Method for Determining the Informativeness and Compliance of Critical Data in the General Field of the Information and Communication System

Mykhailo Strelbitskyi
Bohdan Khmelnytsky National Academy of the State Border Guard Service of Ukraine
Khmelnytskyi, Ukraine
mstrelb@gmail.com

Olha Suprun
National Aviation University
Kyiv, Ukraine
o.n.suprun@gmail.com

Vitalii Bezshtanko
Special Communications and Information Protection of Ukraine
Kyiv, Ukraine
v.bezshtanko@gmail.com

Viktoriia Ivannikova
Dublin City University
Dublin, Ireland
viktoriia.ivannikova@dcu.ie

Evgen Ivanov
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
evgen.ivanov1405@gmail.com

Olena Matviichuk-Yudina
National Aviation University
Kyiv, Ukraine
metalen@ukr.net

2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT) | 979-8-3503-3262-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ATIT58178.2022.10024194

***Abstract* — At the modernization stage of information and telecommunication systems of the national security subjects of Ukraine there is a problem of information reliability when sharing data is used. For estimation of the probability of the information and its properties violation it is necessary to determine the quantity of information entered the component of the system. Also all the information that is used by companies and country, must be checked for intrusion and properly protected. The paper presents the method for determining the quantity of information that flows into the telecommunications system considering aging factor. This method uses dynamic parameters of information and considers different factors of environment. Also the testing was conducted and results are presented.**

Keywords* — *quantity of information, aging information

I. Introduction

Due to the appearance of new types of threats, in particular, the military aggression of Russian Federation against Ukraine, its temporary occupation of the territory of Autonomous Republic of Crimea and the city of Sevastopol, instigation of an armed conflict in the eastern regions of Ukraine, accompanied with the implementation of measures aimed to destabilizing the political and economic situation in Ukraine, development of terrorism and threat of its spreading over the territory of Ukraine, there was an urgent need to modernize components of the integrated information and telecommunication system "Hart" and integrated interdepartmental information and telecommunication system "Arkan" regarding the control of persons, transport means and goods crossing the state border, arrangement of mobile automated workplaces with access to databases at security agencies of the state border, implementation of e-document system with the usage of electronic digital signature, modern complexes of cryptographic protection of information, the latest means of special communications on mobile objects and cyber security mechanisms in information and telecommunication systems [1].

Furthermore, the Strategy of the State border service development foresees formation of integrated, protected information and rescue databases of operational and rescue departments; creation of subsystems at checkpoints across the state border with the functions of processing of information about persons, crossing the state border and their passport details using electronic data carrier, including the function of biometric control; providing access for the immigration control officers to the databases of law enforcement agencies and the International Organization of the Criminal Police - Interpol; modernization of the system of automated identification of foreigners and stateless persons, who are denied the right to enter Ukraine at checkpoints across the state border.

The concepts of integrated border management and development of the security and defense sector of Ukraine provide mutual access to the information systems of competent state bodies, in particular to the State Border Service (SBS) and organization of joint operational protection of the state border of Ukraine with the member states of the European Union, as well as with the Republic of Moldova due to the implementation of the information exchange mechanism - an electronic border information resource.

The material carrier of the electronic border information resource is an integrated information and telecommunication system (IITS) "Hart" [2,3]. Its task is to: increase the completeness and reliability of the information, used by the SBS staff in their activity; efficiency of access to the information by subjects of integrated border management and data processing; expanding the possibility of analysis and generalization of information, used during managing the bodies of the SBS; reducing the time for decision-making on the management of SBS bodies; improving the quality of decisions made; ensuring efficiency and timeliness of the control over the performance of directive orders [4].

In most cases the border information resource contained in the IITS "Hart" has confidential information, for example, personal data of a person, crossing the state border, instructions of law enforcement agencies regarding this person, etc [5].

Thus, current challenges require a huge modernization of

979-8-3503-3262-9/22/$31.00 ©2022 IEEE

the IITS "Hart", which involves interaction not only with information and telecommunication systems of competent state bodies, but also with international systems. This leads to the necessity to transfer old functional tasks into a new hardware and software environment. In the result of this, a common data field is created, which is used by both old and new IITS components. At this stage of the life cycle, the task of joint functioning of different versions of IITS components both within the subsystems and between them arises with maintaining the level of protection of the electronic border information resource. This requires the formation of approaches to assessing the level of protection against information threats during modernization of IITS components and exchanging data with other systems.

