Journal scientific and applied research, vol. 24, 2023
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

A MODEL FOR EVALUATING INFORMATION SECURITY SYSTEMS IN INDUSTRIAL ENTERPRISES AND ASSESSING ITS IMPACT ON INCREASING THE COMPETITIVENESS OF ENTERPRISES

Zuhran Kadieva, Krasimira Dimitrova

TECHNICAL UNIVERSITY OF VARNA; DEPARTMENT OF INDUSTRIAL MANAGEMENT
VARNA 9010, STUDENTSKA STR. 1

E-mail: kadieva@tu-varna.bg,
E-mail: krasimira.dimitrova@tu-varna.bg

Abstract: *Globalization covers all spheres of life and economy in the modern world. The innovative development of information and communication technologies is a key factor in maintaining the competitiveness of companies on local, regional and global markets, which, however, is associated with certain risks.*

Information systems contribute to increasing the productivity of companies by catalyzing innovation and thus organizations gain an advantage over other players in their market. This process over the last few decades has established itself as a determining factor in the global market. The innovative development strategy of companies leads to competitive recovery, expansion and consolidation of market positions. In the fight against competitors, companies are looking for new solutions to optimize business, introducing intelligent information technologies in order to reduce the probability of making incorrect management decisions that would lead to adverse consequences.

Key words: *digitization, information technology, information systems, information security, risk, cyber security, competitiveness*

INTRODUCTION

Digitalization of industry or integration of information technology in industry is increasingly becoming an efficiency tool contributing to the increase of competitiveness of all industries.

The development of information and communication technologies affects all categories of activities, allows computer assistance in technological development and automation of various production and management processes. The information revolution is impacting competition by creating a competitive advantage by giving companies new ways to stay ahead of their competitors. It

changes the industrial structure, which in turn leads to a change in the rules of competition.

1. Impact of information technology on the value chain

The modern business environment confronts organizations with the need to constantly change their business practices and procedures in order to respond adequately to the requirements, expectations and needs of customers and competition. A 2008 study by the IT Governance Institute indicates that the top 10 most important business goals related to information technology, consolidated across a number of industry sectors, are:

- improving customer orientation and service;
- ensuring compliance with external laws and regulations;
- establishing continuity and accessibility of services;
- management of IT business risks;
- offering competitive products and services;
- improving and maintaining the functionality of business processes;
- ensuring a good return on business investments;
- acquiring, developing and maintaining qualified and motivated people;
- creating flexibility in response to changing business requirements;
- obtaining reliable and useful information for making strategic decisions.

Information technology is changing the way businesses operate, affecting the entire process by which companies create their products. An important concept that emphasizes the role of information technology in competition is the "value chain". A company's value chain is a system of interdependent and related activities, where the way one activity is performed affects the cost or efficiency of other activities. The company's infrastructure, including functions such as production, placement, legal and accounting and general management, supports the entire chain.

Good relationship management is a significant source of competitive advantage. Relationships not only connect the elements of the value chain within a company, but also create interdependencies between its chain and those of its suppliers, partners and other stakeholders. By optimizing these connections any company can create a significant competitive advantage.

An essential function of a company's value chain is competitive cost advantage or differentiation. The value of a given firm reflects the total cost of carrying out all its activities compared to its competitors. In the search for competitive advantage, companies often differ in terms of their competitive scope or the scope of their operations. (Fig. 1)

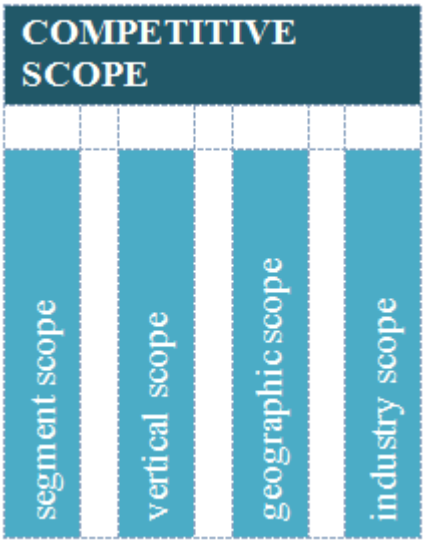

Fig. 1. Key dimensions of competitive scope

Information technology permeates the value chain at every point, transforming the way value activities are performed and the nature of the relationships between them, affecting competitive scope and reshaping the way products meet customer needs.

