Restricted Information Identification Model

Yurii Dreis[1], Yevhen Ivanichenko[2], Olena Nesterova[2,3], Yuliia Zhdanova[2], and Kate Dmytriienko[2]

[1] *Polissia National University, 7 Staryi ave., Zhytomyr, 10008, Ukraine*
[2] *Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*
[3] *National Pedagogical Dragomanov University, 9 Pyrohova str., Kyiv, 01601, Ukraine*

Abstract

In this paper, the models and methods of using information with limited access are analyzed, the model of identification of restricted information is developed. An experimental study of the developed software module for identifying restricted information is conducted. The developed model can be used to identify information to restricted information by both common users and employees of companies to prevent leakage of restricted information.

Keywords

Information, restricted information, personal data, official (service) information, state secret.

1. Introduction

Sharing information in the digital environment is an integral part of most people's daily lives. The spread of information is so rapid that it is often impossible to trace the source, who and from where started some gossip. Today, unfortunately, there is an unintentional dissemination of restricted information on the network due to ignorance of citizens about the limited access to it [1].

Especially now, in times of war, when any information can be key in certain issues, people just so need to know what information can be put on the network, and which in any case should not fall into the wrong hands. Unfortunately, this is another important problem in our world: people are so used to sharing their lives and emotions on social networks that they do not even think that some information can cause real harm to the state or even to themselves. Yes, the lists of information that are classified as restricted are publicly available, but there are so many that a person probably does not want to spend a lot of time analyzing all the documents. Therefore, it is important to automate the process of identifying restricted information to prevent its further dissemination [2].

The purpose of the work is to develop a model for identifying restricted information.

2. Types of Restricted Information

The first thing we need to do in this work is to determine what information is in general and what information relates to restricted information, and also why information should be restricted at all. Also in this section, need to be studied the methods of classifying information as restricted and analyze their advantages and disadvantages.

2.1. Data and Restricted Information

First of all, lets define what is information itself. But it could be not so easy, because the concept of information is one of the most controversial in science and everyone understands this concept on an intuitive level. In general, information—is any messages from the world around us that we can see, hear, taste, smell or feel and our brain identifies it as useful on a conscious or subconscious level [3].

An example of the perception of information on a conscious level can be anything that makes you think and draw some conclusions: by sight, smell and taste, you can determine whether an object is edible or not spoiled; hearing certain signals, you can identify them whether dangerous or not, even while reading this text you perceive

CPITS-2022: Cybersecurity Providing in Information and Telecommunication Systems, October 13, 2022, Kyiv, Ukraine
EMAIL: dreisyuri@gmail.com (Y. Dreis); y.ivanichenko@kubg.edu.ua (Y. Ivanichenko); o.nesterova@kubg.edu.ua (O. Nesterova); y.zhdanova@kubg.edu.ua (Y. Zhdanova); k.dmytriienko.asp@kubg.edu.ua (K. Dmytriienko)
ORCID: 0000-0003-2699-1597 (Y. Dreis); 0000-0002-6408-443X (Y. Ivanichenko); 0000-0002-0402-0370 (O. Nesterova); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0001-7984-7279 (K. Dmytriienko)

information on a conscious level. An example of subconscious perception of information is the reaction of the body to stimuli, as your brain sends signals, that you may not be even aware of, to any part of the body.

Based on this, information can be defining as a designation of the content received from the outside world in the process of our adaptation to it and the adaptation of our feelings to it. However, we are accustomed to perceive the concept of information as a message in text form as data. Usually we hear it from someone or read it from somewhere. It can be concluded that information can be stored and transmitted. The Law of Ukraine "On Information" states [4]: information—any information and/or data that can be stored on physical media or displayed in electronic form.

