DOI: 10.55643/fcaptp.4.51.2023.4108

Oksana Zghurska
D.Sc. in Economics, Associate Professor of the Department of Entrepreneurship, Trade and Stock Exchange, State University of Telecommunications, Kyiv, Ukraine;
ORCID: 0000-0003-3878-3007

Oleksandr Turovsky
D.Sc. in Engineering, Professor of the Department of Information Security, National Aviation University, Kyiv, Ukraine;
ORCID: 0000-0002-4961-0876

Olena Shevchenko
PhD in Economics, Associate Professor of the Department of Marketing named after A.F. Pavlenko, Kyiv National Economic University named after Vadym Hetman, Kyiv, Ukraine;
ORCID: 0000-0002-9770-4906

Inna Zelisko
D.Sc. in Economics, Academician, Professor of the Department of Management, State University of Telecommunications, Kyiv, Ukraine;
ORCID: 0000-0002-0803-2598

Ruslan Dymenko
D.Sc. in Economics, Professor of the Department of Goods Management and Commercial Activity in Building, Kyiv National University of Construction and Architecture, Kyiv, Ukraine;
e-mail: drainc@ukr.net
ORCID: 0000-0002-6980-8038
(Corresponding author)

Yuriy Safonov
D.Sc. in Economics, Professor, Deputy Director, Scientific Institute for Modernization of Educational Content, Kyiv, Ukraine;
ORCID: 0000-0001-5623-1965

Received: 06/07/2023
Accepted: 14/08/2023
Published: 31/08/2023

IMPROVEMENT OF METHODOLOGICAL PRINCIPLES OF BRAND PROTECTION IN CYBERSPACE

ABSTRACT

The main purpose of this scientific work is to improve the theoretical and methodological foundations of ensuring data protection in cyberspace in the direction of forming a brand protection system to increase its level of recognition, strengthen reputation and increase brand capital as factors of competitive advantages of the organization for the long run.

In order to achieve the purpose, general scientific and special research methods have been used in the article, the main of which were the methods of scientific abstraction, generalization and synthesis, analytical diagnostics, descriptive statistics and the index-criterion method. Method of system analysis has been used in the research in order to comprehensively characterize the main aspects of brand protection in the information environment. Methods of steganographic protection of information, areas of their use and requirements for the characteristics of steganographic methods are considered.

The importance for companies to carefully research the issues of ensuring a brand image in the environment of a potential target audience by tracking manifestations of abuse of public opinion and a positive attitude towards the brand in order to ensure a high image level, the business reputation of the organization's branding policy, increase the level of data protection in the virtual space, as well as satisfaction and trust of the target audience for the long term are substantiated. Selection and justification of the coefficient of importance and evaluation criteria of steganographic methods, which were chosen and justified for use in ensuring cyber protection of the brand (stability, invisibility, security, complexity of embedding and extracting information). There was carried out the calculation of the weight characteristics in relation to the selected methods of hiding information to ensure cyber protection of the brand.

It was established that in a comprehensive comparison of information embedding methods for use in steganographic applications designed to increase brand cyber protection, the best result was shown by integrated methods based on discrete wavelet transformation and discrete cosine transformation.

Keywords: brand, branding policy, innovative development, brand cyber protection, brand capital, brand management, information environment, steganographic method

JEL Classification: M15, M31, O14, O31, C83

INTRODUCTION

By its essence, an effective branding policy is focused on the creation and promotion of a brand, which, in turn, forms the added value of product offers, and ensures sustainability and economic security of the business entity. In today's economic conditions, characterized by the presence of a commodity surplus and increased competition, branding is considered one of the most valuable intangible assets of the organization, which directly affects the financial results of operation.

In the conditions of fierce competition and the dynamic development of market relations, the brand from the consumer's point of view is a kind of "guide" that makes it possible to determine and make the right choice when buying goods or using certain services, thereby increasing loyalty to the choice made, which is based on trust in the brand. The information society dictates its conditions, knowledge spreads instantly, and

new ideas, technologies, and physical characteristics are easily counterfeited and copied. New tools of differentiation are gaining relevance, namely the unique, emotional, individual characteristics of the object of the offer, which is achieved with the help of a brand.

All organizational structures, including non-commercial ones, strive to create a strong, positive and unique brand image – as a key factor for successful activity and achieving competitive advantages, regardless of the differences with which it is associated – functional, rational or emotional.

At the same time, a brand is not only a name but also a whole complex of attributes, associative reactions and processes of perception of marketing actions by the consumer. In this context, it is very important and responsible to solve the issue of brand protection in virtual (cyberspace), which is one of the key problems in modern realities. As a result of illegal use of the brand in the network, the organization can lose its own reputation in the market and receive huge material losses. Solving such problems requires preventive measures in order to avoid inevitable consequences in the future.

LITERATURE REVIEW

Such well-known economists as Albert, N., Merunka, D., Bachman, K., Wilkins, S., Chen, H.-B., Yeh, S.- S. & Huan, T.-C., Fetscherin, M., Kuenzel, S. & Vaux Halliday, S. and others.

A number of scientific works by domestic and foreign authors are devoted to the issue of developing a system of criteria for steganographic methods and evaluating their effectiveness when performing the task of cyber brand protection.

The works of Konakhovich, G.F., Kuznetsov, O.O., Ryabko, B.Y. are devoted to consideration of the theoretical aspects of the application of steganography methods, in which the requirements for steganographic methods are described at a sufficient level and an overview of those areas where the indicated methods are most appropriate to be applied is carried out. Scientific studies by well-known authors do not contain a generalized system of requirements for steganographic methods of hiding information in images and cannot be fully used to evaluate these methods when applying them to branding policy.