The structure of an industry is shaped by five competitive forces, namely: the power of buyers; the power of suppliers; the threat of new entrants; the threat of substitute products and/or rivalry between existing competitors. Information technology can change each of the five competitive forces, and hence the attractiveness of an industry.

Information technology is changing the relationship between scale, automation and flexibility. In today's economic environment, large-scale production is far from an essential factor in achieving automation, which in turn removes barriers to entry in a number of industries. At the same time, automation no longer necessarily leads to flexibility. Computer-aided design not only reduces the cost of designing new products, but also greatly reduces the cost of modifying or adding features to existing products. The cost of adapting products to market segments decreases, affecting the pattern of rivalry between industries and companies.

Automation and flexibility are achieved simultaneously and this changes the pattern of rivalry between competitors. The reduction in product design costs through automation combined with the increase in flexibility is undoubtedly leading to increased opportunities for customization and catering to small niche markets.

3. Creating a competitive advantage

Information technology in a company has a significant impact on competitive advantage, regardless of cost or differentiation. They affect value activities by allowing companies to gain competitive advantage by exploiting changes in competitive scope.

Cost reduction. Information technology can change a company's costs in every part of the value chain.

Improving differentiation. Information technology enables product customization, the key differentiator in the buyer's value chain.

Change in competitive scope. Information technology can change the relationship between competitive scope and competitive advantage. Information technology enhances a company's ability to coordinate regionally, nationally, and globally, which in turn can unlock the power of a wider geographic reach to create a competitive advantage.

The information revolution creates relationships between previously separate industries. An important example of this is the convergence of computer and telecommunications technologies, which is having a profound impact on the structure of both industries. However, the benefits of extending reach are only possible when information technology distributed throughout the organization can communicate.

4. The role of information systems in the management of organizations in the 21st century

Management information systems focus on the use of information and communication technologies in the management of various business organizations.

In the 21st century, almost all organizations use information and communication technologies to more effectively manage enterprise operations, help managers make decisions and achieve competitive advantage, and ensure seamless internal and external communication with their employees. , customers, partners and other stakeholders.

Today, the focus of companies is global competitiveness, as the main tool for this is modern information and communication technologies (ICT), which are used by companies to provide products and services of the highest quality at affordable prices and enter new markets through e-commerce. The global market provides companies with a chance for greater revenue and greater business prospects. To help them grow and remain globally competitive, companies are investing in advanced information systems (ERP systems) that help companies manage their operations seamlessly across the globe by eliminating the inaccuracy of paper-based tracking. These systems integrate the various functional areas of the business and provide consistent real-time data for rapid decision making. ERP uses common software that connects various

functional departments such as finance, human resources, production, warehousing, planning, purchasing, inventory, sales and marketing on a modular basis.

Today's world is a world of knowledge. Knowledge becomes an invariable element of competitiveness and success in the production and consumption of a good or service. Therefore, it is vitally important that the information is safe and reliable. Effective process management requires information security.

Today, all kinds of valuable information are stored in a computer environment. Information security is of paramount importance to ensure the business continuity of any organization and to ensure the protection of the organization's critical and confidential information and other information assets, especially in an electronic environment.

Information security management is increasingly important in a way that covers ever-changing risks and the application of international standards, relevant national or international legal regulations, commercial obligations, measurement methods, technology development and changing business processes.

5. Importance of Information Security Risk Measurement

One of the most important challenges for all organizations is the protection of the information at their disposal - intellectual property, know-how, lists of customers and suppliers. Information, in all its forms - electronic and physical, must be reliably protected both from external attacks - hackers or natural disasters, and from internal - current and former employees, partners and suppliers. Their right of access to the organization's resources such as systems, networks and data requires that protection against unregulated leakage of information follows a strategy different from that of traditional protection against threats external to the organization. [4], [5]

There are numerous methods for measuring and assessing information security risk, as well as a wide range of software applications that are used in implementing these methods.

6. Major threats in cyberspace

With the evolutionary development of technologies, requiring new approaches to communication and data storage, new operating systems, protocols or simply their new versions, new vulnerabilities appear, leading to new threats and, accordingly, attacks. Periodic study, research, systematization and development of new protective procedures, techniques, mechanisms and solutions are of vital importance for modern information security.

