Some aspects of protection information by linguistic methods

Kushch Sergii[1], Kolesnyk Dareena[2]

1. Department of Computer Science and Information Security, Cherkasy State Technological University, blvd. Shevchenlo, 460, Cherkasy, UKRAINE, E-mail: kushch@ieee.org

2. Foreign Languages Department, Cherkasy State Technological University, blvd. Shevchenlo, 460, Cherkasy, UKRAINE, E-mail: dareena@yandex.ua

Abstract – This article deals with the issues and concepts of linguistic data analysis and protection within the framework of modern communication paradigm. The models of communication and different ways of assessment, analysis and information security are also considered. The paper considers the cases in which the protection of information and its transmission is represented by methods of indirect communication and interpretation.

Keywords – linguistic analysis, linguistic methods of data protecting, communication model, information security.

In the modern world with the rapidly increasing power of computers and speed of information transmission by various channels, the protection of information stored and transmitted among users becomes an important theoretical and practical problem. The concept of information security traditionally exists in the theory of information security and is defined as "prevention of loss and leakage of confidential information and the loss of open information that is protected" or "activities aimed at preventing information leakage, unauthorized and unintended impacts on information protected" [1].

In this aspect information security is seen as a set of organizational, regulative, technical and other measures to protect official information set be the owner and first of all documented information that is attached to the physical medium with the use of props allowing to identify it. In the first place there are the most important organizational measures governing the access to information by various categories of persons; it is assumed that there may be also subjects physically not admitted to the storage medium.

To define the concept and classify the types of DLP it is necessary to answer the question who and in what circumstances wishes to protect such information and from whom information may be concealed, hence it is necessary to determine the threat to information. Among the traditional threats we can identify unauthorized access which results in the loss (theft) and leakage (disclosure) of information, unauthorized intentional and unintentional influences on information (destruction, copying, modification, distortion, blocking and so on). In this case, we are considering two main

threats - unauthorized distribution of information and violation of the rights of the owner for possession and disposal of information.

In the conditions of information threats communication model is as follows: the information owner by implementing DLP generates a message to the user requiring to comply with the measures of protection of information provided. Communicative model taking into account the threat of unauthorized intentional and unintentional influences on information suggests that the transmitted information is not secret. In forming the message the information owner marks it in some way, thereby protecting the rights to it and its integrity.

DLP as a need. What is the subject's of communication awareness of the need of information security? We can assume that in different situations the degree of awareness is different, therefore, the text with DLP can be characterized by one of the signs located on the scale of "intentional" - "conventional." This graduation is connected with the size of the group that dictates the requirements for DLP. Thus, if the subject is recognized by society as irrelevant/inadmissible for communication, we can talk about conventional DLP.

Conclusion

Thus it can be concluded that the use of DLP allows both to protect the information that is used by various social and professional groups as well as to reduce the possibility of rapid decoding of confidential information, and to analyze information (information flow) in the aspect of the reaction of society to the situation in the country, a region, a city to any significant social problem. Therefore, the authors are view DLP as a promising scientific and practical method that can be used in different fields of information technology, including in the systems of information security and other related areas.

References

1. Aleksentsev, A. I. Essence and correlation of the concepts "the protection of information", "safety of information", "information safety" // Safety of information technologies, 1999. № 1.
2. Kulko, O. I. Information safety as a linguistic problem // Volgograd state university. Series 2. Linguistics, 2009. №1(9).
3. Kovalev, N. S. Old Russian Literary Text: Problems of Studies of meaning structure and evolution aspects of evaluation category /. Volgograd. Publishing House of the Volga, 1997. 260 pp.
4. Kovalev, N. S. Old Russina text: Principles of formation and factors of evolution (in Galicia-Volyn chronicles) / Volgograd. Publishing House of the Volga, 2001.179 pp.