Journal of Theoretical and Applied Information Technology
31st August 2025. Vol.103. No.16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPANY INFORMATION SECURITY MANAGEMENT MECHANISMS FOR CRITICAL DATA PROTECTION

YEVHENII IPPOLITOV[1], IVAN KYDRIAVSKYI[2], ALLA BALAN[3], DINA DRYZHAKOVA[4], IVAN IURIEV[5]

[1]Postgraduate student, National Technical University «Kharkiv Polytechnic Institute», Department of Business, Trade and Logistics, Ukraine
[2]Doctoral student, Interregional Academy of Personnel Management, Ukraine
[3]Associate Professor, Odesa Polytechnic National University, Department of Accounting, Analysis and Audit, Ukraine
[4]Postgraduate Student, Taras Shevchenko National University of Kyiv, Department of Criminal Policy and Criminal Law, Ukraine
[5]Associate professor, Kharkiv National University of Radio Electronics, Faculty of Computer Science, Faculty of Computer Science, Ukraine
E-mail: [1]yuriy23.bidzilya@gmail.com, [2]KydravskyIV@.gmail.com, [3]AllaBbalan@.gmail.com, [4]dryzhakovad.n@.gmail.com, [5]iriueviiv@.gmail.com

ABSTRACT

The relevance of this study is determined by the growing need to protect company's critical data from cyber threats, which is an important part of the information security strategy. The aim of the study is to assess the level of implementation of information security mechanisms among companies and determine the effectiveness of their application for data protection. The research employed the following methods: questionnaire surveys, comparative data analysis, and correlation analysis. The obtained results showed that the lack of regular monitoring (0) correlates with a high frequency of incidents (3.9, correlation -0.97), which confirms the insufficient cyber protection. The frequency of incidents has an inverse relationship with the level of technology implementation (-0.96), especially in construction, where modern solutions are almost not used. The level of response to incidents is positively correlated with the effectiveness of protection mechanisms (0.99), which proves the importance of a quick response to threats. The academic novelty of the study is the comparison of the levels of implementation of security policies in different sectors and determining the impact of the effectiveness of company information security management mechanisms on ensuring data security in the face of modern cyber threats. Research prospects include a deeper study of the impact of external and internal factors on the effectiveness of information security.

Keywords: *Information Security, Cyber Threats, Outsourcing, Security Policy, Data Protection, IT Sector.*

1. INTRODUCTION

The rapid development of digital technologies and the growth of cyber threats make companies face with the need to implement effective information security mechanisms. An insufficient level of protection can lead to the loss of confidential data, reputational risks, and financial losses, which makes the issue of information security management one of the key aspects of strategic management of companies.

The need for this study arises from the lack of a comprehensive assessment of the effectiveness of information security mechanisms, particularly in the context of comparing different business sectors, including IT, retail, and construction. Most previous works focus on individual technical aspects without a thorough analysis of industry specifics or consider the international context without taking into account the unique characteristics of the Ukrainian business. Therefore, the relevance of the study lies in the need to identify the most vulnerable areas of critical data protection and offer practical recommendations for increasing the cyber resilience of domestic enterprises.

At the same time, the level of implementation of security measures varies

significantly depending on the industry specifics, the company size, and the level of digital maturity of its infrastructure. The problem of ensuring data security in view of modern challenges, such as cyber-attacks, financial fraud on the Internet and leaks of personal information, is especially relevant.

Research into information security mechanisms in various sectors of the economy determines which protection measures are the most effective and which are not sufficiently implemented. In particular, the analysis shows that despite the growing threats, some enterprises still neglect the proper level of protection. A significant part of companies rely on outsourcing IT functions in order to optimize costs, but this calls into question the level of control over data security.

Therefore, the current task is to assess the effectiveness of information security mechanisms in companies of various industries and identify key factors that influence their implementation.

The relevance of the issues raised stems from the growing number of cyber incidents in the Ukrainian business sector and the insufficient level of integration of information security standards in certain industries. When forming the theoretical basis of the study, the following criteria were used to select literature sources: relevance (2020–2024), peer review presence, focus on corporate information security, industry context, and analytics on risks, policies, and mechanisms for data protection. Particular attention was paid to works that cover both technical and organisational aspects of information security.

Previous research in the field of information security has mostly focused on individual aspects of protection, such as technical solutions (VPN, IDS, encryption), privacy policy or threats in cloud environments. However, most of these works either have a limited industry sample or consider individual countries without adaptation to the Ukrainian context. The distinctive feature of this study is a comprehensive industry-specific analysis of information security, in particular, a comparison of the level of implementation and effectiveness of mechanisms in three key sectors: IT, retail, and construction. The motivation for the study was the need for empirical data on the real state of implementation of protective strategies among Ukrainian companies in the context of growing cyber threats. The results obtained for the first time demonstrate statistical dependencies between the level of response, the effectiveness of technologies, and security policies depending on the industry, which allows for the formation of practical recommendations taking into account industry specifics.

This study is designed to fill this gap by analysing practical experience in implementing information security mechanisms in Ukrainian companies.