Presented in the works of such famous scientists as Wolf, O.O. and Kutter, M. A. the material sufficiently reveals the essence of one of the main criteria for evaluating the use of steganographic methods. However, in these studies, there is no systematization of the requirements for steganography methods, and a holistic methodology for evaluating steganographic methods is not clearly generalized.

In the work of Yudin, O.K. a system of criteria and requirements for certain steganographic methods is generally defined. But there is no complete systematization of them, and no assessment of the effectiveness of their use for solving certain steganographic problems has been carried out.

Scientific research Lagoon, A., Vovk, O.V. is devoted to the consideration of individual steganographic methods according to the criterion of stability, while other criteria for evaluating steganographic methods are not considered in the work, and there is no integral methodology for their evaluation in this work.

The works of Vovk, O., Fridrich, J., and Seedy, S.A. are quite indicative, in which the basics of the methodology for evaluating the effectiveness of the use of steganographic methods are outlined at a sufficiently high level, while there is no systematization of evaluation criteria and the results of evaluation of certain brand protection methods in cyberspace are not fully presented.

Admitting the significant donation of domestic and foreign scientists, it's worth noting that the systematization of the criteria for assessing steganographic styles and the conception of the methodology for assessing the effectiveness of their operation to ensure the cyber protection of a brand in cyberspace is a critical scientific task, the result of which is devoted to this scientific composition.

AIMS AND OBJECTIVES

The main purpose of this scientific work is to improve the theoretical and methodological foundations of ensuring data protection in cyberspace for the formation of a brand protection system and increase its recognition, strengthen the long-term reputation and increase the company's capital due to its brand as a factor in the competitive advantages of the organization.

DOI: 10.55643/fcaptp.4.51.2023.4108

METHODS

During the exploration, general scientific and special exploration styles have been used in the composition, the main of which were the styles of scientific abstraction, conception and conflation, logical diagnostics, descriptive statistics and the indicator-criterion system, system of system analysis have been used in the exploration in order to exhaustively characterize the main aspects of brand protection in the information terrain. Styles of steganographic protection of information, areas of their use and conditions for the characteristics of steganographic styles have been considered.

The work examines methods of steganographic protection of information, areas of their use and requirements for the characteristics of steganographic methods (Table 1).

Table 1. Requirements for characteristics of steganographic methods. *(Source: constructed by the authors based on [22-24])*

№	Steganographic method	Requirements					
		Capacity	Stability	Invisibility	Security	Complexity embedding	Complexity withdrawal
1	Hidden connection						
2	Copyright protection						
3	Tracking the violator						
4	Adding additional information						
5	Image integrity protection						
6	Copy management						
7	Automatic addition of copy-right information						

Low High

To determine the optimal steganographic method of brand cyber protection, the work uses the results of research based on the application of the expert evaluation method according to selected criteria [22-24]. The content of the expert evaluation method for conducting this research is that an appropriate expert group, which includes independent specialists, is involved in the expert evaluation of steganographic methods [23].

The styles of conception and conflation made it possible to accumulate the entire range of scientific results achieved into a main general conception that represents the applicability of the content, to identify the crucial directions of development, confirm the pretensions, tasks and features of the steganographic styles ' adaption for imprinting policy using in business realities ' exertion.

RESULTS

As of today, e-commerce accounts for almost 15% of the total volume of retail sales in the world. In accordance with these trends, the number of counterfeit goods and services is also increasing. Questions arise more and more often about how to protect your brand in virtual (cyberspace), as well as how to protect your brand from counterfeiting in the online network.

Counterfeit products in the digital world of the information society amount to almost a third of all fakes by volume. In this aspect, brands forfeit hundreds of USD billions per year as a consequence of counterfeit and pirated content in cyberspace.

It is well known that a brand is a complex of distinctive, unique symbols of an organization that helps ensure its recognition. The brand consists of several components, including:

- name of the organization;
- logo and trademark;
- slogan;
- domain name.

In addition, sites, blogs and articles in them, objects protected by copyright, objects of intellectual property, etc., can be considered a brand.

The main difficulty for companies is that many want to use a brand that has been promoted for a long period of time and has a positive reputation in the market. At the same time, the unscrupulous actions of other market participants consist in the use of complete copying of the brand or its elements on the Internet. As a rule, there are two main goals of such actions:

1. Sale of own goods and services under the brand of a company that is already known on the market.
2. Implementation of measures to weaken the reputation of the organization in the target market, deliberate actions to form a negative opinion of customers regarding the quality of certain purchased goods or services provided.

The formation of the final decision to purchase a certain product is influenced by various factors: recommendations and descriptions on the company's official website, reviews on forums and from acquaintances, price acceptability, recognition and trust in the company itself. And if the seller can influence the formation of his positive image on his own website and partner websites, moderating the general picture of loyalty and satisfaction of the target audience, then he is practically not able to influence independent forums, reviews, private recommendations completely, but only indirectly, by prohibiting that or other negative content, which, as a final result, can provoke a negative opinion and the corresponding attitude of customers towards the organization.

Most potential buyers reveal brand websites through search engines, email, social media, mobile or online advertising, rather than by entering the URL directly into their browser's address bar. I.e., it means that a potential purchase can be made not on the official site, but on the site that was one of the first in the search engine. That is why the issue of brand protection against fakes on the Internet is becoming especially urgent. Some websites have personal accounts, shopping carts and additional pages where the user leaves his data. Research by Google and Ipsos shows that one of the key trends in modern marketing and web business, in general, is to build trust in relationships with consumers by taking care of their privacy.

By using content or images, URLs that appear to be authentic, and other techniques aimed at stealing traffic, unscrupulous organizations can easily take over a company's brand, customers, and ultimately profits.