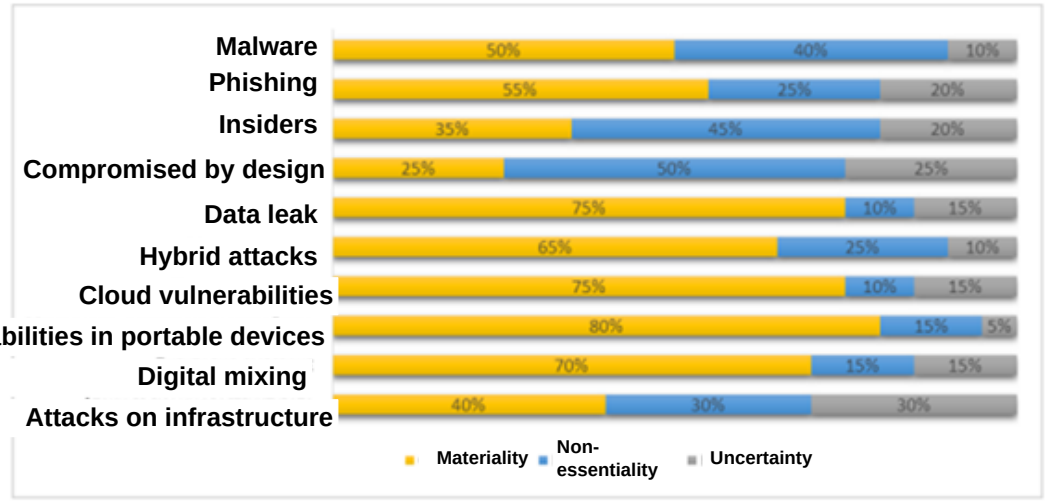

Fig. 2. Top 10 Cyber Threats in 2019

In Fig. 2 shows the summary picture of significance for the 10 areas of cyber threat research in 2019: [6]

1. Exposure to third parties;
2. Management of software updates and patches;
3. Cloud Vulnerabilities;
4. New varieties of "Phishing" attacks;
5. Ransom attacks;
6. Confusion between concepts defined in standards and regulations and real protection of information assets;
7. Mobile Security Threats;
8. The Bring Your Own Device (BYOD) concept;
9. Internet of Things (IoT);
10. Obsolete hardware.

Current threats for 2021 are related to Covid-19. The main results of the analysis can be summarized around the following ten most current risks and threats of a techno-social type (Fig. 3): [7]

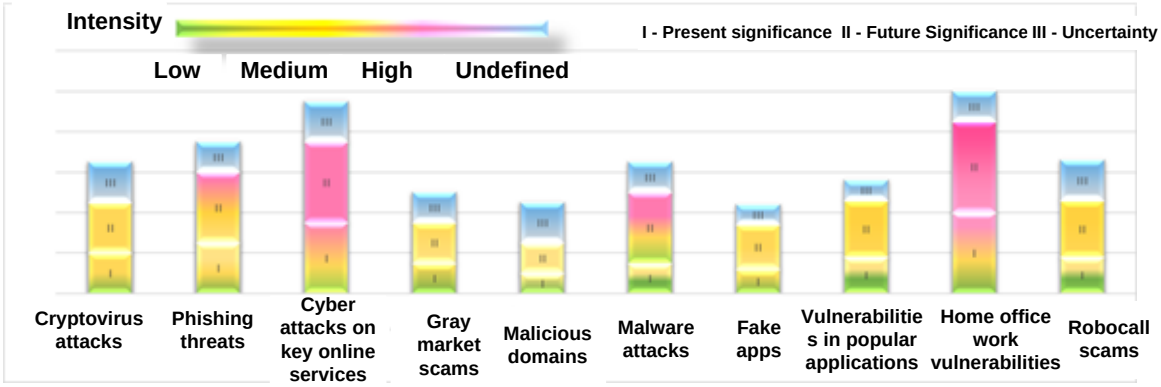

Fig. 3. Summary picture of the current and future significance of the top 10 techno-social risks and threats related to COVID-19 [7]

Major Cyber Security Threats in 2022

According to data from the EU Agency for Cybersecurity (ENISA - European Union Agency for Cybersecurity), eight main types of threats have been identified for 2022 in Table 1: [8]