II. Analysis of Researches and Publications

In many works, the issue of information protection is considered in relation to the system in general, i.e. when creating an information protection system (IPS), the object of information activity is considered as a unique object. When the characteristics or structure of such an object change, the IPS is updated, and in fact it is developed anew. This approach can be applied to small objects that, as a rule, are not territorially distributed, for example, the software and technical complex of border control automation (STC BCA) "Hart-1/P" at the crossing point across the state border. At the same time, the information and telecommunication systems (ITS) of the subjects of the national security of Ukraine have a large number of subsystems that are distributed over the entire state. A peculiarity of such systems is the requirement of their functioning on a real time scale. Moreover, even a minor failure or stoppage in functioning can lead to serious losses at a national scale. An example of such systems can be the “Unified Automated Management System of the Armed Forces of Ukraine”, “Air Transport Flight Safety Management System”, “State Shipping Safety Management System”, Integrated Information and Telecommunication System of the Border Agency “Hart”, etc. One of the problems of the real-time systems life cycle is the process of its modernization in general, which is carried out step by step until the completion of modernization. The researches in the field of scientific evaluation of the quality of applied software (AS) show that about 50% of errors occur at the design stage and they must be eliminated before introducing at a working system [2]. The main way to check the quality of software creation or modernization is its testing. However, the complexity of the system does not allow to create its test version of such a scale [6].

It should be mentioned that during upgrading one or more components of such systems, the protection of information in them after modernization is ensured by known ways and methods. The problem exists in the situation when protection of the information components is provided separately in old and new versions of the special software, but in case of joint functioning of both versions in the heterogeneous environment of the information and telecommunication systems of the national security subjects of Ukraine protection will not be provided in general cases.

In the paper [3], the functional dependence of the generalized indicator is determined on the basis of the given models of the process of information properties violation on the element of the information and telecommunication system. Taking into account given assumptions, the paper examines the issue of data privacy violations only in case of the combined usage of electronic border information resources of different software versions. One of the components of the data vulnerability indicator in ITS is the probability of having certain category of data on its element [7,8].

The necessity in data protection arises only if they are found in the common field of a heterogeneous IITS, i.e., in case of joint usage of the common resources of the system by the users with different rights for the considered data. Only in this case there is a threat to data reliability. In order to determine the probability of finding certain category of data in the common field of IITS, which means necessity of its protection, we will use the logical assumption that the necessity in information depends on the degree of its aging. If the aging degree is high, the probability of information usage is low. Thus, the governing documents define deadlines, after which the necessity to protect confidential information is reviewed [9].

Problem of information aging has been considered in many papers, for instance, the Barton-Kebler model, which proposed to estimate the terms of scientific papers usage, the approaches of Cole and other authors [8]. In these works, the aging process of information is considered as the loss of practical value of the information for the final user due to the constant appearance of new documents (sources, data), which contain more accurate and reliable information. Other authors use information aging models based on the understandable physical processes. For example, P. Ferhlust proposed a logistic model that describes population dynamics and R. Perl presented a model for describing of biological populations. In our opinion, this approach is rational, as it considers the semantic loading of the data, in our case, the electronic border resource [10,11].

The purpose of the paper is: development of a method for determining the amount of information in the information and telecommunication system of the border agency at the stage of its modernization.

III. Main Material

Taking into account the main tasks of the State Border Service of Ukraine, the nature of information circulating in the information, information and telecommunication systems of the IITS "Hart" mainly concerns individuals. Thus, the model for determining the probability of finding certain category data in the common field of IITS is based on the hypothesis about relationship between the aging of person and, accordingly, information about him/her.

The duration of the existence of useful information, or the information, which will be used and, accordingly, will be in the common field of the IITS, is a random value and depends on certain factors. It can be described by the Gompertz-Meikham function, in which the intensity parameter of the exponential distribution has a time trend that can be described by the equation of the modified exponent [5]:

$$\lambda(t)=a+be^{ct} \tag{1}$$

where, α, b, c – parameters of the information life-cycle.

Thus, the information aging function will take the following form:

$$f(t)=\lambda(t)e^{-\lambda(t)t} \tag{2}$$

After substituting (1) into (2), we get the coefficient of information usage:

$$f(t)=\left(a+be^{ct}\right)\cdot e^{-at-\frac{b}{c}e^{ct-1}} \tag{3}$$

The generalized view of the coefficient of information usage at different values of the information life cycle parameters is shown in Figure 1.