GDPR, as arguably the key act on privacy regulation in the world, defines many conditions and requirements: transparency of communication, informed consent, the ability to exercise one's rights, and so on. At the same time, more and more companies, even regardless of whether they are subject to the General data protection regulation, take these requirements as a basis and implement the best privacy UX practices that go beyond the minimum requirements of the GDPR. This is done in order to convince the user that his privacy is really put first and the company cares about him [18].

Regulations are changing, new GDPR guidelines are constantly being released, and websites are being updated with new functionality and mechanics for working with personal data. That is why it is necessary to conduct a GDPR audit of your website from time to time for GDPR compliance and best UX practices.

Since the entry into force of the GDPR, supervisory authorities have actively begun to perform their functions and fine violators of the Regulation. At the moment, it is not possible to talk about a rapid increase in the number of fines, but this number is gradually increasing, which, in general, indicates that the system is actively functioning and gaining momentum. In 2022, the number of fines varies from 27 to 55 per month (Table 2).

DOI: 10.55643/fcaptp.4.51.2023.4108

Table 2. Typology of violations and the number of fines of the world's tech giants, EUR. *(Source: generated by the authors based on [33])*

Company	Country	Amount of fine (Euro)	Type of violation	Year
AMAZON Europe	Luxembourg	746000000	Non-compliance with general principles of data processing	2021
WhatsApp Ireland Ltd.	Ireland	225000000	Improper fulfilment of reporting obligations	2021
Google LLC	France	50000000	Insufficient legal framework for data processing	2020
H&M Hennes & Mauritz Online Shop A.B. & Co. KG	Germany	35258708	Insufficient legal framework for data processing	2020
TIM	Italy	27800000	Insufficient legal framework for data processing	2022
British Airways	Great Britain	22046000	Inadequate technical and organizational measures to ensure information security	2022
Marriott International Inc.	Great Britain	20450000	Inadequate technical and organizational measures to ensure information security	2020
Wind Tre S.p.A.	Italy	16700000	Insufficient legal framework for data processing	2022
Vodafone Italia S.p.A.	Italy	12251000	Non-compliance with general principles of data processing	2020
Notebooksbilliger.de	Germany	10400000	Insufficient legal framework for data processing	2022

The data in Table 1 indicate that well-known techno giants have problems with compliance with the legislation on personal data protection. For example, Amazon was fined 746 million euros for non-compliance with the principles of data processing, which led to a data breach. This fine became the largest for the entire period of GDPR (Figure 1).

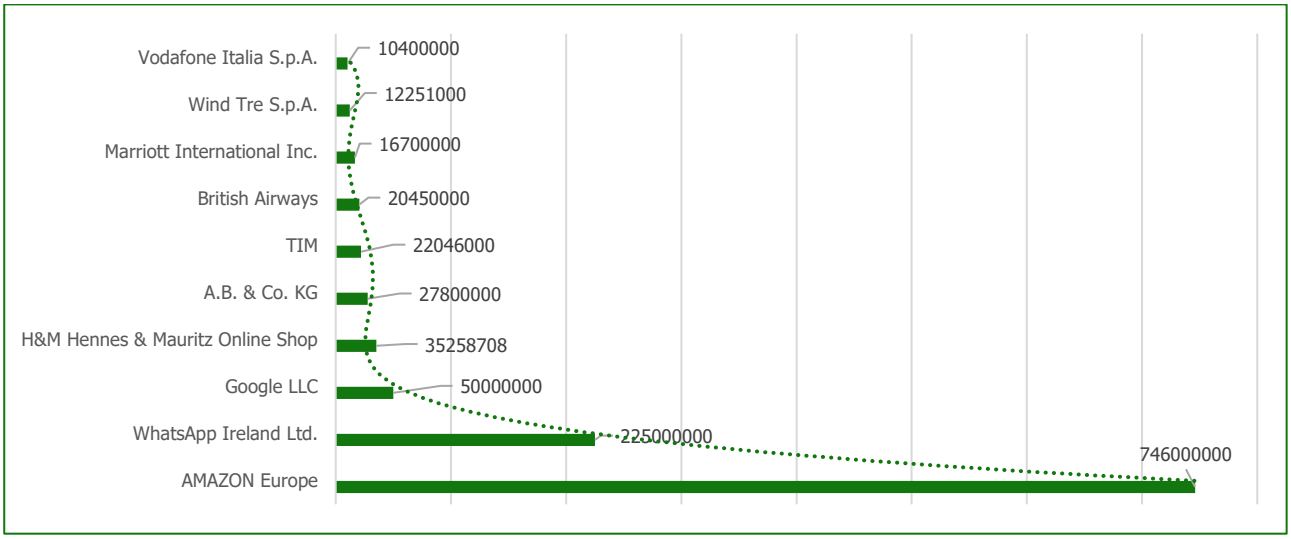

Figure 1. The largest fines of the world's tech giants, EUR. *(Source: built by the authors based on [18])*

Also, WhatsApp and Google were fined USD 225 million and $50 million, respectively. In the case of WhatsApp, the problem was that the company was not transparent enough about its handling of personal data and did not provide enough information to users about exactly how their data was being processed. Also, the supervisory authority had questions regarding the clarity of the information provided in the company's Privacy Policy. Google, in turn, was found guilty of a lack of transparency, adequate information of users and obtaining proper consent for advertising personalization [33].

In the context of the GDPR, "personal data" means any information about EU citizens that allows direct or indirect identification of a person, in particular by reference to an identifier, an online identifier, one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person. And although the mechanism of applying sanctions in Ukrainian realities is not yet clear, taking into account the country's integration course with Europe, it will be introduced in the near future.

Personal information may include online identifiers, device identifiers, cookie identifiers, and IP addresses. Subjects that work with personal data are controllers (determine the purposes and means of data processing) and processors (process data on behalf and on behalf of the controller). The main requirement for them is thorough protection of confidential information.

