Analysis of the state of information security at hotel and restaurant enterprises*

Orest Polotai[1,*,†], Bohdana Polotai[2,†], Oleh Harasymchuk[3,†], and Natalia Kukharska[3,†]

[1] Lviv State University of Life Safety, 35 Kleparivska str., 79000 Lviv, Ukraine
[1] Lviv University of Trade and Economics, 10 Tugan-Baranovskogo str., 79005 Lviv, Ukraine
[3] Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine

Abstract

The article presents a comprehensive study of the state of information security of a conditional hotel and restaurant enterprise operating within the Lviv region. The purpose of the work is to analyze the current level of security of information resources, identify key vulnerabilities and develop recommendations for improving the effectiveness of the information security system. The study uses expert assessment methods, SWOT analysis and mathematical tools to quantify the level of security. The work identifies five main factors that most significantly affect the level of information security of the enterprise: access control to the hotel and restaurant information system; backup and restoration of booking and order data; protection against malicious software and monitoring of network traffic; training of personnel to work safely with information; technical support and updating of information systems. Recommendations are developed to improve organizational, technical and training measures in the field of information security. Re-evaluation after the implementation of the proposed measures showed an improvement in the integral indicators: the quantitative indicator (S) increased from 0.17 to 0.41, and the qualitative indicator (Q) from 0.48 to 0.57. This indicates an increase in the efficiency of the information security system and the formation of a more stable protective environment. The results obtained have practical significance for enterprises in the hotel and restaurant sector, since the proposed approach can be used as a methodological basis for the analysis, evaluation and further improvement of the information security system, taking into account the specifics of the industry.

Keywords

information security, hotel and restaurant enterprise, SWOT analysis; expert evaluation; integral indicator; cyber threats; data backup; access control; staff training; information systems.

1. Introduction

The current stage of society's development is characterized by the rapid digitalization of all spheres of human activity, which leads to an increase in the role of information as a key resource for management, communication and decision-making. For enterprises, information resources have become not only an auxiliary element of functioning, but also a strategic asset, on which the efficiency of business processes, competitiveness and market stability directly depend. In these conditions, the issue of ensuring information and cybersecurity is of paramount importance.

In the context of globalization of the information space, enterprises become participants in complex digital ecosystems, in which data is constantly exchanged between internal and external users, partners, clients, and government agencies. At the same time, the increase in the volume of processed data, the widespread use of cloud technologies, remote access, mobile devices and artificial intelligence systems significantly increase the level of vulnerability of the information infrastructure [1-3], especially in cloud-based and IoT-oriented environments that require continuous protection and monitoring [4]. This is why complementary integrity-preserving and covert-protection techniques remain relevant for sensitive data transmission [5]. The number of

* CSDP'2026: Cyber Security and Data Protection, May 7, 2026, Lviv, Ukraine
* Corresponding author.
† These authors contributed equally.
orest.polotaj@gmail.com (O. Polotai); bogdanaf@ukr.net (B. Polotai); oleh.i.harasymchuk@edu.lpnu.ua (O. Harasymchuk); kukharska.n@gmail.com (N. Kukharska)
0000-0003-4593-8601 (O. Polotai); 0000-0003-1600-2724 (B. Polotai); 0000-0002-8742-8872 (O. Harasymchuk); 0000-0002-0896-8361 (N. Kukharska)

incidents related to cyberattacks, phishing campaigns, virus infections, and the leakage of personal and commercial data is increasing every year.

According to analytical reports from international cybersecurity companies, the number of cyberattacks on small and medium-sized businesses has increased by more than 50% in recent years. Most of these attacks are aimed at stealing financial or confidential information, blocking access to systems with the aim of demanding ransom (ransomware), or disrupting the stability of information systems. This indicates the need for a systematic approach to building and improving information security systems, focused not only on technical but also on organizational, personnel and management aspects [6].

Ukraine, integrating into the global information space, is gradually harmonizing its standards with European requirements (in particular, NIS2, ISO/IEC 27001, GDPR, SOC 2) [7-8]. This involves the implementation of comprehensive information security management systems at enterprises, which require regular auditing, risk analysis and modernization of protection tools.

In addition to external threats, internal factors also pose a significant danger — personnel errors, negligence in complying with security policies, low level of employee awareness, lack of access control or unauthorized use of corporate resources [9-10]. This indicates that an effective information security system should be multi-level, integrated into the overall enterprise management system and be based on the principles of continuous improvement [11].

In today's conditions of instability and hybrid challenges, when cyberspace is becoming one of the key arenas of competition, effective information security management is a critical factor in ensuring business stability, preserving reputation and preventing financial losses.

In today's conditions of digital transformation, the hotel and restaurant sector is increasingly actively implementing information technologies in its activities [12-13]. Online booking systems, electronic customer databases, contactless payments, automated accounting systems and network services have become an integral part of the functioning of enterprises in the industry. At the same time, the volume of personal and financial data processed, transmitted and stored in information systems is growing significantly. This makes hotel and restaurant enterprises potential targets of cyber threats and malicious attacks [14-15].

Violation of confidentiality, integrity or availability of data in such an area can lead not only to financial losses, but also to a serious reputational blow, loss of trust of customers and partners. Leaks of personal data of visitors, information about bank cards or internal management documents are especially dangerous [16]. In practice, this can manifest itself in the form of phishing attacks, infection of network devices with malicious software, unauthorized access to Wi-Fi networks or reservation databases.

At the same time, most small and medium-sized enterprises in the hotel and restaurant business do not have a sufficient level of information infrastructure protection. Often, security measures are reduced only to the use of antiviruses or passwords without a systematic approach to risk management. The lack of information security specialists, underestimation of threats, outdated software and low level of staff awareness — all this creates a favorable environment for cyberattacks.

Therefore, the current task today is a comprehensive assessment of the state of information security of hotel and restaurant enterprises, identification of vulnerabilities and development of effective recommendations for their elimination [17]. Of particular importance is the use of expert analysis methods that provide an opportunity to qualitatively assess not only technical, but also organizational aspects of protection — access policies, personnel training, data backup, incident management, etc.

Conducting such a study makes it possible to increase the level of cybersecurity of the enterprise, prevent possible information leaks and financial losses, provide appropriate protection of guests' personal data, and ensure compliance with current regulatory requirements in the field of information security. This is of particular relevance in the context of increasing requirements for personal data processing under the GDPR framework and Ukrainian legislation, which obliges enterprises to implement adequate technical and organizational measures to protect information.

According to the Global Cybersecurity Index published by the International Telecommunication Union (ITU) [18], Ukraine has significantly improved its cybersecurity readiness in recent years, moving toward alignment with international frameworks such as ISO/IEC 27001 and NIST CSF. However, sector-specific implementation of these standards, particularly within small and medium-sized enterprises in the hospitality industry, remains insufficient. Research conducted by the European Union Agency for Cybersecurity (ENISA) [19] indicates that the hospitality sector processes large volumes of sensitive personal and financial data while often underinvesting in cybersecurity measures. Furthermore, the Verizon Data Breach Investigations Report (2025) [20] identifies accommodation and food service organizations among the sectors most affected by credential theft, ransomware, and point-of-sale intrusions. This confirms the need for sector-oriented information security assessment methodologies and forecasting approaches capable of tracking cybersecurity trends over time [21].

