Diachkov Dmytro,
Candidate of Economic Sciences, Associate Professor
Poltava State Agrarian Academy, Poltava, Ukraine

PECULIARITIES OF CLASSIFICATION OF INFORMATION SECURITY THREATS FOR DIFFERENT SUBJECTS OF INFORMATION RELATIONS

The real world geopolitical space and the state's internal relations are formed in conditions of information confrontation. This problem is especially urgent for the Ukrainian business entities and a country as a whole. Despite the uncertainty of the economic vector, the political instability, the instability of information space, Ukraine is under systematic information pressure, which is realized by the occurrence of circumstances or events that may cause violations of information security policy, changes in the properties of information or damage to the automated system. Actually, such events or the potential possibility of their occurrence are threats to information security.

Numerous scientific works of Artemov A., Bishop M., Gliedman C., Horbulin V., Dodonov O., Lande D., Kosogov O., Tuskov M., Semenov V. and other national and foreign scholars are devoted to the determination of the essence of threats to information security and information security. However, the classification of threats to information security, acceptable to practical use in Ukraine, does not exist either at the theoretical, or the practical and legislative level.

In general, any threat [4] is a potentially possible event, action, process or phenomenon that may cause damage to someone else's interests. Obviously, a threat is considered to be one of the key concepts in the field of information security.

Therefore, the Law of Ukraine "On National Security of

Ukraine" states that the threat of information security is an attempt to manipulate the public consciousness, in particular by disseminating unreliable, incomplete or biased information. Additionally, other threats include:

– any slight manifestation of restriction of freedom of speech and access of citizens to information;

– the distribution by the media of a cult of violence, cruelty, pornography;

– computer crime and computer terrorism;

– the disclosure of information constituting state secrets, as well as confidential information that is the property of the state or is aimed at meeting the needs and national interests of society and the state [1].

In the Doctrine of Information Security of Ukraine, signed by the President of Ukraine in July 2009, the following threats to information security of the country are clearly defined:

– distribution of distorted, unreliable and preconceived information in the global information space that harms the national interests of Ukraine;

– external destructive information impact on the public consciousness through the media, as well as the Internet;

– negative information effects aimed at undermining the constitutional order, sovereignty, territorial integrity and inviolability of Ukraine's borders;

– use of mass media and the Internet for propaganda of separatism by ethnic, verbal, religious and other features [2].

In May 2018, the Law of Ukraine "On the Basic Principles of Cyber Security of Ukraine" came into force, which noted that any business entity could be exposed to the cyber threats as a new kind of information danger. Threats of this nature are the existing and potentially possible phenomena and factors that pose a threat to Ukraine's vital national interests in cyberspace, and also have a negative impact on the current state of cybersecurity of the country [3].

Thus, at the legislative level, the issues of defining the nature of threats, their classification and determining the directions for their prevention are considered fragmentarily and at the state level only. As for micro-level entities, the problematic of identifying threats to information security is either considered at the level of theoretical generalizations of individual researchers and research teams, or at the empirical level of business entities.

Consideration of different points of view regarding the essence of information security threats [4-12] allows us to conclude that at present there is no well-founded definition of the essence of information security threats and their unified classification.

On the basis of generalization of theoretical studies, it is worthwhile to note that threats to information security can be either real or those that have already manifested themselves in their negative, destructive impact on the security object, and potential, that is, their negative influence can manifest itself in numerous ways in the near or distant future.

The most common classification of threats to information security is related to the sources caused by human factors, hacking and malicious software and those, caused by natural rather than anthropogenic factors.

“Human factor” (also known as the anthropogenic sources of threats to information security) is related to the subjects whose actions can be qualified as an intentional or accidental violation or a crime. This group of threats is the most voluminous and is of the greatest interest from the point of view of organizing protection, since the actions of the subject can always be forecasted, evaluated and taken adequately. Counteraction methods in this case are manageable and directly depend on the requirements for the organization of information protection.