GDPR, as arguably the key act on privacy regulation in the world, defines many conditions and requirements: transparency of communication, informed consent, the ability to exercise one's rights, and so on. At the same time, more and more companies, even regardless of whether they are subject to the General data protection regulation, take these requirements as a basis and implement the best privacy UX practices that go beyond the minimum requirements of the GDPR. This is done in order to convince the user that his privacy really comes first and the company cares about him [19].

The above substantiates the importance for companies of carefully researching the issues of ensuring the brand image in the environment of the potential target audience by tracking manifestations of abuse of public opinion and attitude towards the brand and monitoring the formation of pricing policy for goods and services by official partners. In the event of a threat to brand safety, which consists in a targeted attack on the company's brand, intellectual property, and pricing, there is a need to develop a brand protection strategy, because, as practice shows, the market for counterfeit products, according to experts' estimates, may grow to USD 4.8 trillion in 2025, which, in comparison, makes up the budget of some European countries.

In order to understand what you need to pay attention to when choosing a protection strategy, you need to know and understand the degree of risk situations that are the source of direct financial losses (damages), which can be divided into three categories:

- Risk of sanctions, fines, tax risks;
- Risk of information leakage (personal data of potential customers);
- Risk of fraud and targeted activity of competitors, including manipulation of intellectual property.

Creation of fraudulent fake sites, online stores with counterfeit products in the name of a well-known brand, production of counterfeit products, targeted attacks on customers using social engineering, an unfair game with product prices, tarnishing the reputation of a partner sales network, attempts to re-register and buy domain names of sites from for the purpose of their resale or fraudulent use (cybersquatting) – deliberate actions of criminals and competitors, the main purpose of which is to cause direct or indirect damage to the company, systematically reducing the level of its image, as well as the trust and loyalty of customers to the company's brand.

In the event that counterfeit products disappoint the organization's target audience, the issue of ensuring a decent reputation on the market needs to be urgently resolved. It is a well-known fact that consumers are increasingly trusting online reviews over advertising, as the "collective voice" on the Internet overrides compelling family preferences and values, the opinions and beliefs of friends and colleagues when it comes to making a decision about a particular purchase or use of certain services. For example, when someone unknowingly buys a low-quality counterfeit product and will post a negative review or complaint on their own social network, the impact on the brand can lead to devastating consequences. At the same time, fake accounts in social networks are a threat to the general reputation of the information system.

Therefore, it may take a long period of time (years or even decades) to renovate a damaged brand reputation and maintain a strong competitive position of a well-known company in the market, and increase the level of satisfaction, loyalty and trust of consumers. In this aspect, it is extremely important to protect the brand not only offline, but also online by increasing the effectiveness of investments in digital marketing. The main part of the investment should be involved in the development of a unique method of ensuring brand protection in cyberspace.

One of the conceptual approaches and the method based on it for brand protection in cyberspace is the use of mechanisms for steganographic protection of information.

Steganography is the procedures, technologies, methods and methods designed both to hide information in the image and to protect the image itself from unauthorized changes, copying and unauthorized placement and use [11].

To date, it is worth highlighting three main factors of the popularity of technologies in the field of steganography, namely: the urgency of developing new channels of hidden information transmission; restrictions on the use of crypto assets in a number of countries of the world and the emergence of the problem of protecting property rights to information presented in digital form. The first two factors caused a large number of studies in the spirit of classical steganography (that is, hiding the fact of information transmission), and the third factor – even more numerous works in the field of so-called digital

DOI: 10.55643/fcaptp.4.51.2023.4108

watermarks (DWM). DWM – a special label that is inconspicuously inserted into an image or other signal with the aim of controlling its use in one way or another [7].

The most developed steganographic methods are based on changing the spatial area of the image or on using the area of the image change and transformation for hiding information, within which the hidden information is placed [8].

In the modern areas of hidden data transmission and the development of multimedia technologies, there is a wide range of areas of application of steganographic methods [4-5]. Each of these software applications has different requirements for the data embedding method. It should be noted that each steganographic method has its distinctive qualities and shortcomings in an application for a specific task of information protection and, in general when it is used in the chosen field of application [6]. The main task of steganography when implementing brand protection is to hide the very fact of existence of secret data when transmitting, storing or processing an image. Solving the specified task involves the selection and justification of certain steganography methods, the application of which can provide the most effective level of brand cyber protection.

Taking into account the specifics of brand cyber protection requires a direct evaluation of each method according to the accepted system of criteria regarding its optimality of protection for solving the steganographic problem in the chosen field of application. That is, in the field of brand cyber protection. That is, the problem of evaluating steganographic methods arises, and related to this problem is the scientific task of developing a system of criteria for evaluating steganographic methods, and then, with their involvement, developing a holistic methodology for evaluating steganographic methods intended for cyber brand protection [8].

Methods that use the spatial domain of the image embed the hidden data in the domain of the primary image. Their advantage is that there is no need to perform computationally complex and time-consuming image transformations for embedding. The research has found wide applications in the method of replacing the least significant bit (LSB) and the Kutter-Jordan-Bossen method, the most well-known among the methods of changing the spatial area of the image, which is more protected from various distortions, including bit compression, are methods that use the frequency domain of the container, in which useful information is hidden [25].

Wide application at this stage has found several ways to hide the necessary image in the frequency domain. As a rule, a certain method of image decomposition is applied, which is used as a container for hiding information. Such methods include methods using discrete cosine transform (DCP), discrete Fourier transform (DFT), wavelet transform, Karunen-Loev transform etc. Their positive feature is the possibility of application both to the full volume of the container image or to its separate part.

A list of the main methods based on the application of the image-container transformation area is given below [9]:

- a method based on the relative change in the values of the coefficients of the discrete-cosine transformation (the method of Koch and Zhao);
- the method of Bengham-Memon-Eo-Jung;
- methods based on the discrete wavelet transform (DWP);
- methods of spectrum expansion, which embed a watermark by modulating the coefficients of discrete-cosine transformation (DCP).