In order for information to facilitate the adoption of the right decisions based on it, it must meet such criteria as [3]:

- Reliability is means that information corresponds to reality. Inaccurate information can lead to misunderstandings or wrong decisions. Because reliable information has the property of becoming obsolete, or failing to reflect the current state of circumstances, it may become unreliable in the future.
- Completeness – information is complete if it is enough to understand the situation and make a decision. Both incomplete and superfluous information hinder decision-making or can lead to mistakes.
- Timeliness is means that information is exactly what is needed at the moment, relevant, important at this time. This property of information is also called actuality.
- Usefulness is the tasks that can be solved with the use of information determine its usefulness.
- Clarity is the consumer who received the message might restore the meaning that the broadcaster of information invested in the message due to the clarity of the information.

According to the order of access, the information shall be divided into publicly available information and restricted information (confidential information, secret information and official (service) information) [4]. Structure of information distribution by access mode on the Fig. 1. All of that kinds of information also divided into different types that may be divided.

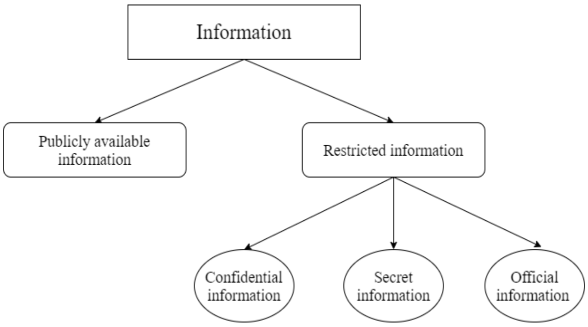

Figure 1: Structure of information distribution by access mode

2.1.1. Personal data or confidential information

According to Law of Ukraine "On Personal Data Protection," personal data is information or a set of information about an individual who is identified or can be specifically identified [5]. Understanding which person is identifiable is key. As a rule, there are no questions about such information as name, address, individual tax number. This data, individually or in combination, allows the owner of this data to clearly identify a particular person.

The situation is a bit more complicated with indirectly identifying data. For example, you buy certain products in a store and use a discount card. Information about purchased products is not in itself personal data, although it relates to an individual. After all, anyone could buy the same products in this or that store. But if you bought and used a discount card, it allows the seller to identify a specific person, so your purchase history combined with card information becomes personal data. Yes, we can say that personal data will be information about the card number, the name of its holder, the date and time of purchase, its value, as well as information about the purchased items. And this data will be protected in accordance with the law and must be collected for lawful purposes. That is, if certain information allows the owner to identify a specific person from a group of people, it can be considered personal data. Therefore, data that are not in themselves personal data become certain in certain circumstances (when they make it possible to identify a person) [6].

An interesting detail is that the law equates the concepts of confidential information and personal data. After all, according to the Law [4]: confidential information shall include information about an individual, as well as information restricted by an individual or legal entity, except for public authorities. Confidential information may be disseminated at the request (consent) of the person concerned in the manner prescribed by him in accordance with the conditions provided by him/her, as well as in other cases specified by law [4]. It should also be noted that not all information can be classified as confidential. There are many cases when different laws provide for the disclosure of certain information, such as information about positions and work contacts, disposal of budget funds, information from open registers, and so on. Therefore, the law may prohibit anyone from restricting access to certain information. In fact, the person to whom the information relates has no right to determine the mode of access to such information [6].

Experts stressed that the legislator probably assumed that in most cases an individual would not take active steps to restrict access to information about himself (as required by the definition contained in the Law "On Access to Public Information"): access to which is restricted to a natural or legal person [7]).

Thus, the state provided protection against the disclosure of certain, mostly sensitive, information even to the restriction of access to it by a natural or legal person, thus assuming the person's desire to restrict access to such information because of its "sensitivity." At the same time, the person retains the right to decide on the disclosure of this information and not to further restrict access to it [8].

2.1.2. Official Information

According to the Law of Ukraine "On Access to Public Information," official (service) information may information contained [7]:

- In documents of public authorities, which constitute the interagency official correspondence, in particular, reports, recommendations, if they are related to the development the direction of the institution or the implementation of control, supervisory functions of public authorities, the decision making process, and precede public discussion and/or decision-making.
- Information collected in the course of operational and investigative, counterintelligence activities in the field of national defense, which is not classified as a state secret.

