Review Article

UDC: 004.738.5:640.4(477)
004.056
doi: 10.5937/menhottur2301145B

Digital security of the hotel brand

Lyudmyla Bovsh[1], Myroslava Bosovska[1], Alla Okhrimenko[1*], Alla Rasulova[1]

[1] State University of Trade and Economics, Kyiv, Ukraine

Abstract: This article is devoted to the study of the brand digital security and its impact on the business processes of hotel businesses. The emphasis is on the fact that digital communications as key drivers of the sales system create increased risks to the security of the hotel business. The cost markers of hotel brands, operating in the market of hotel services of Ukraine in the dynamics of the pre-quarantine and post-quarantine periods are estimated. The structure of the capital's hotel services market by categories and price segments has been studied. There are described the factors related to the formation of the system of protection quality of content and information at different levels of formal and informal communications, necessary for providing digital security of the hotel brand. There are offered possible ways to increase the level of digital security based on the implementation of cyber resilience tactics in hotels, based on brand carriers and risk categories, as well as monitoring and control of informal communication channels.

Keywords: hotel brand, digital security, cyberspace, Ukraine
JEL Classification: F52, H56, D73

Digitalna sigurnost hotelskog brenda

Sažetak: Ovaj rad je posvećen proučavanju digitalne bezbednosti brenda i njegovog uticaja na poslovne procese hotelskih preduzeća. Akcenat je na činjenici da digitalne komunikacije kao ključni pokretači prodajnog sistema stvaraju povećane rizike po bezbednost hotelskog poslovanja. Procenjuju se odrednice troškova hotelskih brendova koji posluju na tržištu hotelskih usluga Ukrajine kada je u pitanju njihova dinamika u periodu pre i posle karantina. Proučavana je struktura tržišta hotelskih usluga prestonice države po kategorijama i segmentima cena. Opisani su faktori koji se odnose na formiranje sistema zaštite kvaliteta sadržaja i informacija na različitim nivoima formalnih i neformalnih komunikacija koji su neophodni za obezbeđivanje digitalne bezbednosti hotelskog brenda. Ponuđeni su mogući načini povećanja nivoa digitalne bezbednosti na osnovu implementacije taktike sajber otpornosti u hotelima koja se bazira na nosiocima brendova i kategorijama rizika, kao i praćenju i kontroli neformalnih kanala komunikacije.

Ključne reči: hotelski brend, digitalna sigurnost, sajber prostor, Ukrajina
JEL klasifikacija: F52, H56, D73

[*] a.okhrimenko@knute.edu.ua

1. Introduction

Brand forming is an imperative for the successful operation and development of a business, which often becomes a working intangible asset and brings additional income, providing the commitment of consumers. Maintaining a positive brand reputation is a difficult task in today's environment, particularly in cyberspace. After all, the main communications in the conditions of the pandemic lockdown and the war in Ukraine today have moved to the Internet environment (Prokopyuk & Chernysh, 2023). This situation provoked waves of cyber-attacks and cyber incidents (Upadhyay & Rathee, 2022). Therefore, to be an asset, brand communication platforms must become secure. In Ukraine, hotel chains are represented by both national and international brands that survived the difficult times of quarantine, and today are under the influence of constant physical threats of destruction and information wars as a result of Russia's military aggression. This led to the cessation of tourist flows – sources of loading the room stock. Therefore, the relevant task in the current perspective is to work on strengthening and developing the brand, managing databases with customer-oriented remote service, as well as protecting the brand from various threats that cause reputational and financial losses.

Oversaturation of information content, hybrid threat, cybersecurity, social engineering and digital transformation are manifestations of online communication that are progressing under the influence of pandemic quarantine. Until recently, the Internet was a promising information application, and today it often becomes a source of risks and a tool for the most powerful manipulators that can harm the brand (Odarenko & Vasylyshina, 2023). Therefore, the identification of threat sources and potential risks, brand security management is an urgent tactical and strategic task for economic entities, including the hotel business.

Thus, the main goals of the research are to formulate the definition of "digital brand security", to identify and categorize cyber risks, as well as to form approaches to ensuring the security of the hotel brand in today's realities.

2. Literature review

With the transition to a new reality in the relations of brands with consumers and stakeholders, that is, to online communications, cyber security issues become the focus of scientific research and practical insights. The main activity in the academic field falls precisely on the COVID frame time. Thus, opportunities, which mean threats in the process of accelerating digital transformation, as well as the impact on cybersecurity are described in the works of Wilson (2020) and Kalamkar and Prasad (2022). A study of awareness and understanding of information security threats in the small business sector, as well as recommendations for the formation of proactive mitigation strategies, was demonstrated in his work by Ncubukezi (2022). The security of data resources, which must be organized and at the same time characterized by confidentiality, integrity and availability, is characterized by Antczak (2022), Gawade and Shekokar (2022), Köse (2023), Mouloudj et al. (2023) and Sakhnini and Karimipour (2020).

Regarding hotel brands, the impact of the pandemic is also covered widely enough in the scientific literature and is represented by studies of a regional nature by Ghazali and Ishak (2021) – Malaysia; Khasaia and Nana Kvirtia (2021) – Georgia; Choirisa (2022) – Indonesia; Coutinho dos Santos et al. (2023) – Portugal; Kanamura (2023) – Japanese and US and others.

There is a dearth of scientific research on the cyber security of hotel brands during the global Covid-19 pandemic, and in particular military action. The articles of Arcuri et al. (2020) and

Gwebu and Barrows (2020) studied cyber attacks in the field of hospitality, while McCartney and McCartney (2020), Thomaidis (2022) and Verezomska et al. (2022) investigated the issue of cyber protection of hotel brands. With the development of artificial intelligence and its implementation in business management systems (Köse, 2023; Sakhnini & Karimpour, 2020), the issue of cyber protection will be constantly updated and will require innovative approaches in managing the security of hotel brands.

There are aspects of the hotel business as brand and security that are relevant for scientific development. Thus, the formation and promotion of the brand is quite a popular topic: branding issues are covered in the works of Faivishenko (2020), Karachyna (2017), Upshow (2015) and others. Peculiarities of brand communication support are reflected in the works of Ovsiienko (2021) and Shapovalenko (2013). In particular, the brand's communication strategy in the digital space was the subject of research by Buryak (2019), who identified points of contact with the consumer in brand perception: advertisements, news, conversations with family and friends, personal experience, etc., while Kirnosova (2021) examined the issue of brand authenticity in the communication policy of the enterprise. During the pandemic lockdown and the beginning of the war in Ukraine, the digital space expanded, as did the number of points of contact between the brand and the consumer. At the same time, a large amount of information comes from channels that brand owners do not control (Buryak, 2019). Therefore, ensuring the security of the brand is relevant today and requires special attention because you can lose consumer loyalty at the same time due to a cyber-attack, cyber incident, inadequate posting on social media, etc. In this perspective, important developments include studies by Sosnovska (2015), Tretyak and Gordiienko (2010), Zaichenko and Dima (2021), who studied theoretical issues of economic security of enterprises; Dovbnia and Hichova (2008) examined – the diagnostics of economic security of the enterprise, while Malyuk and Varypaieva (2019) and Sahirova (2021) discussed problems in ensuring the security of hotel and restaurant business services.