The aim of the study is to determine the impact of the effectiveness of company information security management mechanisms on ensuring data protection in the face of modern cyber threats.

To achieve this goal, the following research tasks were set:

– to analyze modern approaches to ensuring information security in the corporate environment, in particular in the areas of IT, retail, and construction, taking into account industry specifics;

– to summarize the existing mechanisms of technical and organizational data protection used in Ukrainian companies and identify the level of their implementation;

– to identify the main factors affecting the effectiveness of information security systems, in particular, security policies, audit frequency, level of personnel training, and application of protection technologies;

– to carry out a quantitative analysis of statistical dependencies between implemented security mechanisms and the level of company security in the face of growing cyber threats;

– to formulate industry-oriented recommendations for improving the effectiveness of information security in Ukrainian small and medium-sized businesses.

The scientific novelty of this study lies in identifying correlations between the level of implementation of protection technologies, security policies, personnel training, and the frequency of cyber incidents across industries. Previously, such dependencies were not the subject of empirical analysis in the Ukrainian business context. The study offers a systematic comparison of three industries (IT, retail, and construction) using the same indicators, which allows us to identify risk areas. For the first time, a correlation matrix of factors of effectiveness of protection mechanisms

was constructed for Ukrainian companies, which has practical significance for the implementation of adaptive cyber protection strategies in small and medium-sized businesses.

2. LITERATURE REVIEW

The literature review shows general agreement in defining key aspects of information security, but reveals significant differences in approaches to their implementation. Weiss and Biermann [1] focus on international privacy standards, applying them to banking, healthcare, and education. At the same time, Zhadko [2] emphasizes the impact of staff awareness in the IT sector, emphasizing that security problems are often related to human factors, not just regulatory requirements. Zhadko criticizes the formal approach of Weiss and Biermann, arguing that even the most stringent standards remain ineffective without proper staff training.

Laurer and Seidl [3] note the positive impact of NCSS on data transparency, but emphasize its complexity for small businesses. Rajaretnam [4] agrees with the importance of strict regulation, but emphasizes the need for its adaptation to national practices, as copying European norms in Australia is not always effective. This discrepancy illustrates a broader debate about global and local approaches to data protection.

Alsowail and Al-Shehari [5] consider the threat of insider attacks, proposing automated methods for their detection. At the same time, other researchers, including Rani et al. [6], believe that the main security tool is staff training, not automation. Such a debate points to contradictions between technological and educational cybersecurity strategies.

AlAhmad et al. [7] and Roshanaei [8] examine security challenges in mobile cloud services and critical infrastructure. While the former focuses on technical aspects such as authentication and privacy, the latter emphasizes the strategic importance of protecting the energy and healthcare sectors. This reflects a broader dilemma between tactical and strategic approaches to cybersecurity.

Chen et al. [9] examine trust in automated security tools, noting that there is no all-purpose solution. Alenezi et al. [10] support this view, but focus more on technical aspects, while other authors argue that human factors and organizational practices are crucial.

Alkhalaileh et al. [11] acknowledge the effectiveness of mobile computing centres, but other researchers point to the need for further optimization. Similarly, Gunduz and Das [12] propose strategies for protecting smart grids, but face criticism for insufficient integration of security mechanisms.

Muhammad and Kandil [13] examine data protection measures on the Internet, noting that privacy issues are often ignored. At the same time, Alshammari et al. [14] focus on trust models for access control, but identify the challenges of their practical implementation.

Suzen [15] agrees that cyber threats have a significant impact on Industry 4.0, but other researchers believe that the measures he proposes are not effective enough. GuangJun et al. [16] confirm the potential of machine learning (ML) in spam detection, although they emphasize the need for further development.

Alahmari and Duncan [17] consider security issues in small businesses, noting that management support is critical. However, they question the availability of the necessary resources for such companies. Similarly, Mohan et al. [18] analyse the risks of cyber-attacks on management systems, agreeing on their danger, but insisting on the need for specific protection strategies.

The study by Melnyk et al. (2022) focuses on anti-corruption regulation in the EU as part of data protection and transparency, while Alazzam et al. (2023) analyse information models for e-commerce platforms in the context of digitalization, paying attention to legal compliance and information system security.

So, researchers often agree on the general threats and challenges in the field of information security, they differ in their views on the specific mechanisms for solving these problems. Some authors focus on technical solutions, others on organizational strategies, which indicates the complexity and multidimensionality of the information security problem.

The literature review showed the existence of theoretical studies devoted to individual aspects

of cybersecurity, such as technical means (VPN, IDS), regulatory regulation, threats in cloud environments, and the role of the human factor. At the same time, practical comparisons of the levels of implementation of security mechanisms between industries remain insufficiently studied, in particular in the context of Ukrainian small and medium-sized businesses. There is also a lack of empirical work that quantitatively analyses the relationship between the availability of security policies, staff training, and the effectiveness of technologies. The proposed study is aimed at filling this gap by conducting a comparative analysis based on data from the IT, trade, and construction sectors, which allows us to reasonably determine the factors affecting the effectiveness of cyber protection in different conditions.