2. Materials and Methods

The study used a set of methods that combine analytical, expert and mathematical approaches to assessing the state of information security of a hotel and restaurant enterprise. The object of the study was a conventional average hotel and restaurant enterprise in the Lviv region, which reflects the typical characteristics of small or medium-sized businesses in the region. The enterprise operates in a mixed format — it combines temporary accommodation, catering and leisure services for clients. Its information infrastructure includes an automated room reservation system, an internal accounting system, a human resources management system (HRM), a local computer network, wireless Wi-Fi access for guests, as well as a number of peripheral devices connected to the network. The basis of the study is an expert method for assessing the level of information security, which involves the involvement of specialists in the field of cyber security to determine the current state of the information system according to a number of criteria. The expert group consisted of cybersecurity specialists, system administrators, and IT auditors with practical experience in information security management and risk assessment. The selection of experts was based on their professional experience, qualifications, and involvement in the implementation or maintenance of enterprise information systems.

In addition to the expert method, the study used SWOT analysis (Strengths, Weaknesses, Opportunities, Threats), which allows for a systematic assessment of internal and external factors affecting the state of information security.

- Strengths (S) include the availability of basic IT solutions, a centralized customer base, and the use of antivirus protection.
- Weaknesses (W) — lack of backup, non-unified access policy, and weak control over personnel.
- Opportunities (O) — implementation of modern cyber security technologies, increasing the digital literacy of employees, and engaging security consultants.
- Threats (T) — phishing attacks, personal data leakage, network equipment failures, and the influence of the human factor.

SWOT analysis allows for a combination of qualitative characteristics with quantitative indicators of expert assessment, which contributes to the formation of a holistic vision of the state of information security. To increase the objectivity of the results, the weighted average method was used, which takes into account the different importance of criteria for a specific type of enterprise.

The obtained analysis results became the basis for developing a system of recommendations for improving the level of information security: improving password policies, implementing backups, creating internal instructions for responding to incidents, improving staff training, etc. After implementing the proposed measures, a repeated expert assessment was conducted, which allowed assessing the dynamics of changes and confirming the effectiveness of the proposed solutions.

Thus, the use of a combination of the expert method, SWOT analysis and mathematical calculations provides a comprehensive and objective approach to studying the level of information security of a hotel and restaurant enterprise, allowing not only to determine the current state, but also to build a strategy for its further improvement.

3. Results

At the current stage of development of Ukrainian society, there is a constant increase in the importance of the information sphere of hotel and restaurant enterprises. It covers not only information resources and infrastructure, but also subjects that collect, process, form, distribute and use information, as well as mechanisms for regulating social relations that arise in this process. The formation of an effective information security system for hotel and restaurant enterprises is an objective necessity, which is due to a number of factors [22]. One of the key factors is the rapid growth of information volumes in the activities of such enterprises. In the conditions of the information society, information technologies have become widespread in the production sector, in particular in the process of transition from traditional paper document flow to electronic. The dynamic development of digital technologies leads to the mass use of computer equipment and its integration into local and global networks, which significantly simplifies the processes of processing, exchange and access to data for all participants in entrepreneurial activity. Recent studies on the hospitality sector emphasize that digital transformation has also expanded the attack surface through online booking systems, guest Wi-Fi, POS terminals, and cloud-based services [23-24]. Furthermore, the active adoption of cloud computing, mobile applications, and AI-driven customer service tools increases the importance of cybersecurity governance and real-time threat detection in hospitality enterprises. Modern information security strategies therefore focus not only on technical protection measures but also on cyber resilience and rapid incident response capabilities.

Information security is one of the key components of the modern information society, as it determines the level of protection of data, information systems and technologies from threats of unauthorized access, violation of integrity or loss of confidentiality. In scientific research, the essence of information security is considered as a set of organizational, technical, legal and social measures aimed at ensuring the stability of the information environment to external and internal threats. It integrates both fundamental theoretical provisions and applied protection mechanisms that allow guaranteeing the continuity of the functioning of information processes.

Any business entity, including a hotel and restaurant business enterprise, operates under conditions of constant threat exposure that can negatively affect its information resources, business processes and competitiveness. In the modern digital environment, information is a strategic asset, and therefore its loss, distortion or unauthorized use can cause significant economic losses and reputational risks. This is especially relevant for hospitality enterprises, where customer profiles, reservation records, payment data, and operational documents are processed simultaneously across multiple systems. In addition, the increasing integration of contactless payment technologies and mobile check-in services requires enhanced protection of personal and financial data. The growing dependence on interconnected digital platforms also increases the potential impact of cyber incidents on customer trust and business continuity. That is why in scientific research and practical activities, special attention is paid to the analysis of threats to information security and their systematization.

Any external threat negatively affects the information security of a hotel and restaurant business enterprise, reducing its stability and ability to function effectively in a digital environment. In practice, these threats often include phishing campaigns, compromise of guest Wi-Fi networks, attacks on booking platforms, malware infections, and misuse of third-party services. Cybersecurity experts also note a significant rise in social engineering attacks targeting hotel employees through fake booking requests and fraudulent emails. Such attacks exploit human factors and demonstrate the importance of regular cybersecurity awareness training for staff. At

the same time, a separate category is made up of internal threats that arise within the enterprise and directly affect the information security of the business entity. Internal risks are often associated with weak password practices, insufficient staff awareness, outdated software, lack of segmentation of internal and guest networks, and irregular security updates. These internal challenges can create risks for the overall economic security system of the company and require the introduction of additional organizational and technical protection measures (Table 1).

Table 1
Internal threats affecting the information and cybersecurity of a business entity

№	Description of information security threats	Impact on the overall system of economic security of the business entity
1	Personnel threat, information leakage due to employee actions	Decline in financial results, losses, exit from the market
2	Loss of information due to dishonest work of information security personnel	Availability of innovative developments to competitors, loss of new sales markets
3	Reducing the protective potential of software and servers in the organization	Increased organizational costs, lack of resources
4	Insufficient funding for information security	Lack of capital, as a result of lack of funds for the development of the organization, threat of bankruptcy
5	Low rate of updating of protective systems, untimely replenishment of data banks with new threats	Loss of resources, information leakage
6	Customer data leak	Loss of customers, costs of restoring security data

Figure 1 shows the key components of cybersecurity for a hospitality business and their percentage impact.