These scientific sources allow a detailed approach to the theoretical basis and formulate the practical feasibility of this publication, which is the relevance of identifying and categorizing risks to ensure the brand and approaches to the brand security management. The transition to digital relations, accelerated by pandemic quarantine and exacerbated by the war in Ukraine, has created many threats to business security, including reputational and financial losses. The number of cyber-attacks and cyber incidents that the hotel management has to deal with on its own has increased because such crimes often remain unsolved. Given that brands in the domestic hospitality industry have been actively developing and have positive prospects after the occupation attacks, despite the risks of destruction of property assets, protecting their intellectual property becomes a strategic task of the hotel management. For theoretical research on brand security, it is necessary to determine the key categories and concepts that form the basis of research.

Contamination of the term "brand security" involves consideration of its individual components: brand and security. Linguistically, a brand is defined as a marking, a way of identifying products (Karachyna, 2017). Practical approaches demonstrate the following points of view on the brand: for marketers – a set of product qualities that make each purchase offer unique and recognizable; for strategists – a way of managing the relationship between the organization and its target audience (Web-promo.ua, 2022).

Many scientists tend to interpret the brand as a trademark that has already gained popularity, embodies the trust of the buyer through the right marketing strategy, etc. (Table 1).

Table 1: Semantic analysis of the concept of "brand" in the scientific literature

Author	Brand – is …	Key characteristics
Anholt (2007)	a special name or symbol intended to identify the goods or services of one seller or a group of sellers, as well as to differentiate these goods or services from similar products of competitors	Differentiation and identification
Brubaker et al. (2014)	a name, term, symbol, image or combination of these elements, designed to identify goods or services of a particular manufacturer and differentiate them from competitors	
Razumov (2022)	a set of a name and other features (brand identity, logo, slogan, symbol, corporate identity, etc.) of the company or its products, forming a holistic image that determines their differences from competitors in the perception of potential consumers	
Ogilvi (2007)	elusive set of product qualities, its name, packaging and price, its history, reputation and methods of advertising	Identification and advertising
Moroz (2003)	a consistent set of functional, emotional, psychological and social promises to the target consumer that are unique and meaningful to them and best meet their needs	Emotional impact on consumer needs satisfaction
Kapferer (2017)	a name that influences the behavior of market buyers, becoming a criterion for purchase	Emotional consumer choice
Tamberh & Badyn (2015)	the result of communicative influence, which is in the creation of a unique and attractive image of the object of consumption	The result of communicative influence
Zozulyov & Nesterova (2018)	successfully differentiated brand, which in the minds of consumers is associated with certain advantages and benefits, clearly distinguished from competing brands and characterized by a high level of loyalty from consumers	differentiated brand that creates high loyalty through the benefits and advantages
Davis et al. (2002)	intangible but critical to the organization component that it owns, and is a kind of contract with the consumer about the level of quality and value received by them, inherent in the goods or services of this organization	Intangible contract, which confirms the quality and value of the product

Source: Compiled by the authors

The concepts presented in Table 1 allow us to formulate a complementary definition of a brand: an intangible asset that identifies the value of the object (location, business, product, etc.) through communicative influence on the consumer, forming his a priori or a posteriori inclination (loyalty). The hotel brand is an image of the expected comfort and atmosphere in the premises (lobby, room, restaurant, etc.) and a certain level of service, which is confirmed by its category and consumer experience of online audiences (reviews on the site, reviews, social media, distribution platforms). etc). Regarding the term "digital security", comparative studies, according to scientific sources (Table 2), show a fairly wide range of meanings.

Contamination of the structural elements of the presented approaches (Table 2) allows us to interpret digital security as a set of measures to protect, defend, prevent and neutralize threats to the subject from the likelihood of harm, damage to its interests and property during using cyberspace.

Table 2: Comparative analysis of the concept of digital security

Source	Definition	Structural elements
Safety – is …		
Cambridge dictionary	things that are done to secure someone or something; a situation in which something is likely to fail or be lost; self-confidence and the situation in which you are; protection of information from theft, used illegally or illegally	security, situation of probable failure / loss; protection
Malyuk & Varypaieva (2019)	absence of any kind of danger and threat that can cause unacceptable damage (damage)	absence of danger and threat
Tyhiy (2016)	captures the dominant way of existence of the object as a state in which someone, for some reason is not in danger	as a state when there is no danger
Industrial safety – is …		
National standard of Ukraine-DSTU 2293 (2014)	protection of life, health of workers and other people and / or property from the influence of harmful and dangerous production factors	protection from the influence of harmful and dangerous factors
Economic security – is …		
Dovbnia & Gichova (2008)	An ability of the enterprise to effective functioning (now) and successful development (in the future)	effective functioning and development
Sosnovska (2015)	universal category that reflects the security of the subjects of socio-economic relations at all the levels, starting from the country to each of its citizens	security of subjects
Tretyak & Gordiienko (2010)	transformations aimed at improving the functioning of individual enterprises, their associations and entrepreneurs	transformations aimed at improvement
Informational security – is …		
Rohova (2020)	public relations on the creation and maintenance of the regime of information systems, telecommunications systems; a set of measures to protect, defend, prevent and overcome natural and socio-genic threats	a set of measures to protect, defend, prevent and overcome threats
Cyber-security – is …		
Law of Ukraine	protection of vital interests of people and citizens, society and a country during the use of cyberspace, which ensures sustainable development of information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to national security of Ukraine in cyberspace	the state of interest protection during using cyberspace
Indevlab (2022)	protection against viruses, hacker attacks, data forgery, which can apart from deleting / stealing data, but also affect the work and productivity of employees, use information against a person or structure, and stop production	protection against viruses, hacker attacks, data forgery

