



Olena Sadchenko, Dr.Sc. (Economics), Prof. Head, Department of Marketing & Business Administration Odesa I.I.Mechnikov National University (Odesa, Ukraine), Prof. dr hab. University of Economics and Humanities (Bielsko-Biala, Poland)  

MARKETING-MANAGEMENT OF INFORMATION SECURITY OF THE ENTERPRISE

Abstract. *The article discusses the main strategies for effective information security management of the enterprise, which take into account the concepts of "information security" and "information threats". The main principles are defined: integrity, confidentiality, availability, authenticity, compliance, continuity of business processes, timeliness. The work is devoted to the study of information security management problems at the enterprise. Potential threats that can adversely affect the security of enterprise information resources have been identified, and information vulnerabilities requiring attention have been identified.*

Keywords: *marketing-management, marketing, information security, digital marketing, information security management, enterprise, information security policy*

Introduction. In the modern world, information security is a vital condition for ensuring the interests of a person, society and the state. Measures to ensure information security should be carried out in various area – the economy, defense, politics, as well as in the social sphere.

Errors and inaccuracies, distortions of information can cause significant damage to the entire human society. Information is becoming a key element in almost all systems of social life. In any industry, be it political security, economic security, environmental security, public security, there is a coherent element that is information security.

The concept of "Information Management" (hereafter IM) appeared relatively recently – at the end of the 70s of the last century. The emergence of MI as a concept, and then as an independent field of knowledge, connected both with the need to make effective decisions in the field of informatization (internal tasks of IM), as well as with the requirements for information management in the main activity enterprises (internal IM tasks). The term "information management" owes its appearance to the US federal government, which in In 1978, he proposed to introduce control over government documents and In 1980,

he adopted a law on reducing the number of paper documents carriers in order to reduce the costs of American firms for preparation various reports [Znakhur S. V. 2009, p. 13].

The marketing-management of information security of the enterprise in theory and practice was examined by many scientists – Vovchak I. S. [Vovchak I. S. 2002], Znakhur S. V. [Znakhur S. V. 2009], Kucherenko, V. V., Il'yin, V. V. [Kucherenko, V. V., Il'yin, V. V. 2019], Koval'chuk, V. I. [Koval'chuk, V. I. 2020], Dovbysh, I. YU., Chepurko, V. V. [Dovbysh, I. YU., Chepurko, V. V. 2017], Antonyuk L.V., Sytnikov V.O. [Antonyuk L.V., Sytnikov V.O. 2018], Posun'ko M.S., Cherkasova V.YU.[Posun'ko M.S., Cherkasova V.YU 2019], Sadchenko O.V. [Olena Sadchenko, Hanna Obykhod, and other (2022)], Sadchenko O.V. [Sadchenko, 2017, 2020, 2021], Robul Yu.V. [Sadchenko, Robul 2020], [Robul, 2020], Sil'chenko O.V., Korchevna O.M., Korchevnyy S.YU. [Sil'chenko O.V., Korchevna O.M., Korchevnyy S.YU. 2019] etc.

Scientists have focused their attention on various aspects of marketing-management of information security, but this concept has not been fully integrated into marketing system. Basically, the authors considered the management aspects of information security, but this concept was not fully integrated into the marketing system.

According to the above, the **aim of the article** is to develop and methodologically substantiate the model of marketing strategy into which marketing-management of information security of the enterprise.

Research results. Information security is the state of protection of the company's information resources from unauthorized access, loss, destruction, exposure of confidential information or violation of the integrity and availability of information systems. It provides a set of measures aimed at preventing, detecting and responding to threats to information security in order to ensure uninterrupted operation of the enterprise and preserve its reputation.

"Information security" refers to measures, procedures and technologies aimed at protecting information from unauthorized access, loss, destruction or modification. It covers all aspects of the security of information resources, including physical security, data security, network security, protection against intrusions and other aspects related to the protection of confidentiality, integrity and availability of information.

Information threats are potential hazards or events that can lead to a breach of enterprise information security. They can be natural (e.g. natural disasters, fires) or man-made (e.g. hacker attacks, data theft, espionage). Information threats can occur both externally from

unauthorized persons, and arise within the enterprise itself due to the negligence of personnel or internal system vulnerabilities.

Information threats are potentially dangerous factors or events that can lead to a violation of the company's information security. They can be natural (for example, natural disasters, fires) or man-made (for example, hacker attacks, data theft, espionage). Informational threats can originate both externally from third parties and arise from within the enterprise itself due to personnel negligence or by internal system vulnerabilities.