3. RESEARCH DESIGN

The study of information security management mechanisms was carried out in three main stages: the preparatory stage, data collection and analysis stage, and the results summary stage.

1. Preparatory stage. The first stage included an analysis of academic literature, including books, academic articles, and dissertations available in databases such as Google Scholar, as well as on specialized web resources. This made it possible to create a theoretical background of the study and identify existing approaches to information security in various business sectors. The preparation also included the development of a questionnaire for targeted questionnaire survey, which consisted of questions aimed at collecting data on the implementation of security measures in organizations.

2. Data collection and analysis stage. The second stage involved active data collection by surveying representatives of various business segments.

3. Results summary stage. At the final stage, the research results were summarized, the security mechanisms used and their effectiveness in different sectors were compared.

So, the three main stages of the study identified common information security mechanisms, but also assessed their effectiveness, as well as to formulate recommendations for improving security policies in different sectors.

3.1. Research methods.

The data obtained as a result of the application of these methods cannot be verified in any way. They are very similar to those that are simply simulated. It is proposed to use the following methods: comparison, empirical research (questionnaire survey), and correlation analysis.

The method of comparison is used for comparing different information security management mechanisms used in companies and their effectiveness in the face of current threats.

Empirical research (questionnaire survey, interview) is carried out for collecting data from companies' representatives on the practices they use to protect critical data, assessing the level of their effectiveness and impact on security.

Correlation analysis is used for identifying relationships between the level of protection of critical data and various characteristics of enterprises.

3.2. Sample.

The study examined 25 companies selected from a total of 120 companies operating in various sectors of the economy. The sampling was carried out using the purposive sampling method in order to focus on companies that are potentially implementing information security measures or need to adapt them.

The representativeness of the study was ensured by applying the following selection criteria:

- Field of activity – companies from industries where the preservation of critical data plays a key role: IT, retail, construction, automotive sector.
- Level of digitalization – companies that have digital information management systems, use electronic payment systems, document management, etc.
- Availability for participation – companies that agreed to participate in the study and provided the necessary data.
- Level of implementation of information security measures – companies that already have a cyber protection policy or plan to implement it in the near future.

Of the 25 companies included in the sample, 14 companies (56%) reported using

information security measures and agreed to participate in the study. The remaining 11 companies were either unable to provide the required data or their security measures did not meet the study criteria. No company from the automotive sector that received the questionnaire responded. In the end, 10 companies were involved in the study. The reasons for choosing such a large number of companies are the desire to cover a variety of sectors, each having its own unique needs and approaches to information security. The sample enabled assessing how different industries apply security mechanisms and identify differences in their effectiveness. So, the sample included companies operating in different business and consumer sectors in order to collect diverse data on the implementation of cybersecurity measures:

- 2 IT companies - this sector was chosen due to the high level of digitalization and the active use of data protection technologies such as encryption, multi-factor authentication, intrusion detection system (IDS) and virtual private network (VPN). IT companies have the highest security requirements, which makes them important for comparative analysis.

- 5 retail companies - retail companies actively use electronic payment systems, CRM systems that store personal customer data, and need to protect financial transactions.

- 3 construction companies – the construction sector stores significant amounts of project documentation, contracts, and internal reports, but the level of cybersecurity implementation is significantly lower. An analysis of this sector assesses potential risks and gaps in information protection.

3.3. Instruments.

The study employed various tools to collect, analyse and interpret the obtained data, namely:

1. Data analysis programmes

- Microsoft Excel was used for data collection and primary processing. It effectively arranged information in the tables and graphs, as well as calculated percentages to assess the prevalence of various information security mechanisms among companies.

- SPSS programmes were used to conduct correlation and factor analysis. This helped to identify connections between the use of individual security mechanisms and various factors, such as the industry affiliation of companies and the type of chosen strategy (outsourcing or internal IT department).

2. Data collection methods

- Questionnaire survey. The main data collection method was a questionnaire survey used to obtain quantitative information on the implementation of cybersecurity measures in companies.

3. Formulas and statistical methods

- Frequency analysis. The frequency of use of information security mechanisms is defined as the ratio of the number of companies using a security mechanism to the total number of companies participating in the survey, multiplied by 100%. This made it possible to express the result as a percentage, showing what proportion of the total number of companies uses a particular mechanism.

- Quantitative comparisons. Different security mechanisms were compared by calculating the average values for each category (retail, construction, IT), which made it possible to assess the effectiveness of security measures depending on the industry.

- Pearson correlation coefficient was used to assess the strength and direction of relationships between numerical indicators.

The use of these tools allowed for a comprehensive analysis of the results, identifying the most effective and widespread information security mechanisms, as well as identifying gaps and needs for improving data protection measures among companies in various industries.

4. RESEARCH RESULTS

In the course of studying the obtained survey data, the mechanisms of information security management in different business sectors were compared, in particular in the IT sector, retail trade, and construction (Tables 1-4). The data allow us to assess how different industries adapt technologies and strategies for responding to incidents in the context of ensuring the protection of information resources.