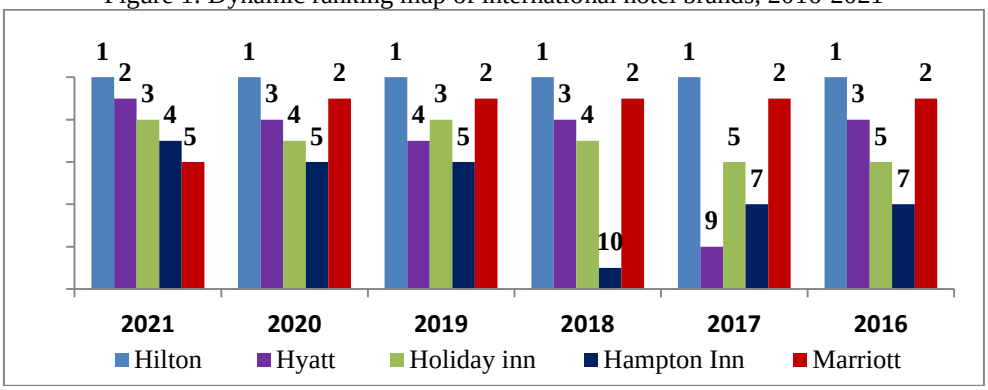
Source: Compiled by the authors

3. Results and discussion

Brand safety is ensured by a set of measures, the main task of which is to protect the brand from the information environment that negatively affects its image and mission: mentioning the hotel in content that contradicts its policy and corporate culture, etc. This challenge requires online marketing activity in an environment that is compatible with the brand and promotes its values. The biggest reputational threats posed by the Internet environment concern well-known brands. Cybersecurity experts note that hackers are targeting large corporations, with online fraud increasing by 12% year-over-year, including loyalty programs, by 89% (Edgedefense, 2023). Information attacks, hacking of online platforms and databases are initiated and carried out by both competitors and criminals for the purpose of blackmail or other fraud. In addition, the hacking of customer databases and their accounts is aimed at seizing customer funds, the hotel brand itself, spoiling the hotel's image and reputation as a partner. Indeed, in 2018, Marriott announced a security incident in its guest reservation database. The unauthorized access to the database, which contained guest information, took place between 2014 and 2018 (Marriott, 2018). Loyalty and rewards programs are vulnerable for hotel brands because the hotel operator must constantly protect these rewards and loyalty accounts from hacking and theft by cybercriminals.

A separate point is the imitation of the website (brand book) of the hotel brand. To this end, it is important to study the top brands that have a significant customer base and significant cash flows – which means that they are the targets of cybercrimes and require the development of cyber protection and insurance measures. In particular, bright representatives of hotel brands are international hotel operators. According to the annual report on the most expensive and strongest hotel brands in the world (Brandirectory, 2021), the TOP-5 rating scale for the past 6 years looks as follows (Figure 1).

Figure 1: Dynamic ranking map of international hotel brands, 2016-2021



Source: Brandirectory (2021)

The analysis shows that in 2016-2021 the top positions of the rating do not change, which indicates the stability of hotel operators in the world market. Hotel brands Hilton and Marriott remain the undisputed leaders, although the Covid-19 period significantly reduced their positions in 2021. The Standard & Poor's Credit Score Survey shows a rating of hotel brands, with the highest AAAs being those with the highest quality financial obligations and the highest level of bond reliability. Accordingly, in value terms, Hilton retains the status of the most expensive hotel brands in the world (Table 3), despite the loss of capitalization by 30% compared to 2020.

Table 3: Evaluation markers of brands of international hotel operators for 2018-2021

Rating in 2021	Brand name	Brand evaluation parameters	Years			
			2018	2019	2020	2021
1	Hilton	value, billion dollars	6,330	8,023	10,833	7,610
		credit scoring	AAA-	AAA-	AAA-	AAA-
2	Hyatt	value, billion dollars	3,512	3,677	4,532	4,695
		credit scoring	AA+	AA	AA	AA+
3	Holiday Inn	value, billion dollars	3,292	3,945	4,496	3,776
		credit scoring	AAA	AAA	AAA-	AAA-
4	Hampton Inn	value, billion dollars	1,784	3,182	3,871	2,863
		credit scoring	AAA-	AAA-	AAA-	AAA-
5	Marriott	value, billion dollars	5,464	5,039	6,028	2,408
		credit scoring	AAA-	AA+	AA+	AAA-

Source: Brandirectory (2021)

Therefore, the hotel brands in question remain the focus of cybercrimes. In total, the cost of the world's 50 most expensive hotel brands fell by 33% ($ 22.8 billion) as a result of the pandemic. The Hyatt brand is the fastest growing in the TOP-10 and one of the two brands that recorded an increase in its value by 4% (Figure 2).

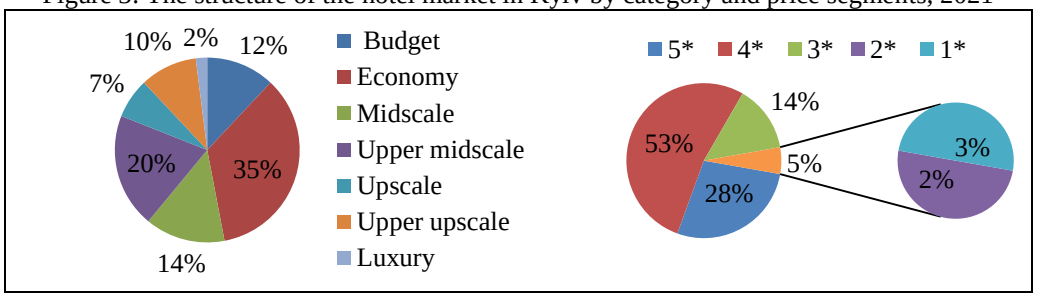
Figure 2: Dynamics of the value of international hotel brands, 2016-2021

Source: Brandirectory (2021)

However, despite the pandemic crisis, the need to protect customer databases, loyalty and rewards programs, as well as the financial accounts of hotel brands still remains a priority for the management of hotel operators and the hotels that are part of their network. After all, the popularity of the brand is information for criminals that there is a significant financial benefit in case of hacking.

It should be noted that hotel operators shown in Figure 2, in addition to Hampton Inn, are represented in the hotel market of Ukraine, including the capital. Evaluating the hotel services market of the capital of Ukraine as the most economically attractive, it should be noted that there are some significant financial losses due to the pandemic quarantine over the past two years, but, nevertheless, it is less than in most of the larger European cities. Thus, in Prague, hotel occupancy in 2020 fell by an average of 4.6 times per year, in Warsaw – by 2.7 times, in Geneva – by 2.6 times, in Kyiv – by 1.9 times (Artbuild, 2021). However, the start of a full-scale war in Ukraine created a springboard for information attacks and hacking aimed at destroying the country's economy, in particular by destroying brands. Therefore, studying the listing of hotel brands in the capital of Ukraine is an urgent issue in the formation of cyber protection, in particular at the national level. Today, the Kyiv hotel market is represented in various price segments (Figure 3).