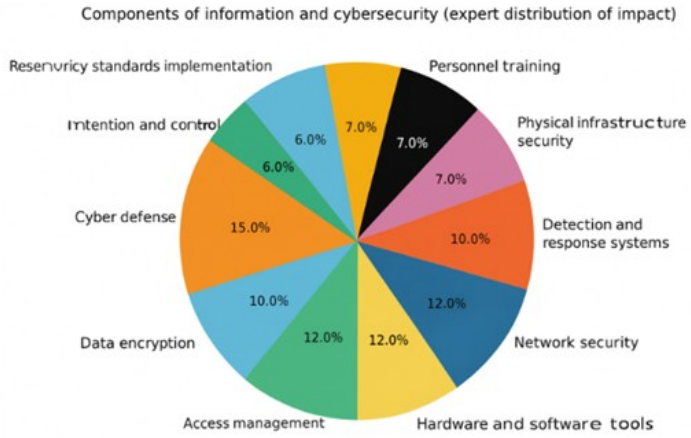

Figure 1: Key components of a business entity's cyber security and their percentage impact

This study examines a conventional average hotel and restaurant enterprise located in the Lviv region, which in terms of its parameters reflects the typical structure of a small or medium-sized business in this area. The enterprise has been operating in the tourism and hotel and restaurant services market for over ten years and combines in its activities services of temporary accommodation of guests, organization of catering, holding banquets, corporate events, as well as provision of related services — booking, food delivery and online payment.

The enterprise has three main structural divisions: a hotel complex with 40 rooms of various categories, a restaurant with 80 seats and an administrative and accounting department. All

divisions are managed through an integrated information system that provides customer registration, room reservations, calculations, reporting and personnel management.

The information infrastructure of the enterprise includes a centralized local computer network, to which the workstations of the administration, reception, accounting, room service and restaurant hall are connected. The network is divided into an internal segment (for administrative needs) and a guest segment (Wi-Fi for customers). Access to the Internet is provided via a router with basic traffic filtering functions. The server part is implemented on the basis of one central server, which houses the customer database, accounting programs, reservation management system and copies of e-mail.

Among the information assets of the enterprise, the following can be distinguished:

1. customer personal database (full name, passport data, phone numbers, addresses, payment information);
2. data on room reservations and restaurant service orders;
3. financial and accounting documentation;
4. internal reports, personnel documentation and commercial information.

Modern technologies are used to serve customers: an online booking system on the official website, a mobile CRM system for order management, and POS terminals for cashless payments. At the same time, some information processes are of a mixed nature — some documents are stored in paper form, which creates additional risks of data leakage or loss.

The number of employees of the company is about 35 people, among whom only one specialist is partially responsible for the technical maintenance of computer equipment and the network. The company does not have its own information security specialist or IT department. This is a typical situation for most small business hotels and restaurants, where information protection issues are often resolved situationally or are left without due attention.

Information protection at the company is carried out mainly at a basic level — antivirus software is installed, password access to accounts is used, and a log of access to administrative systems is partially kept. However, data backup is carried out irregularly, the security policy is not documented, and personnel training on cyber security is not carried out.

In view of the above, the selected enterprise can be characterized as typical for the hotel and restaurant industry at the regional level, which actively uses information technologies, but has limited resources to build a full-fledged information security system. That is why it is an illustrative example for analyzing the state of information protection, identifying the main problem areas and developing recommendations for their elimination.

The study of this conditional enterprise allows not only to simulate real threats and risks characteristic of the industry, but also to assess the effectiveness of practical measures to improve the information security system, which are of universal importance for similar hotel and restaurant establishments in the Lviv region and beyond.

In order to comprehensively study the state of information security of a conditional hotel and restaurant enterprise in Lviv region, it is advisable to conduct a SWOT analysis. Its use allows not only to quantitatively assess individual indicators, but also to qualitatively analyze internal and external factors that affect the level of information protection of the enterprise.

Conducting a SWOT analysis is necessary to:

1. systematize existing advantages and disadvantages in the field of information security;
2. determine opportunities for the development of information infrastructure;
3. identify external threats that may negatively affect data security;
4. form strategic directions for improving the enterprise's information security system.

Such an analysis allows you to build a holistic picture of the current state, determine priorities for further actions and develop recommendations for increasing the level of cyber protection, taking into account the specifics of the enterprise's activities.

Table 2 shows the results of the SWOT analysis.

Table 2
SWOT analysis of a hotel and restaurant type enterprise

Strengths	Weaknesses
• Availability of basic IT infrastructure (local network, server, Wi-Fi). • Use of automated booking system and CRM solutions. • Partial use of antivirus protection and access passwords. • Experience of personnel in using computer technology. • Positive attitude of management towards digitalization of processes.	• Lack of a comprehensive information security policy. • Irregular backups and lack of a data recovery plan. • Low level of staff awareness of cybersecurity issues. • Lack of an IT specialist or department. • Use of outdated equipment and unlicensed software. • Insufficient control of network access and accounts.
Opportunities	**Threats**
• Implementation of modern information security management systems (for example, basic SIEM solutions). • Switching to licensed software with security system updates. • Increasing the digital literacy of personnel through education and training. • Using cloud services with built-in data protection mechanisms. • Obtaining advice from external IS experts. • The ability to attract funding for IT infrastructure modernization.	• Cyber threats: phishing, malware, account hacking, customer data leaks. • Human factors: accidental deletion or transfer of confidential information. • Reputational losses in the event of a security incident. • Technical failures due to equipment failure or lack of redundancy. • External pressure from competitors and fraudulent structures. • Changes in legislation regarding the processing of personal data.

Building a SWOT analysis is an important stage in studying the state of information security of a conventional hotel and restaurant type enterprise [25]. The main goal of this analysis is to systematize the existing strengths and weaknesses of the enterprise, as well as identify external opportunities and threats that may affect its information infrastructure. This approach allows you to form a holistic picture of the current state of information protection and develop an effective strategy for improving security.

Building a SWOT analysis was carried out in several consecutive stages:

Identification of internal factors. At the first stage, the key strengths and weaknesses of the enterprise were identified. Strengths characterize the available resources and advantages that can contribute to increasing the level of information security, for example: basic IT infrastructure, the presence of automated reservation systems and CRM, partial use of antivirus protection.

Weaknesses reflect existing gaps and shortcomings in the security system: lack of a comprehensive information security policy, irregular backups, low level of personnel competence in the field of cyber protection, lack of an information security specialist, use of outdated equipment and software.

Identification of external factors. At the second stage, opportunities and threats coming from the external environment of the enterprise were identified. Opportunities describe the potential for improving the security system, for example: implementation of modern IT solutions, use of cloud services, involvement of experts, training for personnel, software updates.

Threats reflect external and internal risks that can negatively affect the security of the enterprise: cyberattacks (phishing, malware), technical failures, human factor (employee errors), reputational losses and changes in legislation on the processing of personal data [26-28].

Classification and ranking of factors. After determining the factors, each of them was classified by the degree of importance and impact on the state of information security. For this, the expert assessment method was used, which allowed assigning a score to each factor according to its

significance. This step makes it possible to identify priority areas for improving security measures and effectively allocate enterprise resources.

Construction of the SWOT matrix. All identified factors were located in the SWOT matrix, where internal factors (strengths and weaknesses) are placed horizontally, and external (opportunities and threats) are placed vertically. Such structuring allows you to clearly see the relationships between internal and external elements and form strategic directions for development.

Interpretation of results. Thanks to the SWOT matrix, it became possible to:

1. determine the strengths of the enterprise on which future security measures can be based;
2. realize weaknesses that need to be eliminated as a priority;
3. assess external opportunities that can be used to increase the level of protection;
4. identify threats that require systematic control and monitoring.