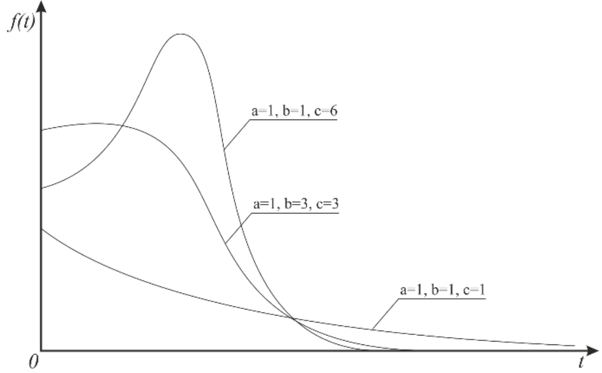

Fig. 1. Generalized view of the coefficient of information usage at different values of information life cycle parameters

In order to determine the amount of information that enters into the ITS, it is necessary to consider the tasks and technological processes in which it is involved. As a case study, we will choose the software and technical complex of border control automation "Hart-1/P" which is used at the checkpoint across the state border of Ukraine. This system can be considered as a queueing system (QS), which is characterized by: the incoming flow of applications (time interval between arrival of applications or the moment of the application arrival); number of service channels and the average service time per one application by one channel; the queue discipline; service discipline. Peculiarities of the technology of state border crossing distinguish these systems from the typical queueing systems. In order to develop models of the STC BCA functioning, it is necessary to find out the characteristics of the flows circulating in the system and the discipline of their servicing. It has been established in the paper [6] that the incoming flow of applications (people, vehicles and goods) can have the following characteristics: unusualness, irregularity, recurrence, lack of aftereffect. The input flow has the properties of stationarity only at some defined time intervals. The peculiarity of the output flow of served applications is that it will not have the property of no aftereffect. Only on the basis of statistical data analysis, it is possible to make assumptions about the type and parameters of the distribution function of the incoming flow of applications.

To describe the method for determining the probability of finding certain category of data in the common field of the IITS, we will assume that during the operation of the STC BCA a new information constantly enters into the system with the flow parameter $\lambda_{вх}$ and the distribution function:

$$P(\hat{t}\le t)=F_{вх}(t)=1-e^{-\lambda_{вх}t} \tag{4}$$

It should be noted that this assumption does not limit the type and parameters of the distribution function for the probability of new information entering the system, which is determined on the bases on analysis of statistical data in each specific case.

As the unit of information that enters the system, we will understand a certain block of data, which is connected by the logic of the system's functioning (information about crossing the border by a person, transport means, a mandate from law enforcement agencies, etc.).

Thus, the coefficient of information usage is a random value and depends on the moment of information appearance (Figure 2), the probability of which is distributed according to the formula (4).

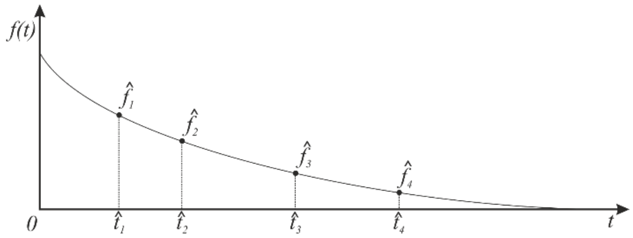

Fig. 2. Dependence of the coefficient of data usage on the time of their stay in the IITS

The distribution function of the random value of the data usage coefficient will have the following form:

$$F(K)=P\left(f(\hat{t})\le K\right) \tag{5}$$

where, K – acceptable coefficient of information usage, determined by norms.

As a result of transformations of a one-dimensional random variable, we obtain the following:

$$F(K)=F_{вх}\left(f^{-1}(K)\right) \tag{6}$$

where, $f^{-1}(t)$ – inverse function to $f(t)$.

The expression (6) means the probability of the information appearance in the common data field with the value of usage coefficient not less than K.

In accordance with the Little's formula, the amount of information, entered into the system in a stable mode, with a level of the usage coefficient not less than *K*, equals:

$$N=\lambda_{вх}f^{-1}(K) \tag{7}$$

As it is visible from (7), the amount of information with a given level of the usage coefficient does not depend on the time of ITS operation, but depends only on the intensity of the input flow.