The most important qualitative characteristics of steganographic systems, formed on the basis of the use of various methods of hiding information, include [5-8]:

- *Bandwidth* – the number of bits of hidden information transmitted covertly using a specified method in an image of a set size;
- *Resilience* - the possibility of obtaining hidden information during general operations on image-container processing;
- *Invisibility* – a characteristic that provides for the inability of human vision to detect a steganographic message without the use of special means;
- *Security*-placed hidden information cannot be extracted from the container image by deliberate attacks using known placement and extraction algorithms (except for the secret key) and using information about one or more media with hidden information;
- *The complexity of embedding and extraction* – the number of standard operations that will be carried out to embed and detect a hidden message.

It is worth noting that, based on the scientific task defined for our study, the selection of qualitative characteristics of the information-hiding method should be optimized to improve the quality of brand cyber protection. That is why the main qualitative characteristics that will be important when evaluating the steganography method will be: the invisibility, security, and complexity of embedding and extraction.

To determine the optimal steganographic method for covert data transmission over communication networks, it seems optimal to use the results of research based on the application of the expert evaluation method according to selected criteria [10-12].

To generalize the results of the examination, there is a need to use a parameter that would reflect the expert's assessment. For this purpose, it is proposed to use the importance coefficient, which is widely used when constructing a solution in multi-criteria problems and mathematical programming [10, 14].

In works [15], the results of a detailed study were presented and the requirements for characteristics were assessed separately for each of the widespread steganographic fields of application according to a color scale (Table 1). Using the set of characteristics proposed above (Table 1), it is proposed to conduct a pairwise comparison of indicators using the method of analyzing hierarchies for each of the applications.

The representation form of pairwise comparisons is an inverse-symmetric matrix (Table 3), the values of which WIJ are reflections of the elements' intensity of the hierarchy (i) relative to the hierarchy (j), which are compared on an intensity scale from 1 to 9. At the same time, the following values can be taken for estimating the values:

- 1 – the values have equal values;
- 3 – slight advantage of one over the other;
- 5 – the average advantage of one over the other;
- 7 - a great advantage of one over the other;
- 9 - a great advantage of one over the other;
- 2, 4, 6, 8 – intermediate values of the evaluation comparisons.

Table 3. Inverse-symmetric matrix (appendix – hidden transmission of information). *(Source: compiled by the authors based on [31])*

W	***a***	***b***	***c***	***d***	***e***	***f***
A	–	6	1	1	5	5
B	1/6	–	1/6	1/6	1/3	1/3
C	1	6	–	1	5	5
D	1	6	1	–	5	5
E	1/5	1	1/5	1/5	–	1
F	1/5	2	1/5	1/5	1	–

Based on the data of the inverse-symmetric matrix, priority matrices were constructed (Table 1, Table 4, which include: throughput (a), stability (b), invisibility (c), security (d), embedding complexity (e) and complexity extraction (f).

In the process of forming priority matrices, the following procedure has been used: when comparing element (i) with element (j), the position W_{IJ} = b is formed, then W_{JI} = 1/b; the precedence of each element in the scale is determined by calculating the corresponding element of the regularized main eigenvector of the matrix V.

Table 4. Matrix of priorities (application – image integrity protection).

W	***a***	***b***	***c***	***d***	***e***	***f***
a	—	5	1	1	4	4
b	1/5	—	1/5	1/5	1/3	1/3
c	1	5	—	1	4	4
d	1	5	1	—	4	4
e	1/4	1	1/4	1/4	—	1
f	1/4	1	1/4	1/4	1	—

DOI: 10.55643/fcaptp.4.51.2023.4108

By the method of averaging the results, we've obtained the weights (importance) of each of the characteristics of the steganographic methods intended for brand cyber protection (Table 5).

Thus, the evaluation results showed that the most important characteristics of steganographic methods are security (weight R = 0.3), invisibility (weight R = 0.22) and resilience (weight R = 0.2).

Table 5. General weights of characteristics. *(Source: calculated by the authors based on [32])*

Characteristic (i)	Weight (R)
Capacity	0,08
Resilience	0,2
Invisibility	0,22
Security	0,29
Complexity of embedding	0,07

The attained scores are used for the analysis of the named steganographic styles of information embedding and for the multi-criteria selection of the stylish system. Grounded on the information presented in [16-18], and using the method of assigning coefficients to factors, *where:*

- *A1 – method of least significant bit substitution (LSB);*
- *A2 – Kutter-Jordan-Bossen method;*
- *A3 – Koch-Zhao method;*
- *A4 – Bengham-Memon-Eo-Young method;*
- *A5 – method with spectrum expansion;*
- *A6 is a method based on 3-level fiberboard.*

Where:

- *a is the bandwidth;*
- *b – stability;*
- *c – invisibility;*
- *d – security;*
- *e – embedding complexity;*
- *f is the difficulty of detection.*

In Table 6 indicator "7" is the stylish value of the characteristic, "1" is the worst. To understand the values described in Table 6, the computation of the average values of the coefficients for throughput was applied.

Table 6. Comparative analysis of embedding methods. *(Source: compiled by the author based on [31])*

W	***a***	***b***		***c***	***d***	***e***	***f***
A1	6	1		5	1	6	6
A2	4	2		5	2	5	5
A3	1	5		3	5	3	3
A4	1	4		4	5	3	3
A5	2	5		6	4	1	1
A6	1	6		6	6	1	1

After calculating the average values, the throughput coefficients were determined (the first column in Table 6) by the direct arrangement of the methods.