Building a SWOT analysis in combination with expert assessment and mathematical calculations of an integral indicator of the level of information security allows you to obtain both quantitative and qualitative results. This creates a basis for developing recommendations for strengthening the protection of the enterprise's information assets and increasing overall resilience to cyber threats.

In scientific literature, SWOT analysis is considered one of the effective strategic tools for assessing information security management systems and identifying priority directions for their improvement [29]. In addition, researchers emphasize that the integration of expert assessment methods with SWOT analysis increases the reliability of decision-making in the field of cybersecurity and risk management [30].

Figure 2 shows a summary overview of the state of information security at the enterprise.

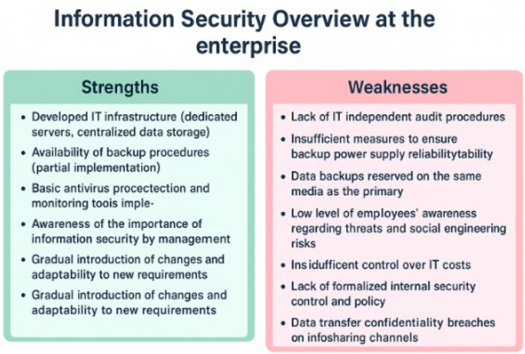

Figure 2: Summary overview of the state of information security at the enterprise

Based on the conducted comprehensive analysis of information security of a hypothetical hotel and restaurant type enterprise and the results of the SWOT analysis, a number of factors were identified that have a key impact on the state of information asset protection. In particular, among all the indicators considered, five factors were selected by expert method, which, in our opinion, are the most critical for ensuring a high level of information security:

1. Access control to the hotel and restaurant information system.

The management of accounts of reception, kitchen, administration and accounting staff, access rights to reservation systems, client databases and internal documentation are assessed. Insufficient control can lead to leakage of personal data of guests or financial documents.

2. Backup and restoration of information on reservations and orders.

Includes regular backups of data on rooms, reservations, restaurant orders and financial transactions, as well as readiness to quickly restore information after technical failures or cyber incidents.

3. Malware protection and network traffic control of the hotel and restaurant.

Includes the use of antivirus programs, threat detection systems and monitoring of the Wi-Fi network for guests, the internal local network and POS terminals, which minimizes the risks of malware infection or unauthorized access.

4. Training staff to work safely with customer data and orders.

Assess the level of knowledge of reception, kitchen and administration staff regarding the processing of guest personal data, the safe use of booking systems and POS terminals, as well as compliance with internal information security policies.

5. Technical support and updating of hotel and restaurant information systems

Includes the status of servers, computers, POS terminals, the relevance of reservation and restaurant management software, the availability of a specialist or IT support service to quickly resolve technical problems.

The selection criteria were based on the following principles:

1. Impact on confidentiality, integrity and availability of data — factors that directly determine the security of key information resources.
2. Risk to the enterprise's business processes — factors, the violation of which can lead to significant financial losses or reputational damage.
3. Possibility of implementing practical improvement measures — factors that can be used to promptly implement changes or improvements.
4. Frequency of threat manifestation — factors that are subject to repeated risk from external or internal threats.
5. Interconnection with other elements of the information system — factors that affect other security components and can create cascading consequences if violated.

The selection of these five critical factors allows you to focus further analysis on the most significant aspects that determine the quality of the enterprise's information security. This allows you not to waste resources on less significant elements and provides a targeted assessment of risks and the state of the protection system.

For further research, an information security status matrix was constructed, which includes these five critical factors and their assessment on a point scale. The matrix allows you to clearly present the current state of the enterprise in key areas, identify the most vulnerable elements and prepare the basis for calculating the integral indicator of the level of information security.

The information security status matrix is a tool that combines expert assessments and mathematical calculations, which allows you to obtain an objective quantitative characteristic of the current state of information protection at the enterprise. On its basis, you can not only identify weaknesses, but also assess the dynamics of changes after the implementation of the proposed security improvement measures.

Thus, the construction of an information security status matrix based on critical factors is a key stage of the study, which provides data systematization, structured risk assessment and preparation for calculating the integral indicator for further making informed management decisions on improving the enterprise's information asset protection system.

Let's build a matrix of knowledge (assessments) of the state of information security of the studied enterprise (Figure 3).

The matrix reflects a detailed assessment of the state of information security of a conditional hotel and restaurant enterprise according to five critical factors:

1. Access control to the hotel and restaurant information system
2. Backup and restoration of reservation and order information
3. Protection against malicious software and control of hotel and restaurant network traffic
4. Training of personnel for safe work with customer data and orders
5. Technical support and updating of hotel and restaurant information systems

Four areas of assessment are considered for each factor:

1. Base — availability of basic data and resources for information protection;
2. Structure — organizational structure and logic of interaction of protection elements;
3. Measures — specific actions and processes implemented to ensure security;
4. Means — technical and software solutions used for protection.

Stages	Directions	Access control to hotel and restaurant information system				Backup and restore booking and order information				Malware protection and network traffic control for hotels and restaurants				Training staff to work securely with customer and order data				Technical support and updating of hotel and restaurant information systems			
	Foundations	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means
1	Defining information to be protected	0,6	0,6	0,5	0,6	0,6	0,8	0,5	0,5	0,7	0,8	0,5	0,4	0,5	0,6	0,5	0,4	0,5	0,8	0,5	0,7
2	Identifying threats and information leakage channels	0,5	0,5	0,5	0,7	0,7	0,5	0,4	0,8	0,7	0,5	0,8	0,7	0,5	0,5	0,8	0,7	0,5	0,7	0,8	0,7
3	Conducting vulnerability and risk assessments	0,7	0,4	0,4	0,4	0,7	0,4	0,6	0,8	0,6	0,4	0,8	0,7	0,6	0,4	0,6	0,7	0,7	0,4	0,7	0,7
4	Determining requirements for an information security system	0,7	0,4	0,5	0,5	0,7	0,5	0,6	0,8	0,7	0,6	0,6	0,8	0,7	0,6	0,6	0,7	0,7	0,6	0,8	0,7
5	Making a choice of protection measures	0,7	0,5	0,6	0,4	0,7	0,5	0,6	0,7	0,6	0,5	0,6	0,8	0,7	0,5	0,6	0,8	0,7	0,7	0,6	0,8
6	Implementation of selected measures and tools	0,4	0,8	0,8	0,7	0,4	0,8	0,8	0,7	0,5	0,8	0,8	0,7	0,5	0,7	0,8	0,7	0,5	0,7	0,8	0,8
7	Integrity control and protection management	0,7	0,5	0,2	0,2	0,7	0,5	0,6	0,2	0,7	0,4	0,7	0,8	0,7	0,4	0,7	0,5	0,7	0,7	0,8	0,6

Figure 3: Knowledge matrix (assessments) of the state of information security of a hotel and restaurant type enterprise

The rows of the matrix reflect the stages of information security research, that is, the sequential steps taken to assess and improve the state of protection:

1. Determining the information to be protected;
2. Identifying threats and information leakage channels;
3. Conducting an assessment of vulnerabilities and risks;
4. Determining the requirements for the information protection system;
5. Selecting protection tools;
6. Implementing selected measures and tools;
7. Integrity control and protection management.