IV. Conclusions

The structure and functional tasks of the departmental information and telecommunication systems foresee the exchange of data between its components, the modernization of which may cause threat to the information properties. The obtained functional dependencies of the amount of information that enters into the system according to a certain distribution function of applications will allow to estimate the probability of information properties violation.

Using of mathematical background allows to adapt the proposed method to different fields, considering types of threats and their probability.

Also, proposed method uses the data about lifecycle of diagnosed information to find possible intrusions in different moments of time, even if an attack had been conducted in the past.

REFERENCES

[1] Y. A. Gatchin and V. V. Sukhostat, "Research of Vulnerabilities of Information Processing Processes Systems of Critical Information Infrastructure," 2019 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF), St. Petersburg, Russia, 2019, pp. 1-4, doi: 10.1109/WECONF.2019.8840618.

[2] Oleksandr Yudin, Volodymyr Artemov, Maksym Tyshchenko, Yevhenii Makhno, Nataliya Tarasenko, Oleksandr Shapran. Forecast Model of Technical State of Telecommunication System: Intelligent Statistical Data Processing: Proceeding of the International Conference on Advanced Trends in Information Theory (ATIT 2021), Kyiv, Ukraine, 15.12.21-17.12.21, 2021. IEEE Catalog Number: ISBN 978-1-6654-3847-6/21/$31.00 © 2021 IEEE, pp.165-168. DOI: 10.1109/ATIT54053.2021.9678738

[3] S. Popereshnyak, O. Suprun, O. Suprun and T. Wieckowski, "Intrusion detection method based on the sensory traps system," 2018 XIV-th International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, Ukraine, 2018, pp. 122-126, doi: 10.1109/MEMSTECH.2018.8365716.

[4] W. Hurst, M. Merabti and P. Fergus, "Big Data Analysis Techniques for Cyber-threat Detection in Critical Infrastructures," 2014 28th International Conference on Advanced Information Networking and Applications Workshops, Victoria, BC, Canada, 2014, pp. 916-921, doi: 10.1109/WAINA.2014.141.

[5] S. Gnatyuk, M. Aleksander and V. Sydorenko, "Unified data model for defining state critical information infrastructure in civil aviation," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, UKraine, 2018, pp. 37-42, doi: 10.1109/DESSERT.2018.8409095

[6] Oleksandr Yudin, Mykhailo Strelbitskyi, Valentyn Mazur, Viktoriia Ivannikova, Olha Suprun, Mykola Prysiazhniuk. Harmonization of Systems of Discretionary Differentiation of Access to Information Systems at the Stage of Modernization: Proceeding of the International Conference on Advanced Trends in Information Theory (ATIT 2021), Kyiv, Ukraine, 15.12.21-17.12.21, 2021. IEEE Catalog Number: ISBN 978-1-6654-3847-6/21/$31.00 © 2021 IEEE, pp.191-194. DOI: 10.1109/ATIT54053.2021.9678793

[7] C. J. Romanowski, S. Mishra, R. K. Raj, T. Howles and J. Schneider, "Information management and decision support in critical infrastructure emergencies at the local level," 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 2013, pp. 113-118, doi: 10.1109/THS.2013.6698985.

[8] Olha Suprun, Maksym Ivasenko, Oleh Suprun. Information Transmission Protection Using Linguistic Steganography With Arithmetic Encoding And Decoding Approach. Proceeding of the 3rd International Conference on Advanced Trends in Information Theory (ATIT 2021), Kyiv, Ukraine, 15.12.21-17.12.21, 2021. IEEE Catalog Number: ISBN 978-1-6654-3847-6/21/$31.00 © 2021 IEEE, pp.175-178. DOI: 10.1109/ATIT54053.2021.9678855

[9] V. Mokhor, S. Honchar and A. Onyskova, "Cybersecurity Risk Assessment of Information Systems of Critical Infrastructure Objects," 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2020, pp. 19-22, doi: 10.1109/PICST51311.2020.9467957.

[10] Barannik, V., Hahanova, A., Slobodyanyuk, A. Architectural presentation of isotopic levels of relief of images. IEEE 10th International Conference on Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2009, pp. 385–387

[11] Y. Ulianovska, S. Florov, A. Hrebeniuk, T. Katkova, D. Prokopovich-Tkachenko and R. Gvozdov, "Formalized Designing Methodology of ISMS for Critical Infrastructure," 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), Kharkiv, Ukraine, 2021, pp. 587-590, doi: 10.1109/PICST54195.2021.9772182.