authorization	MFA (password + biometrics/code), RBAC.	Prevent unauthorized access.
2	Cryptographic protection	AES, RSA, TLS, electronic signature, key management.	Confidentiality and integrity of data are ensured.
3	Network security	IDS/IPS, firewall, VPN.	Network boundaries are strengthened, and unusual activity is stopped.
4	Monitoring and log analysis	SIEM systems.	Early detection of attacks in real time.
5	Employee training	Trainings, phishing simulations, internal politics.	Reduction of errors due to the human factor.

Analysis of current trends Table 3

№	Direction	Technologies used	Advantages
1	Security based on artificial intelligence	AI, ML, anomaly detection.	Rapid attack detection, prediction, automated response.
2	Cloud security	Zero Trust Security Model, SaaS/PaaS/IaaS protection mechanisms.	Each entry is strictly checked, ensuring data integrity.
3	Blockchain technologies	Decentralized transactions, cryptographic chain.	Prevention of data falsification, reliable transactions.

Conclusion

The security of business platforms is multifaceted and requires constant attention to cyberattacks, data theft, insider threats, and technical vulnerabilities. To ensure security, it is necessary to combine technical and organizational measures such as MFA and RBAC, cryptographic protection, network control, SIEM monitoring, and employee training. Modern trends — AI/ML, the Zero Trust model, and blockchain — take security to a new level, but it is important to consider privacy, transparency, and legal requirements when implementing them.

References

1. Smith, J., & Johnson, R. (2021). *Cybersecurity for Business Platforms*. New York: TechPress.
2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
3. Stallings, W. (2021). *Cryptography and Network Security: Principles and Practice*. Pearson.
4. NIST. (2020). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology.
5. Cisco Systems. (2021). *Network Security Best Practices for Enterprises*. Cisco Press.
6. Chapple, M., & Seidl, D. (2021). *Certified Information Systems Security Professional (CISSP) Study Guide*. Wiley.

7. Kshetri, N. (2021). *Blockchain and Business: Applications and Security Implications*. Springer.
8. Cybersecurity Ventures. (2022). *Global Cybercrime Report*. Cybersecurity Ventures Research.
9. Zero Trust Security Model Guidelines. (2021). *Forrester Research Reports on Enterprise Security*.