DOI: https://doi.org/10.12958/1817-3772-2024-4(78)-190-193

UDC 330.322:004.9:628

V. Diachenko,
PhD (Economics), Associate Professor,
ORCID 0000-0002-0055-9256,
Scopus Author ID 57994193000,
e-mail: dyachenko.v@ukr.net,
Kyiv University of Intellectual Property and Law,
National University "Odessa Law Academy"

CONSIDERING RISKS WHEN USING INFORMATION TECHNOLOGY

The Internet, information and communication technologies (ICT), the provision of services in digital format, which have become an indispensable condition of today, from electronic document management, online stores, online banking, intelligent business management systems, require not only knowledge, skills and abilities in using ICT, but also experience in managing information protection and cyber security systems, since cyber threats are evolving intensively, cyber crimes are constantly improving, acquiring transnational features.

Analysis of recent research and publications. A number of well-known domestic scientists have devoted attention to the study of risks, threats and dangers when using information and communication technologies, in particular, O. Haiduk and V. Zverev analyzed cyber threats in the context of the rapid development of information technologies (Hayduk; Zverev, 2024, p. 229). A. Lyseyuk and T. Svintsytska investigated the legal support for Ukraine's cybersecurity under martial law and European integration (Lyseyuk; Svintsytska, 2024). K. Movchan identified cybersecurity risks in the era of robotics (Movchan, 2023).

The purpose of the study is to identify the main types of risks and threats in cloud data storage.

Presentation of the main research material. Under the conditions of the modern legal regime of martial law in Ukraine and the rapid growth of cyber risks and cyber threats, there is an urgent need to train highly qualified specialists in this field who could analyze already implemented measures in the field of protecting computer and communication networks from cyber attacks, as well as predict possible risks and threats and promptly respond to their manifestations.

Systemic power outages that occurred in certain periods caused disruptions in the provision of electronic services. And cyberattacks caused the blocking of the activities of state authorities and the work of enterprises, institutions and organizations important for the economy and the formation of the foundations of national security.

In today's conditions, it is extremely necessary to strengthen the cyber security of enterprises, institutions, organizations and critical infrastructure, adhering to the principle of "security-first thinking".

In order to form basic knowledge of cybersecurity, a number of educational institutions offer free courses, in particular, the Higher School of Public Education offers a general short-term program "Fundamentals of Cybersecurity and Counteraction to Disinformation", which provides for a distance learning form, two areas - information security and cybersecurity. The program's drafting partner is the "International Academy of Information". The goal of the program is to develop students' cybersecurity competencies, including the use of tools that ensure confidentiality, integrity or availability of data, prevent cyberattacks and counter disinformation by acquiring professional skills in working with information, mastering digital literacy and the basics of cybersecurity.

Taking into account today's challenges, not only cyber literacy of ICT users is needed, but also coordination and reorientation of research in the field of computer development, because new generations of software and hardware must guarantee the security of operations and compliance with the principle of confidentiality of private, business or state information.

The prerequisite for forming a circle of highly qualified specialists in the field of information technologies is the training of higher education applicants in accordance with the educational program "Management of Information Protection and Cybersecurity Systems", the purpose of which is the development of social and intellectual capital by training highly qualified, socially responsible cybersecurity specialists with a high level of ethical standards and professional dignity in the field of information technologies, who, in the context of promoting the implementation of cybersecurity and information security strategies, meet the modern needs of the labor market, society and the state, are focused on protecting the rights, freedoms and legitimate interests of citizens in the information space, possess theoretical and practical knowledge and skills necessary to understand the principles of managing information and/or cybersecurity systems and complexes of the state as a whole or individual entities of their infrastructure, are capable of continuous learning and self-improvement, and apply methods and means of technical and cryptographic protection of information from the risk of external cyber influence, which involves the development of new, improvement or further development of existing developments and research.

The educational and professional program "Management of Information Protection and Cyber-security Systems" is based on well-known scientific results in the field of information technologies and is focused on the formation of a complex of knowledge, skills and abilities in modeling, design, development, integration and maintenance of information and/or cybersecurity systems and complexes based on modern information and communication technologies, which provide higher education graduates with broad opportunities for self-realization in the field of employment and career growth.