Figure 3: The structure of the hotel market in Kyiv by category and price segments, 2021

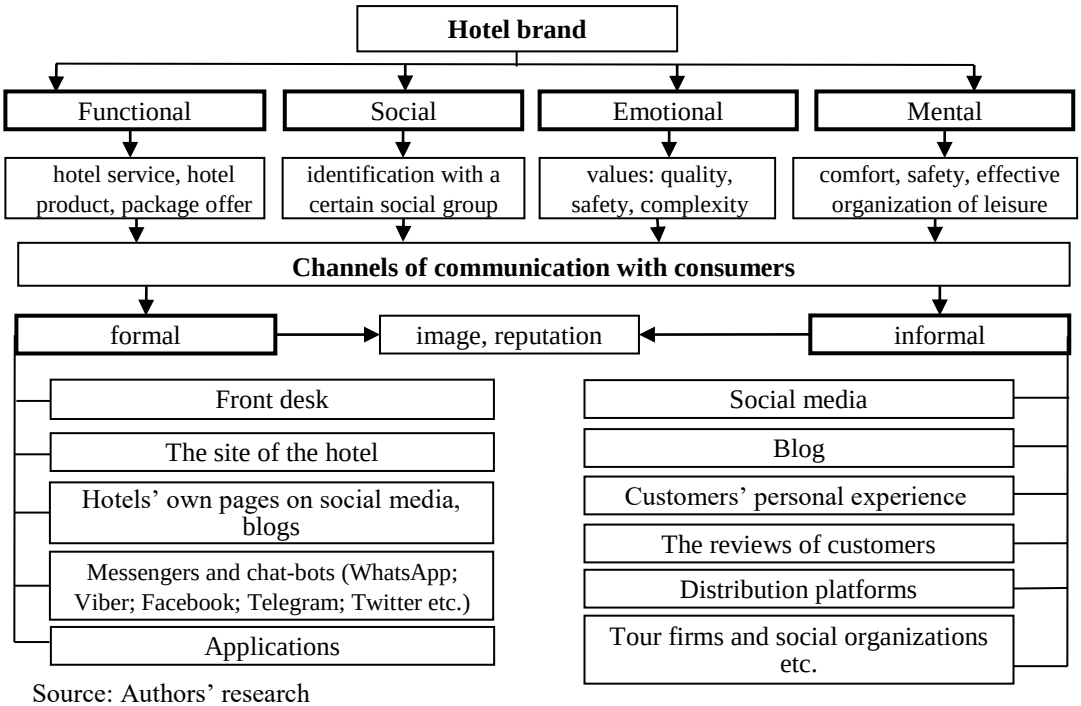


Source: Artbuild (2021)

Among the presented categories, in particular 3-, 4-, and 5- star hotels, there are domestic brands, represented by both chain and autonomous hotels. Among the chain ones, we should mention Premier Hotels and Resorts, Reikarts Holes Group, Black Sea Hotels Group, Royal Hotels and SPA Resorts, "7 days", which include brands differentiated by the level of comfort and regional distribution. If autonomous hotels personally take care of brand security, then for chain hotels it is a complex task, which consists of both individual and complementary brand security.

To form approaches to managing the security of the hotel brand, consider its components – potential sources of threats (Figure 4). At the same time, summarizing the image of the hotel product, its concept can be reflected as a four-dimensional adapted structure. In particular, formal communication channels are structured in the hotel services market by the hotel itself and with participants in economic interaction, including informing and consulting, influencing the creation of the concept of brand functionality. Informal – consumers, bloggers who form the social, emotional and mental values of the hotel product.

Figure 4: Sources of communication support for the hotel brand



Source: Authors' research

The above allows us to state that the digital security of a hotel brand depends on the quality of the content and information protection system at various levels of formal and informal communications. We summarized the processed information and systematized protection levels by protection objects (Table 4).

Table 4: Levels and objects of protection in the digital security system of the hotel brand

Objects of protection	**Protection levels**	**Characteristics**
Consumer interests	*Physical security (protection of property and values)*	– fire safety systems, control of the critical infrastructure of the hotel building (electricity, water, energy supply, etc.) and access to the hotel by third parties; – electronic (mobile) keys to hotel rooms; systems of protection of property and values of consumers
	Security of personal data (protection of guest privacy)	– system of protection of consumer profiles, information on the status and peculiarities of the stay of guests, etc.; – protection system of financial online transactions, personal accounts and electronic wallets, including cryptocurrencies
	Security of communication	– reliability of available information online and offline on sales channels; – CRM-platforms - systems of interaction with consumers; – established system of geoanalytics, geoservices and geomap; – complex service of feedback and NPS like Revision; – customer-oriented support (chat-bots, messengers, social networks) etc
Systems and resources of the hotel's internal environment	*Security of property and values of the hotel*	– internal system of protection and intrusion protection; – automated systems of accounting for the movement and reporting of tangible assets in different departments.
	Financial security	– system of protection of internal confidential information on the current financial condition, data transmission of a commercial nature, etc.
	Informational security	– anti-virus data protection databases on internal servers; – protection against hacker attacks
	Security of the hotel product sales system	– coordinated functioning of the internal property management system (Internal Property Management System) with the network of distributors of hotel services; – established communication system on various platforms of aggregation of hotel services (OTA - online travel agents, IDS - Internet distribution systems, ADS - alternative distribution systems, GDS - global distribution systems (Amadeus, Saber, Worldspan, Galileo) – protection of the brand book (site) of the hotel
	Reputation and image security	– system of external communication with the mass media, society; – monitoring of content about the hotel brand in the information space

Source: Authors' research

Each interpreted component involves the identification of interested parties at a certain level of protection. Thus, the consumer's interests include physical security (protection of property and valuables), which can be caused by cyber-interference in the hotel's integrated security

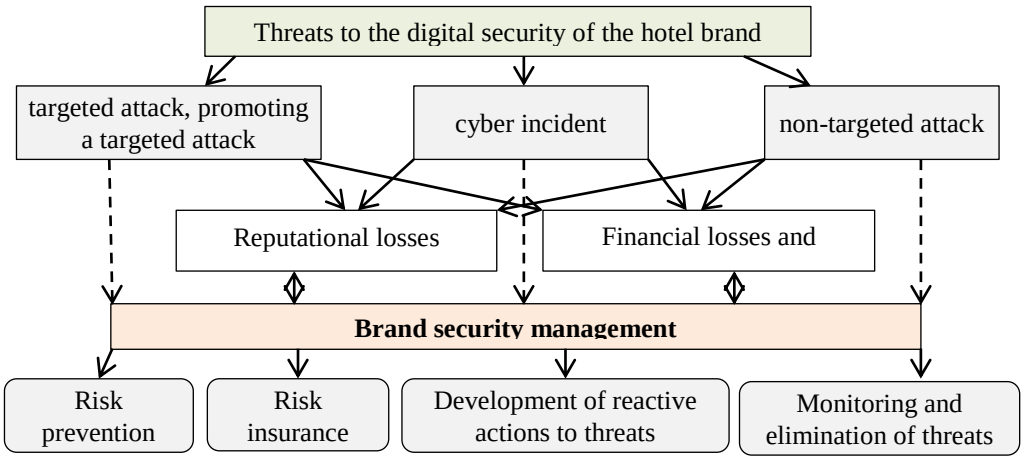
system and giving criminals access to rooms, hidden cameras, safes, etc. Security of personal data, as already mentioned earlier, discloses commercial (current and card accounts, blockchain and electronic wallets, IP addresses, accrued rewards, etc.) and personal information about the hotel's customers, partners and beneficiaries (owners). This information can lead to money theft, data corruption, blackmail, etc.

