UDC 621.396.7.

Pashkevitch V.
Educational-production part
Lviv Polytechnic National University,
S.Bandery Str., 12, Lviv, 79013, Ukraine
E-mail: Pashkevitch@polynet.lviv.ua

GENERAL ORGANIZATION OF INFORMATION TECHNOLOGY OF DEFENCE OF POLYGRAPHY DOCUMENTS WITH CERTAIN SIZE OF RISK OF THEIR USE

© *Pashkevitch V., 2006*

Functional unit scheme of technology functioning of document's authentication is developed and represented the mathematical way of calculation the risk of usage the protected documents and methods of management by the risk.

Keywords - the risk of usage of protected documents, statistical risk, structural risk, measure of saturation, measure of divisibility, local density, measure of counts similarity.

1. Introduction

At present polygraphy documents have wide application in the social sphere and management sphere. Plenty of their falsifications can result in a critical situation in the control system. In this connection the tasks of document defence from imitation are extraordinarily actual.

Actuality of document defence does not cause doubting and is especially important in separate industries of the control system. However in most organizations, in which documents of different level of meaningfulness are used, there are the systems of automated document turnover, which must provide safety of documents not only within the framework of the system, with the help of which they are prepare, but also in other structures and spheres where the proper documents will be used. The existent systems of document turnover today do not provide safety the documents usage of among their potential users. Obviously, the system of document defence must foresee their operative authentication in all stages of their usage. Such approach to authentication of documents requires creation of inexpensive technology of their defence and with the use of modern inexpensive portable equipment with the help of which it is possible to make operative authentication, as visual authentication of documents does not give reliable information about originality of the document.

2. Organization of information technology of document defence.

The whole row of tasks is solved within the framework of general organization of information technology of document defence, to which belong the following:

- Planning graphic facilities of defence.
- Determination of necessary level of document defence.
- Determination the size of risk of usage the documents with different facilities of defence.
- Forming the methods of document defence, that are based on the processes of their authentication.
- Tasks of management by the level of defence, or security level of documents.
- Tasks of determination of dangers, that initiate or can initiate the attacks on documents.
- Tasks of counteraction to the attacks on a document.

Generally it is accepted for estimation of defence level to use such of parameter, as size of risk of usage protected documents. Within the framework of this work we will measure a risk size by a dimensionless size which it is possible to define in percents, or in the range of values [0,1]. Due to such range of values of this parameter it is possible to get the maximum values of risk. If risk value is equal zero, the risk is fully absent, and if the value of risk is equal one, that certain as the undesirable will take place in relation to documents. Obviously, that size of risk which we will mark by the R character must occupy the intermediate value. This parameter is determined by the following factors [1, 2]:

- By the size of counteraction to the attacks, which can be provided by facilities of defence.

173

   – By intensity of attacks which are initiated in relation to documents.

   – By the size of threats, which exist in documents which are on the defensive.

   – By the presence of dangers which exist in relation to documents.

   – By the technological parameters of the control system by the level of protection, that is a member of information technology of documents.

Determination of risk size to which the document is added at the use of facilities of defence is the key element of information technology, as the shortchanged size of the R risk is initial for realization of management after the change of defence level of the document in the system of document turnover on the whole and is described by the following correlation:

$$R = F\left[f_B\left(X_{B1},...,X_{Bn}\right), f_N\left(X_{N1},...,X_{Nm}\right)\right] \tag{1}$$

Where $\Omega = f_B(X_{B1},...,X_{Bn})$ is firmness to the document in relation to the attacks; $\Omega_N = f_N(X_{N1},...,X_{Nm})$ are statistical information about the attacks on documents.

As counteraction to the attacks is carried out by authentication of the document, the measure of firmness can be measured through parameters, that characterize, in this case, facilities of defence. To such parameters belong η, it is measure of saturation of a fragment of graphic appearance, μ is measure of divisibility of two contiguous lines of the pattern, χ is change of divisibility of two contiguous lines, γ is local density of defence means of e_i. Except for geometrical parameters which are listed above, which are direct descriptions of graphic appearance, the count influence on the size of firmness Ω parameters. The count parameters, in certain sense is possible to name functional, because they are used for description of recreation process of graphic appearances, at modification, or for the change of graphic facilities of defence. It is also one of factors of firmness of defence facilities, as the basic type of attack on documents is based on the imitation of defence facilities, which consists of their unauthorized making. General descriptions which influence on firmness of graphic defence facilities, are the features of realization of algorithms trajectories forming of graphic appearance, which are determined by the terms of implementation of separate fragments or steps of such algorithms. One of such descriptions is the measure of similarity of two fragments of counts which interpolate the fragments of different graphic appearances $\pi(G_i, G_{i+1})$. Such parameters belong to the parameters of this type, as length of trajectory of count *of* l_i, orientation of fluid rib α_i the count G_i and the nearest surroundings ε_i.