Article 9 of the Law [7] provides that such information may be classified as official (service). That is, the information contained in any memorandum should not automatically have the status "for official (service) use." This is possible if the use of the "three-part test" showed that there are grounds for restricting access to it [7]. Let's show on Fig. 2 to understand what is official (service) information more clearly.

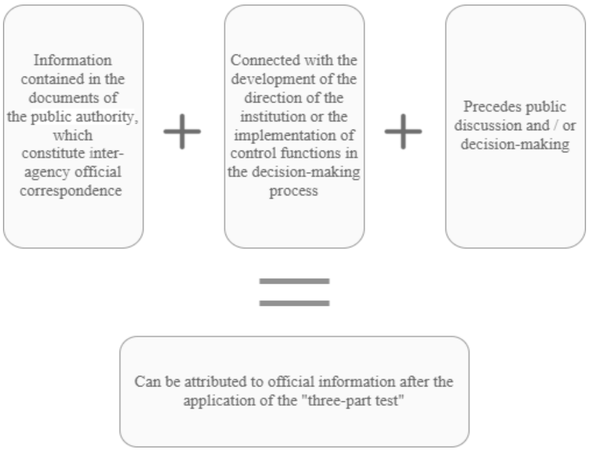
Information contained in the documents of the public authority, which constitute inter-agency official correspondence
+
Connected with the development of the direction of the institution or the implementation of control functions in the decision-making process
+
Precedes public discussion and / or decision-making
=
Can be attributed to official information after the application of the "three-part test"

Figure 2: "Three-part test" for restricting access to official (service) information

2.1.3. Secret Information

According to the Law [7]: secret information—information to which access is restricted in accordance with the second part of Article 6 of this Law, the disclosure of which may harm the person, society and the state. Information that contains state, professional, banking, pretrial investigation secrets and other secrets provided by law shall be considered secret [7].

Let's create a figure to visually see what main types of secret information there are (see Fig. 3.)

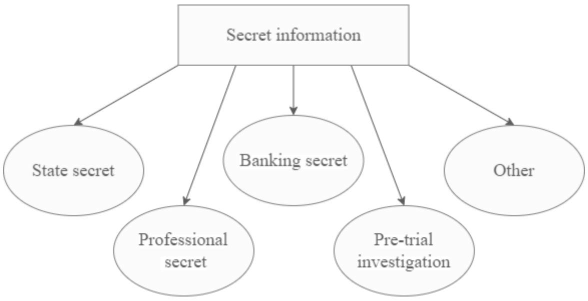

Figure 3: Main types of secret information

Now let's look on these types of secret information more closely:

1. State secrets are information in the field of defense, economics, science and technology, foreign relations, state security and law enforcement, the disclosure of which may harm the national security of Ukraine and which are recognized in accordance with the Law of Ukraine "On State Secrets," state secrets and subject to state protection (Law of Ukraine "On State Secrets") [9];

2. Banking secret is information on the activities and financial condition of the client, which became known to the bank in the process of customer service and relationships with him or third parties in providing bank services and disclosure of which may cause material or moral damages to the client, including [10]:

- Information on the client's bank accounts, including correspondent accounts of banks with the National Bank of Ukraine, on transactions that were carried out for the benefit or on behalf of the client, transactions carried out by him.
- About the financial and economic condition of the client.
- About bank and customer protection systems.
- Information on the organizational and legal structure of the legal entity—the client, its leaders, activities.
- Information on the client's business or trade secret, any project, inventions, product samples and other commercial information.
- Information on reporting by individual bank, except for the one to be published.
- Codes used by banks to protect information, as well as information about banks or customers collected during banking supervision (Law of Ukraine "On Banks and Banking") [10].

3. The secrecy of the investigation is the data of the pretrial investigation [11, p. 12].

4. A lawyer's secret is a set of information from which a citizen or legal entity has applied to a lawyer, the essence of consultations, advice, clarifications and other information obtained by a lawyer in the performance of his professional duties (Law of Ukraine "On Advocacy") [12].