The increase in demand for information from all parties (hotel brands, their customers and stakeholders) has drawn attention and raised concerns about security, as noted by many of the scientific studies we reviewed (Arcuri et al., 2020; Gwebu & Barrows, 2020; Ncubukezi, 2022) The digital dependency created by online communications facilitates attackers to exploit vulnerabilities in every sector (Kalamkar & Prasad, 2022), including the operation of hotel brands. Therefore, the determinant of the cyber security of a hotel brand is its internal business processes and communication platforms.

The results of our research in the academic field showed that a pandemic crisis, multiplied by a military one, destabilizes the work of hotel brands at various points of contact in the communication process (Prokopyuk & Chemsysh, 2023; Ulynets, 2022): 1) staff as a bearer of the brand in a crisis situation do not have coherent position and script for response and action, and therefore can spread misinformation and rumors; 2) partners and counterparties who do not understand internal processes in the hotel may refuse to cooperate; 3) media workers and the public, who can spread unreliable data, unsupported by comments and facts; 4) clients with whom communication can be completely lost. Therefore, the intellectual (in particular, informational) resources of the hotel brand, which are its property and communication tools, need cyber protection. And in the difficult crisis situation that the market of hotel services of Ukraine is experiencing today, the effective use of digital skills turns out to be a factor of sustainability (Bondarenko, 2021) of the hotel brand.

The application of the specified objects and risks requires the creation of a "layer" that will ensure cyber-protection of the hotel's digital security through the creation of countermeasures (insurance, withdrawal of assets to a safe digital/financial zone, etc.) and tools (antivirus, anti-hacker and other services and protection platforms). This allows us to state that the digital security management of the hotel brand will be aimed at achieving protection of the brand from possible reputational and financial threats and stress, provided by constant monitoring and controlling the communication process in particular information and cyber environment, business partners, etc. (Figure 5).

Figure 5: Model of digital security management of the hotel brand



Source: Created by the authors

Solving this current problem of digital security involves creating a favorable business environment, ensuring consumer loyalty, preventing conflicts of interest, distribution of managerial powers, etc., as well as a rapid response to new environmental challenges (war, pandemic, innovation, increasing the role of human intelligence, globalization of the economy). Digital brand security management of the hotel brand is required through innovative digital methods and social technologies.

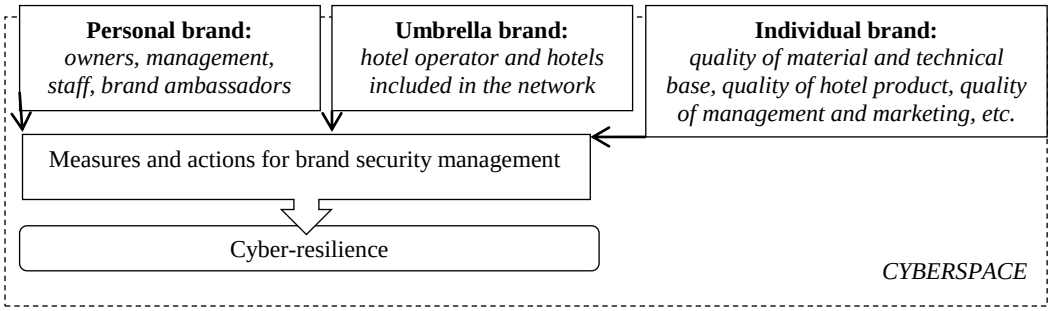
At the same time, risk prevention consists of their identification and categorization. Yes, they are divided into the following groups: business, organizational and technical (Mukherjee, 2019).

Business risks (or business process risks) are associated with economic activities and, when incurred, reduce the financial benefits and value of the brand, provoking financial losses. Organizational risks, in turn, are related to the hotel staff, as insufficient experience in cloud technology and cyberspace in general can lead to serious business disruptions. A separate point should be noted – organizational issues of the operational context of the hotel as a user and cloud provider. Technical risks include problems that may arise when interacting with cyberspace: the impact of malicious code on the cloud platform, attacks at the hypervisor level, data leakage, system failures or unauthorized transmission, and so on. In particular, the loss of privacy for the hotel will also mean reputational losses, which are almost impossible to recover.

In light of of recent events in Ukraine, we propose to identify more information and military risks. Many brands have left the Russian market amid strong international sanctions, condemning the war. Currently, there is no information about hotel brands and their motives in the Russian market, but, for example, Booking.com and Airbnb no longer allow you to search for and book accommodation in the Russia (Zaborona, 2022). Moreover, they inspired the purchase of beds in Ukraine, directing the funds to humanitarian causes. As for support activities, a volunteer headquarters have been set up in Odessa at the initiative of the Ribas Hotels Group (2022), and the Reikartz Hotel Group (2022) is hosting guests in areas far from fire with heightened security measures.

In view of the above, risk insurance is an important task of ensuring brand security, as insurance indemnities cover such hotel costs as (Mamonova & Pozdniakova, 2020): information security breaches due to viruses, destruction, modification or deletion of information, physical theft or loss of equipment; damage to software or computers; theft or destruction of information. In the event of a cyber-incident, there are costs for legal support, coverage of fines and penalties; legal costs related to liability for hacking a database of confidential information. In the case of phishing and karting technologies, which resulted in the loss of funds and assets of the hotel, prevention tactics (competent management of protection systems), insurance and rapid response to recover reputational and financial losses are also possible. Given the above areas of digital security management, we offer to implement in the hotel brand (personal, umbrella, individual) tactics of cyber resilience, based on brand carriers and risk categories (Figure 6).

Figure 6: Complementary tactics of cyber-resilience of hotel brand carriers



Source: Boyko (2010); Bovsh et al. (2021); Finansovaentsyklopediia (2021); Zozulyov & Nesterova (2018)

Thus, the management of formal channels of communication is to form a model of tactical behavior of all participants influencing the brand: personal, network and individual content in cyberspace must match and relate to the values and corporate culture of the hotel and society as a whole.

Regarding the management of hotel brand security through informal communication channels provides for the following actions (Koch, 2021; Ulynets, 2021):

1) digital hygiene: reputational protection against contact with Russian and Belarusian channels (consumers, marketplaces, etc.), placement on their own channels only verified and reliable information, etc.;
2) constant review and updating of brand security settings to prevent the display of hotel advertising alongside negative content, including Audience Network, Facebook and Instagram, etc.;
3) content filtering and inventory, which gives an additional level of control over confidential content in instant articles and blogs Facebook, Facebook In-stream, Instagram In-stream and Audience Network;
4) exclusion of topics for embedded videos on social media;
5) exclusion of content types in partner platforms: stop showing Facebook In-stream ads in live videos, as well as those published by non-partners, but monetized by the owners of intellectual property rights; creating block lists that prevent advertisements from appearing by certain publishers, Facebook In-Stream videos, instant Facebook articles, In-stream videos on Instagram and overlay Facebook ads on Reels, etc .; formation and selection of publisher permission lists: Audience Network, Instagram In-Stream and Facebook In-stream, in which hotel ads are displayed;
6) view and configure the lists of permitted content in the Brand Safety Controls interface to control information messages in terms of ensuring the authenticity and confidentiality of certain data;
7) view reports about the hotel information.