So, based on the data given in Table 6, it is possible to carry out a comprehensive comparative analysis of the selected methods A1–A6. For this, the method of pairwise comparisons is used (Table 7).

Summarizing the values of all the parameters of Table 5, and normalizing them, we obtain the parameters of the weighted assessment of the quality of the applied methods. A comparative analysis of the methods, based on a detailed analysis of each of the characteristics, is displayed in the form of a matrix (Table 7).

Table 7. Method comparison matrix (by security). *(Source: compiled by the author based on [32])*

	A1	***A2***	***A3***	***A4***	***A5***	***A6***
A1	—	1/2	1/2	1/2	1/2	1/2
A2	1/2	—	1/2	1/2	1/2	1/2
A3	1/2	1/2	—	1/2	1/2	1/2
A4	1/2	1/2	1/2	—	1/2	1/2
A5	1/2	1/2	1/2	1/2	—	1/2
A6	1/2	1/2	1/2	1/2	1/2	—

Table 8. Comparison of steganographic methods without taking into account the significance (weight) of characteristics. *(Source: compiled by the author based on [30])*

Method (a)	Value (WW)
A1	0.261
A2	0.179
A3	0.125
A4	0.096
A5	0.136
A6	0.192

As can be seen from Table 8, the loftiest value was demonstrated by the method of replacing the least significant bit (LSB) method of least significant bit substitution (LSB) (A1, WW = 0.261).

Taking into account the accepted assessment methods, the weight of the obtained values, given in Table 8, can be changed into the values given in Table 9. The specified Table 9 shows the values of the parameters, taking into account their importance according to the security and reliability criteria, which are the most important for the cyber protection of the brand.

Thus, in a comprehensive comparison of information embedding methods for use in steganographic applications to increase brand cyber protection, the best result was shown by integrated methods based on the discrete wavelet transform (DVP); (A6, WW1 = 0.34) and discrete cosine transformation (DCP) (A3, WW1 = 0.184).

Table 9. Comparison of methods, taking into account the significance (weight) of characteristics. *(Source: compiled by the author based on [30])*

Method (a)	Value (WW)
A1	0.081
A2	0.086
A3	0.184
A4	0.146
A5	0.170
A6	0.333

DISCUSSION

Prospective directions for the development of the branding policy of business entities regarding the registration of an international brand and its development in the online network is positioned as a key component of business development in today's conditions, while most famous brands prefer the "real world" without having a comprehensive strategy for

DOI: 10.55643/fcaptp.4.51.2023.4108

protecting their own brand from fakes on the Internet. Ensuring brand protection in the global network helps strengthen brand reputation, reduce online fraud, and identify unauthorized sales channels and product sales.

Most researchers seek to solve important issues of brand protection in cyberspace by focusing their own work on the consideration of theoretical aspects in the field of personal branding, while the applied nature of the use of tools and methods of branding management, which is aimed at the final audience of practitioners, are neglected. As a result, many questions remain debatable regarding the specifics of brand formation and management, as well as its protection in the online environment.

That is why, in modern realities, the main part of the issues devoted to the study of the effective attraction of internal and external investments for the development of unique non-counterfeit packaging, the development of a supply chain management system, the development of effective brand protection strategies not only in the physical but also in the virtual world needs an urgent solution. At the same time, to protect the brand in both digital and real environments, the necessary measures are the development of a comprehensive brand protection strategy, which is based on the development of a unique methodology for ensuring brand protection in cyberspace and is closely related to the risk management system, corporate policy and proper level of consciousness of the target audience.

Taking into account foreign experience in solving issues of information protection in cyberspace, as well as the consequences of illegal use of data, the regulation and control of these issues at the state level are among the urgent tasks to be solved by the highest level of government management. Only with the right approach to creating a safe and attractive brand not only for business entities on the market but also for the country as a whole, a positive result will allow positioning itself as an attractive national environment for business. In the near future, urgent issues regarding the intensification and stimulation of the development of international trade and the attraction of foreign investments need to be resolved, Ukraine must demonstrate itself as a country, first of all, with a safe, transparent and stable business environment.

CONCLUSIONS

Thus, the scientific work substantiates the importance for companies of carefully researching the issues of ensuring the brand image in the environment of the potential target audience by tracking manifestations of abuse of public opinion and positive attitude towards the brand in order to provide a high image level, stable business reputation of the organization's branding policy, increase the level of data protection in virtual space, as well as the satisfaction and trust of the target audience for the long term.

Selection and justification of the coefficient of importance and evaluation criteria of steganographic methods, which were chosen and justified for use in ensuring the cyber protection of the brand, were carried out. Stability, invisibility, security, and complexity of embedding and extracting information is proposed as criteria. Requirements for steganographic methods of hiding information intended for brand cyber protection are summarized.

The calculation of the weight characteristics in relation to the selected methods of hiding information to ensure the cyber protection of the brand was carried out, and priority matrices were constructed in accordance with the requirements of information-hiding methods.

On the basis of a comprehensive comparison of information embedding styles for use in steganographic operations to increase brand cyber protection, the choice of the most optimal steganographic styles was determined and justified, and it was also established that the most important characteristics of steganographic styles are security, difficulty of discovery and stability.

