Фінанси, банківська справа, страхування та фондовий ринок

UDC 336.71:351.746.1:005.96

DOI **https://doi.org/10.5281/zenodo.16463619**

Approaches to Determining the Essence of Personnel Security in Banks

Zinaida Zhyvko

doctor of economic sciences, professor, professor of the department of aviation management, Ukrainian State Aviation Academy, Kropyvnytskyi, Ukraine,

zinaukraine@gmail.com,

https://orcid.org/0000-0002-4045-669X

Oleksandr Demchenko

doctor of economic sciences, of the department of aviation management, Ukrainian State Flight Academy, Kropyvnytskyi, Ukraine,

demchenkoaleksandr85@gmail.com,

https://orcid.org/0000-0002-0796-7164

Mykhailo Zhyvko

candidate of Law, Junior Researcher, Scientific Center of Innovative Research, Pussi, Estonia, zhivko_m@ukr.net,

https://orcid.org/0000-0002-0099-3562

Anastasiia Shehynska

Junior Researcher, Scientific Center of Innovative Research, Pussi, Estonia, astyvol@gmail.com,

https://orcid.org/0009-0007-5785-6730

Accepted: 06.07.2025| Published: 16.07.2025

Annotation. *Personnel security is a critical component of an enterprise's overall security system, ensuring its stability, competitiveness, and resilience against both internal and external threats. In the era of economic transformations, digitalization, and globalization, enterprises face increasing risks related to human capital, including fraud, corporate espionage, information leaks, conflicts of interest, and unethical behavior. As labor relations become more complex and the human factor plays a more significant role in organizational sustainability, the importance of personnel security continues to grow.*

The study underscores the necessity of developing and implementing effective personnel security strategies to mitigate risks associated with employee behavior, workplace loyalty, and insider threats. It highlights key elements such as recruitment and selection policies, ethical standards, employee monitoring systems, motivation and retention programs, as well as legal and regulatory compliance. Furthermore, the research emphasizes the integration of personnel security within the broader framework of an enterprise's economic security system, ensuring a proactive approach to risk management. In the context of digitalization, hybrid warfare, and intensified cyber and internal threats, ensuring personnel security in banks has become a strategic necessity. Human-related risks have multiplied due to remote work, higher staff turnover, socio-political pressure, and the psychological burden of operating under crisis conditions. Therefore, revisiting and clearly defining the essence of personnel security is essential for safeguarding the financial system’s integrity, trust, and resilience.

This article aims to explore and analyze various approaches to defining the essence of personnel security within an enterprise, emphasizing its interconnection with economic security and overall risk management. The study delves into both theoretical foundations and practical frameworks, identifying best practices for workforce protection and the creation of a secure corporate environment. A systematic approach to personnel security is advocated, combining preventive

measures, strategic HR management, and innovative security solutions to safeguard enterprises against human-related risks.

Keywords: *personnel security, enterprise security, risk management, human resource policies, economic stability, corporate governance, workforce protection.*

Підходи до визначення сутності кадрової безпеки в банках

Живко Зінаїда Богданівна
доктор економічних наук, професор, професор кафедри менеджменту авіаційної діяльності, Українська державна льотна академія, м. Кропивницький, Україна, zinaukraine@gmail.com ,
https://orcid.org/0000-0002-4045-669X

Демченко Олександр Вікторович
доктор економічних наук, кафедри менеджменту авіаційної діяльності, Українська державна льотна академія, м Кропивницький, 25006, Україна,
demchenkoaleksandr85@gmail.com ,
https://orcid.org/0000-0002-0796-7164

Живко Михайло Олександрович
кандидат юридичних наук, молодший дослідник,
Науковий центр інноваційних досліджень, Пюссі, Естонія,
zhivko_m@ukr.net, https://orcid.org/0000-0002-0099-3562

Шегинська Анастасія Іванівна
магістр комп'ютерних наук, магістр психології, молодший дослідник,
Науковий центр інноваційних досліджень, Пюссі, Естонія,
astyvol@gmail.com , https://orcid.org/0009-0007-5785-6730

Анотація. *Кадрова безпека є ключовим елементом загальної системи безпеки підприємства, що забезпечує його стабільність, розвиток, конкурентоспроможність і стійкість до внутрішніх та зовнішніх загроз. В умовах економічних трансформацій, цифровізації та глобалізації підприємства стикаються з дедалі більшими ризиками, пов'язаними з людським капіталом, зокрема шахрайством, корпоративним шпигунством, витоками інформації, конфліктом інтересів і неетичною поведінкою. Ускладнення трудових відносин і зростаюча роль людського фактора в забезпеченні стійкості організацій підвищують значення кадрової безпеки.*

У дослідженні наголошено на необхідності розробки та впровадження ефективних стратегій кадрової безпеки для мінімізації ризиків, пов'язаних з поведінкою працівників, рівнем лояльності та загрозами з боку інсайдерів. Виокремлено ключові елементи кадрової безпеки, такі як політика добору персоналу, етичні стандарти, системи моніторингу, програми мотивації та утримання кадрів, а також дотримання правових і регуляторних норм. Особлива увага приділяється інтеграції кадрової безпеки в ширшу систему економічної безпеки підприємства як складової проактивного управління ризиками. В умовах цифровізації, гібридної війни та посилення кіберзагроз і внутрішніх викликів, забезпечення кадрової безпеки в банках набуває стратегічного значення. Ризики, пов'язані з людським чинником, зростають через дистанційну роботу, високу плинність кадрів, соціально-політичний тиск і психологічне навантаження, пов'язане з роботою в умовах кризи. Тому переосмислення та чітке визначення сутності кадрової безпеки є необхідною умовою для збереження цілісності, довіри та стійкості фінансової системи.