Each cell of the matrix contains a score from 0 to 1, which shows the level of implementation or effectiveness of the corresponding direction at this stage. For example:

- A value closer to 1 indicates a high level of organization or effectiveness of the measure;
- A value closer to 0 indicates a weak point or insufficient implementation of the measures.

Thus, the matrix allows you to systematize and quantify the state of information security of the enterprise in all critical areas, identify weaknesses, track the dynamics of changes and use this data for further calculation of the integral indicator of information security.

Based on this matrix, an analysis of the state of information security at the enterprise under study will be carried out.

Figure 4 presents data for assessing the first factor access control to the hotel and restaurant information system.

Let us explain the content of Figure 4:

1 column: stage number from 1 to 7.

2 column: list of indicators (m) for the corresponding elements (from 1 to 28).

3 column: importance coefficients (aj), which are determined for the indicators of each stage.

4 column: indicators of the required safety profile (Qn). A constant value of 0.8 is set for all indicators.

5 column: indicators of the achieved safety profile (Qd). Their values are determined by the expert method.

6 column: indicators of the achieved safety profile taking into account the importance coefficients (Qd* aj).

7 column: comparison of profiles (Spr), which is done as follows:

Spr = 1 – if the value of the indicator of the achieved safety profile is equal to or exceeds the value of the given indicator;

Spr = 0 – if the value of the indicator of the achieved safety profile is lower than the value of the given indicator;

8th column: Qgroup is determined taking into account the importance coefficients (Qd* aj) for each of the stages, is calculated as the sum of Qd* aj of each stage;

9th column: qualitative assessment (Q) is determined based on the values of the indicators calculated for the corresponding stages and is calculated as the average value. In our case, Q1 = 0.57.

The quantitative assessment (S) is determined by counting the values (Spr = 1), namely the units obtained when comparing profiles and determining their percentage value from the total number 28. This is a rough estimate that determines the number of fulfilled (achieved) requirements S1 = 0.07.

№ stage	List of indicators	Importance factor	Security profile required	Safety profile achieved	Indicators of the achieved safety profile taking into account importance factors	Profile comparison	Degree of fulfillment of groups of requirements	Qualitative assessment	Quantitative assessment
	m	a_j	Q_d	Q_d	Q_d* a_j	S_{pr}	Q_{group}	Q	S
1	2	3	4	5	6	7	8	9	10
1	1	0,4	0,8	0,6	0,24	0		0,57	0.07
	2	0,2	0,8	0,6	0,12	0			
	3	0,2	0,8	0,5	0,1	0			
	4	0,2	0,8	0,6	0,12	0	0,58		
2	5	0,45	0,8	0,5	0,225	0			
	6	0,25	0,8	0,5	0,125	0			
	7	0,15	0,8	0,5	0,075	0			
	8	0,15	0,8	0,7	0,105	0	0,53		
3	9	0,5	0,8	0,7	0,35	0			
	10	0,25	0,8	0,4	0,1	0			
	11	0,15	0,8	0,4	0,06	0			
	12	0,1	0,8	0,4	0,04	0	0,55		
4	13	0,55	0,8	0,7	0,385	0			
	14	0,15	0,8	0,4	0,06	0			
	15	0,15	0,8	0,5	0,075	0			
	16	0,15	0,8	0,5	0,075	0	0,595		
5	17	0,4	0,8	0,7	0,28	0			
	18	0,3	0,8	0,5	0,15	0			
	19	0,2	0,8	0,6	0,12	0			
	20	0,1	0,8	0,4	0,04	0	0,59		
6	21	0,25	0,8	0,4	0,1	0			
	22	0,15	0,8	0,8	0,12	1			
	23	0,15	0,8	0,8	0,12	1			
	24	0,45	0,8	0,7	0,315	0	0,655		
7	25	0,45	0,8	0,7	0,315	0			
	26	0,25	0,8	0,5	0,125	0			
	27	0,15	0,8	0,2	0,03	0			
	28	0,15	0,8	0,2	0,03	0	0,5		

Figure 4: Data for evaluating the information protection system in the direction of "Access control to the hotel and restaurant information system"

A comparison of protection profiles in the direction of "Access control to the hotel and restaurant information system" can be seen in the graph shown in Figure 5.

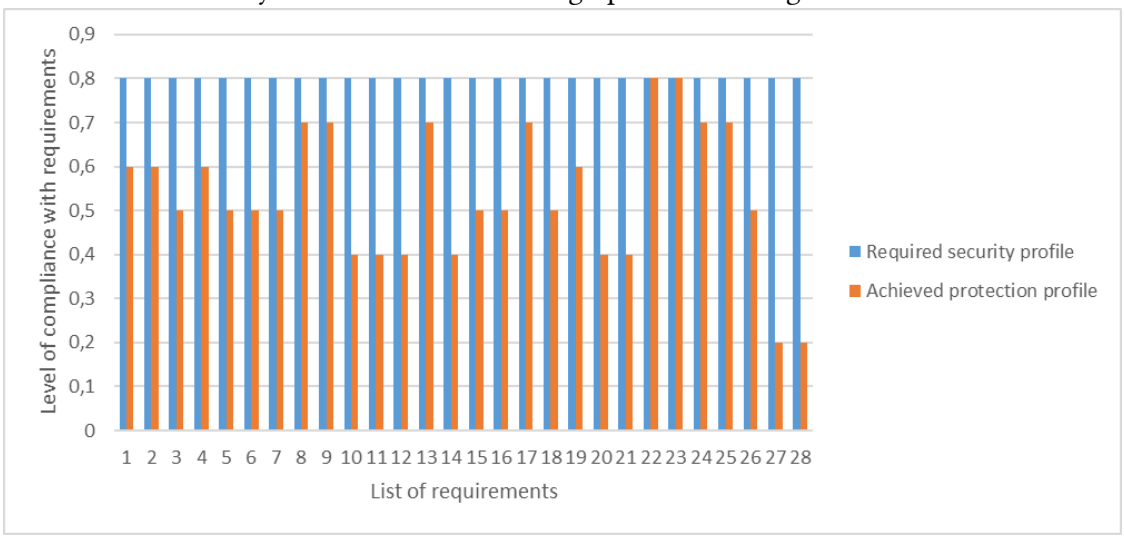

Figure 5: A comparison of protection profiles in the direction of "Access control to the hotel and restaurant information system"

Figure 6 shows a graphical representation of the quality level of the first factor at each stage.

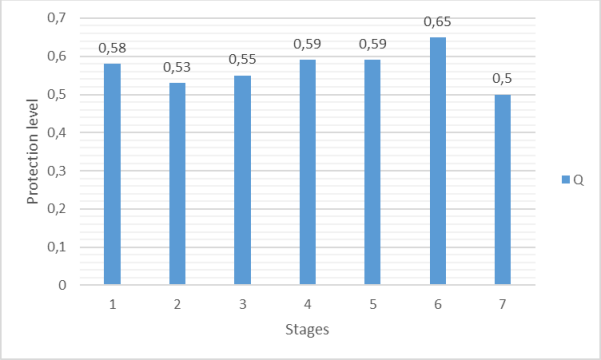

Figure 6: Evaluation of the stages of protection factors

Similarly, we calculate the same indicators for the other four areas of information security.