5. Notarial secrecy is a set of information obtained during a notarial act or appeal to the notary of the person concerned, including the person, his property, personal property and non-property rights and obligations, etc. (Law of Ukraine "On Notaries") [13].

2.2. Criteria Assigning for Restricted Information

Consider the criteria by which information is classified as personal data, official (service) information and state secrets.

Criteria for assigning information to personal data [3, 5, 6]:

- To be sent to confidential information about a person by law or by a corresponding person.
- To be accurate, reliable and updated as needed, as determined by the purpose of their processing.
- To be appropriate in terms of composition and content, adequate and unreliable with regard to the defined purpose of their processing.
- To be processed in a form that allows identification of the individual concerned, no longer than necessary for legitimate purposes for which they were going to or were further processed.
- to be processed without the consent of the subject of personal data until the receipt of the consent becomes possible to protect vital interests of the person.
- The primary sources of information about an individual are: the documents issued on its name; the documents signed by it; the information which the individual provides about himself.

Criteria for assigning information to official (service) information [3, 7, 8]:

- To be in lists of official (service) information, which consist of abstract categories of information that can be classified as official (service), regardless of the specific information (specific document).
- To use the "three-part test" in each case where specific information is given the status "for official (service) use."
- Lists of official (service) information should be approved among all possible central authorities, ministries, services, etc.

Criteria for assigning information to state secret [9, 14–17]:

- To be in the field of defense, economics, science and technology, foreign relations, state security and law enforcement.
- To be in the List of Information Constituting a State Secret (LISS) [14].
- Assignment of information to a state secret is carried out by motivated decisions of the state expert on secrets.

- Determination of the level and description of the threat and damage to national security (national interests) in case of non-classification of information as a state secret.
- Determining the date or event of declassification of information.
- The degree of secrecy of this information.
- The amount of funding for measures necessary to protect such information.
- State body, local self-government body, enterprise, institution, organization or citizen who has submitted a proposal to classify this information as a state secret, and state body (bodies), which has the right to determine the range of entities that will have access to this information.
- The period during which the decision to classify the information as a state secret is valid.

3. Models and Methods of Assigning data to Restricted Information

In this section analyze few methods of classification and assigning data to restricted information. There will be considered the following methods and models:

1. *Fuzzy modeling of the linguistic variable "information"* [18]. The formalization of "information" as a component of the general information security system is carried out. The theory of fuzzy sets is used for expert assessment of the definition of the rules of legal delimitation and the establishment of the appropriate category of protection of information on the content of information. The linguistic variable "information" is determined by the content of its information as: open; confidential private property; confidential state property; other secret information; state secret. For the linguistic variable, the basic scale is a hierarchical scale of authority, which is introduced on the basis of the category of information security and access rights of users. The hierarchical scale of authority is a scale of basic operations on a linguistic variable depending on the rights to access it, namely: entering or editing, viewing, modifying or saving and deleting data. Depending on the fuzzy set (consisting of the distribution described above), basic operations on a linguistic variable are performed, and the membership function determines how confident it is that an operation can be classified in this category of information security [18].

2. *Method of fuzzy classification of information with limited access* [17]. Proposes a method for fuzzy classification of information according to established criteria based on the theory of fuzzy sets and complex oriented information network "List of Information Constituting a State Secret" during the examination of material media for the presence of such information [19].

3. *Methods of constructing an ontological hierarchy for determining the value of information* [20] and *Model of complex oriented information network LISS* [21]. Decision-making is based on the use of specific hierarchical structures is ontologies, it is an attempt to comprehensively and in detail formalize some area of knowledge with the help of a conceptual scheme. Typically, such a scheme consists of a data structure that contains all relevant classes of objects, their exact specifications for a particular subject area, relationships and rules (theorems, constraints) adopted in this area. The level of detail in the areas of the ontological hierarchy is individual for each level and is closely related to the ability to calculate the value of information at the lowest level of the hierarchy. Yes, if the value of the lowest "atomic" cells of the hierarchy is calculated by the loss from blocking or modifying this information. In general, the value of information is determined by assessing the impact of the negative consequences of the implementation of threats to the integrity or availability of this information [20, 21].