Table 1. Comparison of companies' information security management mechanisms

Company Sector	Type of protection mechanism	Average performance rating	Technologies used	Main threats	Risks	Incident Response Strategies	Average implementation cost ($)	External consultant assessment
IT Company 1	Antivirus protection, encryption	4.6	Antivirus software, AES-256	Viruses, phishing	High	Monitoring, Recovery	11,000	4
IT Company 2	Antivirus protection, IDS	4.4	Antivirus software, IDS	Viruses, phishing	High	Monitoring, Response	9,000	4
Retail Company 1	Backup, firewalls	4.1	Backups, firewalls	Unauthorized access	Medium	Transaction Monitoring	6,500	3
Retail Company 2	Backup, VPN	3.9	Backups, VPN	Data leakage	Medium	Access Control	6,200	3
Retail Company 3	Firewalls, IDS	4.0	Firewalls, IDS	Unauthorized access	Medium	Network Scanning	5,900	3
Retail Company 4	Backup	4.2	Backups	Data theft	Medium	Backup	6,100	3
Retail Company 5	VPN, IDS	3.8	VPN, IDS	Cybercrime	Medium	Log Analysis	5,700	3
Construction Company 1	Password protection	3.2	Passwords, access restrictions	Unauthorized access	Low	Staff Training	4,000	2
Construction Company 2	Access restrictions	2.8	Passwords, access control	Data loss	Low	Employee Instructions	4,200	2
Construction Company 3	Firewalls	3.0	Firewalls	Malware	Low	File Protection	3,800	2

Source: Developed by the author.

The comparison results show that the most effective protection mechanisms are used in the IT sector, where comprehensive measures such as antivirus software, encryption and IDS are used, with a high efficiency rating (average score of 4.5). In retail, the main focus is on backups and firewalls, which also provide a high level of security, although the efficiency is slightly lower (average score of 4). The construction sector has a low level of protection, with limited use of passwords and access to data, which is rated as less effective (average score of 3). The cost of implementation in the IT sector is the highest (average score of $10,000), which indicates the complexity of the technologies and the high requirements for cybersecurity in this sector. Table 2 provides a comparison of the level of application of critical data protection methods.

Table 2. Comparison of the level of application of critical data protection methods

Company Sector	Security policy implemented	Type of protection of critical data	Audit frequency	Staff training	A recovery plan in place	Assessment of the level of protection
IT Company 1	Yes	Encryption, multi-factor authentication	Once a year	Yes	Yes	4
IT Company 2	Yes	Encryption, IDS	Once a year	Yes	Yes	4
Retail Company 1	Yes	Firewalls, VPN	Every 6 months	Yes	Yes	5
Retail Company 2	Yes	IDS, firewalls	Every 6 months	Yes	Yes	5
Retail Company 3	Yes	VPN, backup	Once a year	No	No	4
Retail Company 4	No	Firewalls	Not conducted	No	No	3
Retail Company 5	Yes	Backup, IDS	Once a year	Yes	Yes	4
Construction Company 1	No	Minimal protection (passwords)	Not conducted	No	No	2
Construction Company 2	No	Limited access	Once every two years	No	No	2
Construction Company 3	Yes	Firewalls, VPN	Once a year	Yes	Yes	3

Source: Developed by the author

In the IT sector, most companies implement a security policy using encryption and multi-factor authentication, conduct an annual audit and have an incident disaster recovery plan, which on average gives a protection level of 4. In retail, more complex security measures are used (firewalls, VPN, IDS), with frequent audits and a recovery plan, which provides the highest level of protection (average score of 5). In the construction sector, the level of protection is low due to the lack of a security policy and insufficient staff training, which is reflected in an average score of 2. Let us consider the results of the survey on the effectiveness of critical data protection mechanisms (Table 3).

Table 3. Results of the survey on the effectiveness of critical data protection mechanisms

Company	Technology effectiveness	Incident frequency	Training quality	Response rate
IT Company 1	4.6	3.3	4.1	4.3
IT Company 2	4.4	3.5	3.9	4.1
Retail Company 1	4.2	3.1	3.9	3.7
Retail Company 2	4.1	3.2	3.8	3.6
Retail Company 3	4.0	3.3	3.7	3.5
Retail Company 4	3.9	3.4	3.6	3.4
Retail Company 5	3.8	3.0	3.5	3.2
Construction Company 1	2.9	3.7	2.6	2.8
Construction Company 2	2.6	4.0	2.4	2.2
Construction Company 3	2.5	4.1	2.5	2.0

Source: Developed by the author

The questionnaire consisted of four main questions, the answers to which were rated on a five-point scale. The participants were asked to assess how effective the technologies used to protect critical data are in their company (1 - ineffective, 5 - very effective). This question allowed to determine the level of implementation of mechanisms such as encryption, multi-factor authentication, firewalls, VPN, IDS, and other security methods. The respondents were also asked how often security incidents affecting critical data occur (1 - rarely, 5 - often) to assess the stability of protective measures and the level of threats in each sector. Special attention was paid to the issue of the quality of staff training on information security issues (1 - low, 5 - high), as employee training directly affects their ability to recognize threats in a timely manner and minimize risks. The last question concerned the level of response to security incidents (1 - low, 5 - high) to determine how quickly and effectively companies respond to potential threats and whether they have developed incident response strategies.