The program provides for the formation of competencies in higher education applicants in modern methods, techniques, information and communication technologies and technologies for ensuring information and/or cybersecurity, necessary for solving basic tasks and practical problems in the IT sphere, taking into account the methodology of system IT audit for identifying cyber threats and intrusions, as well as current trends in the development of new, improvement or further development of existing developments and research in the field of information technologies.

Among the features of the educational program "Management of Information Protection and Cybersecurity Systems" it is worth highlighting the combination of a complex of educational components that form competencies in the specialty, take into account the strategic directions of ensuring cybersecurity and information security of Ukraine, focused on the development of the intellectual capital of the individual, with an emphasis on the ability of applicants to understand the content of managing information and/or cybersecurity systems and complexes, the application of modern concepts and tools for ensuring information security, the methodology of system IT audit to counter cyber threats and the design of new, improvement or further development of existing developments and research.

The program provides for the availability of tools and equipment, in particular modern software and hardware of information and communication technologies, which provides for the use of the open source SimuLand laboratory environment developed by Microsoft as part of interactive training, designed to help deploy a laboratory environment that reproduces well-known methods used in real attack scenarios, actively test and verify the effectiveness of the corresponding detections of Microsoft 365 Defender, Azure Defender and Microsoft Sentinel, as well as expand threat research using telemetry and forensic artifacts created after each simulation exercise, test and improve protection.

One of the current issues is the use of the Internet, in particular, cloud services. Cloud technologies are a service that allows remote use of data storage, processing and storage facilities.

The basic concept of cloud storage and data processing is based on various models of providing IT services, including: CaaS, WaaS, SaaS, DaaS, PaaS, EaaS (Table 1). Among the services offered, it is worth highlighting SaaS (Software as a Service) as a profitable alternative to purchasing software, because SaaS allows you to receive software as a service, rather than expensively purchasing licensed programs.

Table 1

Features of providing IT services via cloud services

Service name	Description
CaaS (Communication as a Service)	Provides communication services: IT telephony, postal services, etc.
WaaS (Workplace as a Service)	Specializes in providing virtual workplaces
SaaS (Software as a Service)	The provider hosts the application, and users pay for the service for using the application
DaaS (Data as a Service)	Provides data on demand to the user regardless of his location
PaaS (Platform as a Service)	Provides an integrated IT platform for creating, deploying, testing and supporting applications
EaaS (Everythinge as a Service)	A complex of cloud services that meets a wide range of user needs

Among the popular SaaS products is Salesforce.com (https://www.salesforce.com/) – the world's largest SaaS provider (Salesforce, 2024), which provides access to its own CRM system (customer relationship management system).

The set of applications from Google Inc. (https://www.google.com/) includes an email service with advanced capabilities and other effective functionality for optimizing activities, both private and business or government (Google Inc., 2024).

Among the popular and easy-to-use cloud storages, we can arbitrarily single out:

– Google Drive – a data storage owned by Google Inc., which allows users to store information on cloud servers and share it with other users on the Internet.

– OneDrive (officially Microsoft OneDrive) – a file storage based on the cloud organization of an online file storage service with additional file sharing functions (Microsoft OneDrive, 2024);

– Dropbox – a file sharing and file synchronization service from Dropbox Inc., located in San Francisco, USA (Dropbox Inc., 2024).

When using cloud services, it is necessary to take into account the risks:

– cloud services are provided by a specific company, therefore the preservation of private information completely depends on it;

– you must be online to view your own information or process it;

– a power outage may cause a temporary inability to access your own databases stored in cloud services.

The above cloud service providers provide protection for personal data, in particular:

– Google Drive provides protection during data transfer;

– Dropbox provides protection through authentication;

– OneDrive provides two-factor authentication.