4. *Method of expert assessments* [15, 22]. Expert commissions to calculates the level of potential harm to the state in areas defined by law economic damage, which means the level of reduced efficiency of the allocated funds to ensure the operation of the object due to disclosure of information about this object and an indicator that characterizes the damage to the state from other serious consequences that cannot be calculated in economic terms or value. The calculation of funds for the definition of indicators is carried out in units "specific weight" of individual important objects [15, 22].

Compare of existing models and methods for assigning data to restricted information by some characteristics in a Table 1.

Table 1
Comparison of existing models and methods for assigning data to restricted information

Characteristics	Fuzzy modeling and fuzzy method	Method of fuzzy classification of information	Methods of building an ontological hierarchy	Method of expert assessments
Ease of implementation	+\–	+\–	–\+	–
Ability to identify any restricted information	+	+	+	–\+
Objectivity of the relation of data to restricted information	–	–	–\+	–
Customize to the desired requirements	+	+	+	–\+
Decisions are based on the law	+\–	+\–	–\+	+
Easy to use and understand	–	–	–\+	+\–

4. Restricted Information Identification Model

To solve this problem, a mathematical model of value formation (or basic model) is proposed, the basis of which is a tuple consisting of an identifier (ICD) of the type of restricted information (*RI*), as well as components such as subsets: possible parameters; possible fuzzy (linguistic) standards; current values of fuzzy parameters; basic detection rules.

To formalize the process of formation of these components, we introduce many possible types of restricted information *RI*, the leak (loss or disclosure) of which may harm national security in a certain period of time interval τ_f (f is the number of the time interval $= \overline{1, max_\tau}$), that is:

$$RI^{\tau_f} = \{\bigcup_{\mathrm{i=1}}^{\mathrm{n}} RI^{\tau_f}{}_i\} = \\ = \{RI^{\tau_f}{}_1, RI^{\tau_f}{}_2, \dots, RI^{\tau_f}{}_n\}, (i = \overline{1, \mathrm{n}}) \quad (1)$$

where *n* determines the number of possible types of restricted information, each of which is displayed by a generalized tuple:

$$RI^{\tau_f}{}_i = \langle RI_i, P_i, T_i{}^e, P^{\tau_f}{}_i, DR_i \rangle, \quad (2)$$

in which: RI_i is ICD of the i^{th} type restricted information; P_i is a subset of possible parameters used to determine the i^{th} type of restricted information; T_i^e is a subset of possible fuzzy (linguistic) standards, reflecting the expert's judgment on the availability of basic parameters of possible damage (by type of procedure for assigning information to the restricted information) from the subset P_i to restrict access; $P^{\tau_f}{}_i$ is a subset of the current values of fuzzy parameters formed on the basis of T_i^e at time τ_f ($f = \overline{1, \max_\tau}$) for the time interval $\tau_h = \tau_f - \tau_{f-1}$; DR_i - a subset of basic detection rules (causal and spatio-temporal characteristics and features of information *I*), which became the basis for building a generalized scheme for classifying information according to a certain order and degree of restriction of access to species restricted information: by access order (DR_1); by legal regime (DR_2); by right of access (DR_3); by type of secret (DR_4); on the stamp of restriction of access to the material information carrier (DR_5); by degrees of secrecy (DR_6); by type of activity (DR_7) and others (DR_n).

Thus, the proposed tuple model of formation of a set of basic components (or basic tuple model), which by formalizing the procedure of restricting access to information, allows to form a set of private tuples that reflect the classification of ICD and identify basic parameters given time interval.