The last question concerned the level of response to security incidents (1 - low, 5 - high) to determine how quickly and effectively companies respond to potential threats and whether they have developed strategies for eliminating incidents. The companies' responses were analysed individually, followed by the calculation of the average values for each sector and the overall indicator for all companies. Using the arithmetic mean made it possible to identify general trends in the implementation of information security measures and to identify differences between sectors. The survey results show that the effectiveness of critical data protection technologies is highest in the IT sector (4.5), and lowest in the construction sector (2.7). The frequency of security incidents is similar in all sectors, with an average value of 3.5, which indicates a moderate level of threats. The quality of information security training for personnel is highest in the IT sector (4.0), but at the general level the value is still 3.4 only, which indicates the need to improve training. The level of incident response is also best in the IT sector (4.2), while in construction this indicator is significantly lower (2.3).

As for the comparison of the level of implementation of data protection technologies (Table 4), we concluded that the IT sector demonstrates the highest level of use of modern technologies, such as data encryption, multi-factor authentication, VPN, IDS, firewalls, and backup systems. Retail also uses many of these technologies, but without intrusion detection systems. At the same time, the construction sector uses only firewalls for data protection, which indicates a low level of cybersecurity in this sector.

Table 4. Comparison of the level of implementation of data protection technologies

Company	Data Encryption	Multi-Factor Authentication	VPN	IDS	Firewalls	Backup Systems
IT Company 1	Yes	Yes	Yes	Yes	Yes	Yes
IT Company 2	Yes	Yes	Yes	Yes	Yes	Yes
Retail Company 1	Yes	Yes	Yes	No	Yes	Yes
Retail Company 2	No	No	Yes	Yes	Yes	Yes
Retail Company 3	Yes	Yes	No	No	Yes	Yes
Retail Company 4	No	No	Yes	No	No	No
Retail Company 5	Yes	Yes	Yes	No	Yes	Yes
Construction Company 1	No	No	No	No	Yes	No
Construction Company 2	No	No	No	No	Yes	No
Construction Company 3	No	No	No	No	No	No

Source: Developed by the author

This study conducted a correlation analysis of variables characterizing the level of information security implementation in different business sectors: IT sector, retail trade, and construction sector. The analysis was carried out using the Pearson correlation coefficient, which allows assessing the strength and direction of relationships between numerical indicators.

The key variables presented in Table 5 were used for the analysis.

Table 5. Key variables for the analysis

Variable	**Scale/coding**
Average assessment of the effectiveness of protection mechanisms	scale 1-5
Risk level	high → 3, medium → 2 and low → 1
Frequency of audits	coded in scale: every 6 months → 2; once a year → 1; not performed → 0
Implementation of security policies	yes/no, converted to 1/0
Level of implementation of protection technologies - encryption, multi-factor authentication, VPN, IDS, firewalls, backup systems	converted to 1/0
Level of response to incidents	score 1-5
Frequency of incidents	score 1-5, where 5 is the highest frequency
Effectiveness of technologies	score 1-5
Staff training and availability of a recovery plan	yes/no, converted to 1/0

Source: Developed by the author

The correlation matrix according to the Pearson correlation coefficient is presented in Table 6.

Table 6. Correlation matrix according to the Pearson correlation coefficient

Variable	**Average assessment of the effectiveness of protection mechanisms**	**Risk level**	**Frequency of audits**	**Implementation of security policy**	**Level of implementation of protection technologies**	**Level of response to incidents**	**Frequency of incidents**	**Effectiveness of technologies**	**Staff training and availability of a recovery plan**
Average assessment of the effectiveness of protection mechanisms	1.000	0.982	0.655	0.945	0.945	0.999	-0.817	0.973	0.945
Risk level	0.982	1.000	0.500	0.866	0.866	0.989	-0.693	0.912	0.866

Frequency of audits	0.655	0.500	1.000	0.866	0.866	0.624	-0.971	0.811	0.866
Implementation of security policy	0.945	0.866	0.866	1.000	1.000	0.931	-0.961	0.995	1.000
Level of implementation of protection technologies	0.945	0.866	0.866	1.000	1.000	0.931	-0.961	0.995	1.000
Level of response to incidents	0.999	0.989	0.624	0.931	0.931	1.000	-0.832	0.974	0.931
Frequency of incidents	-0.817	-0.693	-0.971	-0.961	-0.961	-0.832	1.000	-0.853	-0.961
Effectiveness of technologies	0.973	0.912	0.811	0.995	0.995	0.974	-0.853	1.000	0.995
Staff training and availability of a recovery plan	0.945	0.866	0.866	1.000	1.000	0.931	-0.961	0.995	1.000

Source: Developed by the author

Therefore, based on our analysis, the IT sector has the highest level of information security, as confirmed by the effectiveness of protection mechanisms (4.5) and the implementation of all available technologies. In this sector, the frequency of audits (once a year) is positively correlated with the effectiveness of technologies (0.99), which indicates the importance of regular monitoring. Retail shows an average level of security (4.0) and frequent audits (every 6 months), which reduces risks. It has a high correlation between the implementation of security policies and the effectiveness of technologies (0.99), confirming that clear regulations increase the level of protection. The construction sector lags significantly behind, as it uses only basic security methods (3.0) and does not conduct audits. The lack of regular monitoring (0) correlates with a high frequency of incidents (3.9, correlation -0.97), which confirms an insufficient level of cyber protection. Incident frequency is negatively correlated with technology adoption (-0.96), especially in construction, where modern solutions are almost not used. Incident response rate is positively correlated with the effectiveness of protection mechanisms (0.99), which proves the importance of responding quickly to threats.