Generalized indicators of the level of information and cybersecurity at the enterprise (qualitative and quantitative) are presented in Table 3.

Table 3

Generalized indicators of information security quality level

Indicators	Protective factors					IILIS
	1	2	3	4	5	
	Importance factors by direction IFD					
	0,25	0,2	0,25	0,1	0,2	
Quantitative S	0,07	0,18	0,29	0,11	0,25	0,17
Qualitative Q	0,57	0,62	0,63	0,58	0,68	0,48

Each qualitative and quantitative indicator of the level of information security has its own weight coefficient IFD, which was determined by an expert method.

IILIS (S) — integral quantitative indicator of the level of information security, is calculated by the formula (1).

$$IILIS = S1 * IFD1 + S2 * IFD2 + S3 * IFD3 + S4 * IFD4 + S5 * IFD5 \quad (1)$$

Where

S1….Sn — quantitative indicator of the level of information security;

IFD1….IFDn — indicator weighting factor.

IILIS (Q) = integral qualitative indicator of the level of information security, is calculated by the formula (2).

$$IILIS = Q1 * IFD1 + Q2 * IFD2 + Q3 * IFD3 + Q4 * IFD4 + Q5 * IFD5 \quad (2)$$

Where

Q1….Qn — qualitative indicator of the level of information security;

IFD1….IFDn — indicator weighting factor.

Exceeding the value of the qualitative indicator over the quantitative one indicates that the fulfilled requirements are more important in their value than the unfulfilled ones.

Given the results of the diagnostics, the state of information security at the enterprise can be considered insufficient, which necessitates the implementation of a number of recommendations aimed at improving existing and developing new protection mechanisms.

Given the results of the diagnostics, the state of information security at the enterprise can be considered insufficient, which necessitates the implementation of a number of recommendations aimed at improving existing and developing new protection mechanisms.

1. Technical protection of information systems and networks.

Problem: insufficient network segmentation, weak passwords, outdated software, low level of antivirus protection.

Recommendations:

Install modern antivirus and antimalware protection systems with centralized monitoring [31].

Separate the guest Wi-Fi network from the internal corporate network (separate VLANs).

Regularly update operating systems, cash register and reservation system software.

Implement a policy of complex passwords and two-factor authentication for administrative accounts.

Use backup systems and store backups on secure media.

2. Training personnel in information security

Problem: hotel and restaurant employees are often unaware of the risks of phishing, social engineering, or customer data leakage.

Recommendations:

Conduct regular information security training for all employees, including receptionists, waiters, and managers.

Develop brief instructions on the safe use of email, CRM, and POS systems.

Create a system for periodic knowledge testing (tests, simulations of phishing attacks).

3. Availability and effectiveness of the regulatory framework for information security [32-33].

Problem: absence or formal existence of security policies.

Recommendations:

Develop and approve internal documents: Information Security Policy, Regulations on the Processing of Customer Personal Data, Incident Response Procedure similar to policy development approaches used for other digital services and user-facing platforms [34].

Appoint a person responsible for information security or define this role in the IT staff structure.

Implement a system for monitoring compliance with information access rules and recording user actions.

4. Level of protection of customer personal data.

Problem: a large amount of guests' personal data (passport data, telephone numbers, card details) is often stored without proper protection.

Recommendations:

Use specialized booking software with customer data encryption and consider additional integrity-verification mechanisms for image- and document-based records [35].

Restrict access to the customer database only to authorized persons.

Implement automatic data cleaning after the expiration of the storage period (in accordance with the privacy policy).

Ensure compliance with the requirements of the GDPR or Ukrainian legislation on the protection of personal data.

5. Physical protection of technical means and media.

Problem: uncontrolled access to servers, computers at the reception, POS terminals, etc.

Recommendations:

Limit physical access to server equipment, routers and administrator workstations.

Install video surveillance systems in areas where equipment is stored.

Introduce procedures for marking and accounting for external media (flash drives, disks) [35].

Use encryption tools on mobile devices and laptops of staff [36].

The implementation of the proposed recommendations will allow for a comprehensive increase in the level of information security of a hotel and restaurant enterprise, reduce the risks of leakage of confidential information, ensure compliance with regulatory requirements, and strengthen customer trust.

Having fulfilled most of the requirements, a new knowledge matrix was obtained using the expert method and the quality of the information protection system, or the degree (completeness)

of fulfillment of information security requirements, was calculated based on the new initial data. The new data was modeled in accordance with the implemented recommendations, i.e. the state of information protection taking into account the improved level of fulfillment of the requirements.

The updated matrix for constructing the required safety profile is presented in Figure 7.

Stages	Directions	Access control to hotel and restaurant information system				Backup and restore booking and order information				Malware protection and network traffic control for hotels and restaurants				Training staff to work securely with customer and order data				Technical support and updating of hotel and restaurant information systems			
	Foundations	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means	Base	Structure	Activities	Means
1	Defining information to be protected	0,8	0,6	0,5	0,8	0,8	0,8	0,5	0,7	0,9	0,8	0,5	0,6	0,7	0,6	0,5	0,6	0,7	0,8	0,5	0,9
2	Identifying threats and information leakage channels	0,7	0,5	0,5	0,9	0,9	0,5	0,4	1	0,9	0,5	0,8	0,9	0,7	0,5	0,8	0,9	0,7	0,7	0,8	0,9
3	Conducting vulnerability and risk assessments	0,9	0,4	0,4	0,6	0,9	0,4	0,6	1	0,8	0,4	0,8	0,9	0,8	0,4	0,6	0,9	0,9	0,4	0,7	0,9
4	Determining requirements for an information security system	0,9	0,4	0,5	0,7	0,9	0,5	0,6	1	0,9	0,6	0,6	1	0,9	0,6	0,6	0,9	0,9	0,6	0,8	0,9
5	Making a choice of protection measures	0,9	0,5	0,6	0,6	0,9	0,5	0,6	0,9	0,8	0,5	0,6	1	0,9	0,5	0,6	1	0,9	0,7	0,6	1
6	Implementation of selected measures and tools	0,6	0,8	0,8	0,9	0,6	0,8	0,8	0,9	0,7	0,8	0,8	0,9	0,7	0,7	0,8	0,9	0,7	0,7	0,8	1
7	Integrity control and protection management	0,9	0,5	0,2	0,4	0,9	0,5	0,6	0,4	0,9	0,4	0,7	1	0,9	0,4	0,7	0,7	0,9	0,7	0,8	0,9

Figure 7. Knowledge matrix (assessments) of the state of information security of a hotel and restaurant type enterprise

We similarly calculate the quantitative and qualitative information security indicator at a hotel and restaurant enterprise after introducing additional information security mechanisms that were recommended for implementation.

The generalized indicators of the level of information and cybersecurity at the studied enterprise (qualitative and quantitative) after implementing the recommendations are presented in Table 4.