Table 1. Eight main types of threats for 2022

1. Ransomware	In these attacks, hackers attempt to gain control of a device's data and then demand the payment of a certain amount to gain access to the data back. A study by ENISA shows that in the period 2021/2022. about half of the surveyed companies or their employees have been the target of such attacks
2. Malware	Malware includes computer viruses, worms, Trojan horses, and spyware that attempt to infiltrate and harm a system
3. Exploiting Human Errors	Many hackers try to trick their victims into opening a dangerous file or visiting a website. In this way, criminals can gain unauthorized access to computer systems or data. Around 60% of system breaches in Europe, the Middle East and Africa are linked to the use of human error, ENISA research shows.
4. Threats to data	Many companies and technologies, including artificial intelligence, depend on the use of large amounts of data, making data an attractive target for cybercriminals. Threats to data can be classified as breaches (deliberate attacks) and leaks (inadvertent release of data).
5. Threats against the availability of data or services	These are some of the most dangerous attacks for information systems, as they are associated with attempts to terminate user access. One of the most commonly used ways is by overloading the network infrastructure and taking the system out of service.
6. **Threats to Internet Access**	This includes taking control or destroying the internet connectivity infrastructure.
7. Disinformation and Propaganda	Advances in technology allow the creation of fake images, video or audio clips that are almost indistinguishable from the real thing.
8. Attacks on the supply chain	Some cybercriminals try to take advantage of the relationships that exist between supplier companies and customers by attacking them simultaneously. Organizations are vulnerable to such attacks because they often depend on multiple suppliers with whom they enter into complex relationships

Depending on the specifics of their activity, organizations generate, use or process data that are diverse in type, content and structure. Each organization must determine for itself which data is vital to its operation and which is secondary or supporting. Sensitive data is that data that an organization cannot afford to lose, be disclosed, or come into the hands of unauthorized persons. Main types of sensitive data are systematized in Table 2.

Table 2. Basic types of sensitive data

Intellectual Property	Production and placement data	Legal - financial data
•technological documents •formulas •inventions •new product design •development plans •source code	•pricelist •customer lists •orders •customer product profiles •supplier list •inventories •contact history •purchase information •purchase history •user preferences •status of payments •trade discounts •payment conditions	•personal data •legal documents •bank payments •non-public financial data •sales volume •potential profits •expected sales •financial balance sheets •transaction history •commercial contracts

In information security, a number of protection approaches are used, each of which has a specific area of application. In Fig. 4 shows a multi-layered model of information protection. [9]

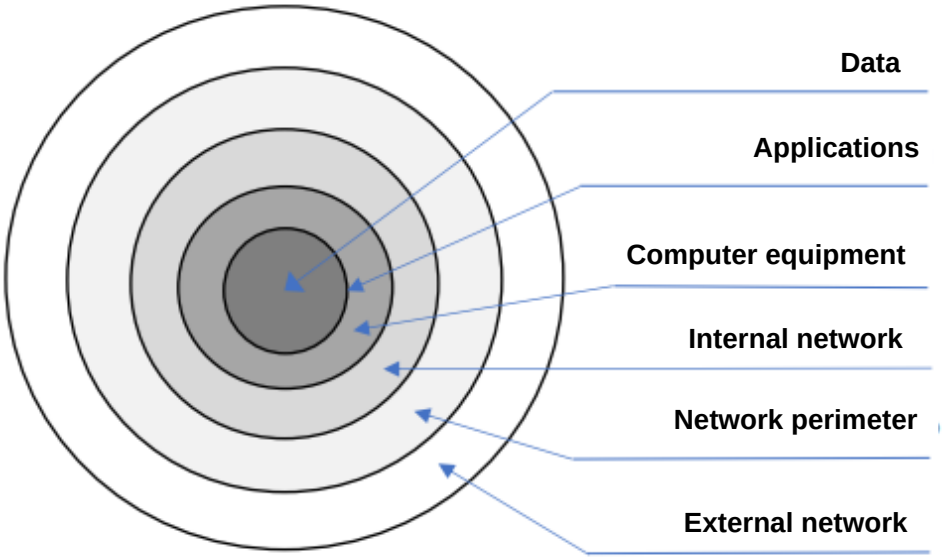

Fig. 4. Multi-layered protection model [9]

Each security layer is subject to different types of threats and has a certain set of security approaches to protect against them. Therefore, the information security concept of any enterprise must meet the requirements of all these elements of the system. [9]