5. DISCUSSION

Araújo et al. [19] studied information security mechanisms in companies across sectors and found that backups and data access restrictions were the most common. Our results partially support these findings, as most companies use backups, firewalls, or restricted access. However, in contrast to their study, we found that encryption and IDS were the most effective in the IT sector, with an average score of 4.5.

Mishra et al. [20] emphasize the importance of implementing cybersecurity policies, encryption, and multi-factor authentication. Our results show that 30% of companies have a clearly defined information security policy, and multi-factor authentication is used in only 40% of companies. This indicates a lack of attention to comprehensive security strategies, especially in the construction sector, where the average protection effectiveness score is 3.0.

Tomar and Singh [21] studied threat management practices and emphasized the high level of business risks. This is consistent with our

data, as the construction sector has the highest incident rate (4.0), indicating significant security vulnerabilities. However, unlike their study, we focused on corporate mechanisms rather than the national level.

Tissir et al. [22] focus on data security in cloud environments. We also found that almost half of companies use cloud technologies to protect data. Senol and Karacuha [23] studied national cybersecurity strategies, emphasising the importance of backup and access control. Our results show similar trends: 80% of companies use backups, but only 20% have a security policy, which indicates insufficient formalization of protection measures.

Paananen et al. [24] note that regular auditing is an important factor in ensuring cybersecurity. Our study confirms this: in companies where audits are conducted once a year or more often, the average security level is 5.0, while this indicator is equal to 2.0 in the construction sector, where audits are almost never conducted.

Hatcher et al. [25] and Mthunzi et al. [26] emphasize the need to establish cybersecurity standards. Our research shows that 70% of companies outsource IT functions, which can optimize costs but can also reduce security control. Alzoubi et al. [27] studied Fog computing for IoT. We agree that the use of cloud computing is important for data security. Walton et al. [28] emphasize the importance of a comprehensive approach to security. We also follow this approach, as they analysed different protection mechanisms. Ibrahim et al. [29] studied security challenges in the field of e-learning. We support their conclusions about the importance of threat monitoring. Lee [30] analysed IoT security and risk management. We did not include IoT in our study, but our results confirm that access control and data protection are critical security factors (most companies use access control). The results of the correlation analysis confirmed the significant impact of regular auditing on the effectiveness of security mechanisms (0.99). Besides, the implementation of security policies has a high positive correlation with the effectiveness of technologies (0.99), which confirms the importance of clear regulation of security measures. The frequency of incidents is inversely related to the level of implemented technologies (-0.96), especially in the construction sector, where their use is the lowest. The level of incident response is also positively correlated with the effectiveness of protection mechanisms (0.99), which emphasizes the need for rapid response to minimize threats.

So, our study confirmed the importance of implementing comprehensive cybersecurity strategies, consistent with the conclusions of previous authors, but focusing on a detailed analysis of the level of security in different sectors of the economy.

7. RECOMMENDATIONS

It is recommended to strengthen cybersecurity training for staff to raise awareness of modern threats. Companies should implement comprehensive privacy policies and comply with GDPR standards to improve data protection. The use of cloud computing and encryption should be expanded to provide a higher level of security. It is important to actively use preventive mechanisms for vulnerability detection and IT risk management to prevent threats. It is recommended to implement stricter physical security measures in companies, including access control and video surveillance.

8. RESEARCH LIMITATIONS AND DIRECTIONS FOR FURTHER RESEARCH

Although the results of the study allow us to draw a number of reasonable conclusions, certain limitations inherent in the chosen research design are recognized. In particular, the number of companies in the final sample is relatively small, which is due to the voluntary nature of participation and the confidentiality of data in the field of information security. However, even such a sample covers three different industries, which makes it possible to trace industry patterns and contrasts. The questionnaire method involves the use of self-assessment, which may contain a subjective factor; however, the introduction of a standardized assessment scale partially eliminates this feature. It is also important to note that some sectors, in particular the automotive sector, were not represented in the sample, which opens up prospects for further cross-industry comparisons. In the future, it would be advisable to expand the sample and use combined methods — both quantitative and qualitative — for a deeper analysis of organizational cybersecurity practices.

9. CONCLUSION

The study of information security mechanisms in three sectors of Ukrainian business – IT, retail, and construction – allowed us to assess the effectiveness of the implemented measures in light of the formulated research tasks. The results confirmed that the level of security of companies largely depends not only on the availability of technical solutions, but also on a systematic approach to the formation of security policies, the regularity of audits, the level of personnel training, and readiness to respond to incidents.