Метою статті є дослідження та аналіз різних підходів до визначення сутності кадрової безпеки в межах підприємства, з акцентом на її зв'язок з економічною безпекою та загальним управлінням ризиками. Розглянуто як теоретичні засади, так і практичні моделі, спрямовані на захист персоналу та створення безпечного корпоративного середовища. Обґрунтовано

необхідність системного підходу до кадрової безпеки, що поєднує превентивні заходи, стратегічне управління персоналом і сучасні інноваційні рішення для протидії ризикам, пов'язаним із людським чинником.

Ключові слова: *кадрова безпека, безпека підприємства, управління ризиками, політика управління персоналом, економічна стабільність, корпоративне управління, захист працівників.*

Problem statement. Despite the critical role of personnel in ensuring the stable operation of banks, there is still no unified conceptual understanding of personnel security in the banking sector. Existing approaches often fragment the phenomenon into legal, psychological, or operational dimensions without integrating them into a coherent system. This creates difficulties in developing effective security policies, identifying threats, and implementing preventive strategies against internal risks, such as fraud, information leakage, or staff disloyalty.

Scientific Background and Literature Review. Numerous scholars have contributed to the conceptualization of personnel security, offering diverse perspectives on its role and components. O. V. Arefyeva and O. Yu. Lytovchenko (2008) analyze the human capital component in the economic security of machine-building enterprises, highlighting the link between personnel stability and business resilience [1]. The study by A. O. Bosak, V. P. Dalyk, Yu. I. Maznyk, S. K. Tulika, B. V. Matsevko, M. V. Prokopiv, and A. O. Staretskyi , titled «Personnel Security in the System of Economic Security of an Enterprise» (2023), examines the role of personnel security within the broader framework of an enterprise's economic security, the authors analyze various factors that influence personnel security, including recruitment processes, employee loyalty, and internal threat management. They propose strategies to enhance personnel security, emphasizing the importance of comprehensive personnel policies, regular risk assessments, and the implementation of effective internal controls.he study concludes that strengthening

 ISSN: 2786-9431

personnel security is crucial for maintaining the overall economic stability and competitiveness of an enterprise [2]. I.Ya. Burda discusses the role of personnel security in the broader framework of enterprise economic security, stressing the need for continuous monitoring and risk assessment [3]. E. N. Grechko (2013) explores the essence of enterprise security, identifying personnel-related risks as key determinants of corporate stability [4]. The studies conducted by Z. B. Zhyvko, O. Z. Slipa, and Kh. Z. Bosak focus on the formation of an optimal personnel security system in enterprises, particularly within the framework of Ukraine's sustainable economic development. Their research provides a comprehensive analysis of personnel security, its structure, and the mechanisms required for its effective implementation in modern business environments. In their work «Formation of an Optimal Personnel Security System in the Conditions of Sustainable Economic Development of Ukraine», included in the collective monograph edited by R. I. Trynko and Ya. S. Pitsur (2014), the authors explore the key challenges and strategies for ensuring personnel security at enterprises. They emphasize that effective personnel security is crucial for business resilience and long-term success, particularly in an unstable economic environment [5]. Their main findings include: the importance of integrating personnel security into the broader economic security framework of enterprises; the need to develop mechanisms that prevent insider threats, workforce instability, and unethical behavior; a focus on human capital management as a key determinant of business security, linking employee loyalty and motivation with overall organizational stability; the development of preventive security measures, such as improved recruitment policies, background checks, and ethical corporate culture formation. The study underscores that an optimal personnel security system should balance risk management, workforce development, and corporate governance, ensuring that enterprises remain competitive and resilient against potential threats.

In the article «Personnel Security of an Enterprise: Concept, Structure, and Basic Mechanisms of Its Ensuring», published in the International Scientific Journal

«Scientific Review» (2014), Slipa O. Z. provides an in-depth examination of the conceptual foundations of personnel security. The research presents: a structured definition of personnel security, highlighting its role in protecting an enterprise from both internal and external threats; a breakdown of the main components of personnel security, including recruitment integrity, corporate culture, employee monitoring, and legal compliance; key mechanisms for ensuring personnel security. Key mechanisms for ensuring personnel safety are: the use of psychological assessments to identify potential risks; the implementation of loyalty-building strategies to reduce turnover and prevent security breaches; the legal regulation of employee conduct, including non-disclosure agreements (NDAs) and compliance with labor laws; the role of HR policies in preventing security risks related to information leaks, fraud, and unethical practices. This research highlights that personnel security should not be viewed solely as a set of protective measures but rather as a strategic function within an enterprise's risk management system. It reinforces the idea that companies should proactively cultivate a secure working environment by investing in employee engagement, ethical leadership, and regulatory compliance.

S. V. Kondratieva (2015) traces the evolution of the «personnel security» concept, offering insights into its theoretical development [6]. O. Yu. Lytovchenko (2010) studies personnel security formation in the agricultural sector, identifying industry-specific risks [7]. N. H. Mekheda and A. I. Marenych (2012) explore the social and motivational components of personnel security in enterprises. The study highlights the role of employee motivation, workplace culture, and social factors in ensuring personnel security. The authors emphasize that a well-developed motivation system, employee engagement, and a positive organizational environment contribute to reducing internal threats and strengthening workforce stability. The research also suggests strategies for improving personnel security through HR policies, incentive programs, and ethical corporate practices [8]. I. P. Moiseienko & O. M. Marchenko (2011) explore strategies for managing financial and economic security within enterprises, emphasizing risk assessment and

 ISSN: 2786-9431

protective measures [9]. M. I. Petrov (2002) analyzes the essence of economic security, presenting different interpretations and perspectives [10]. N. O. Podluzhna (2003) examines organizational approaches to managing economic security, discussing key management principles [11]. O. Z. Slipa (2014) defines personnel security, its structure, and mechanisms for ensuring it within enterprises [12]. N. I. Reverchuk (2004) focuses on economic security management in business structures, highlighting financial stability and resilience [13]. O. F. Yaremenko (2016) provides conceptual foundations for ensuring personnel security, emphasizing HR policies and risk management [14].