Information threats indicate potential risks and dangers that may affect the security of an enterprise's information. This can be misuse or unauthorized access to information, viruses and malware, cyber attacks, phishing, data theft, information leaks, unauthorized use of accounts, technical failures and other similar situations.

To effectively manage the information security of an enterprise, it is necessary to have a strategy that takes into account the concept of "information security" and "information threats".

Such a strategy should include a number of important steps:

- **Analysis and identification of threats:** To begin with, it is necessary to conduct an analysis of potential threats that may affect the information security of the enterprise. These can be cyber attacks, data leaks, social engineering, etc. It is important to consider both external and internal threats.
- **Risk assessment:** After identifying threats, it is necessary to assess their risks. This will help establish priorities and identify potential business implications. Risk assessment includes analysis of system vulnerabilities, likelihood of threats and impact on business processes.
- **Development of policies and procedures:** Based on the identified threats and risk assessment, it is necessary to develop appropriate information security policies and procedures. These documents establish rules and requirements for information security, use of passwords, access control, data backup, etc.
- **Incident monitoring and detection systems:** The enterprise must have incident monitoring and detection systems that will allow timely detection of potential threats and response to them. These can be network monitoring systems, intrusion detection systems, log analysis systems, etc.
- **Staff training and awareness:** One of the most important aspects of information security management is staff training and awareness. Employees must be familiar

with security policies, procedures, rules for handling information and identifying potential threats.

These steps will help to form a system for ensuring information security at the enterprise, which will function effectively and ensure the protection of information from potential threats. The main principles of information security management of the enterprise include a wide range of approaches and strategies aimed at ensuring reliable protection of information and ensuring uninterrupted business processes.

Below is a detailed description of the main principles of information security management of the enterprise:

1. Integrity: The principle of integrity involves ensuring the confidentiality, availability and reliability of information. The enterprise must develop policies and procedures that guarantee the preservation and prevention of unauthorized alteration or loss of data.
2. Confidentiality: The principle of confidentiality is to ensure the protection of confidential information from unauthorized access. This may include the application of encryption, access control and user identification.
3. Availability: The principle of availability states that information should be available to authorized users at the right time and place. The enterprise must ensure adequate infrastructure, data backup and recovery mechanisms to ensure uninterrupted system operation.
4. Authenticity: The principle of authenticity involves ensuring accuracy and unavailability of unauthorized data modification. The enterprise must apply mechanisms for checking data integrity, access control and user authentication.
5. Compliance: The principle of compliance requires that the enterprise adheres to relevant legislative norms, regulatory requirements and standards in the field of information security. This may include developing security policies, conducting audits and assessing risks.
6. Continuity of business processes: The principle of continuity of business processes involves the implementation of measures and plans in the event of accidents, disasters or other negative events that may affect the operation of the enterprise. This includes backing up data, creating backup systems, and planning for business recovery.
7. Timeliness: The principle of timeliness involves constant monitoring and response to potential threats and information security incidents. The enterprise must have

mechanisms for detection, analysis and response to events occurring in the information system.

These principles are the basis for effective information security management of the enterprise. With their help, the enterprise can create a system that ensures reliable protection of information, minimizes risks and promotes smooth functioning of business processes.

In order to analyze the vulnerabilities of the company's information infrastructure, it is necessary to perform several steps:

1. Inventory of assets: First, you need to compile a complete list of all assets used in the information infrastructure of the enterprise. These can be servers, computers, network devices, software, databases, etc. Record the characteristics and details of each asset.
2. Risk assessment: Next, the potential risks associated with each asset should be assessed. This means determining what threats could affect assets and what the consequences would be in the event of a successful attack. For example, there may be threats from cyber attacks, physical damage or misuse of assets.
3. Detection of vulnerabilities: Conduct a technical analysis of the information infrastructure to identify potential vulnerabilities. These can be weak points in the network, outdated software, insufficient security settings, lack of data backup, etc. It is important to thoroughly document any identified vulnerabilities.
4. Analysis and prioritization: Assess the severity and likelihood of exploitation of each vulnerability. Determine which vulnerabilities require immediate remediation and which can be accepted as a risk or require additional security measures.
5. Development of a plan of security measures: Based on the results of the analysis, develop an action plan to eliminate vulnerabilities and improve the security of the information infrastructure. Determine specific actions needed to correct identified vulnerabilities, establish protections, and improve security policies and procedures.
6. Implementation and monitoring: Implement planned security measures, perform necessary updates and adjustments. Ensure constant monitoring of the information infrastructure to identify new vulnerabilities and respond immediately to potential threats.

This analysis will help identify weak points in the information infrastructure of the enterprise and develop strategies and plans to ensure their protection and security.