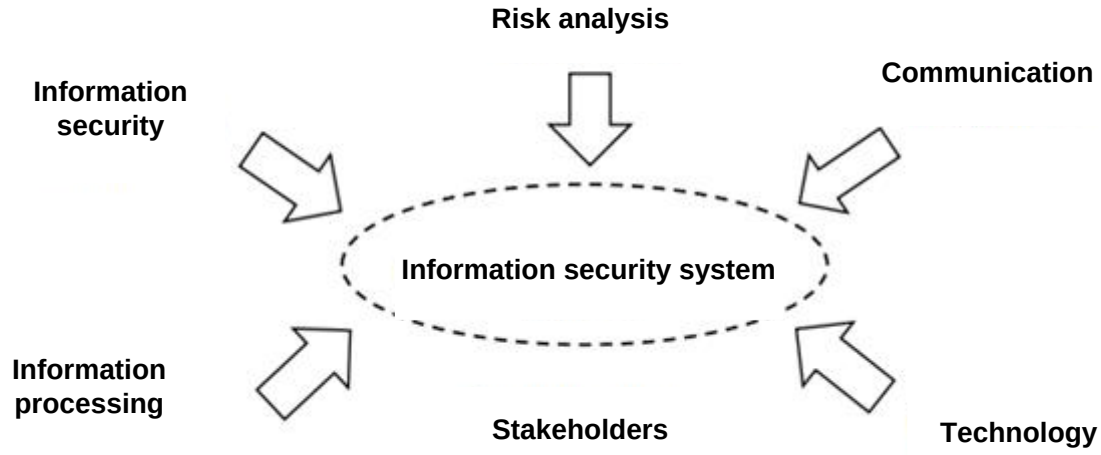

Fig. 5. Information security system field [9]

7. A model for information security and protection of corporate knowledge in industrial enterprises

The security policy must provide for the complex use of legal and moral and ethical standards, organizational (administrative) measures, physical, technical (hardware and software) methods and means of information protection, as well as determine the rules and procedures for their application in the information system. [3]

Conceptual positions for the protection of the corporate information system
➢ The development of information resources is considered as a set of processes, procedures, individual operations that ensure the development of various properties of information.
➢ The set of information properties is determined by the level of management and, accordingly, those tasks that are primarily solved by the entity in the course of its activity to achieve the goals.
➢ The security of the information system is determined by the safety of the operation of its subsystems and components, which ensure the confidentiality, integrity, accessibility of information at all levels of enterprise management.
➢ The main function of the information system - the provision (support subsystem) of the secure development of information properties at all levels of enterprise management.

Fig. 6. The conceptual provisions for the protection of the information system of the enterprise

Ensuring the information security of the company is possible by adopting a functional model for the protection of the information system of the enterprise (Fig. 7).