The study concludes that personnel security should be viewed as a multidimensional concept that integrates HR management, risk assessment, and corporate governance. An effective personnel security strategy enhances business sustainability, protects intellectual property, and fosters employee loyalty. The findings provide valuable insights for business leaders, HR professionals, and policymakers aiming to develop robust personnel security frameworks.

Presentation of the main material. To facilitate a more precise understanding of the research area, this study introduces original interpretations of essential concepts

Personnel security in banks is a system of preventive, regulatory, and organizational measures aimed at minimizing internal threats posed by employees, ensuring their reliability, loyalty, and integrity in order to protect financial, informational, and reputational assets of the institution.

Personal security of bank employees refers to the protection of individuals working in banking institutions from physical, psychological, legal, digital, and professional threats that may arise in the course of their duties or as a result of external or internal risks.

Personal security of bank clients encompasses a set of guarantees and safeguards provided by a bank to ensure the confidentiality, integrity, and protection

 ISSN: 2786-9431

of clients' personal data, financial assets, and trust-based interactions from fraud, identity theft, unauthorized access, or abuse.

Main Approaches to Defining Personnel Security (fig. 1):

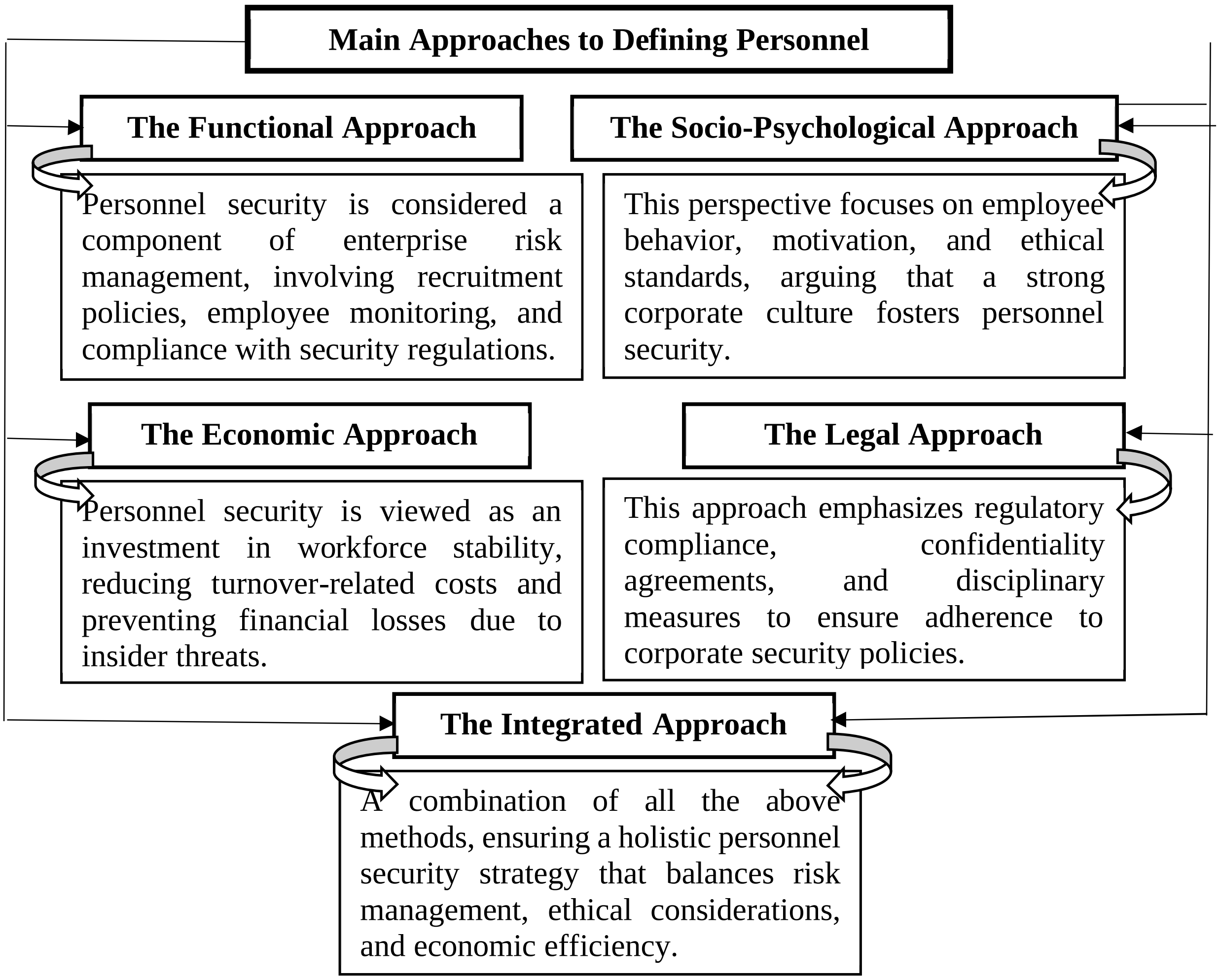

Fig. 1. Main Approaches to Defining Personnel Security*

* Developed by the authors

Personnel security is a fundamental component of an enterprise's overall economic security system. It ensures that human resources do not become a source of internal threats while also contributing to the organization's stability, competitiveness, and long-term development. Various theoretical and practical approaches have been developed to define the essence of personnel security, each emphasizing different aspects, including risk management, organizational resilience, ethical behavior, and strategic human resource management.

Risk-Oriented Approach (fig.2).