However, in addition to deliberate violations in this group,

it is also necessary to include “unintentional” violations of information security. According to the statistical data provided by LETA [11], these are as follows:

– every fourth user leaves an opportunity for the malicious intruders to enter the corporate network;

– every second user is not familiar with the rules of information security;

– 2 out of 3 users visit potentially dangerous sites from a desktop PC;

– 1/3 of users store their passwords in an easily accessible place;

– 5% of employees are ready to transfer confidential information to third parties;

– over 60% of mobile phones are not password-protected;

– every third employee constantly uses the same password when registering on the websites;

– 8 out of 10 users do not destroy media containing corporate information.

On the contrary, the second group of threats (i.e. “hacking and malicious software”) contains sources of threats, which are determined by man’s technocratic activity and the development of civilization. These sources of threats are less predictable, which directly depend on the properties of the technology and therefore require special attention. This class of sources of threats to information security is especially topical, because in modern conditions experts expect an increase in the number of man-made disasters caused by physical and moral aging of the technical park of the equipment used, as well as the lack of resources for its renovation.

The third group of sources of threats includes non-anthropogenic factors that combine circumstances that create an insuperable force, that is, those circumstances that are objective and absolute ones. These include natural disasters or other circumstances that can not be foreseen or prevented or

possible to provide, but impossible to prevent. Such sources of threats are completely incalculable in forecasting and therefore measures of protection against them must be applied continuously.

The classification of threats to information security that deserves attention, is offered by VPS.house [12]. This classification is based on the main characteristics and properties of information [6] (See Figure 1).

Among the main factors of influence Artemov A. V. proposes to distinguish the following threats, which cause information losses and lead to various types of harm and increase in losses from illegal actions:

– accidents that cause the failure of equipment and the loss of information resources (fires, explosions, accidents, collisions, falls, exposure to chemical or physical substances);

– breakdown of the elements of information processing equipment;

– effects of natural phenomena (floods, storms, lightning, earthquakes);

– theft of tangible assets and intentional damage to these assets;

– crashes and failure of hardware, software and databases;

– errors in the accumulation, storage, transmission and use of information;

– errors of perception, reading, interpretation of the content of information, compliance with the rules, as well as errors that arise due to inability, obstacles, failures and distortions of individual elements and signs or messages in general;

– operating errors: violation of protection, file overflow, data management language errors, errors in the preparation and input of information, operating system errors, programming, hardware errors, instruction interpretation errors, skipping operations, etc.;