Methods of calculation of statistical information about results which are up to the exposed and unexposed attacks are based on the usage of concepts about the trees of events and trees of threats, which represent logic-probabilistic dependences between the sequences of factors, that stipulate the proper events and usage of these or other threats. Thus, in correlation for $\Omega_N = f_N(X_{N1},...,X_{Nm})$ it is possible to include parameters which are got on the basis of statistical information about history of the use of facilities of defence. As a rule, and scopes of calculational methods of statistical information about successful and exposed attacks, that are based on the usage of logic-probabilistic trees, the risk sizes of successful realization of attack on the basis of the use of credible models of estimation of the proper events are calculated. Therefore we will not enter in a function Ω_N constituents, which represent the results of statistical data analysis about events which took place in relation to documents and which also characterize such parameters as risk of the use of documents., within the framework of this technology. Logic-probabilistic approach in accordance with the known methods of its realization [3, 4], but the calculated sizes of the R_s risk will be used for the analysis of adequacy of the size risk R, which is calculated on the basis of local parameters which characterize the measure of protected and threat of defence facilities.

Thus it is possible to write down the following dependence for determination of risk size R:

$$R = a\sum_{i=1}^{n}\left\{\left[\sum_{j=1}^{k}\left[(\alpha_j X_{Bij})/k\right]\right]/\left[\sum_{j=1}^{m}\left[(\beta_j X_{Nij})/m\right]\right]\right\}, \tag{2}$$

where a is the coefficient of setting norms of the R size, α_j is the coefficient of activity of the use of j mean of defence, at counteraction to the attacks, X_{Bij} the parameters which characterize defence facilities, κ is the amount of parameters which are used for description of mean of defence within the framework of one fragment, n is amount

of fragments which are selected in graphic appearances, for realization of control and exposure of attack on a document, during its authentication, β_j is the coefficient similar to the coefficient α_j for X_{Bi}, X_{Nij} the parameters of threats which take place in facilities of defence, m is the amount of parameters of threats.

Size of the usage threat of the protected documents is straight proportional to exactness with which documents are identified and inversely proportional to exactness of reflection, or exactness of realization of parameters of defence, that is interpreted as parameters of threats.

Expedience of the risk use to the type R, which is determined on the basis of analysis of parameters of defence facilities and parameters of threats, and risk to the type R_s, that is determined on the basis of statistical information about exposed and unexposed attacks, are based on the fact that disagreements between the sizes of these two parameters are used for determination of realization necessity of managing actions which are oriented to replacement of parameters of defence facilities and parameters of threats. The necessity of initiation of management by the level of defence and level of threats in the system of authentication of documents is determined on the basis of the use of correlation between R and R_s, which is written down as following:

$$\left| R - R_s \right| \le \delta R , \tag{3}$$

where δR is the possible size of declination between the sizes of risk, that is shortchanged on the basis of analysis of defence parameters and parameters of threats and risk size, that is shortchanged on the basis of analysis of successful and unsuccessful attacks. However, the management by a risk size can be carried out in relation to the parameters of defence in two directions: in direction of the increase level of defence and in direction of lowering level of defence, we will write down the correlation resulted above as following:

$$\left\{ \left[(R_s - R) \rangle 0 \right] \to \left[U(R) = \varphi(\Omega + \Delta\Omega) \right] \right\} \vee \left\{ \left[(R_s - R) \langle 0 \right] \to \left[U(R) = \varphi(\Omega - \Delta\Omega) \right] \right\} , \tag{4}$$

where $U(R)$ is the function of management by the risk, $\varphi(\Omega+\Delta\Omega)$ is the function which will realize the necessary measure of increase of firmness of defence facilities, by the increase of values parameters of defence facilities, $\varphi(\Omega-\Delta\Omega)$ is the function which will realize diminishment the sizes of parameters of defence facilities, that results in diminishment of firmness of defence facilities to the possible attacks.