However, among the main threats to cloud data storage, it is worth highlighting (Table 2):

Table 2

Main types of threats to cloud data storage

Threat	Description
Data theft	Possible when attacking a server when accessing a database of email addresses
Data loss, corruption	Data can be lost or damaged due to system errors, software imperfections of cloud services
Interface vulnerability	Errors in the design of cloud services make them vulnerable to cyberattacks
Adjacent vulnerability	Sharing access to the same resources creates repeated vulnerability

As part of the interactive and practice-oriented training of higher education students in mastering the educational components of the program "Management of Information Protection Systems and Cybersecurity", it is advisable to use a cyber polygon.

The deployment of a cyber polygon on the basis of the Department of Cybersecurity and Information Technologies of the Kyiv University of Intellectual Property and Law – a set of special software and hardware complexes that are combined with wired and wireless means of communication, which can be integrated into the Internet and used to monitor the impact on control systems that may be of interest, to protect their own systems from unauthorized access – contributes to the formation of skills in the use of tactics for predicting cyber attacks, methods for identifying and simulating cyber attacks, and practicing methods for repelling them. The cyber training ground contributes to the formation of a system of professional skills among higher education students, as it allows simulating cyber attacks, cyber attacks on servers that serve the infrastructure of an enterprise, institution or organization to find vulnerabilities, eliminate their vulnerability, establish an effective system for protecting existing computer and information and communication resources, and restore their normal functioning. The software and visualization systems of the cyber training ground contribute to the practice of cyber actions carried out in a virtual environment. The visualization systems provide the ability to simulate cyber attacks that can be carried out on computer networks, which involves reducing or completely avoiding the costs of purchasing cloud technology resources.

The training cyber polygon allows you to simulate cyberattacks, cyberattacks on servers that serve the infrastructure of a higher education institution to search for vulnerabilities, eliminate their vulnerability, establish an effective system for protecting existing computer and information and communication resources, restore the normal functioning of information, information and telecommunication (automated) systems after the implementation of threats, cyber-attacks, failures or failures of various levels and origins.

Conclusions and prospects for further research. Under the conditions of the modern legal regime of martial law in Ukraine and the rapid growth of cyber risks and cyber threats, there is an urgent need to analyze and determine trends and tendencies in the course of cyber threats, their mutual influence and factors that are not directly related to cyberspace, which are capable of contributing to the emergence of a significant negative impact on the processes of development of computer and information and communication systems and networks. Identification of new types of threats and risks, determination of their key characteristics will contribute to the delineation of their essential properties, the development of algorithms for their analysis and methods for their management.

Conclusions and prospects for further research. Under the conditions of the modern legal regime of martial law in Ukraine and the rapid growth of cyber risks and cyber threats, there is an urgent need to analyze and determine trends and tendencies in the course of cyber threats, their mutual influence and factors that are not directly related to cyberspace, which are capable of contributing to the emergence of a significant negative impact on the processes of development of computer and information and communication systems and networks. Identification of new types of threats and risks, determination of their key characteristics will contribute to the delineation of their essential properties, the development of algorithms for their analysis and methods for their management.

References

1. Haiduk, O., Zvieriev, V. (2024). Analiz kiberzahroz v umovakh strimkoho rozvytku informatsiinykh tekhnolohii [Analysis of cyber threats in the context of rapid development of information technologies]. *Kiberbezpeka: osvita, nauka, tekhnika – Cybersecurity: Education, Science, Technique*, 3(23), pp. 225-236. DOI: https://doi.org/10.28925/2663-4023.2024.23.225236 [in Ukrainian].

2. Lyseiuk, A., Svintsytska, T. (2024). Pravove zabezpechennia kiberbezpeky Ukrainy v umovakh voiennoho stanu ta yevrointehratsii [Legal support for Ukraine's cybersecurity in the context of martial law and European integration]. *Pravo ta innovatsii – Law and innovations*, 4 (48), pp. 32-38. DOI: https://doi.org/10.37772/2518-1718-2024-4(48)-4 [in Ukrainian].