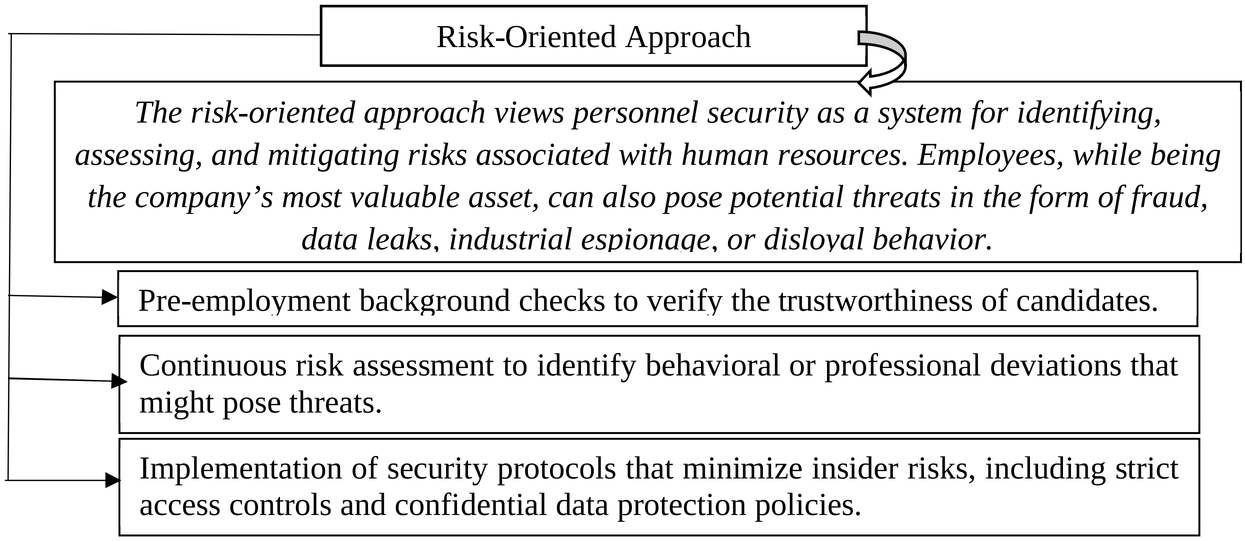

Fig. 2. Risk-Oriented Approach *

* Developed by the authors

Ensuring personnel security begins long before an individual becomes an official employee. It requires a structured approach to vetting candidates, continuously assessing risks, and implementing robust security measures that minimize insider threats. The following key strategies contribute to strengthening personnel security and safeguarding an organization from internal risks (fig. 3).

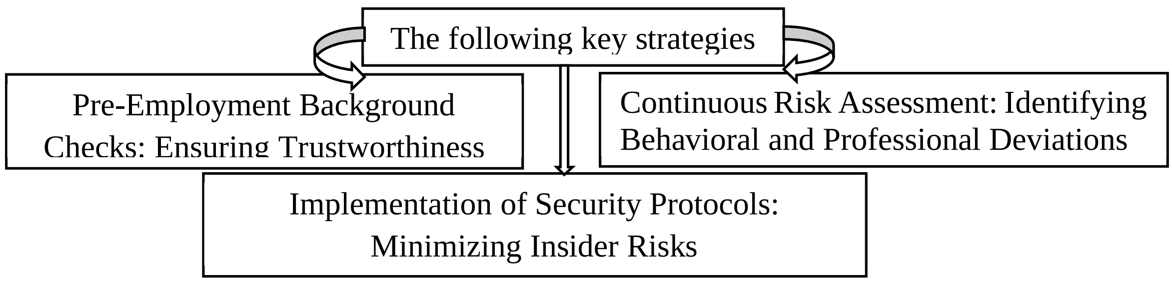

Fig. 3. The following key strategies*

* Developed by the authors

Hiring the right people is the first and most crucial step in building a secure workforce. Pre-employment background checks help verify a candidate's integrity, reliability, and suitability for the role. These checks may include: 1) Criminal Background Checks – Identifying any past legal violations that might indicate a risk

ISSN: 2786-9431

to the company. For roles involving financial transactions, cybersecurity, or sensitive information, these checks are essential. 2) Employment History Verification – Confirming a candidate's previous work experience, roles, and responsibilities to ensure that their claims align with reality. This process helps detect falsified credentials or unexplained gaps in employment. 3) Educational Verification – Ensuring that the candidate possesses the necessary qualifications and certifications for the role. Fake degrees and exaggerated academic achievements can pose risks, especially in highly specialized fields. 4) Credit and Financial Background Checks – Evaluating financial stability, particularly for positions handling corporate finances. Employees facing financial distress are more susceptible to fraud, bribery, or insider threats. 5) Reference Checks – Speaking with former employers and colleagues to assess a candidate's reliability, professionalism, and ethical conduct. 6) Social Media and Online Footprint Review – Analyzing publicly available online behavior to detect potential red flags, such as extremist ideologies, unethical views, or negative comments about former employers.

By implementing thorough pre-employment background checks, organizations can significantly reduce the risk of hiring individuals who may pose security threats, engage in unethical behavior, or compromise sensitive company data.

Personnel security does not end once an employee is hired. Employees' behaviors, attitudes, and job performance should be continuously monitored to detect any potential risks. Continuous risk assessment helps identify deviations that might indicate security threats, such as insider fraud, information leaks, or unethical conduct.

Key methods of continuous risk assessment include: 1) Behavioral Monitoring – Supervisors and HR professionals observe changes in employee behavior, such as increased secrecy, unexplained financial gains, or sudden hostility toward colleagues. These changes could indicate potential security risks. 2) Psychological Assessments – Periodic assessments to evaluate stress levels, job

 ISSN: 2786-9431

satisfaction, and emotional stability. Employees experiencing high stress or dissatisfaction are more prone to misconduct or breaches of security protocols. 3) Performance Evaluations – Regular performance reviews help identify employees who may be struggling with their tasks, potentially leading to unintentional errors or security lapses. 4) Access and Activity Monitoring – Tracking employees' access to sensitive information, systems, or facilities. Any unusual or unauthorized access patterns could signal insider threats. 5) Anonymous Reporting Mechanisms – Establishing a confidential system where employees can report suspicious activities without fear of retaliation. This helps identify risks early and prevents security breaches before they occur.

Continuous risk assessment allows organizations to proactively detect and address potential security threats, rather than merely reacting after a security breach has occurred.