Information security threats and vulnerabilities represent potential risks that can harm information systems, data, and organizations. Let's consider some of the main threats and vulnerabilities of information security:

1. Viruses and malware: Malicious programs such as viruses, worms, Trojans, and spyware can infect computers and networks, causing a variety of adverse effects, including data loss, loss of system control, or unauthorized access to confidential information.

Example: The WannaCry virus, which spread to many countries in 2017, encrypted data on infected computers and demanded a ransom for their recovery.

2. Phishing and social engineering: Phishing and social engineering attacks are aimed at tricking users into obtaining their sensitive data, such as passwords or bank details.

Example: A fake email pretending to be an official request from a bank asking for personal data. The user, unaware of the attack, can provide his data to fraudsters.

3. Software security flaws: Vulnerabilities in software can be used by attackers to gain unauthorized access to systems, execute malicious code, or intercept data.

Example: The Heartbleed vulnerability discovered in 2014 affected a large number of web servers and could be used to obtain sensitive information such as passwords and encryption keys.

4. Weaknesses in physical security: Inadequate protection of physical infrastructure, such as server rooms, communication channels or data warehouses, can give attackers physical access to systems and information.

Example: Theft of a computer or server containing confidential data from an unsecured premises.

5. Social Networks and Online Platforms: Using social networks and other online platforms can create security risks, such as the leakage of personal information, identity theft or cyberbullying.

Example: Unauthorized access to a user's social network account and publication of personal photos or information without their consent.

6. DDoS attacks: Denial-of-service (DDoS) attacks aim to overload servers and networks by generating a huge number of requests. This can lead to denial of service to legitimate users and reduced system performance.

Example: An attack on a company in which attackers used a botnet (a network of infected computers) to send a huge number of requests to the company's servers, causing them to become overloaded and unavailable to users.

7. Internal threats: Threats to information security can come from within the organization. These can be unscrupulous employees or attackers who have physical or network access to systems and information.

Example: A company employee who has access to confidential data sells this information to competitors or uses it for his own personal interests.

8. System failures and equipment failures: Technical failures and equipment failures can create vulnerabilities in security systems and lead to unavailability of data or loss of information.

Example: A failure in the company's data warehouse, which led to the loss of valuable data or its unavailability for a certain period of time.

9. Physical threats: Physical threats to information security include physical damage to equipment or access to it by unauthorized persons.

Example: Breaking into a server room, where an attacker gets physical access to servers and can copy, change or steal data.

10. Weaknesses in security processes and policies: Lack of strict security procedures and policies can create vulnerabilities and make an information security system more susceptible to attack.

Example: Failure to regularly update software and operating systems, which can lead to the presence of known vulnerabilities that attackers can use for attacks.

These threats and vulnerabilities are serious and can potentially have a detrimental effect on the information security of organizations. To prevent these problems, it is important to pay due attention to the protection of information, establish appropriate security policies and use modern technologies to detect and prevent such threats.

Criminals compromised confidential information in 47% of successful attacks on organizations. More than a third of the stolen information (36%) was personal data, as well as information related to commercial secrets (17%). Credentials accounted for 14% of stolen data. In successful attacks targeting individuals, attackers managed to steal data 64% of the time. Credentials (41%), as well as personal (28%) and payment card data (15%) were mostly compromised. There is an increase in the share of personal data among stolen information relative to the results of 2021: for organizations – 4 percentage points (from 32% to 36%), for private individuals – 8 percentage points. p. p. (from 20% to 28%) [Znakhur S. V. 2009, p. 16].

In 2022, the activities of the following groups of extortionists using the same encryptors were the most noticeable:

- LockBit is one of the most active encryption groups. It has gone through several iterations of updating its VPO, which also has cross-platform execution. Differs in thorough selection of both affiliates and victims.
- Hive – is distinguished by a particularly aggressive type of behavior, attacks KII objects of various countries, as well as socially significant objects (hospitals, transport, police). In early 2023, the FBI hacked the attackers' servers and the decoder was released.
- Vice Society – extortionists active since 2021, whose main targets are educational and scientific institutions, as well as medical organizations.
- BlackCat (ALPHV) is a relatively new, but no less formidable group of extortionists that consistently attacks large organizations. It is a continuation of DarkSide and BlackMatter, has extensive experience in extortion and was one of the first to use the Rust language to create a cross-platform version of its pest.
- Conti is a long-standing threat that was the leader of the ransomware as a service market before retiring from the scene in May 2022 due to being pursued by intelligence services and breaking up into smaller entities [Vovchak I. S. 2002, p. 18].

