ON THE CLASSIFICATION OF INFORMATION SECURITY THREATS

Mikhailovskaya L. V., Valakhanovich E. V.
Department of Higher Mathematics of the Military Academy of the Republic of Belarus
Minsk, Belarus
E-mail: ludmila_mi@mail.ru

An analysis of the development of modern information technologies demonstrates a substan-tial increase in the speed of receiving, processing and presentation of information in various spheres of human activity. At the same time, these new opportunities require serious measures aimed to in-crease information security of an asset. One of the first steps set out in an information protection algorithm is listing and classification of potential threats.

Without due regard to the issue of security of automated information processing systems, consequences of adoption of advanced technologies may be disastrous: along with their benefits, these technologies make it easier to mishandle, destruct or disclose certain data [1]. For that reason, data protection issues become of even more importance. And one of the first steps in developing an information protection algorithm is determining a list of potential threats to information assets and classifying them.

An information security threat is a probable event, action, process or condition that may result in a loss. Today we know a lot of such threats and group them based on various characteristics. Thus, paper [2] considers information security threats targeted at an entity's hardware. Paper [3] lists internal information security threats of a company (insider threats), along with threats from cyberterrorists, as the most urgent. Authors of paper [4] consider use of email and loss of individual in-formation media (laptops, mobile phones, etc.) to be major sources of information security threats. Paper [5] gives the most detailed classification of threat types:

1. Threats caused by force majeure
2. Organization-level threats
3. Threats relating to human error
4. Technical threats
5. Threats arising at a pre-design stage

However, the authors believe that this classification is yet to be finalized. Thus, threats of the second type are caused by misinterpretations in assessing the situation and planning data protection measures, or, in other words, by human errors, while we have a separate category for those (threat type no. 3). Likewise, when considering threat types 4 and 5, we are likely to note that data protec-tion means and projects are designed by people, who are prone to make mistakes. Therefore, we may include them into group 3 – threats relating to human error.

The authors believe that information security threats should be classified by two basic crite-ria (their nature and security class), depending on the nature of loss they may cause.

We are proposed to classify threats by their nature in two categories: natural threats and human threats (caused by human activity).

A distinctive feature of natural threats is that they are highly unlike to realize, but when real-ized, the consequences may be significant.

According to the authors, sources of human threats may be classified in three groups: will-ful, technology-related and accidental.

Willful threats are related to willful misconduct by penetrators. (Operator may also be a penetrator, if willfully violating the procedure).

Technology-related threats include technical failures and are caused by internal and external reasons. Externally induced threats, including electrical failures, or mains voltage fluctuation, may be indirectly related to organizational deficiencies or unethical practices of staff. Threats induced by internal reasons may be related to deterioration in hardware reliability or faults in their design or software.

Accidental threats are often related to erroneous or insufficient management activities, or lack of competence of staff. Errors of a human operator are considered accidental when caused by fatigue, negligence or lack of experience. The impact of these threats may range from a trivial loss of time due to unavailability of data to a significant loss of information due to violation of both data integrity and confidentiality.

In addition, security threats are classified based on a source of impact depending on the nature of loss they may cause. For this purpose, all threats are considered based on probability of an attack on assets, and feasibility of the attack in specific context of operation of such assets. Information security threats are also appropriate to be grouped by security categories: threats of violation of integrity, confidentiality and availability.

Thus, we propose the following classification of information security threats (Figure 1).

Due to continuous evolution of means and methods of information processing, transfer and protection, the list and classification of information

security threats may be reviewed to include new types of threats and penetration methods.

Therefore, continuous and reliable protection of information in automated data processing systems involves development of information security threats classification as a first step of a procedure aimed to avoid and prevent such threats.

1. DPC/F4.1 Government framework on cyber security – Information Security Management Frame-work [ISMF], version 3.3, September 2017.
2. Domarev, V. IT Security. Methodology for Creating the System / V. V. Domarev. – Kiev: DiaSowt, 2010. – 673 pages.
3. Malware Threats [Electronic source]. – Moscow, 2010. – Available at: http://www.pcmag.ru/elearning/course/lesson.php.
4. Information security threats [Electronic source]. – Moscow, 2011. – Available at: http://www.infobezpeka.com/publications.
5. Mehrhoff, M. IT-Grundschutzhandbuch. Standard – Sicherheitsmapnahmen. Bundesamt fur Sicherheit in der Informationstechnik / M.Mehrhoff. – DBUS-Jahrestagung, 2004.