To maintain a high level of personnel security, companies must implement strong security protocols that regulate employee access, ensure confidentiality, and prevent unauthorized activities. These security measures include: 1) Strict Access Controls – Limiting access to sensitive information and facilities based on job roles. Employees should only have access to the data necessary for their tasks. Multi-level authentication and biometric security can further enhance access control. 2) Confidentiality Agreements and NDAs – Requiring employees to sign non-disclosure agreements (NDAs) to legally bind them to protect sensitive company information. Violations should result in legal consequences. 3) Cybersecurity Measures – Enforcing strict cybersecurity policies, including secure password management, encryption of sensitive files, and restrictions on external device usage (e.g., USB drives) to prevent data theft. 4) Regular Security Training – Conducting ongoing training sessions to educate employees on security policies, cybersecurity threats, and best practices for protecting confidential data. 5) Incident Response Protocols – Establishing clear procedures for handling security breaches, including investigation processes, response teams, and immediate action plans to mitigate

 ISSN: 2786-9431

damage. 6) Exit Strategies for Departing Employees – Ensuring that employees who leave the company no longer have access to company systems, facilities, or confidential data. This includes deactivating login credentials, retrieving company-owned devices, and conducting exit interviews to assess potential security concerns.

A comprehensive approach to personnel security involves multiple layers of protection, starting with thorough pre-employment background checks, followed by continuous risk assessment, and reinforced through strict security protocols. Organizations that implement these measures create a secure work environment where employees are trusted and safeguarded against potential security threats. By proactively managing personnel security, companies can significantly reduce the risk of insider threats, protect sensitive information, and ensure long-term organizational stability. By focusing on potential vulnerabilities, this approach allows companies to develop preventive measures that reduce personnel-related threats before they materialize.

This approach integrates personnel security into the broader framework of human resource management (HRM). It views personnel security not as an isolated function but as an integral part of HR policies that ensure workforce stability, loyalty, and efficiency. Key components include:

1) Talent acquisition strategies that attract individuals who align with the company’s values and ethical standards.

2) Employee retention programs that enhance job satisfaction and reduce turnover, minimizing security risks related to staff exits.

3) Career development and training initiatives that strengthen employees' commitment to the organization and enhance their ability to respond to security challenges.

A company’s ability to maintain a secure and stable workforce depends on its ability to attract, retain, and develop employees who align with its values, ethical standards, and long-term goals. Effective personnel security strategies go beyond

 ISSN: 2786-9431

hiring procedures and must incorporate proactive measures that ensure employees remain engaged, committed, and prepared to handle security-related challenges.

The foundation of personnel security starts with hiring individuals who not only possess the necessary skills and expertise but also share the company's ethical standards and cultural values. A well-designed talent acquisition strategy ensures that new employees integrate smoothly into the organization, reducing the likelihood of security risks related to misalignment or disengagement.

The following key approaches help build a resilient workforce while mitigating risks associated with turnover, disengagement, and unethical behavior (fig. 4).

Fig. 4. Key approaches to help create a resilient workforce*

* Developed by the authors

 ISSN: 2786-9431

Key strategies for talent acquisition include: 1) Value-Based Hiring – Organizations should assess candidates not only based on their professional qualifications but also on their ethical integrity, reliability, and cultural fit. This can be achieved through behavioral interview techniques, scenario-based assessments, and personality evaluations. 2) Comprehensive Vetting and Screening – In addition to traditional background checks, companies should use tools such as psychological assessments and integrity tests to identify candidates who align with the organization's security expectations. 3) Employer Branding – Companies that promote a strong ethical culture and commitment to employee security attract like-minded candidates. A clear emphasis on corporate values, employee well-being, and career growth opportunities enhances the company's reputation among potential hires. 4) Internship and Apprenticeship Programs – Partnering with universities and training institutions to create internship programs allows companies to cultivate talent that is already aligned with their ethical and security standards before full-time employment. 5) Structured Onboarding and Orientation – A strong onboarding process ensures that new employees understand the organization's security policies, ethical guidelines, and confidentiality expectations from the beginning of their employment.

By prioritizing the alignment of new hires with the company's ethical and security culture, organizations can reduce the risk of future security breaches, misconduct, or internal threats.

High employee turnover can pose serious security risks, including the potential leakage of sensitive information, loss of institutional knowledge, and vulnerabilities created by disgruntled former employees. To mitigate these risks, companies must focus on employee retention strategies that foster job satisfaction, loyalty, and long-term commitment. Effective employee retention programs include: 1) Competitive Compensation and Benefits – Fair and competitive salary packages, performance-based incentives, and comprehensive benefits (e.g., health insurance, retirement plans, and wellness programs) contribute to job satisfaction and reduce

ISSN: 2786-9431

the likelihood of employees seeking opportunities elsewhere. 2) Work-Life Balance Initiatives – Providing flexible work arrangements, remote work options, and mental health support helps employees feel valued, reducing stress and enhancing overall commitment. 3) Employee Recognition and Engagement – Acknowledging employees' contributions through awards, public recognition, and promotions fosters a sense of belonging and appreciation, which strengthens their commitment to the organization. 4) Open Communication and Feedback Mechanisms – Establishing transparent communication channels where employees can voice concerns, share feedback, and feel heard prevents frustration and disengagement, which could lead to security threats.

5) Strong Workplace Relationships and Team Building – Encouraging collaboration and positive workplace relationships through team-building activities, mentorship programs, and leadership development enhances trust and reduces the likelihood of internal conflicts. 6) Confidential Exit Interviews and Risk Assessments – When employees leave, organizations should conduct exit interviews to assess potential risks. This helps identify any security concerns, such as possible intellectual property leaks or unresolved grievances that could lead to future security threats.

By investing in employee retention, organizations create a stable and secure workforce that is less likely to engage in unethical behavior, corporate espionage, or data leaks.