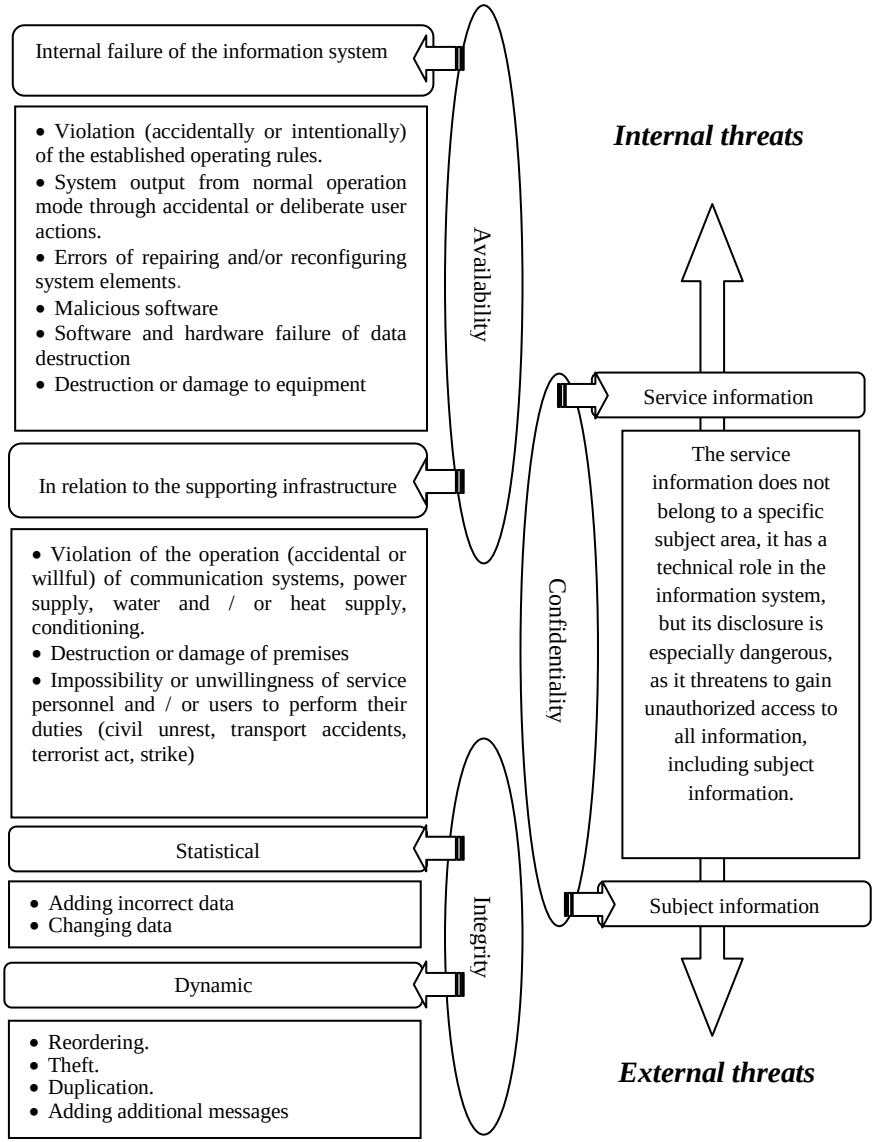

Figure 1. Classification of types of threats to information security [developed by author on the basis of sources: 5, 6, 12]

– conceptual errors of implementation;

– malicious acts in the material sphere;
– disclosure of information;
– social losses (liberation, strike, etc.) [4].

Representatives "Searchinform", a leading company-developer of information security tools, from a practical point of view determine the following groups of vulnerabilities in relation to threats to information security (Table 1).

Table 1

Groups of vulnerabilities in relation to information security threats [grouped by the author on the basis of sources: 4, 10, 11]

Groups of vulnerabilities	Information security threats	Characteristics of factors
Random types of vulnerabilities A group of factors that depend on unforeseen circumstances and the characteristics of the environment of the information environment. They are almost impossible to provide in the information space, but it is important to be ready for their rapid elimination. Such threats can be eliminated through engineering and technical inspection.	1. Failures of systems	• malfunctions of technical facilities at various levels of processing and storage of information (including those that are responsible for the operability of the system and for controlling access to it); • malfunctions and aging of individual elements of the system; • malfunctions of various software that supports all links in the chain of information storage and processing; • interruptions in the operation of auxiliary equipment of information systems;
	2. Threats that weaken the information security	• damage to communications systems such as water supply or power supply, etc..; • malfunctions in the operation of protective devices (fences, floors in the house, equipment cases where the information is stored);
Objective types of vulnerabilities A group of factors directly depends on the technical construction of equipment at the site, which requires appropriate protection. A complete disposal of these factors is impossible, but their partial elimination is achieved with the help of engineering	1. Threats that are associated with technical means of radiation	• electromagnetic techniques; • sound options; • electrical techniques;
	2. Activating threats	• malware, illegal programs, technological exits from programs and other program bags; • "hardware bags";
	3. Threats caused by features of an object under protection	• location of the object (visibility and absence of a controlled zone around the information object, presence of vibration or sound reflecting elements around the object, presence of remote parts of the object);