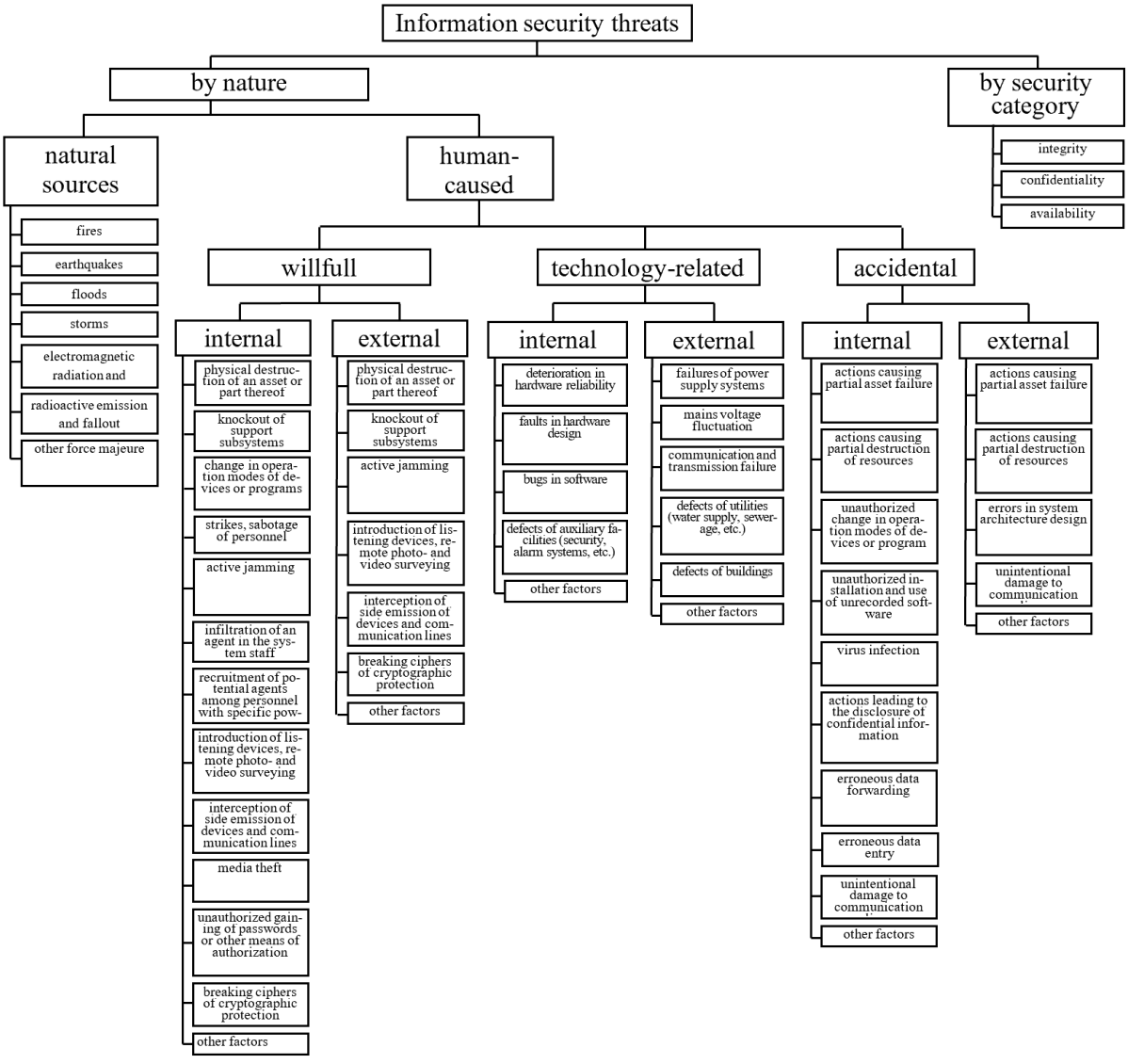

Рис. 1 – Classification of information security threats of an asset