It was established that in a comprehensive comparison of information embedding methods for use in steganographic applications designed to increase brand cyber protection, the best result was shown complex by integrative methods based on discrete wavelet converting and discrete cosine converting.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

Conceptualization: *Oksana Zghurska, Oleksandr Turovsky*
Data curation: *Olena Shevchenko*
Formal Analysis: *Oleksandr Turovsky*

Methodology: *Oksana Zghurska, Oleksandr Turovsky, Yuriy Safonov*
Resources: *Ruslan Dymenko*
Supervision: *Yuriy Safonov*
Validation: *Inna Zelisko*
Investigation: *Oleksandr Turovsky, Inna Zelisko*
Visualization: *Olena Shevchenko, Ruslan Dymenko*
Project administration: *Oksana Zghurska*

REFERENCES

1. Albert, N., & Merunka, D. (2013). The role of brand love in consumer-brand relationships. *Journal of Consumer Marketing, 30*(3), 258–266. https://doi.org/10.1108/07363761311328928
2. Bachman, K., & Wilkins, S. (2014). Brand commitment and consumer-brand Identification as Determinants of consumers' brand loyalty and repurchase intentions. Research with Plymouth University, 11-32.
3. Chen, H.-B., Yeh, S.-S., & Huan, T.-C. (2014). Nostalgic emotion, experiential value, brand image, and consumption intentions of customers of nostalgic-themed restaurants, *Journal of Business Research, 67*, 354–360. https://doi.org/10.1016/j.jbusres.2013.01.003
4. Fetscherin, M. (2014). What type of relationship do we have with loved brands? *Journal of Consumer Marketing, 31*(6/7), 430–440. https://doi.org/10.1108/jcm-05-2014-0969
5. Fridrich, J. (1999). Applications of Data Hiding in Digital Images. Tutorial for the ISPAC S'98 Conferece. Melbourne, Australia. https://doi.org/10.1109/ISSPA.1999.818099
6. Hornitska, D.A., Volianska, V.V., & Korchenko, A.O. (2012). Vyznachennya koefitsiyentiv vazhlyvosti dlya ekspertnoho otsinyuvannya u haluzi informatsiynoyi bezpeky. Information protection, 1, 108–121. https://er.nau.edu.ua/bitstream/NAU/36033/1/2072-5951-1-SM.pdf
7. Kinzeryaviy, O.M. (2015). Stehanohrafichni metody prykhovuvannya danykh u vektorni zobrazhennya, stiyki do aktyvnykh atak na osnovi afinnykh peretvoren': dys. kand. tekhn. nauk. Spetsial'nist' 05.13.21 Systemy zakhystu informatsiyi. Kyiv, 324 p.
8. Konakhovich, G.F. (2006). Komp'yuterna stehanohrafiya. Teoriya i praktyka. Kyiv: MK-Press.
9. Kuenzel, S., & Vaux Halliday, S. (2008). Investigating antecedents and consequences of brand identification. *The Journal of Product and Brand Management, 17*(5), 293–304. https://doi.org/10.1108/10610420810896059
10. Kutter, M. A., & Petitcolas, F. (1999). Fair benchmark for image watermarking systems. Proc. of SPIE: Security and Watermarking of Multimedia Contents. San Jose, France, 3657, 226–239. http://dx.doi.org/10.1117/12.344672
11. Kuznetsov, O. O. (2011). Stehanohrafiya: navchal'nyy posibnyk. Kharkiv: View. XHEU.
12. Ladychenko, K.I., and Tronko, V.V. (2015). Modern trends in the development of the world market for information and communication services, Efektyvna ekonomika, 2. http://www.economy.nayka.com.ua/?op=1&z=3830 (Accessed 27 May 2023).
13. Lagoon, A., & Lagoon, I.A. (2013). Vykorystannya veyvlet-peretvorennya dlya prykhovuvannya informatsiyi v nerukhomykh zobrazhennyakh. Protection of information and security of information systems, 98 – 99. http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VNULP_2013_774_11.pdf
14. National Informatization Program, Law of Ukraine of 04.02.1998, 74/98–VR. Official Bulletin of Ukraine, no. 27–28, pp. 181. http://zakon1.rada.gov.ua/laws/show/74/98-вр
15. Ruanaidh, Ó. J., & Pun, T. (1997). Rotation, scale and translation invariant digital image watermarking. Proc. of the ICIP'97. California, 1, 536–539. https://doi.org/10.1109/ICIP.1997.647968
16. Sazonets O. M., Pinchuk O. L., & Kunytskyi S. O. (2015). Hlobalni informatsiini ta naukometrychni systemy naukovo-tekhnolohichnoho rozvytku Ukrainy. Rivne: Volyn. oberehy.
17. Seedy, S.A., & Sadykhov, R.H. (2013). Sravneniye metodov steganografii v izobrazheniyakh. Informatics. BGUIR. Belgorod, 66 – 75. https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CDgQw7AJahcKEwjY_ufo_duAAxUAAAAAHQAAAAAQAw&url=https%3A%2F%2Finf.grid.by%2Fjour%2Farticle%