techniques.		• organization of information exchange channels;
	4. Threats, depending on the characteristics of the individual elements or carriers	• individual elements with electro-acoustic modifications (transformers, telephone devices, microphones and loudspeakers, inductors); • various means that fall under the influence of the electromagnetic field (carriers, microcircuits and other elements);
Subjective types of vulnerabilities A group of factors in most cases is the result of incorrect actions by employees at the level of developing information storage and protection systems.	1. Threats caused by inaccuracies and gross errors that violate information security	• at the stage of downloading the finished software or preliminary development of algorithms, as well as at the time of its use; • at the stage of managing programs and information systems; • when using technical equipment (at the stage of switching on or off, operation of devices for transmitting or receiving information);
	2. Threats caused by system disruption in the information space	• violation of the regime for the protection of personal data (the problem is created by laid-off employees or active employees during off-hours that gain unauthorized access to the system); • violation of the storage and security of information (when accessing the facility or technical devices); • violation when working with technical devices (these can be related to the violation in energy saving or provision of equipment); • violation when working with data (information conversion, storage, search and destruction of data, elimination of defects and inaccuracies).

Based on the generalization of the views of scientists and practitioners to the problem of identifying threats to information security, in this study, under the threat of the object of information security, it is proposed to understand a set of factors and conditions of a subjective nature that arise in the process of interaction of various objects (or parts thereof) and are capable of adversely affecting a specific object information security. Particular attention in this aspect is focused on subjectivism, because both objective and accidental threats to

information security arise due to inability, unwillingness, inattention to results, lack of competence or experience of a specific individual as a subject.

The distributions of the groups of threats to information security considered by us are rather arbitrary one, and require integration with other threat classifications. This explains the need to combine real and potential threats, threats that arise at different levels of management (international, national, regional and local one), and threats to information security caused by anthropogenic and non-anthropogenic factors (not excluding subjectivism).

Based on the aforementioned findings of the study, it is rather important to build a corresponding model for identifying threats to information security, taking into account the following components: actual threats, sources of threats, information attacks, information security objects, vulnerabilities of the information security object and countermeasures.

Reference:

1. Verkhovna Rada of Ukraine. 2003. On the Fundamentals of National Security of Ukraine: law. [ONLINE] Available at: http://zakon2.rada.gov.ua/laws/show/964-15. [Accessed 29 May 2018].

2. President of Ukraine; Ordinance. 2014. About the doctrine of information security of Ukraine. [ONLINE] Available at: http://zakon5.rada.gov.ua/laws/show/514/2009. [Accessed 30 May 2018].

3. Verkhovna Rada of Ukraine;. 2017. About the basic principles of providing cyber security of Ukraine. [ONLINE] Available at: http://zakon3.rada.gov.ua/laws/show/2163-19. [Accessed 6 June]

4. Artemov, A., 2014. Information Security. Lecture course. 1st ed. Moscow: Academy of Security and Survival.

[ONLINE] Available at: https://tech.wikireading.ru/12973 [Accessed 23 May 2018].

5. Bishop, M. (2013). What Is Computer Security?, IEEE Security & Privacy, Vol. 1,1, 67-69.

6. Horbulin, V., Dodonov,, O., Lande, D. 2009. Information operations and public safety: threats, counteraction, modeling: monogr. 1st ed. Kyiv: Intertechnology.

7. Information security of Ukraine: Wikipedia. 2018. [ONLINE] Available at: https://uk.wikipedia.org/wiki/ Інформаційна_ безпека_України. [Accessed 3 June 2018].

8. Information threat : Wikipedia. 2018. [ONLINE] Available at: https://uk.wikipedia.org/wiki/Інформаційна_ загроза. [Accessed 3 June 2018].

9. Kosogov, O.M., 2015. Approach to building a state system for counteracting information threats in a special period. collection of scientific works of the Kharkiv University of Air Forces, 4(45), 76-79.

10. Searchinform information security. 2018. Information security Solutions of "SorchInform":. [ONLINE] Available at: https:/ /searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugr ozy-informatsionnoj-bezopasnosti/. [Accessed 18 June 2018].

11. Tuskov, M.V., Semenov, V.V., (2017). The problems of information security in Russia and its regions [ONLINE] Available at: https://www.science forum.ru/2018/pdf/678.pdf. [Accessed 15 May 2018].

12. VPS.house. (2017). Fundamentals of Information Security. Part 1: Types of Threats. [ONLINE] Available at: https://habr.com /company/vps_house/blog/343110/. [Accessed 3 June 2018].