Providing employees with growth opportunities enhances their commitment to the organization and ensures they are well-equipped to handle security challenges. Employees who feel that their career development is supported are more likely to remain loyal and actively contribute to the company's security and success.

Key career development initiatives include: 1) Security Awareness Training – Regular training sessions on cybersecurity, data protection, and ethical decision-making help employees understand their role in maintaining organizational security.

ISSN: 2786-9431

2)Leadership Development Programs – Encouraging employees to take on leadership roles within the company fosters a sense of responsibility and accountability, reducing the likelihood of unethical behavior. 3) Cross-Training and Role Diversification – Allowing employees to gain experience in multiple roles within the organization enhances their understanding of security protocols and reduces knowledge gaps that could be exploited by malicious actors. 4) Certification and Skills Enhancement Opportunities – Providing employees with access to industry-recognized certifications and specialized training programs not only enhances their skills but also increases their engagement and motivation to contribute positively to the organization. 5) Mentorship and Career Planning – Establishing mentorship programs where experienced employees guide junior staff strengthens company culture and ensures knowledge transfer while reinforcing ethical and security values. 6) Simulated Security Drills and Crisis Management Exercises – Training employees to respond to security threats, such as cyberattacks, insider breaches, or data leaks, ensures they are prepared to protect the organization in real-world scenarios. By fostering a culture of continuous learning and professional development, organizations empower employees to become active participants in maintaining security and ethical standards. This, in turn, reduces the likelihood of internal threats and enhances the company’s overall resilience.

Personnel security is a critical component of organizational stability, and it begins with effective talent acquisition, employee retention, and career development strategies. By hiring individuals who align with company values, fostering a secure and engaging work environment, and providing opportunities for growth, organizations can build a workforce that is committed to ethical behavior and security-conscious decision-making.

A proactive approach to personnel security ensures that employees not only contribute positively to the organization but also serve as its first line of defense against internal threats. In an era where corporate security risks are constantly evolving, investing in people remains one of the most effective ways to protect a

 ISSN: 2786-9431

business from potential vulnerabilities. By embedding personnel security into HRM, organizations create a workforce that is both productive and aligned with security objectives.

The behavioral approach emphasizes the role of corporate culture, ethical values, and trust in ensuring personnel security. It assumes that security threats often arise due to unethical behavior, lack of engagement, or dissatisfaction among employees. To mitigate such risks, organizations: foster a culture of integrity where employees are encouraged to act ethically and report suspicious activities; implement psychological assessments to detect potential threats such as high stress levels or unethical tendencies; promote employee well-being to ensure job satisfaction, as dissatisfied employees are more likely to become security risks.

Let's conduct a SWOT analysis of six Ukrainian banks: Taskombank, Bank Lviv, PrivatBank, Raiffeisen Bank, Oschadbank, and Monobank, and consider the interdependence of bank security with employee activities. Let's conduct a SWOT analysis of six Ukrainian banks: Taskombank, Bank Lviv, PrivatBank, Raiffeisen Bank, Oschadbank, and Monobank, and consider the interdependence of bank security with employee activities. Here is the SWOT analysis of six Ukrainian banks: Tascombank, Bank Lviv, PrivatBank, Raiffeisen Bank, Oschadbank, and Monobank (fig. 5 - 10).

Tascombank	
Strengths:	**Weaknesses:**
Clear hierarchical structure ensures control and consistency in decision-making.	Complexity and length of decision-making processes due to a multi-level hierarchy.
Strong risk control and financial management.	Lack of flexibility in adapting to rapid market changes.
Commitment to innovation, particularly in digital solutions.	Possible lack of close coordination between different departments due to weak horizontal communication.

ISSN: 2786-9431

Opportunities:	**Threats:**
Implementation of more flexible management decisions and reduction of hierarchy levels to increase efficiency.	Competition from banks that have already completed digital transformation and have more flexible structures.
Further digital transformation to improve customer interaction and internal efficiency.	Regulatory changes that may complicate management processes and affect efficiency.
Development of new products based on big data analysis.	Risks associated with slowing innovation in the banking sector due to external or internal constraints.

Fig. 5. SWOT analysis of Tascombank

* Developed by the authors

Bank Lviv	
Strengths:	**Weaknesses:**
Focus on small and medium-sized businesses, allowing it to occupy a niche market.	Small asset size limits opportunities for large-scale investments and development.
Flexibility in decision-making due to a smaller organizational structure.	Limited geographical presence reduces potential for attracting new clients.
Close relationships with local clients and a deep understanding of their needs.	Fewer resources for investing in modern technologies and innovation.
Opportunities:	**Threats:**
Expansion into other regions to attract new clients.	Competition from larger banks that can offer better conditions.
Partnerships with other financial institutions to broaden the range of services.	Economic instability, which may negatively impact small and medium-sized businesses.
Introduction of specialized products for small and medium-sized businesses.	Regulatory changes that may require additional resources to comply with new standards.

Fig. 6. SWOT analysis of Bank Lviv*

* Developed by the authors

PrivatBank	
Strengths:	**Weaknesses:**
The largest bank in Ukraine by assets, ensuring economies of scale.	Large scale may lead to bureaucracy and slower processes.
High level of digitalization and innovative solutions.	State ownership may limit flexibility in business decisions.
Extensive network of branches and ATMs across the country.	Potential reputational risks due to past financial issues.
Opportunities:	**Threats:**
Further development of digital services and mobile banking.	Competition from private banks and fintech companies.
Expansion of services for corporate clients.	Changes in state policy regarding state-owned banks.
Entry into international markets or partnerships with foreign financial institutions	Cyber threats due to a high level of digitalization.

Fig. 7. SWOT analysis of PrivatBank*

* Developed by the authors

Raiffeisen Bank	
Strengths:	**Weaknesses:**
Support from the international financial group Raiffeisen Bank International	Moderate flexibility in decision-making due to adherence to global banking standards.
High standards of corporate governance and risk management	The need to comply with both Ukrainian and EU banking regulations.
A wide range of banking products for corporate and individual clients.	Limited focus on small businesses compared to competitors.
Opportunities:	**Threats:**

Strengthening positions in Ukraine through new financial products.	Macroeconomic risks in Ukraine affecting financial stability.
Expanding cooperation with international companies.	Competition with global and local banks.
Investments in digital banking and innovative solutions.	Regulatory changes that may impose additional financial obligations.