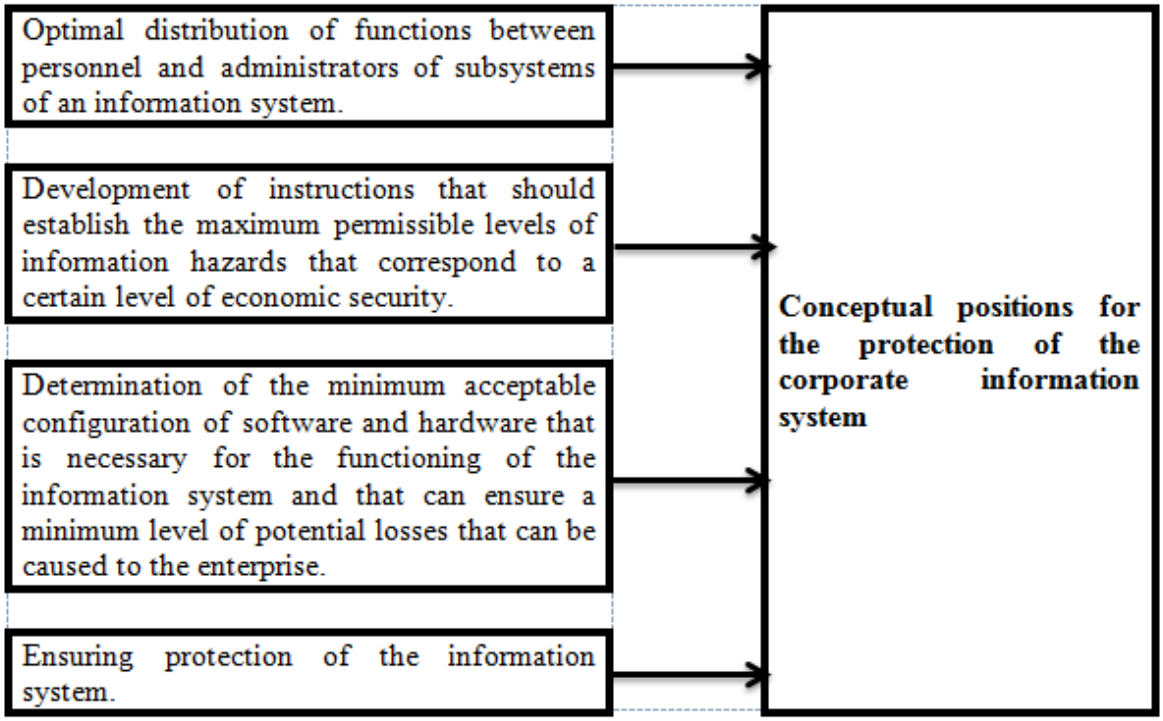

Fig. 7. Functional model for the protection of the corporate information system

The information security model shown in Fig. 7 allows to detail the different levels of enterprise management.

Special protection in the current operating conditions of the corporate information system requires information that is a trade secret. The content and volume of information constituting a trade secret and the methods of their protection are determined by the enterprise. Therefore, the right to trade secret protection must be enshrined in the company's articles of association. [2] This allows to build relations with partners, own employees and to organize a trade secret protection regime in the enterprise on a legal basis.

Equally important for the creation of the trade secret storage regime is the formation of the enterprise's information system and, in particular, the order for the distribution of trade secret information, as well as for the storage, reproduction and destruction of documents - carriers of trade information.

The next step in consolidating a company's trade secret protection rights should be the right relationship with their counterparties. For this purpose, contracts for the purchase and supply of goods, components and raw materials, if they are subject to trade secrets, must provide for the preservation of confidential information about the terms of these contracts.

The ultimate goal is to increase the development of methods for increasing the stability of the information system by minimizing the risks associated with the task of damaging both the enterprise's activity and its information infrastructure and increasing the stability of all information

processes, including methods and means of obtaining, entering, processing and analyzing information.

Every single enterprise is created with a certain business model and work processes, which in most cases differ from another company. Sometimes this happens even when they are from the same sector and of similar scale. In simulation modeling, the structure of the modeled system is adequately shown in the model and the processes of its functioning are reproduced on the constructed model. Such modeling can be seen as conditions that determine the state of the system in the future. Simulation modeling allows obtaining the performance of processes over time at certain values. [1]

The main role of cyber security is to allow the enterprise to carry out its business normally, taking into account its resources, needs and customers. Because of these characteristics, the appropriate cybersecurity measures for one enterprise differ from those of another.

The system for the protection of the information assets of the production enterprise should include the following stages and modules:

Step 1: IDENTIFICATION
> structure of information flows; > threats, vulnerabilities and asset risk.
Step 2: PROVIDING PROTECTION
> cybersecurity policy > management of access to assets and information; > user training; > the protection of sensitive data; > regularly creating backup copies of data; > regular maintenance of information systems
Step 3: INCIDENT DETERMINATION
> drawing up an incident detection procedure; > maintaining security logs; > knowledge of common data flows
Step 4: RESTORATION OF SECURITY
> preparing rules for reporting incidents; > maintaining recovery plans.

Fig. 8. Stages and modules of the system for the protection of the information assets of the production enterprise.

In general, the structure of information flows - of receipt, processing and storage of external and internal data and information in production enterprises can be represented by the model shown in Fig. 9.