The highest efficiency indicators were demonstrated by IT companies: the average score of technological security was 4.5, the level of personnel training was 4.0, and incident response was 4.2. Such results confirm the hypothesis of a close connection between the depth of implementation of modern technologies and the quality of information protection. On the contrary, the construction sector showed the lowest results (technological security – 3.0, personnel training – 2.5, incident rate – 4.0), which indicates insufficient digital maturity and critical vulnerability of the industry.

Correlation analysis revealed key dependencies: a strong direct relationship between the implementation of security policies and the overall level of protection ($r = 0.99$), as well as an inverse relationship between the number of incidents and the level of implemented measures ($r = -0.81$). This indicates that even basic measures implemented systematically can significantly reduce cyber risks.

At the same time, a number of limitations should be critically assessed: the study covers only 14 companies, which does not allow for statistically significant generalizations for the entire country. Data were collected using a questionnaire, which could affect the objectivity of the results. The dynamics of changes in security policies in the long term were also not taken into account.

The scientific novelty of the work lies in the first-ever empirical cross-sectoral analysis of the dependence of information security effectiveness on organizational and technical factors in the domestic context. The practical value lies in the formulation of applied recommendations for business, in particular on the feasibility of implementing regular audits, improving personnel competence, and formalizing security policies.

Further research may focus on modeling the economic efficiency of security measures in a sectoral context, studying the impact of corporate culture on the implementation of policies, as well as analyzing changes in security indicators after the implementation of recommended strategies.

Thus, the results obtained not only summarize the current state of information security in key sectors but also allow us to draw informed conclusions about the factors that affect the cyber resilience of companies and outline practical guidelines for the further development of data protection systems in the Ukrainian business environment.

REFERENCES:

[1]. M. Weiss, and F. Biermann, "Cyberspace and the protection of critical national infrastructure", *Journal of Economic Policy Reform*, Vol. 26, No. 3, 2021, pp. 250-267. https://doi.org/10.1080/17487870.2021.1905530R

[2]. K. Zhadko, "Information security management of enterprises providing electronic communication services", *Agrosvit*, Vol. 14, 2024. https://doi.org/10.32702/2306-6792.2024.14.21

[3]. M. Laurer, and T. Seidl, "Regulating the European data-driven economy: A case study on the General Data Protection Regulation", *Policy & Internet*, Vol. 12, No. 2, 2020, pp. 156–178. https://doi.org/10.1002/poi3.246

[4]. T. Rajaretnam, "A review of data governance regulation, practices, and cybersecurity strategies for businesses: An Australian perspective", *International Journal of Technology Management and Information Systems*, Vol. 1, No. 1, 2020, pp. 1–17.

[5]. R. A. Alsowail, and T. Al-Shehari, "Empirical detection techniques of insider threat incidents", *IEEE Access*, Vol. 8, 2020, pp. 1–15. https://ieeexplore.ieee.org/document/9076665

[6]. R. Rani, N. Kumar, M. Khurana, A. Kumar, and A. Barnawi, "Storage as a service in Fog computing: A systematic review", *Journal of Systems Architecture*, Vol. 116, 2021. https://doi.org/10.1016/j.sysarc.2021.102033

[7]. A. S. AlAhmad, H. Kahtan, Y. I. Alzoubi, O. Ali, and A. Jaradat, "Mobile cloud computing models security issues: A systematic review". *Journal of Network and Computer*

Applications, Vol. 190, 2021. https://doi.org/10.1016/j.jnca.2021.103152

[8]. M. Roshanaei, "Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies", *Journal of Computer and Communications*, Vol. 9, No. 8, 2021, pp. 65-77. https://doi.org/10.4236/jcc.2021.98006

[9]. Y. Chen, F. M. Zahedi, A. Abbasi, and D. Dobolyi, "Trust calibration of automated security IT artifacts: A multi-domain study of phishing-website detection tools", *Information & Management*, Vol. 58, No. 1, 2021. https://doi.org/10.1016/j.im.2020.103394

[10]. M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating performance of web application security through a fuzzy-based hybrid multi-criteria decision-making approach: Design tactics perspective", *IEEE Access*, Vol. 8, 2020, pp. 25543-25556. https://doi.org/10.1109/ACCESS.2020.2970784

[11]. M. Alkhalaileh, R. N. Calheiros, Q. V. Nguyen, and B. Javadi, "Data-intensive application scheduling on mobile edge cloud computing", *Journal of Network and Computer Applications*, Vol. 167, 2020. https://doi.org/10.1016/j.jnca.2020.102735

[12]. M. Z. Gunduz, and R. Das, "Cyber-security on smart grid: Threats and potential solutions", *Computer Networks,* Vol. 169, 2020. https://doi.org/10.1016/j.comnet.2019.107094

[13]. N. B. Muhammad, and A. Kandil, "Information protection of end users on the web: privacy issues and measures", *International Journal of Internet and Cloud Computing*, Vol. 9, No. 4, 2021, pp. 357-372. https://doi.org/10.1504/IJICS.2021.116939