Fig. 8. SWOT analysis of Raiffeisen Bank*

* Developed by the authors

Oschadbank	
Strengths:	**Weaknesses:**
One of the most stable banks in Ukraine, fully backed by the government.	Slower adaptation to new market trends due to bureaucratic processes.
Large branch network covering all regions of Ukraine.	Limited flexibility compared to private banks.
Active participation in government programs for financial support.	The need for significant modernization of banking services.
Opportunities:	**Threats:**
Expansion of digital banking to increase competitiveness.	Competition from private banks and fintech companies.
Strengthening cooperation with businesses and SMEs.	Possible reduction of state funding for development programs.
Developing new investment and savings programs for the population.	Economic instability affecting depositors' confidence.

Fig. 9. SWOT analysis of Oschadbank*

* Developed by the authors

ISSN: 2786-9431

Monobank	
Strengths:	**Weaknesses:**
Fully digital bank with a modern technological platform.	Lack of physical branches, which may limit customer access in some regions.
High level of customer service and loyalty.	Dependence on partner banks for some operations.
Fast innovation and introduction of new financial products.	Increased vulnerability to cyber risks.
Opportunities:	**Threats:**
Expanding the range of financial products, including insurance and investment tools.	Competition from traditional banks that are improving their digital services.
Entering international markets or expanding partnerships with foreign fintech companies.	Regulatory risks related to digital-only banking.
Further development of AI-based services for personalized banking.	Potential cybersecurity threats.

Fig. 10. SWOT analysis of Monobank

* Developed by the authors

PrivatBank and Oschadbank are the largest and most financially stable banks but face challenges due to government ownership and bureaucratic processes. Monobank leads in digital banking but lacks physical infrastructure, which could be a disadvantage in certain customer segments. Raiffeisen Bank benefits from international backing and high corporate standards but faces constraints due to strict regulations. Tascombank and Bank Lviv are more niche-oriented, with strengths in specific market segments but with limitations in scale and resources. Each bank has its own strengths and challenges, making their competitive advantages highly dependent on the specific needs of customers and businesses.

The Impact of Personnel on Bank Security: Potential Issues and Solutions. Bank employees play a crucial role in ensuring financial and operational security. Their actions directly affect risk management, fraud prevention, customer trust, and compliance with regulatory requirements. A well-trained and motivated workforce enhances a bank’s stability, while weaknesses in personnel management can lead to severe security risks.

Potential Issues Related to Bank Personnel: internal Fraud and Financial Misconduct; Lack of Competence and Training Gaps; Employee Dissatisfaction and High Turnover; Cybersecurity Risks; Regulatory Non-Compliance.

Internal Fraud and Financial Misconduct - employees may engage in fraud, embezzlement, or unauthorized access to customer data; Insider threats, where employees collaborate with external fraudsters, pose a major risk; lack of Competence and Training Gaps; insufficient knowledge of banking regulations and security protocols can lead to errors and vulnerabilities; poorly trained employees may mishandle customer data, leading to breaches.

Employee Dissatisfaction and High Turnover - low morale or dissatisfaction with working conditions can lead to disengagement and increased risk-taking behavior; frequent turnover disrupts operations and increases the likelihood of data leaks.

Cybersecurity Risks **- e**mployees may fall victim to phishing, ransomware, or social engineering attacks; weak password management and improper handling of sensitive information can lead to data breaches.

Regulatory Non-Compliance **-** lack of awareness or negligence regarding banking laws can result in legal and financial penalties; non-compliance with anti-money laundering (AML) and Know Your Customer (KYC) requirements can expose banks to criminal activity.

 ISSN: 2786-9431

Solutions to Mitigate Risks and Ensure Personnel Reliability (fig. 11):

Solutions to Mitigate Risks and Ensure Personnel

- **Strengthening Employee Background Checks and Security**
- **Regular Training and Development Programs**
- **Implementing Strong Internal Controls**
- **Enhancing Workplace Culture and Employee Engagement**
- **Monitoring and Early Detection Systems**
- **Cybersecurity Measures**
- **Strengthening Legal and Ethical Compliance**

Fig. 11. Solutions to Mitigate Risks and Ensure Personnel Reliability*

* Developed by the authors

Strengthening Employee Background Checks and Security Policies - **i**mplement rigorous screening procedures before hiring to verify qualifications and detect any history of misconduct; establish clear policies regarding ethical behavior, data security, and fraud prevention. Regular Training and Development Programs - **c**onduct mandatory cybersecurity awareness and fraud prevention training. Provide continuous professional development to enhance employees' financial and regulatory knowledge. Implementing Strong Internal Controls - use multi-level authentication and restricted access to sensitive data; implement a dual-control system for high-risk transactions. Enhancing Workplace Culture and Employee Engagement - foster a transparent, ethical, and inclusive work environment to increase job satisfaction; recognize and reward employees for compliance and integrity.

Monitoring and Early Detection Systems - use AI-driven monitoring tools to detect suspicious behavior in transactions and employee activities; encourage anonymous reporting of unethical behavior through whistleblower programs. Cybersecurity Measures - require strong password policies and multi-factor

 ISSN: 2786-9431

authentication; regularly test employees with simulated phishing attacks to improve cyber awareness. Strengthening Legal and Ethical Compliance - regularly update policies to comply with national and international regulations; assign compliance officers to ensure adherence to AML and KYC regulations.