Approbation of the proposed measures is confirmed by the practical results of the research. Thus, with the help of the resource SimilarWeb – the official tool for measuring digital space, analytics was developed to evaluate the websites of the TOP-5 hotel brands and determine their place in the system of informal communications, including service distribution (Table 5).

Analysis of the sources of traffic on brand.com showed a high rating of consumer awareness of the websites of hotel brands, which ranges from 39.5 to 49.0%. The high level of

consumer trust in the hotel product requires increased attention to the development and protection of this communication channel.

Undoubtedly, the COVID-19 pandemic has become an objective reality of the deteriorating situation in the hotel services market. However, most entities have used this time to innovate and deepen the digitalisation of commercial space. Digital technologies are implemented in the attributes of the hotel brand, the success of which depends, inter alia, on the quality of the system of protection of content, information and other values at different levels. The mentioned measures to ensure the digital security of the hotel brand are not exhaustive and are constantly updated in connection with the development of digital innovations: technologies, services and payment systems. Thus, digital security is formed from such components as people (brand carriers and stakeholders), technology (information, distribution, marketing) and business processes (communication, guest cycles, calculations, etc.), which in the cyber environment create innovative competence of the hotel brand – cyber resilience.

Table 5: Website analysis of the TOP-5 brands of international hotel operators

Site evaluation parameters	**The name of the website**				
	hilton.com	hyatt.com	ihg.com	hamptoninn.com	marriott.com
Rating in the category Travel and Tourism/ Accommodation and Hotels	8	14	9	n/d	4
Traffic view					
total visits, million	25.60	9.96	14.96	n/d	39.90
the average duration of page visits	00:05:17	00:05:37	00:03:55	n/d	00:05:06
the average number of web pages viewed per visit	5.11	4.49	4.28	n/d	4.54
refusal of further actions, %	35.26	42.81	42.63	n/d	43.70
Traffic sources for brand.com					
direct	41.77%	39.54%	49.06%	n/d	39.70%
referral	6.37%	9.91%	12.59%	n/d	10.72%
Metasearch	44.57%	46.38%	34.08%	n/d	39.28%
Social media	1.07%	1.07%	1.21%	n/d	2.09%
Email	3.64%	1.93%	1.84%	n/d	5.70%
media	2.59%	1.17%	1.21%	n/d	2.51%

Source: Compiled by authors based on Similarweb (2021)

4. Conclusions

The research showed the relevance of constant work on the hotel brand, which is exposed to risks, in particular in cyberspace. Therefore, the development of a scientific approach to digital brand security today is the basis for the formation of innovative tactics of management and development in today's economic environment, when every careless response or post on the Internet becomes the beginning of the end for a business.

The operationalization of the theoretical basis was carried out on the basis of approaches formulated in the scientific literature to the definition of the terms "brand" and "security". Thus, digital security is presented in the research as a set of measures to protect, safeguard, prevent and neutralize the threats to the subject from the likelihood of damage, harm to his interests and property while using cyberspace.

The meaningful characteristics of these definitions were formed, revealing the a priori probabilities of strengthening certain components of hotel brand security in general: people (brand carriers and relationship participants), technologies and business processes that shape communications, particularly in cyberspace. Based on these communications (formal and informal channels), proposals have been developed for managing the digital security of the hotel brand: risk prevention and insurance, reactive response to threats, monitoring and elimination of threats.

Since the brand as a result of the communicative process consciously creates a unique image of a quality and valuable product and forms a lasting emotional attachment to a consumer, in the digital space, security will be aimed at protecting and preserving these values.

The pandemic crisis has had a negative impact on the financial stability of hotels, leading to savings, including the use of cybersecurity consulting and outsourcing services and the retention of relevant staff. However, the greatest danger, including digital, is Russia's military invasion, which completely destroys urban infrastructure and tourist attractions - that is, Ukraine's tourism potential in general. Therefore, the proposed measures for brand security management are the optimal tactics for risk protection of the hotel business in today's conditions and promising for strategic foresight.

The process of collecting and processing the research material encountered problems and limitations related to the practical lack of fact-finding on the results of the impact of the coronavirus pandemic on hotel brands in Ukraine. In addition, the escalation of the war time frame does not yet allow an objective assessment of the impact of information wars, in particular cyber-attacks and cyber incidents on Ukrainian hotel brands and those that remained operating in the aggressor country. In addition, due to military stressors that create obstacles in direct communications with hotels, carry out tests of proposed cyber security measures. Further research is possible in the post-war period and will include the study of effective practices and examples of resistant strategies and tactics of Ukrainian hotel brands in countering cyber threats. It is also promising to study the impact of artificial intelligence on the cyber security of hotel brands and evaluate its role from a legal, economic, social and ethical point of view.

Conflict of interest

The authors declare no conflict of interest.

References

1. Anholt, S. (2007). *Competitive identity: The new brand management for nations, cities and regions* (1st ed.). PalgraveMacmillan.
2. Antczak, J. (2022). The impact of the Covid-19 pandemic on business entity cyber security. *Inżynieria Bezpieczeństwa Obiektów Antropogenicznych*, *1*, 7–15. https://doi.org/10.37105/iboa.128
3. Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080
4. Artbuild. (2021). *ABHG: Overview of the Kyiv hotel real estate market as of October 2021*. Retrieved February 6, 2023 from http://artbuild.ua/ua/category_13/item_82.html
5. Bondarenko, O. (2021). Impact of the Covid-19 pandemic on the formation of digital skills. *Grail Of Science*, 150–154. https://doi.org/10.36074/grail-of-science.19.11.2021.026
6. Bovsh L., Bosovska M., & Okhrimenko A. (2021). Compliance-strategizing of economic security of the business in digitalization conditions. *Herald of KNUTE*, *6*, 42–60. http://doi.org/10.31617/visnik.knute.2021(140)03
7. Boyko, M. (2010). Organizational and economic mechanism of national brand formation. *Theoretical and Applied Issues of Economics*, *21*, 304–311.
8. Brandirectory. (2021). *Hotels 50 2021. The annual report on the most valuable and strongest hotel brands*. Retrieved February 6, 2023 from https://brandirectory.com/rankings/hotels
9. Brubaker, P., Mower, J., Curtis, M., & Gillespie, I. (2014). Global brands and message content: the use of images in social media. *Proceedings from the 17th International Public Relations Research Conference* (pp. 62–72). http://www.instituteforpr.org/wp-content/uploads/IPRRC17-Proceedings.pdf
10. Buryak, T. (2019). Brand communication strategy in the digital society. *Abstracts of reports of the international scientific and practical conference KNTEU*. http://dx.doi.org/10.31617/k.knute.2019-03-19.24
11. Cambridge dictionary (n.d.). *Security*. Retrieved February 10, 2023 from https://dictionary.cambridge.org/dictionary/learner-english/security
12. Choirisa, S. F. (2022). The impact of the Covid-19 pandemic on the hotel industry in Indonesia. *Economics Management and Sustainability*, *7*(1), 86–94. https://doi.org/10.14254/jems.2022.7-1.7
13. Coutinho dos Santos, M., Magano, J., & Mota, J. (2023). The impact of the Covid-19 pandemic on the hotel industry's economic performance: Evidence from Portugal. *Heliyon*, *9*(5), e15850. https://doi.org/10.1016/j.heliyon.2023.e15850
14. Davis, S. M., Duun, M., & Aaker, D. A. (2002). *Building the brand-driven business: Operationalize your brand to drive profitable growth* (1st ed.). Jossey-Bass.
15. Dovbnya, S., & Gichova, N. (2008). Diagnostics of the level of economic security of the enterprise. *Finances of Ukraine*, *4*, 88–97. Retrieved February 10, 2023 from http://nbuv.gov.ua/UJRN/Fu_2008_4_11
16. *Economic security of enterprises, organizations, institutions* (n.d.). Retrieved February 15, 2023 from https://pidru4niki.com/1822061151265/ekonomika/osnovi_ekonomichnoyi_bezpeki_pidpriyemstva
17. Edgedefence. (2023). *Why do cybercriminals love brand loyalty programs?* Retrieved February 10, 2023 from https://edgedefence.com/uk/blog/why-cybercriminals-love-brand-loyalty-programs