DOI: 10.55643/fcaptp.4.51.2023.4108

2Fview%2F37&psig=AOvVaw3OnxRTUKxb4zGJHNzdSzuP&ust=1692096764225591&opi=89978449

18. Sidorov, V., & Babenko, V. (2016, December 16). Clusterization the Countries by the Level Information in the Conditions of International Globalization. International Scientific Conference the Development of International Competitiveness: State, Region, Enterprise: Conference Proceeding, 1, 11-15. Lisbon, Portugal: Baltija Publishing.
19. The Global Information Technology Report 2020. https://www.weforum.org/reports/the-global-informationtechnology-report-2016
20. Totsenko, V.G. (2002). Metody i sistemy podderzhki prinyatiya resheniy. Algoritmicheskiy aspekt. Kiev: Science. opinion.
21. Vovk, O. (2015). Synthesis of optimal steganographic method meeting given criteria. Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal). Lublin, Poland. https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-48f178a4-420c-4bbc-8fd4-a92736b5a457/c/Vovk.pdf
22. Vovk, O.V. (2015). Synthesis of steganographic data transmission method, effective in terms of reliability and security. Electronic scientific professional publication of KNURE "Problems of telecommunications", 1 (16), 103–115.
23. Wallace, E., Buil, I., & de Chernatony, L. (2014). Consumer engagement with self-expressive brands: brand love and WOM outcomes, *Journal of Product & Brand Management, 23*(1), 33–42. https://doi.org/10.1108/jpbm-06-2013-0326
24. Wolf, O.O. (2016). Metody pidvyshchennya stiykosti ta propusknoyi zdatnosti system prykhovanoyi peredachi informatsiyi: dys. kand. tekhn. nauk. Spetsial'nist' 05.12.02 – Telekomunikatsiyni systemy ta merezhi. Kharkiv, 177 p.
25. Yudin, O.K. (2009). Zakhyst informatsiyi v merezhakh peredachi danykh. K. "INTERSERVICE", 716 p.
26. Zghurska, O., Somkina, T., Dymenko, R., & Kapelyushna, T. (2019). Diversification strategy of entrepreneurial activity in conditions of European integration. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9, 4809–4815. https://www.ijitee.org/wp-content/uploads/papers/v9i1/J94430881019.pdf
27. Zghurska, O., Somkina, T., Korchynska, O., Fedorchenko, A., Tarasevych, O., & Kubiv, S. (2021). Formation of organizational and economic structure in the process of developing innovative solutions of a diversified enterprise. Journal of Hygienic Engineering and Design (Food Production and Processing), 36. https://keypublishing.org/jhed/wp-content/uploads/2021/11/4.-JHED-Volume-36-FPP-Abstract-%D0%9Eksana-Zghurska.pdf
28. Zghurska, O., Somkina, T., Romashchenko, O., & Korchynska, O. (2021). Formation of market-oriented enterprises' management system in the direction of intensification of innovative processes. Journal of Hygienic Engineering and Design (Food Production and Processing), 35, 129-138. https://keypublishing.org/jhed/wp-content/uploads/2021/08/12.-JHED-Volume-35-FPP-Abstract-%D0%9Eksana-Zghurska.pdf
29. Oksana Zghurska, Olena Korchynska, Karina Rubel, Stepan Kubiv, Andriy Tarasiuk, & Oksana Holovchenko (2022). Digitalization of the national agroindustrial complex: new challenges, realities and prospects. Financial and credit activity problems of theory and practice, 6(47), 388-399. http://dx.doi.org/10.55643/fcaptp.6.47.2022.3929
30. Olexander Turovsky, Sergey Lazarenko, Tatiana Shcherbak, Liubov Ryabova, & Tatiana Meleshko (2022). Method of evaluation of steganographic methods of hidden information in images, 2(02). https://doi.org/10.36994/2788-5518-2021-02-02-23
31. Olesia Vovk, & Andii Astrakhantsev (2015). New steganographic method: Development and comparison with the most relevant. 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, Ukraine, 237-240, https://doi.org/10.1109/INFOCOMMST.2015.7357323
32. Vovk, O., & Astrahantsev, A. (2015). Synthesis of optimal steganographic method meeting given criteria. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 5(3), 27-34. https://doi.org/10.5604/20830157.1166548
33. GDPR abo General Data Protection Regulation. Trendy 2022. (n.d.). https://legalitgroup.com/gdpr-novi-eu-tendentsii

Згурська О., Туровський О., Шевченко О., Зеліско І., Дименко Р., Сафонов Ю.

УДОСКОНАЛЕННЯ МЕТОДИЧНИХ ЗАСАД ЗАХИСТУ БРЕНДУ В КІБЕРПРОСТОРІ

Метою дослідження є вдосконалення теоретичних і методичних засад забезпечення захисту даних у кіберпросторі для формування системи захисту бренду і підвищення рівня його впізнаваності, посилення у довгостроковій перспективі репутації та збільшення капіталу компанії за рахунок її бренду як чинника конкурентних переваг організації.

Для досягнення поставленої мети використано широкий спектр методів дослідження, основними з яких були методи узагальнення, наукової абстракції, аналітичної діагностики, описової статистики та індексно-критеріальний метод. Для комплексної характеристики основних аспектів захисту бренду в інформаційному середовищі в дослідженні використано метод системного аналізу. Розглянуто методи стеганографічного захисту інформації, області їх використання та вимоги до характеристики стеганографічних методів. Для визначення оптимального стеганографічного методу кіберзахисту бренду в роботі використано результати досліджень, що базуються на застосуванні методу експертного оцінювання за обраними критеріями.

Обґрунтовано важливість для компаній ретельного дослідження питань забезпечення іміджу бренду в середовищі потенційної цільової аудиторії шляхом відстеження проявів зловживання суспільною думкою та позитивним ставленням до бренду з метою забезпечення високого іміджевого рівня, ділової репутації брендингової політики організації, підвищення рівня захисту даних у віртуальному просторі, а також задоволення та довіри цільової аудиторії на довгостроковий період.

Здійснено вибір та обґрунтування коефіцієнта важливості й критеріїв оцінки стеганографічних методів, у ролі яких запропоновано стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації, а також проведено розрахунок вагових характеристик відносно обраних методів приховування інформації для забезпечення кіберзахисту бренду.

Установлено, що при комплексному порівнянні методів вбудовування інформації для використання в стеганографічних додатках, призначених для підвищення кіберзахисту бренду, найкращий результат показали інтегровані методи на основі дискретного Вейвлет-перетворення та дискретного косинусного перетворення.

Ключові слова: бренд, брендингова політика, інноваційний розвиток, кіберзахист бренду, капітал бренду, бренд-менеджмент, інформаційне середовище, стеганографічний метод

JEL Класифікація: M15, M31, O14, O31, C83

The main purpose of this scientific work is to improve the theoretical and methodological foundations of ensuring data protection in cyberspace in the direction of forming a brand protection system to increase its level of recognition, strengthen reputation and increase brand capital as factors of competitive advantages of the organization for the long run.

DOI: 10.55643/fcaptp.4.51.2023.4108