Expedience of such management by the risk consists in the following. It is important to make the graphic facilities of defence with the high level of firmness. The price depends on the level of firmness Ω. The lower level of firmness is, the lower cost of making of defence facilities. Such factors of defence are not analysed in this case, as the period of functioning of documents, size of drawing of documents with one type of defence facilities, although they can be described as the proper models of defence and be used for realization of management by a risk size. The edition to the document, as the factor, that determines one, or few parameters of defence, assumes the next interpretation of its communication with firmness. The smaller the edition of documents with facilities of defence of one type is, the higher is the level of firmness to the document. Similar interpretation is possible and in relation to the time of functioning of the document. We will determine the period of functioning of the document by the time domain from a moment the origin of the document to the moment of completion by it the complete period of managing action. Clearly, that there are documents with different periods of managing action, including the permanent periods of action, for example, the document in of jurisprudence and etc. Interpretation of defence factors in relation to the period of functioning of the document, for documents with the limited time of managing action, consists in the following. The shorter time period of functioning of the document is, the higher is level of its protection and vice versa.

We will consider some, basic functional parts of information technology of document authentication. In the Fig. 1 general functional unit scheme of functioning the information technology of document authentication is resulted, including their planning and custom controls by the risk.

Making the polygraphy documents is accompanied by planning the facilities of their defence. In the process of planning cyclic verification of use risk of the protected documents is carried out. If the risk of their use is more than some set size $R_z > R_p$, modification of defence facilities is executed with by turn verification or all parameters of defence facilities are in the set scopes. Disparity though brings one over the parameters of defence facilities to alternative completion of information technology of defence.

175

If the risk of the use of the consequent documents meets the set requirements, there is forming of method of document defence with subsequent verification of marketability its parameters (PM=RZ). Marketability parameters of the formed method of document defence provide exploitation of the protected documents. If the parameters of defence method can not be realized, there is modification of usage risk of protected document and forming of a new method of their defence. Such procedure takes place cyclicly to complete achievement of necessary risk size of the use of the protected documents.

In the process of exploitation of documents verification of difference between the statistical and structural risk is made $|R_s - R| \leq \delta R$. If the size of declination between the statistical and structural risk is in the set scopes, there is verification, whether edition of the document is not exhausted. Ending of drawing of documents foresees normal completion of exploitation of the document within the framework of technology of its defence. Verification of volume of edition of size of drawing and size of declination between the statistical and structural risk is carried out cyclicly. In case of no implementation of condition $|R_s - R| \leq \delta R$ there is modification of firmness measure of the document.

In the figure such reductions are used:
- PZD is planning of facilities of document defence;
- MZZD is modification of facilities of document defence;
- MMSD is modification of measure of firmness of mean of document defence;
- FMZD is forming the method of the document defence;
- EZD is exploitation of the protected to document;
- MUR is modification of risk of the use of the document protected;
- AZIT is alternative completion of information technology;
- NZD is normal completion of exploitation of the document within the framework of technology of its defence;
- $R_z > R_p$ is verification of risk level of the use of the document protected;
- MP=D is verification, whether are parameters of defence in possible scopes;
- PM=RZ is verification, whether are parameters of method of document defence can be realized;
- $|R_s - R| \leq \delta R$ is verification, whether difference between the statistical and structural risk is possible;
- TD=0 is verification, whether edition the document is not exhausted.