18. Faivishenko, D. (2020). Brand strategy: Planning tools. *Scientific Support of Technological Progress of the 21st Century*. International Center for Scientific Research. http://dx.doi.org/10.36074/01.05.2020.v1.03
19. Financial encyclopedia (n.d.). *Types of cyber attacks*. Retrieved February 15, 2023 from https://ua.nesrakonk.ru/cybersecurity
20. Gawade, A., & Shekokar, N. M. (2022). Impact of cyber security threats on IoT applications. In N. Shekokar, H. Vasudevan, S. Durbha, A. Michalas, T. Nagarhalli, R. Mangrulkar & M. Mangla (Eds.), *Cyber Security Threats and Challenges Facing Human Life* (pp. 71–80). Chapman and Hall/CRC https://doi.org/10.1201/9781003218555-8
21. Ghazali, H., & Ishak, M. (2021). Managers view on impact of Covid-19 pandemic: Evidence from hotel industry in Malaysia. *International Journal of Human Resource Studies*, *11*(1), 116–129. https://doi.org/10.5296/ijhrs.v11i1.17927
22. Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: Is the industry different? *Journal of Hospitality and Tourism Technology*, *11*(3), 511–527. https://doi.org/10.1108/JHTT-11-2019-0138
23. Indevlab. (2021). *Information security and cyber security – what is the difference?* Retrieved February 15, 2023 from https://indevlab.com/uk/blog-ua/informatsijna-bezpeka-i-kiberbezpeka-v-chomu-riznitsya/
24. Kalamkar, M. D., & Prasad, R. (2022). Impact of the COVID-19 pandemic on cyber security issues in the healthcare domain. In N. Shekokar, H. Vasudevan, S. Durbha, A. Michalas, T. Nagarhalli, R. Mangrulkar & M. Mangla (Eds.), *Cyber Security Threats and Challenges Facing Human Life* (pp. 24–41). Chapman and Hall/CRC https://doi.org/10.1201/9781003218555-4
25. Kanamura, T. (2023). An impact assessment of the COVID-19 pandemic on Japanese and US hotel stocks. *Financial Innovation*, *9*(1), 87. https://doi.org/10.1186/s40854-023-00478-2
26. Kapferer J. N. (2012). *The new strategic brand management: Advanced insights and strategic thinking (New strategic brand management: Creating & sustaining brand equity)* (5th ed.). Kogan Page.
27. Karachina, N. P. (2017). *Etymology and development of interpretation of the economic category "brand"*. Retrieved February 10, 2023 from https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2017/paper/view%20File/3025/2228
28. Khasaia, I., & Kvirtia, N. (2021). Impact of pandemic on the hotel business in Imereti (Georgia). *World Science*, *3*(64). https://doi.org/10.31435/rsglobal_ws/30032021/7512
29. Kirnosova, M. (2021). Authenticity of brands in the marketing commodity policy of the enterprise. *VUZF Review*, *6*(3), 78–89. https://doi.org/10.38188/2534-9228.21.3.09
30. Koch, T. (2021). *Brand safety – hum or threat?* Retrieved February 10, 2023 from https://morethandigital.info/ru/byezopasnost-bryenda-%CA%90oo%CA%90%CA%90aniye-ili-ooguroza/ (in Ukr)
31. Köse, A. (2023). Artificial intelligence in health and applications. In A. C. Bouarar, K. Mouloudj & D. M. Asanza (Eds.), *Integrating digital health strategies for effective administration* (pp. 20–31). IGI Global. https://doi.org/10.4018/978-1-6684-8337-4.ch002
32. *Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine"* (n.d.). Retrieved February 12, 2023 from https://zakon.rada.gov.ua/laws/show/2163-19#Text
33. Malyuk, L., & Varipayeva, L. (2019). Theoretical foundations of service security. Restaurant and hotel consulting. Innovations. *KNUKiM*, *2*(1), 134–143. http://dx.doi.org/10.31866/2616-7468.2.1.2019.170431 (in Ukr)
34. Mamonova, G., & Pozdniakova, L. (2020). Features of cyber risk insurance. *Interdisciplinary Scientific Research: Features and Trends*, *2*. http://dx.doi.org/10.36074/04.12.2020.v2.12 (in Ukr)