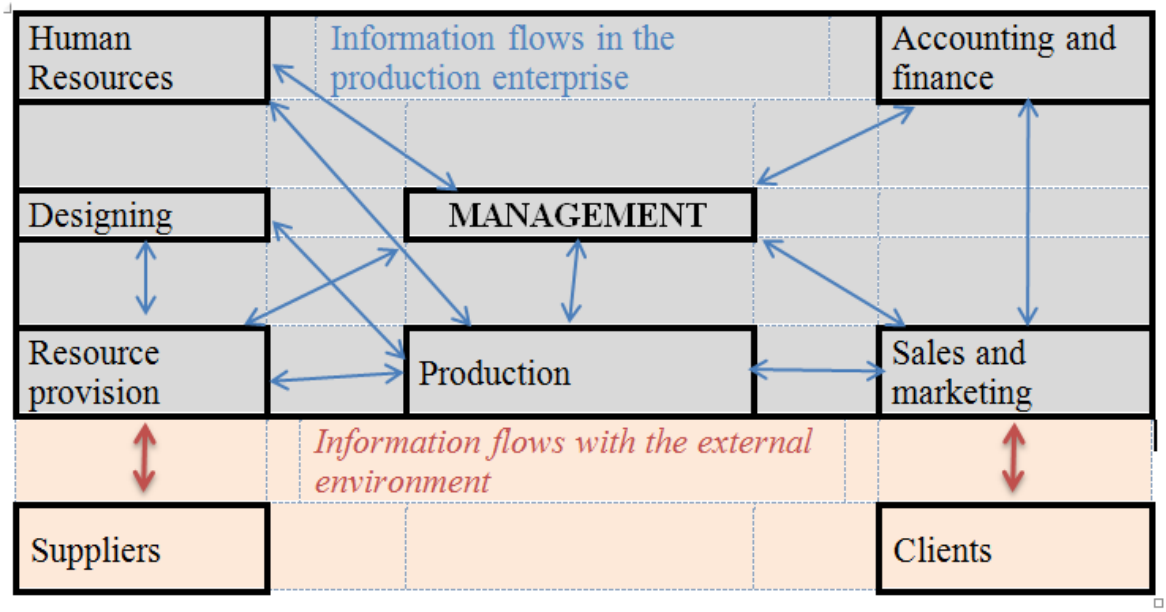

Fig. 9. Model of the structure of information flows

Cybersecurity policies must be integrated with other enterprise risk considerations (investment, financial, reputational). Information policy management includes some very important points about information and its security in the enterprise, especially when it is distributed to third parties who have access to the information and systems of the organization. The information security policy should be reviewed regularly based on an established process and take account of changing circumstances.

An extremely important factor in information security is the management of access to assets and information. It is mandatory to verify the authenticity of users (passwords, multi-factor authentication) before granting them access, as well as ensuring a unique, personal account for each employee with access only to applications and data necessary to perform the tasks related to their position.

Regular training of all users to familiarize them with the company's cybersecurity policies and procedures and maintain a good level of threat awareness is also of utmost importance.

Protection of sensitive business or customer data should be protected by encryption, both while stored on computers (data at rest) and during transfer (data in transit). Regular creation of backup copies of the data/backup. Backing up is an increasingly common practice and according to ENISA, after the Covid crisis, more and more SMEs back up their data (94% vs. 90% before the crisis). These copies should be stored outside the network, for example in a separate cloud (automatically) or on a device that is not connected to the internal network. Thus, in the event of a phishing attack, hackers will not have access to these copies.

An essential element in ensuring information security is maintaining the information systems and installing software patches as soon as they are

available. The ultimate goal is to increase the stability of the information system by minimizing the risks associated with the task of damaging both the enterprise's activity and its information infrastructure and increasing the stability of all information processes, including methods and means of obtaining, inputting, processing and analysis of information.

On the base the above, Fig. 10 presents an author's model of an IT security system of an industrial enterprise.