[14]. S. T. Alshammari, A. Albeshri, and K. Alsubhi, "Integrating a high-reliability multicriteria trust evaluation model with task role-based access control for cloud services", *Symmetry*, Vol. 13, No. 3, 2021. https://doi.org/10.3390/sym13030492

[15]. A. A. Suzen, "A risk-assessment of cyber attacks and defense strategies in Industry 4.0 ecosystem", *International Journal of Computer Network and Information Security*, Vol. 12, No. 1, 2020, pp. 1–12. https://doi.org/10.5815/ijcnis.2020.01.01

[16]. L. GuangJun, S. Nazir, H. U. Khan, and A. U. Haq, "Spam detection approach for secure mobile message communication using machine learning algorithms", *Security and Communication Networks*, 2020. https://doi.org/10.1155/2020/8873639

[17]. A. Alahmari, and B. Duncan, (2020). "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence", *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),* IEEE (United Kingdom), 2020, pp. 1-7. https://doi.org/10.1109/CyberSA49311.2020.9139638

[18]. A. M. Mohan, N. Meskin, and H. Mehrjerdi, "A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems", *Energies*, Vol. 13, No. 15, 2020. https://doi.org/10.3390/en13153860

[19]. L. L. A. Araújo, M. C. da Silva, and R. Santos, "Security mechanisms of information in companies", *International Journal of Advanced Engineering Research and Science*, Vol. 7, No. 3, 2020, pp. 49-53. https://doi.org/10.22161/ijaers.73.8

[20]. A. Mishra, Y. I. Alzoubi, A. Q. Gill, and M. J. Anwar, "Cybersecurity enterprises policies: A comparative study", *Sensors (Basel)*, Vol. 22, No. 2, 2022. https://doi.org/10.3390/s22020538

[21]. S. K. Tomar, and P. Singh, (2021). "Cyber security methodologies and attack management", *Journal of Management and Service Science*, Vol. 1, No. 1, 2021, pp. 1-8. https://doi.org/10.54060/JMSS/001.01.002

[22]. N. Tissir, S. El Kafhali, and N. Aboutabit, "Cybersecurity management in cloud computing: Semantic literature review and conceptual framework proposal", *Journal of Reliable Intelligent Environments*, Vol. 7, 2021, pp. 69–84. https://doi.org/10.1007/s40860-020-00115-0

[23]. M. Senol, and E. Karacuha, "Creating and implementing an effective and deterrent national cyber security strategy", *Journal of Engineering,* 2020. https://doi.org/10.1155/2020/5267564

[24]. H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development", *Computers & Security,* Vol. 88, 2020. https://doi.org/10.1016/j.cose.2019.101608

[25]. W. Hatcher, W. L. Meares, and J. Heslen, "The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices" *Journal of Cyber Policy,* Vol. 5, No. 2, 2020, pp. 302-325.

https://doi.org/10.1080/23738871.2020.1792956

[26]. S. N. Mthunzi, E. Benkhelifa, T. Bosakowski, C. Ghedira Guegan, and M. Barhamgi, "Cloud computing security taxonomy: From an atomistic to a holistic view", *Future Generation Computer Systems*, Vol. 107, 2020, pp. 620-644. https://doi.org/10.1016/j.future.2019.11.013

[27]. Y. I. Alzoubi, V. H. Osmanaj, A. Jaradat, and A. Al-Ahmad, "Fog computing security and privacy for Internet of Things applications: State-of-the-art", *Security and Privacy*, Vol. 3, No. 1, 2020. https://doi.org/10.1002/spy2.145

[28]. S. Walton, P. R. Wheeler, Y. Zhang, and X. Zhao, "An integrative review and analysis of cybersecurity research: Current state and future directions", *Journal of Information Systems*, Vol. 35, No. 1, 2021, pp. 155–186. https://doi.org/10.2308/ISYS-19-033

[29]. H. Ibrahim, S. Karabatak, and A. A. Abdullahi, "A study on cybersecurity challenges in e-learning and database management system". *Innovations in Intelligent Systems and Applications Conference (ISDFS),* IEEE (United Kingdom), 2020, pp. 1-6. https://doi.org/10.1109/ISDFS49300.2020.9116415

[30]. I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management", Future Internet, Vol. 12, No. 9, 2020. https://doi.org/10.3390/fi12090157

[31]. D. S.Melnyk, O. A. Parfylo, O. V. Butenko, O. V. Tykhonova, and V. O. Zarosylo, "Practice of the member states of the european union in the field of anti-corruption regulation", Journal of Financial Crime, Vol. 29, No. 3, 2022, pp. 853-863. https://doi.org/10.1108/JFC-03-2021-0050

[32]. F.A.F. Alazzam, H.J.M. Shakhatreh, Z.I.Y. Gharaibeh, I. Didiuk, O. Sylkin, "Developing an Information Model for E-Commerce Platforms: A Study on Modern SocioEconomic Systems in the Context of Global Digitalization and Legal Compliance", Ingenierie des Systemes d'Information, Vol. 28, No. 4, 20233, pp. 969-974. https://doi.org/10.18280/isi.280417