35. Marriott. (2018). Marriott announces security incident in Starwood's guest reservation database. Retrieved February 10, 2023 from https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/
36. McCartney, G,. & McCartney, A. (2020). Rise of the machines: Towards a conceptual service-robot research framework for the hospitality and tourism industry. *International Journal of Contemporary Hospitality Management*, *32*(12), 3835–3851. https://doi.org/10.1108/IJCHM-05-2020-0450
37. Melnychenko, S., Bosovska, M., & Okhrimenko, A. (2021). The formation of a nation tourism brand of Ukraine. *Baltic Journal of Economic Studies*, *7*(2), 161–169. https://doi.org/10.30525/2256-0742/2021-7-2-161-169
38. Moroz, O. V. (2003). *The theory of modern branding: A monograph*. Vinnytsia: Universum-Vinnytsia.
39. Mouloudj, K., Bouarar, A. C., Asanza, D. M., Saadaoui, L., Mouloudj, S., Njoku, A. U., ... & Bouarar, A. (2023). Factors influencing the adoption of digital health apps: An extended Technology Acceptance Model (TAM). In A. C. Bouarar, K. Mouloudj & D. M. Asanza (Eds.), *Integrating Digital Health Strategies for Effective Administration* (pp. 116–132). IGI Global. https://doi.org/10.4018/978-1-6684-8337-4.ch007
40. Mukherjee, S. (2019). Enterprise risk management for the implementation of cloud security. *SSRN Electronic Journal*. 3435908. http://dx.doi.org/10.2139/ssrn.3435908
41. National standard of Ukraine. (2014). *Occupational health. Terms and definitions of basic concepts. DSTU 2293*. Retrieved February 5, 2023 from https://zakon.isu.net.ua/sites/default/files/normdocs/2-9773-ohorona_praci._terminy.pdf
42. Ncubukezi, T. (2022). Impact of information security threats on small businesses during the Covid-19 pandemic. *European Conference on Cyber Warfare and Security*, *21*(1), 401–410. https://doi.org/10.34190/eccws.21.1.453
43. Upadhyay, N. K., & Rathee, M. (2022). Cyber security in the age of Covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Medicine, Law & Society*, *15*(1), 89–106. https://doi.org/10.18690/mls.15.1.89-106.2022
44. Odarenko V., & Vasylyshina L. (2023). The impact of war on consumer behavior in terms of brand perception. Brand management: marketing technologies. In A. Mazaraki (Ed.), *V International science and practice conference*. Kyiv: State. trade and economy University. https://doi.org/10.31617/k.knute.2023-03-14
45. Ogilvy, D. (2013). *Ogilvy on advertising*. Random House Publishing Group.
46. Ovsienko, N. (2021). *Optimizing the toolkit of the marketing policy of brand activity communications. Economy and society*. Publishing House Helvetica (Publications). http://dx.doi.org/10.32782/2524-0072/2021-24-47
47. Prokopyuk V., & Chernysh T. (2023). Promotion of the brand in the conditions of martial law. Brand management: marketing technologies. In A. Mazaraki (Ed.), *V International science and practice conference*. Kyiv: State. trade and economy University. http://dx.doi.org/10.31617/k.knute.2023-03-14
48. Verezomska I., Bovsh L., Baklan H., & Prykhodko K. (2022). Cyber protection of hotel brands. *Restaurant and Hotel Consulting Innovations*, *5*(2), 190–210.
49. Prykazyuk, N., & Humenyuk L. (2020). Cyber insurance as an important tool for the protection of enterprises in the conditions of digitalization of the economy. *Efficient economy*, *4*. http://dx.doi.org/10.32702/2307-2105-2020.4.6
50. Razumov, D. (2019). *Brand. About marketing*. Retrieved February 5, 2023 from http://aboutmarketing.info/osnovy-marketynhu/brand/ (in Ukr)
51. Reikartz Hotel Group (2022). *Homepage*. Retrieved February 10, 2023 from https://reikartz.com/uk/
52. Ribas Hotels Group (2022). *Homepage*. Retrieved February 5, 2023 from https://ribashotelsgroup.ua/en/

53. Rohova, E. I. (2020). Theoretical foundations of legal provision of information security. *Actual Problems of the State and Law*, *86*, 190–196. http://dx.doi.org/10.32837/apdp.v0i86.2436
54. Sahirova, A. (2021). Ensuring economic security in the hotel business with the help of innovations. *Pryazovsky Economic Bulletin*, *1*(24). http://dx.doi.org/10.32840/2522-4263/2021-1-17
55. Sakhnini, J., & Karimipour, H. (2020). AI and security of cyber physical systems: Opportunities and challenges. *Security of Cyber-Physical Systems: Vulnerability and Impact*, 1–4. https://doi.org/10.1007/978-3-030-45541-5_1
56. Shalamanov, V, & Mladenova, I. (2021). *Digital transformation and cyber resilience*. http://dx.doi.org/10.11610/cybsec04bg
57. Shapovalenko, K. S. (2013). Methodology of brand communication support. *Bulletin of the National Technical University "KhPI". Technical Progress and Production Efficiency*, *45*, 115–121. Retrieved February 10, 2023 from http://nbuv.gov.ua/UJRN/Vcpitp_2013_45_18
58. Similarweb (n.d.). *Website traffic – Check and analyze any website*. Retrieved April 10, 2023 from https://www.similarweb.com
59. Sosnovska, I. (2015). *The concept and significance of economic security of production and economic activity of enterprises*. Retrieved February 10, 2023 from http://www.economy.nayka.com.ua/?op=1&z=4303
60. Tamberg, V., & Badyin, A. (2015). *Retail branding. Algorithm of construction from scratch*. Lviv, Vysoka Vezhca
61. Thomaidis, A. (2022). Data breaches in hotel sector according to general data protection regulation (EU 2016/679). In M. Valeri (Ed.), *Tourism Risk* (pp. 129–140). Emerald Publishing Limited, Bingley. https://doi.org/10.1108/978-1-80117-708-520221009
62. Tretyak, V., & Gordienko, T. (2010). Economic security: Essence and conditions of formation. *Economy and the State*, *1*. Retrieved February 10, 2023 from http://www.economy.in.ua/pdf/1_2010/3.pdf
63. Tyhiy, V. P. (2016). Human security: Concept, legal support, meaning, types. *Bulletin of the National Academy of Legal Sciences of Ukraine*, *2*(85). Retrieved February 15, 2023 from http://visnyk.kh.ua/web/uploads/pdf/ilovepdf_com-31-46.pdf
64. Ulynets, N. (2022). *How to survive a brand in a crisis situation, or what to do if the media officially "buried" the company*. Retrieved February 12, 2023 from https://executives.com.ua/yak-vyzhyty-brendovi-u-kryzovii-sytuatsii/
65. Upshow L. (2015). *Building brand identity: A strategy for success in a hostile marketplace*. University of Texas Press.
66. Wang, J. (2022). Data mining algorithm of hotel customer data based on mobile computing. *Lecture Notes on Data Engineering and Communications Technologies* (pp. 263–269). https://doi.org/10.1007/978-3-030-96908-0_33
67. Web-promo.ua. (n.d.). *Marketer's dictionary. Brand safety*. Retrieved February 12, 2023 from https://web-promo.ua/wordbook/bezopasnost-brenda/
68. Wilson, S. (2020). The pandemic, the acceleration of digital transformation and the impact on cyber security. *Computer Fraud & Security*, *12*, 13–15. https://doi.org/10.1016/s1361-3723(20)30128-7
69. Zaborona. (2022). Росія без айфонів, «Бетмену» та спорту: Онлайн Заборони про санкції у відповідь на війну *[Russia without iPhones, "Batman" and sports: Online Bans on sanctions in response to the war]*. Retrieved February 10, 2023 from https://zaborona.com/rosiya-bez-ajfoniv-betmenu-ta-sportu-onlajn-zaborony-pro-sankcziyi-u-vidpovid-na-vijnu/
70. Zaichenko, K., & Dima N. (2021). Economic security of the enterprise: Essence and role. *Efficient economy*, *5*. Retrieved February 10, 2023 from http://www.economy.nayka.com.ua/?op=1&z=8900

71. Zozulyov, O. V., & Nesterova, Yu. (2018). *Branding models: Classification and brief description*. Retrieved February 10, 2023 from https://zozulyov.ucoz.ru/articules/model_1.pdf

Received: 7 March 2023; Revised: 6 April 2023; Accepted: 12 June 2023