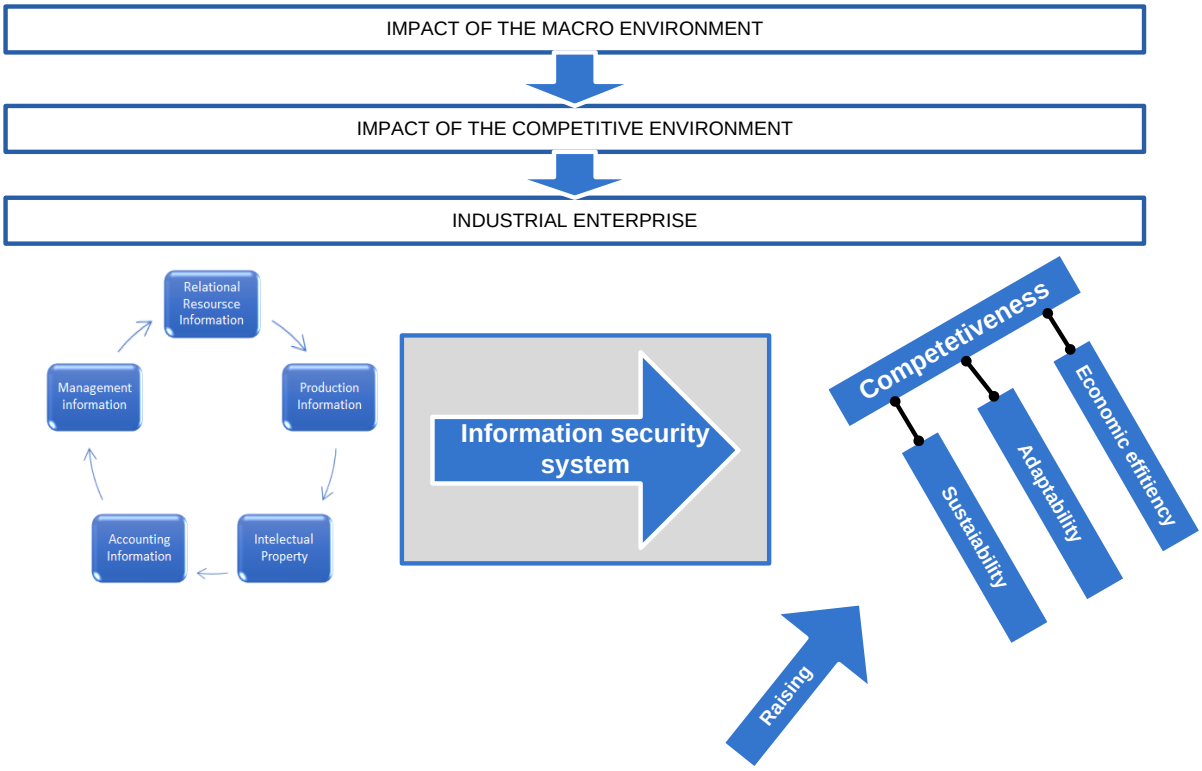

Fig. 10. Model of IT security system in industrial enterprise

Conclusion

In conclusion, it should be noted that the protection of the corporate information system can be perceived as a technical task in its nature, but in reality it is the basis of doing business, since the competitive positions and financial health of any company can be threatened.

References

[1] Antonov, A. (2023). Simulation of multimodal transport with anylogic: simulation of multimodal transport with anylogic. Journal scientific and applied research, 19(1), 33–38. https://doi.org/10.46687/jsar.v19i1.291

[2] Kozhushko O (2014) Semantic model of industrial enterprise intellectual capital protection management system. In The International Scientific and Practical Congress of Economists and Lawyers “The genesis of genius”, pp. 123-126

[3] Kurkin MV, Kozhushko OV, Zima OG, Ponicarov VD, Information Security and Protection of Intellectual Capital: a Manual, 1st edn. (Kiev: Nauka, 2016), 256 p.
[4] Rhodes-Ousley M., "Information Security the Complete Reference", 2nd Edition, The McGraw-Hill, 2013
[5] Suryateja P.S., "Threats and Vulnerabilities of Cloud Computing: A Review", International Journal of Computer Sciences and Engineering, Volume 6, Issue 3, published 30.03.2018
[6] Минчев З., Кутинчев П., Гайдарски И.. Топ 10 заплахи за киберпространство през 2019. IT4Sec Reports, Institute of ICT, Bulgarian Academy of Sciences, 2019, ISSN:1314-5614, DOI:10.11610/it4sec.0133, 133-1-133-12, Национално академично издателство, https://doi.org/10.11610/IT4Sec.0133
[7] Минчев З., Гайдарски И., Кибер рискове, заплахи и мерки за защита, свързани с COVID-19. CSDM Views, Number 37, 2020, ISSN 1314-5622, https://www.bas.bg/?p=29870
[8] https://www.europarl.europa.eu/news/bg/headlines/society/20220120STO21428/kibersighurnost-ghlavnite-i-novite-zaplakhi#ssh
[9] Gaidarski I., Method and models for the development of information security systems in organizations (Dissertation) Sofia, 2022.https://www.iict.bas.bg/konkursi/2022/IGaidarski/disertatsia.pdf