Table 4.
Generalized indicators of information security

Indicators	Protective factors					IILIS
	1	2	3	4	5	
	Importance factors by direction IFD					
	0,25	0,2	0,25	0,1	0,2	
Quantitative S	0,39	0,5	0,61	0,39	0,57	0,41
Qualitative Q	0,69	0,76	0,73	0,68	0,77	0,57

Figure 8 shows a graphical comparison of quantitative and qualitative assessments of the degree of compliance with requirements before and after implementing the recommendations.

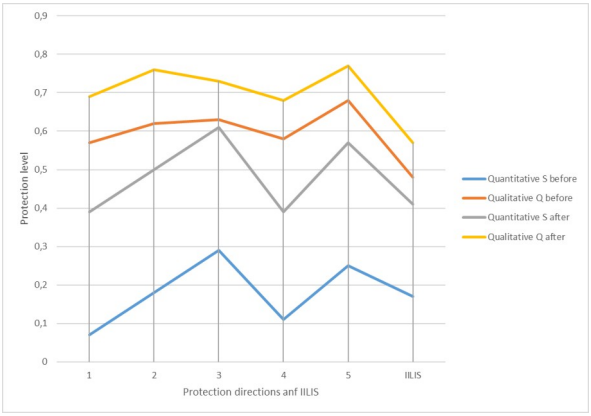

Figure 8: Graphical comparison of quantitative and qualitative assessments of the degree of fulfillment of requirements before and after implementation of recommendations

After the implementation of the proposed organizational, technical and educational and preventive measures, a reassessment of the level of information security of the hotel and restaurant type enterprise was carried out.

The results obtained showed positive dynamics in the state of information resource security. Thus, the quantitative indicator of the level of information security (S), which reflects the integral measure of the implemented technical and organizational measures, increased from 0.17 to 0.41, which indicates a significant increase in the effectiveness of the data protection system and a reduction in vulnerabilities.

At the same time, the qualitative indicator of information security (Q), which characterizes the organizational and procedural aspect — the level of personnel training, the availability of security policies, compliance with procedures and the general culture of information security, increased from 0.48 to 0.57. This demonstrates an improvement in employees' awareness of the principles of safe work with information, as well as more effective functioning of the internal control system and response to potential incidents.

The growth of both indicators together indicates the gradual formation of a comprehensive information security system that combines technical, organizational and human aspects. Thus, the implemented measures have proven their effectiveness and can be recommended for practical application at similar enterprises in the hotel and restaurant sector.

4. Discussion

The results of the study show that information security in hotel and restaurant enterprises is complex and depends not only on technical means of protection, but also on organizational processes, personnel training and the level of digital culture of personnel.

During the analysis, it was found that in most such enterprises, priority is given to customer service and business process support, while cyber security issues remain in the background. This leads to the emergence of a number of vulnerabilities, in particular in the area of protecting guests' personal data, managing access to internal reservation and order processing systems, as well as information backup.

The SWOT analysis made it possible to identify critical factors that most affect the level of information security, including the organization of access control, the effectiveness of antivirus protection, the regularity of updating information systems, personnel training and the availability of established backup procedures.

The implementation of the developed recommendations contributed to the improvement of both quantitative and qualitative indicators of information security, which indicates the effectiveness of the proposed approach. In particular, the increase in the integral security indicator showed that even in medium-sized enterprises without significant financial resources it is possible to achieve

significant results by optimizing processes, training personnel and implementing basic principles of information management.

However, it is worth noting that the study has certain limitations. The assessment model is built on the basis of expert assessments and does not take into account dynamic changes in threats in real time. Therefore, a promising direction for further research is the development of automated systems for monitoring the state of information security of service enterprises, which would provide continuous risk analysis and adaptation of protection measures to new conditions.

5. Conclusions

As a result of the study of the state of information security of a conditional hotel and restaurant type enterprise, the existing level of protection of information resources was comprehensively analyzed, the main threats, vulnerabilities and areas for improving the security system were identified.

The use of expert assessment methods, SWOT analysis and quantitative calculations made it possible to comprehensively characterize the situation and identify five key factors that have the greatest impact on the state of information security:

1. access control to the hotel and restaurant information system;
2. backup and restoration of booking and order data;
3. protection against malicious software and monitoring of network traffic;
4. training of personnel for safe work with information;
5. technical support and updating of information systems.

Based on the constructed assessment model and implemented recommendations, it was possible to achieve positive dynamics of the state of information security indicators. The quantitative indicator (S) increased from 0.17 to 0.41, and the qualitative indicator (Q) from 0.48 to 0.57, which indicates a significant increase in the level of security of the enterprise's information environment.

The results obtained confirm the effectiveness of the proposed measures, including strengthening access control, regular data backup, improving the skills of employees in the field of cyber hygiene, and upgrading the technical components of the information infrastructure.

Thus, the proposed methodology for assessing and improving the state of information security can be used as a practical tool for hotel and restaurant enterprises that seek to increase the reliability of storing and processing customer data.

Prospects for further research lie in the development of automated systems for monitoring and forecasting information security risks, as well as in the application of artificial intelligence methods for dynamic threat analysis and selection of optimal protection measures.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication’s content.

References

[1] V. Dudykevych, G. Mykytyn, T. Stosyk, P. Skladannyi, Platform for the security of cyber-physical systems and the IoT in the intellectualization of society // CEUR Workshop Proc. – 2024, vol. 3654, p. 449-457.

[2] O. Sapsai, Y. Martseniuk, A. Partyka, O. Harasymchuk, Research on automated security incident management in public cloud environments. // CEUR Workshop Proc., 2025, 4042, pp. 226-249.