Typical threats to enterprise information security include cyberattacks, data loss, social engineering, and insufficient staff skills. These threats are increasingly prevalent worldwide due to the increasing dependence on technology and the increase in the volume of digital information.

Ukraine, like many other countries, also faces these threats. Since the rise of cyberattacks on energy infrastructure, Ukraine has witnessed numerous cyberattacks targeting government institutions, industrial facilities, and the business sector. The country is actively improving its information security efforts by implementing strategies and policies to protect against such threats.

The global trend in the use of digital technologies and the growth of threats to the information security of enterprises indicates the need for constant improvement of security measures and a conscious approach to risk management.

Typical threats to the information security of the enterprise:

1. Cyber attacks: This is one of the most common threats to the information security of an enterprise. Cybercriminals use various methods, such as hacking, phishing, malware injection, etc., to break into an enterprise's system and gain unauthorized access to confidential information.

2. Data loss: Data loss can be a serious threat to the information security of the enterprise. This can happen due to technical malfunctions, system errors, malicious attacks or insufficient data backup measures. As a result, the enterprise can lose confidential information, which can lead to significant financial losses and damage to the reputation.
3. Social Engineering: This is a method used by attackers to gain access to information by manipulating people. For example, attackers may attempt to obtain passwords or other sensitive information by posing as a representative of a business or other trusted organization.
4. Insufficient qualification of personnel: An insider threat can arise as a result of insufficient qualification of personnel or an imperfect information culture in the organization. If employees do not have adequate knowledge of security protocols, policies and procedures, this can lead to unauthorized access to information or loss of privacy.
5. Physical threat: Physical factors such as fire, flood or theft of equipment can affect the information security of the enterprise. For example, a fire can damage server rooms or other devices that store valuable information.
6. Inadequate network security: Lack of adequate security measures in computer networks can lead to unauthorized access to enterprise data. Insufficient network protection, weak passwords, lack of data encryption – all this can become easy prey for attackers [Koval'chuk, V. I. 2020, p. 21].

In order to avoid threats to the company's information security, a number of measures and recommendations can be taken. Here are some important steps that can help keep your information secure:

1. Security policies and procedures: Develop and implement clear security policies and procedures that cover all aspects of the enterprise. These documents should define requirements for passwords, access to systems, data backup, network protection and other aspects of information security.
2. Staff awareness: Educate your staff about information security threats and the importance of following security policies and procedures. Organize training and education programs that provide employees with the necessary knowledge and skills to detect and prevent cyber attacks and social engineering.

3. Anti-virus software and updates: Install reliable anti-virus software on all computers and systems in the enterprise. Update this software and operating systems regularly to ensure protection against new threats.
4. Strong passwords and authentication: Require employees to use strong passwords that contain a combination of letters, numbers, and special characters. Consider implementing two-factor or multi-factor authentication to increase access security.
5. Data backup: Regularly back up all important business data to external devices or cloud storage. Periodically check and restore backups to ensure their availability and integrity.
6. Monitoring and Threat Detection: Establish monitoring and incident detection systems to help detect unusual activity, intrusions, or network anomalies. Quick detection of a threat can help prevent significant consequences.
7. Regular security audits: Conduct periodic security audits and reviews to assess the effectiveness of security measures and identify weaknesses. This will help to make the necessary changes and improve the security system.

It is worth remembering that information security is a continuous process, and it requires constant updating, training and improvement.

Conclusions. To summarize, research and analysis of problems related to information security at the enterprise was conducted.

The main principles and methods of information security marketing management are defined. Marketing management strategies and mechanisms have been developed, which will contribute to effective control over the information security of the enterprise.

So, in the article on marketing management of information security of an enterprise, it was carried out comprehensively, which made it possible to obtain valuable conclusions and recommendations on the practical implementation of management measures to ensure information security. The results of the study will help to increase the level of security of the enterprise's information resources and help to avoid potential threats and risks associated with information security. The result of analyzing will be an adjustment to the marketing strategy.