3. Movchan, K. O. (2023). Ryzyky kiberbezpeky v epokhu robototekhniky [Cybersecurity risks in the age of robotics]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Tekhnichni nauky – Scientific notes of the V. I. Vernadsky TNU. Series: Technical Sciences*, Vol. 34 (73), no. 4, pp. 79-83. DOI: https://doi.org/10.32782/2663-5941/2023.4/13 [in Ukrainian].

4. Salesforce.com. Retrieved from https://www.salesforce.com/.

5. Google.Inc. Retrieved from https://www.google.com/.

6. Microsoft OneDrive. Retrieved from https://www.microsoft.com/uk-ua/microsoft-365/onedrive/online-cloud-storage.

7. Dropbox Inc. Retrieved from https://www.dropbox.com/uk_UA/.

Дяченко В. Урахування ризиків при використанні інформаційних технологій

У статті досліджено ризики та загрози при використанні інформаційно-комунікаційних технологій. Мета дослідження – визначити основні типи ризиків і загроз при зберіганні даних у хмарі. Для досягнення цієї мети визначено комплекс заходів щодо формування основ кібербезпеки. Наголошується, що з урахуванням викликів сьогодення необхідна не лише кіберграмотність користувачів інформаційно-комунікаційних технологій, а й координація та переорієнтація досліджень у сфері комп’ютерних розробок, адже нові покоління програмного та апаратного забезпечення мають гарантувати безпеку діяльності та дотримання принципу конфіденційності приватної, ділової чи державної інформації. Методологічні аспекти дослідження враховують концепцію виявлення закономірностей виникнення нових ризиків і загроз інформаційній та кібербезпеці в сучасних умовах стрімкого розвитку інформаційних технологій. У роботі використано комплекс взаємопов’язаних наукових методів, зокрема: діалектичного, порівняльного аналізу та логічного при дослідженні сутності загроз інформаційній безпеці в сучасних умовах невизначеності та ризику; емпіричний метод дослідження при порівнянні особливостей надання хмарних послуг ІТ-сервісами; системний підхід при визначенні комплексу заходів щодо формування основ кібербезпеки. Наукова новизна полягає в комплексному підході до вивчення сутності ризиків і загроз інформаційній та кібербезпеці в умовах стрімкого розвитку інформаційно-комунікаційних технологій та при використанні хмарних сервісів. У результаті теоретичного дослідження виявлено ризики та загрози кібербезпеці. Наголошується, що оперативна ідентифікація нових видів загроз і ризиків, визначення їх ключових характеристик сприятиме окресленню їх сутнісних властивостей, розробці алгоритмів їх аналізу та методів управління ними.

Ключові слова: ризики, загрози, інформаційні технології, хмарні технології.

Diachenko V. Considering Risks When Using Information Technology

The article examines risks and threats when using information and communication technologies. The purpose of the study is to identify the main types of risks and threats when storing data in the cloud. To achieve this goal, a set of measures to form the foundations of cybersecurity has been identified. It is emphasized that, taking into account today's challenges, not only cyber literacy of information and communication technology users is required, but also coordination and reorientation of research in the field of computer development, because new generations of software and hardware must guarantee the security of activities and compliance with the principle of confidentiality of private, business or state information. The methodological aspects of the study take into account the concept of identifying patterns of the emergence of new risks and threats to information and cyber security in modern conditions of rapid development of information technologies. The work used a set of interrelated scientific methods, in particular: dialectical, comparative analysis and logical when studying the essence of threats to information security in modern conditions of uncertainty and risk; empirical research method when comparing the features of the provision of cloud services by IT services; systematic approach when identifying a set of measures to form the foundations of cybersecurity. The scientific novelty lies in an integrated approach to studying the essence of risks and threats to information and cyber security in the context of the rapid development of information and communication technologies and when using cloud services. As a result of the theoretical study, risks and threats to cyber security were identified. It is emphasized that the operational identification of new types of threats and risks, the determination of their key characteristics will contribute to the delineation of their essential properties, the development of algorithms for their analysis and methods for managing them.

Keywords: risks, threats, information technologies, cloud technologies.

Received by the editors: 30.10.2024
Reviewed: 25.11.2024