[3] Y. Martseniuk, A. Partyka, O. Harasymchuk, V. Cherevyk, N. Dovzhenko, Research of the Centralized Configuration Repository Efficiency for Secure Cloud Service Infrastructure Management // CEUR Workshop Proc., 2025, 3991, pp. 260-274.
[4] L. Meshkat, R. Miller, A Systems Approach for Cybersecurity Risk Assessment, Annual Reliability and Maintainability Symposium (RAMS), Tucson, AZ, USA, 2022, pp. 1-9, doi:10.1109/RAMS51457.2022.9893966.
[5] N. Kukharska, A. Lagun, O. Polotai, The steganographic approach to data protection using arnold algorithm and the pixel-value differencing method, In: Proceedings of the 2020 IEEE 3rd International Conference on Data Stream Mining and Processing, DSMP, 2020, p. 174-177.
[6] O. Belej, N. Nestor, S. Panchak, O. Polotai, Developing a Model of Cloud Computing Protection System for the Internet of Things, In: International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020, p. 53-58.
[7] Y. Martseniuk, et al., Cost Observability as a Security Control in Multi-Cloud Environments Based on SOC 2 Security Standard. Comput. Secur. 2025, 161, 104771. doi:10.1016/j.cose.2025.104771/.
[8] O. Deineka, et al., Designing Data Classification and Secure Store Policy According to SOC 2 Type II // CEUR Workshop Proc., 2024, 3654, pp. 398-409.
[9] S. Bhaharin, U. Mokhtar, R. Sulaiman, M. Yusof, Issues and Trends in Information Security Policy Compliance, In: 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, 2019, pp. 1-6, doi:10.1109/ICRIIS48246.2019.9073645.
[10] N. Karim, J. Kaur, M. Khalib, Benefit vs Cost: Examining Factors of Intention to Comply Information Security Policy, In: IEEE International Conference on Computing (ICOCO), Kuala Lumpur, Malaysia, 2021, pp. 291-296, doi:10.1109/ICOCO53166.2021.9673542.
[11] M. Stammler, M. Hamann, J. Becker, Multilevel Security Model for Secure Information Flow Inside Software Components Employing Automated Code Generation, In: 2023 12th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2023, pp. 1-6, doi:10.1109/MECO58584.2023.10154914.
[12] P. Guo, D. Cui, Research on Hotel Industry Informatization, In: 2023 9th Annual International Conference on Network and Information Systems for Computers (ICNISC), Wuhan, China, 2023, pp. 398-401, doi:10.1109/ICNISC60562.2023.00096.
[13] S. Korotkov, et al., Equipment of hotel and restaurant complexes with network equipment, Eur. Sci., 2 (sge19-02), 61-90, 2023. doi:10.30890/2709-2313.2023-19-02-015.
[14] Dr. Sharma, Examination of Cybersecurity Practices in Small Hotels: A Comprehensive Study of Awareness, Challenges and Solutions. University of Fairfax, 2024.
[15] N. Shabani, A. Munir, A Review of Cyber Security Issues in Hospitality Industry, 2020. doi:10.1007/978-3-030-52243-8_35.
[16] X. Li, et al., Precursor of privacy leakage detection for individual user//Comput. & Secur., 2024.
[17] O. Nesterenko, I. Netesin, V. Polischuk, Y. Selin, Multifunctional Methodology of Expert Evaluation Alternatives in Tasks of Different Information Complexity, In: IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2021, pp. 226-231, doi:10.1109/ATIT54053.2021.9678742.
[18] International Telecommunication Union. (n.d.). *Global Cybersecurity Index.*
[19] European Union Agency for Cybersecurity. (n.d.). *Research and innovation.*
[20] K12 Security Information Exchange. (2025, April 23). *K12 SIX contributes to Verizon 2025 Data Breach Investigations Report.*
[21] N. Kukharska, V. Samotyy, A. Lagun, O. Polotai, Trend extrapolation method for qualitative prognosis the global cybersecurity index in Ukraine. ISTCMTM. Vol. 81 (4). p. 30-34.
[22] Inayatulloh, A Blockchain Model in the Hospitality Industry to Increase Traceability and Transparency of Transactions, In: International Seminar on Application for Technology of

Information and Communication (iSemantic), Semarang, Indonesia, 2023, pp. 58-62, doi:10.1109/iSemantic59612.2023.10295327.

[23] S. Daventa, H. Ongowarsito, Factors Affecting The Effectiveness of Hospitality Information Systems, In: International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Bali, Indonesia, 2024, pp. 908-913, doi:10.1109/ICICYTA64807.2024.10913415.

[24] D. Syahchari, N. Astiti, A. Zulkarnain, S. Lake, A. Ridzuan, D. Leonandri, Service Innovation in the Hospitality Sector: The Role of Digital Leadership, Capability of Digital Information Systems, and Digital Ecosystem, In: International Conference on Applied Artificial Intelligence, Data Engineering and Sciences (ICAIDES), Jakarta, Indonesia, 2025, pp. 1-6, doi:10.1109/ICAIDES67265.2025.11404072.

[25] P. Morrow, et al., SWOT Analysis of Two Different Designs of Summer Professional Development Institutes for K-8 CS Teachers, In: IEEE Frontiers in Education Conference (FIE), Lincoln, NE, USA, 2021, pp. 1-9, doi:10.1109/FIE49875.2021.9637451.

[26] S. Schömbs, Communicating Internal and External Risks in Human-Robot Interaction, In: 2025 20th ACM/IEEE International Conference on Human-Robot Interaction (HRI), Melbourne, Australia, 2025, pp. 1881-1884, doi:10.1109/HRI61500.2025.10973977.

[27] S. Sarker, M. Engwall, P. Trucco, A. Feldmann, Internal Visibility of External Supplier Risks and the Dynamics of Risk Management Silos, In: IEEE Transactions on Engineering Management, vol. 63, no. 4, pp. 451-461, Nov. 2016, doi:10.1109/TEM.2016.2596144.

[28] L. Seiling, Beware: Processing of Personal Data — Informed Consent Through Risk Communication, In: IEEE Transactions on Professional Communication, vol. 67, no. 1, pp. 4-25, March 2024, doi:10.1109/TPC.2024.3361328.

[29] S. Shevchenko, Y. Zhdanova, S. Spasiteleva, P. Skladannyi, Conducting a SWOT-analysis of information risk assessment as a means of formation of practical skills of students specialty 125 cyber security. Electron. Prof. Sci. J. «Cybersecurity: Educ. Sci. Tech., 2(10), 158-168, 2020. doi:10.28925/2663-4023.2020.10.158168.

[30] D. Yao, B. García de Soto, A Preliminary SWOT Evaluation for the Applications of ML to Cyber Risk Analysis in the Construction Industry. In: IOP Conference Series: Materials Science and Engineering. 1218, 2021, doi:10.1088/1757-899X/1218/1/012017.

[31] S. Shahid, M. Bangash, M. Hussain, S. Arshad, CyberCure — Malware Defense System, In: 4th International Conference on Innovations in Computer Science (ICONICS), Karachi, Pakistan, 2024, pp. 1-7, doi:10.1109/ICONICS64289.2024.10824664.

[32] J. Edwards; G. Weaver, Cybersecurity Frameworks, In: The Cybersecurity Guide to Governance, Risk, and Compliance, Wiley, 2024, pp. 209-229, doi:10.1002/9781394250226.ch12.

[33] M. Bani-Meqdad, P. Senyk, M. Udod, T. Pylypenko, O. Sylkin, Cyber- Environment in the Human Rights System: Modern Challenges to Protect Intellectual Property Law and Ensure Sustainable Development of the Region. Int. J. Sustain. Dev. Plan., 19(4), 1389-1396, 2024. doi:10.18280/ijsdp.190416.

[34] O. Polotai, B. Polotai, O. Harasymchuk, A. Ivanusa, Development of information security policy for distance education services using risk assessment method. In: CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20-22, 2025, Kyiv, Ukraine. p. 479-495.

[35] N. Kukharska, A. Lagun, S. Semenyuk, O. Polotai, O. Hospodarskyy, M. Ozhha, Embedding a Digital Watermark into an Image Using a Hamming Code and a Solver of the Square Root of a Prime Number. In: 2025 15th International Conference on Advanced computer information technologies ACIT-2025. P. 537-541.

[36] M. Rouaf, A. Yousif, Performance Evaluation of Encryption Algorithms in Mobile Devices, In: 2020 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), Khartoum, Sudan, 2021, pp. 1-5, doi:10.1109/ICCCEEE49695.2021.9429673.