References

1. Olena Sadchenko, Hanna Obykhod, Ivan Yaroshenko, Ludmyla Levkovska, Oleksandr Deineha, Tetiana Dombrovska (2022) Management of the Economy in the Field of Environmental Management and Energy Security as Components of Sustainable

Development. *J Sustain Res. (Journal of Sustainability Research)*; 4(2):e220008. [in English]. <https://doi.org/10.20900/jsr20220008>

2. Sadchenko O.V. (2021) Convergence of Neuromarketing Technologies in Modern Conditions of Economic Development // Mechanism of economic regulation, № 3. С. 97-107. [in English]. <https://doi.org/10.21272/mer.2021.93.09>

3. Sadchenko O.V. (2021) Innovative marketing management in the system of environmental and economic safety. *Economic innovations*. Т. 23. Вип. 2(79). С. 152-164. [in English]. [https://doi.org/10.31520/ei.2021.23.2\(79\).152-164](https://doi.org/10.31520/ei.2021.23.2(79).152-164)

4. Sadchenko O.V. (2017) Tekhnolohiya blokcheyn v sferi finansovykh posluh pidpryyemstva. *Ekonomichni innovatsiyi*. Vyp. 65. S. 145-154. [in English]. [https://doi.org/10.31520/ei.2017.19.3\(65\).145-153](https://doi.org/10.31520/ei.2017.19.3(65).145-153)

5. Sadchenko O.V. (2020) Basic directions of experience economy marketing development in conditions of sustainable development. *Economic innovations*. Т. 22. Вип. 2(75). С. 101-111. [in English]. [https://doi.org/10.31520/ei.2020.22.2\(75\).101-111](https://doi.org/10.31520/ei.2020.22.2(75).101-111)

6. Sadchenko O.V., Robul I.V. (2020) Economic and environmental marketing space of the economics of experience. *Economic Innovations*, vol. 22, no. 1(74). P. 129-139. [in Ukrainian]. [https://doi.org/10.31520/ei.2020.22.1\(74\).129-139](https://doi.org/10.31520/ei.2020.22.1(74).129-139)

7. Robul YU. V. (2021) Napryamy rozvytku tsyfrovyykh marketynhovykh system na makrorivni v umovakh tsyfrovoyi transformatsiyi ekonomiky. *Marketynh i tsyfrovi tekhnolohiyi*. Т. 5. № 3. С. 72-82. [in Ukrainian]. <https://doi.org/10.15276/mdt.5.3.2021.7>

8. Kucherenko, V. V., Il'yin, V. V. (2019) Informatsiyana bezpeka pidpryyemstva: teoriya, metodolohiya, praktyka. Kyiv: Vydavnychyy dim "In Yure", 250 s. [in Ukrainian].

9. Znakhur S. V. (2009) Z-75 Informatsiyyny menedzhment ta marketynh : konspekt lektsiy. Kharkiv: Vyd. KHNEU. 132 s. [in Ukrainian].

10. Vovchak I. S. (2002) Informatsiyni systemy ta komp'yuterna tekhnika v menedzhmenti: Navch. posib. Ternopil': Kart-blansh. 354 s. [in Ukrainian].

11. Koval'chuk, V. I. (2020). Upravlinnya informatsiynoyu bezpekoyu pidpryyemstva. Kyiv: Vydavnytstvo "Naukova dumka", 200 p. [in Ukrainian].

12. Upravlinnya informatsiynoyu bezpekoyu. Konspekt lektsiy [Elektronnyy resurs] : navchal'nyy posibnyk dlya studentiv spetsial'nosti 125 «Kiberbezpeka» / KPI im. Ihorya Sikors'koho ; uklad.: S. O. Nosok, O. M. O. M. Fal', V. M. Tkach. Elektronni tekstovi dani. Kyiv : KPI im. Ihorya Sikors'koho, 2021. 258 s. [in Ukrainian].

13. Dovbysh, I. YU., Chepurko, V. V. (2017). Analiz ryzykiv v informatsiynykh systemakh. Kyiv: Vydavnychyy dim "Kyyevo-Mohylyans'ka akademiya", 180 s. [in Ukrainian].
14. Antonyuk L.V., Sytnikov V.O. (2018) Informatsiyna bezpeka pidpryyemstva: navch. posibnyk. Kyiv: KNEU. [in Ukrainian].
15. Posun'ko M.S., Cherkasova V.YU. (2019) Upravlinnya informatsiynoyu bezpekoyu pidpryyemstva: navch. posibnyk. Kharkiv: Natsional'nyy tekhnichnyy universytet "Kharkivs'kyi politekhnichnyy instytut". [in Ukrainian].
16. Sil'chenko O.V., Korchevna O.M., Korchevnyy S.YU. (2019) Informatsiyna bezpeka pidpryyemstva: navch. posibnyk. Kyiv: KNEU. [in Ukrainian].
17. Sadchenko, O. O (2018). Socjetalnym systemie innowacyjnego rozwoju społeczeństwa. / Innovations in science, society, economics: monograph (Poland) Scientific editing Zbigniew Malara, Jan Skonieczny. Wroclaw, Wroclaw Polytechnic Institute. P. 87-95. [in Polish].