5. Conclusions

In the work was defined what is information and what are main characteristics of information. There are two types of information: open and restricted information. In turn, these types can also be divided into groups and subgroups, in particular restricted information can be confidential, official (service) or secret. Which are also divided into many different groups. From them it is possible to allocate some more narrowly directed kinds which have been considered in more detail, and also used for creation and testing of the model: state secrets, official (service) information and personal data.

Several models and methods of classification of restricted information were considered and analyzed, in particular fuzzy modeling of the linguistic variable, methods of building an ontological hierarchy and Method of expert assessments for State Experts on Secrets. After analyzing these methods, it was concluded that they are imperfect in the form of bias and difficulty for understanding non-professionals. Therefore, based on this, was developed a model to identify restricted information.

6. References

[1] Y. Ivanichenko, et al., Exposing Deviations in Information Processes using Multifractal Analysis, in Cybersec. Prov. Inf. Telecom. Syst. II, vol. 3187, 2021, pp. 251–259.

[2] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in 8th Int. Conf. on “Math. Inf. Tech.. Edu.:” Modern Machine Learn. Tech. Data Sci., vol. 2386, 2019, pp. 222–233.

[3] O. Korchenko, Y. Dreis, Protection of confidential information of the enterprise: Manual, Zhytomyr, NAU, 2011.

[4] On Information. Verkhovna Rada of Ukraine, #2657-XII, 02.10.1992.

[5] On Protection of Personal Data. Verkhovna Rada of Ukraine, #2297-VI, 01.06.2010.

[6] Confidential Information, Personal Information and Personal Data: Relationships AND Regulations, Center for Democracy and the Rule of Law, https://cedem.org.ua.

[7] On Access to Public Information. Verkhovna Rada of Ukraine, #2939-VI, 13.01.2011.

[8] On Access to Public Information. Scientific and Practical Commentary to the Law of Ukraine, Ed. D. Kotlyara, Kyiv, 2012.

[9] On State Secret. Verkhovna Rada of Ukraine, #3855-XII, 21.01.1994.

[10] On banks and banking. Verkhovna Rada of Ukraine, #2121-III, 07.12.2000.

[11] O. Ogdanska, V. Taran, V. Shcherbachenko, Official Information: Procedures of Transfer and Access. Practical Manual, ed. D. Slysikonis, Center of political studios and analysts, 2014.

[12] On Advocacy. Verkhovna Rada of Ukraine, #5076-VI, 05.07.2012.

[13] On Notaries. Verkhovna Rada of Ukraine, #3425-XII, 02.09.1993.

[14] On Approval of the List of Information Constituting a State Secret, Security Service of Ukraine, Order #440, 12.08.2005.

[15] O. Korchenko, O. Arkhipov, Y. Dreis, Assessment Harm to the Ukraine National Security in Case of Leakage State Secrets, Monograph, 2014.

[16] Methodical Recommendations to State Experts on Secrets on Determining the Grounds for Classifying Information As a State Secret and the Degree of Their Secrecy, State Committee of Ukraine for State Secrets; Collection, no. 8, 1998.

[17] O. Arkhipov, Estimation of efficiency of system of protection of the state secret, Monograph, NASSU, 2007.

[18] O. Korchenko, Y. Dreis, Fuzzy Modeling of the Linguistic Variable “Information” According to the Content of Information and the Type of Operations Performed on it, Problems of Creation, Testing, Application and Operation of Complex Information Systems, vol. 2, 2009, pp.102–108.

[19] S. Falchenko, et al., Method of Fuzzy Classification of Information with Limited Access, in IEEE 2nd International Conference on Advanced Trends in Information Theory, 2020, pp. 255–259.

[20] O. Arkhipov, M. Petrenko, Application of Ontological Hierarchy in Problems of Determining Value of Information, Information Protection, vol. 1, no. 54, 2012, pp. 45–52.

[21] O. Korchenko, et al., Model of Complex Oriented Information Network LISS, Information Protection, vol. 3, no. 52, 2011, pp. 87–94.

[22] O. Arkhipov, Criteria for Determining the Possible Harm to National Security of Ukraine if Disclosure Information Protected by State, Monograph, NASSU, 2011.