Ensuring Employee Loyalty and Reliability in Banks: 1) Competitive Compensation and Benefits - offer fair salaries, bonuses, and benefits to enhance job satisfaction and reduce turnover; provide financial incentives for high performance and compliance with security protocols. 2) Career Growth and Professional Development - create clear career progression paths to retain talented employees; offer training programs, mentorship, and leadership development initiatives. 3) Work-Life Balance and Employee Well-being - implement policies that promote work-life balance to reduce stress and burnout; provide mental health support and wellness programs. 4) Ethical Leadership and Open Communication - maintain a transparent and open-door policy for addressing employee concerns; encourage ethical leadership that fosters trust and accountability. 5) employee Recognition and Reward Systems - recognize employees for their contributions to security and compliance; establish performance-based rewards to motivate employees.

Conclusion. A bank’s security is highly dependent on its personnel. By investing in recruitment, training, cybersecurity, and workplace culture, banks can reduce risks and ensure that employees contribute to financial stability and customer trust. Strengthening employee loyalty and engagement will not only enhance security but also improve overall bank performance and reputation.

Ensuring personnel security within an organization requires a comprehensive approach that not only focuses on preventing external threats but also mitigates risks from within. A proactive security strategy includes fostering a strong ethical culture, conducting psychological assessments to identify potential threats, and prioritizing employee well-being to prevent dissatisfaction-related security risks. By integrating these elements, organizations can enhance workplace trust, minimize insider threats,

 ISSN: 2786-9431

and create a resilient workforce committed to safeguarding company assets and information.

Referances

1. Arefieva O.V., Lytovchenko O.Iu. (2008). Kadrova skladova v systemi ekonomichnoi mashynobudivnykh pidpryiemstv. [The human resource component in the economic system of machine-building enterprises]. *Aktualni problemy ekonomiky*. № 11. S. 95–100. [in Ukrainian].

2. Bosak A. O., Dalyk V. P., Maznyk Yu. I., Tulika S. K., Matsevko B. V., Prokopiv M. V., Staretskyi A. O. Kadrova bezpeka u systemi ekonomichnoi bezpeky pidpryiemstva. [Personnel security in the system of economic security of the enterprise]. *Mizhnarodnyi naukovyi zhurnal «Internauka». Seriia: «Ekonomichni nauky»*. 2023. № 10. doi: https://doi.org/10.25313/2520-2294-2023-10-9165 [in Ukrainian].

3. Burda I.Ia. Ekonomichna bezpeka pidpryiemstva ta mistse v nii kadrovoi bezpeky. [Economic security of the enterprise and the place of personnel security in it]. URL:http://economy.nauka.com.ua/index.php. [in Ukrainian].

4. Hrechko E.N. (2013). Sutnist bezpeky pidpryiemstva. [The essence of enterprise security]. *Upravlinnia rozvytkom*. № 12(152). S. 54–56. [in Ukrainian].

5. Zhyvko Z. B., Slipa O. Z., Bosak Kh. Z. (2014). Formuvannia optymalnoi systemy kadrovoi bezpeky pidpryiemstva v umovakh staloho rozvytku ekonomiky Ukrainy. [Formation of an optimal system of personnel security of the enterprise in the conditions of sustainable development of the economy of Ukraine]. *Aktualni problemy staloho rozvytku ekonomiky Ukrainy* : kolektyvna monohrafiia / za red. R. I. Trynka ta Ya. S. Pitsura. Lviv :Liha-Pres. S. 440-455. [in Ukrainian].

6. Kondratieva S.V. (2015). Henezys poniattia «kadrovoi bezpeky» pidpryiemstva. [The genesis of the concept of «personnel security» of an enterprise]. *Naukova dyskusiia. Ekonomika: realii chasu*. № 5(21). S. 194–198. [in Ukrainian].

 ISSN: 2786-9431

7. Lytovchenko O.Iu. (2010). Formuvannia kadrovoi bezpeky pidpryiemstv APK. [Formation of personnel security in agro-industrial complex enterprises] : avtoref. dys. … kand. ekon. nauk. Kyiv. 26 s. [in Ukrainian].

8. Mekheda N.H., Marenych A.I. (2012). Sotsialno-motyvatsiini skladovi kadrovoi bezpeky. [Social and motivational components of personnel security]. *Finansovyi prostir*. № 2(6). S. 38–45. [in Ukrainian].

9. Moiseienko I.P., Marchenko O.M. (2011). Upravlinnia finansovo-ekonomichnoiu bezpekoiu pidpryiemstva. [Managing the financial and economic security of the enterprise] : navch. posib. Lviv. 380 s. [in Ukrainian].

10. Petrov M.I. (2002). Ekonomichna bezpeka pidpryiemstva: sutnist, traktuvannia, tochky zoru. [Economic security of an enterprise: essence, interpretation, points of view]. Menedzher. № 1(17). S. 67–71. [in Ukrainian].

11. Podluzhna N.O. (2003). Orhanizatsiia upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva [Organization of management of economic security of the enterprise] : avtoref. dys. … kand. ekon. nauk: 08.06.01; Instytut ekonomiky promyslovosti. Donetsk. 20 s. [in Ukrainian].

12. Slipa O. Z. (2014). Kadrova bezpeka pidpryiemstva: poniattia, struktura ta osnovni mekhanizmy yii zabezpechennia [Personnel security of the enterprise: concept, structure and main mechanisms for its provision]. Mizhnarodnyi naukovyi zhurnal «Naukovyi ohliad». vypusk 2 №1 (1chastyna). s.56-63. [in Ukrainian].

13. Reverchuk N.I. (2004). Upravlinnia ekonomichnoiu bezpekoiu pidpryiemnytskykh struktur. [Management of economic security of business structures]. Lviv: LBI NBU. 195 s. [in Ukrainian].

14. Yaremenko O. F. (2016). Kadrova bezpeka pidpryiemstva: kontseptualni osnovy zabezpechennia. [Personnel security of the enterprise: conceptual foundations of ensuring]. Visnyk Khmelnytskoho natsionalnoho universytetu. № 2. T. 1. C. 29–32. [in Ukrainian].

 ISSN: 2786-9431