Conclusions

The developed information technology of polygraphy document defence can be used for construction the systems of document preparation in the social sphere and control system. The control system by the risk of the use the protected documents is the important element of the defence system of documents, which allows to provide optimum correlation of price and quality of graphic defence of documents. The system of document defence represented in the work allows to provide their operative authentication on all stages of the use, that substantially promotes strength security of documents in the system of document turnover.
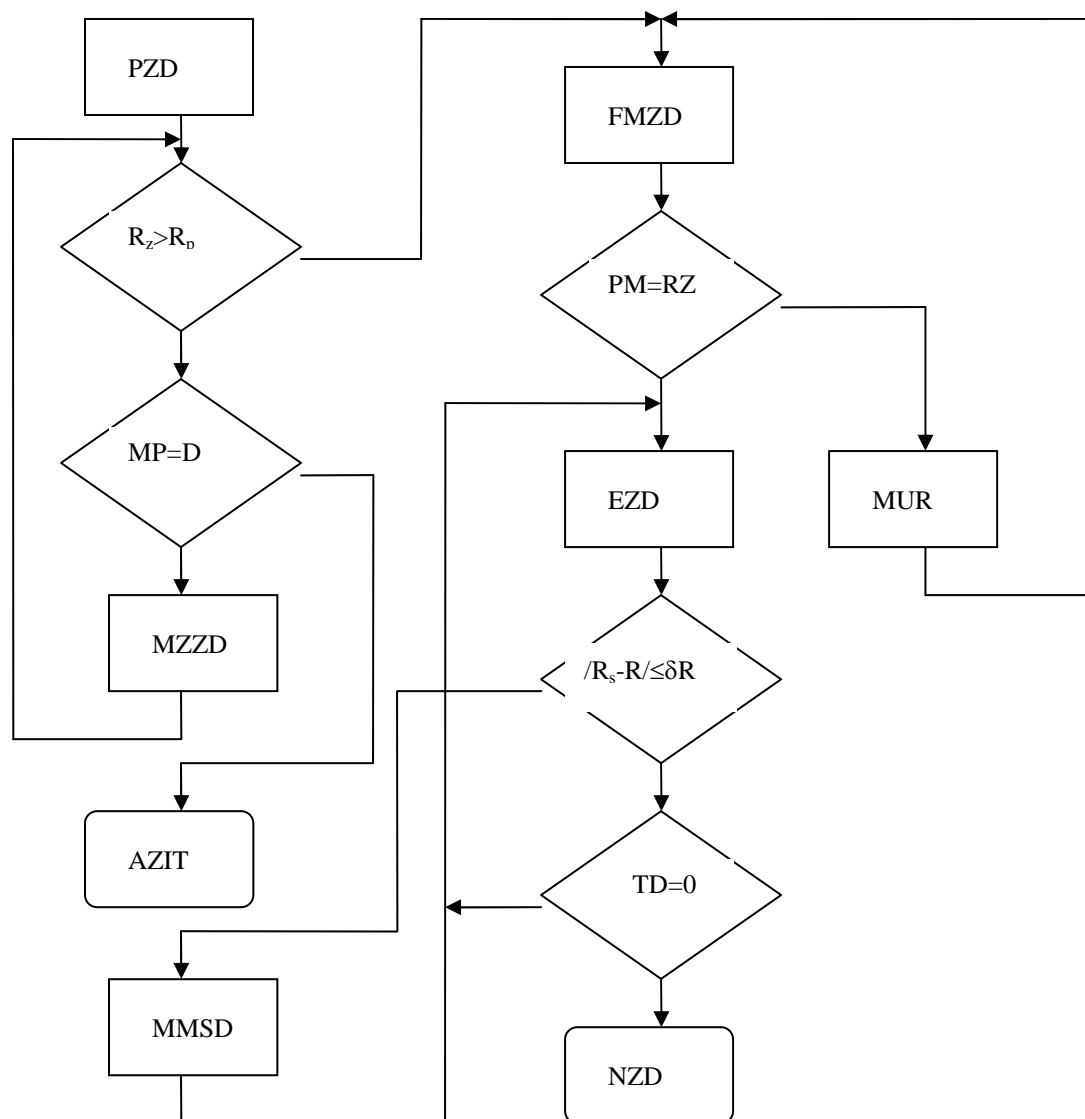
PZD

FMZD

$R_z > R_D$

PM=RZ

MP=D

EZD

MUR

MZZD

$/R_s-R/ \leq \delta R$

AZIT

MMSD

TD=0

NZD

Fig.1. General   functional unit scheme of functioning of authentication technology of the document.

References

[1] Современные технологии анализа рисков в информационных системах. – М.: Компютерная неделя №37(307), 2001.

[2] Практический поход к созданию и поддержанию информационной безопасности. Jet Info, №1-3(8-10), 1996.

[3] В.О. Омельченко, В.Г. Санніков. Теорія електричного зв'язку. Ч.3.Підручник. – К.: ІЗМН, 1997. – 640с.

[4] Вентцель Е.С. Теория вероятностей. М.: Наука, 1969.

[5] Modern technologies of analysis of risks in the informative systems.   M.: Kompyuternaya nedela №37(307), 2001.

[6] Practical approach to creation and maintenance of informative safety. Jet Info,   №1-3(8-10), 1996.

[7] V. O. Omel'chenko, V. G. Sannikov. The theory of electric connection. Ч.3.Підручник. - К.: ІЗМН, 1997. – 640 с.

[8] Ventsel E.S. Theory of chances. M.: Nayka, 1969.