АНАЛИЗ ТЕХНИЧЕСКОЙ ВОЗМОЖНОСТИ МАСКИРОВКИ СУБМАРИНЫ ОТ СРЕДСТВ ПЕЛЕНГАЦИИ

Приводятся результаты лабораторных исследований эффективности ультразвуковых технологий при решении задач маскировки субмарин от средств пеленгации подкильной, опускаемой и буксируемой структуры гидроакустических станций с антеннами переменной глубины. Доказана возможность маскировки субмарины при отсутствии собственного хода. Проанализированы возможности предлагаемого технического решения для создания маскирующего ограждения на основе геометрического резонанса искусственно формируемых ограждающих зон каустики.

Ключевые слова: аберрация, волновое совпадение, поверхность каустики, окружные волны, изгибные волны оболочки.

Karachun Volodimir, *Doctor of Technical Sciences, Professor, Department of Biotechnics and Engineering, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Ukraine, e-mail: karachun11@i.ua, ORCID: http://orcid.org/0000-0002-6080-4102*

Mel'nick Viktorij, *Doctor of Technical Sciences, Professor, Head of Department of Biotechnics and Engineering, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Ukraine, e-mail: vmm71@i.ua, ORCID: http://orcid.org/0000-0002-0004-7218*

Fesenko Sergii, *Postgraduate Student, Department of Biotechnics and Engineering, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Ukraine, e-mail: illusionfes@mail.ru, ORCID: http://orcid.org/0000-0003-1001-0643*

UDC 681.62
DOI: 10.15587/2312-8372.2017.105146

Biziuk A.
Tkachenko V.,
Vovk A.

DEVELOPMENT OF METHODS AND MODELS OF COMPLEX OF SECURITY TECHNOLOGIES FOR PRINTING PRODUCTS

Проведено аналіз існуючої технології опису рівня захищеності поліграфічного виробу від фальсифікації з наступним виявленням її недоліків. Розроблена математична модель, що дозволяє обчислити інтегрований показник захищеності виробу. Особливістю моделі є використання поняття «технологічний ряд», щоб виключити застосування однотипних захисних елементів. Результатами проведеного дослідження є рекомендації з оптимізації вибору захисного комплексу.

Ключові слова: *захищеність поліграфічного виробу від фальсифікації, технологічний ряд, захисний комплекс, захисний елемент.*

1. Introduction

Currently, in Ukraine and most countries of the world there is an objective need to counter falsification of printing products. The urgency of this problem is largely due to the development of printing technology and its widespread use.

With all the variety of currently available technical security methods, there is a certain gap in the field of security of products of wide distribution, such as labels and packaging. The issue of security of the printing design is especially acute in connection with development of reproductive and digital equipment, which makes it possible to easily reproduce the original packaging that does not have security. Unlike traditional objects of application of security equipment, packaging and label products have certain limitations. These restrictions primarily concern the cost of protected products, the nature of the design and the used materials.

Given the cost constraints imposed on the security elements of label and packaging products, the applicability of most of them is low, as well as economic efficiency. For these reasons, it is necessary to create an effective integrated product suitable for the security of labels and packaging products.

Thus, there is a need to develop methods and models for assessing the level of security of a printed product, which will make it possible to comprehensively solve the problem of choice and minimize the cost and time costs for developing the original layout of a protected product.

2. The object of research and its technological audit

The object of research is the process of selection of the elements that make up a complex of security printing technologies to counter the fabrication of a printing product.

The subject of research is optimization methods in the problems of selecting a complex of security printing technologies, information technology of pre-press preparation of publications.

One of the most problematic places is the process of deciding whether to incorporate into the design of a printed product some or other elements that protect the product from falsification. At large and well-known enterprises, such as Ukrspetspoliprografia (Ukraine) or Goznak (Russia), such decisions are made on the basis of collective analysis in the relevant departments. Secured printing products number dozens (securities, documents) and even hundreds (money banknotes) of security elements

ISSN 2226-3780

of varying degrees of complexity. The expediency and necessity of counteraction to falsifiers in these cases often cause the use of complex and expensive elements of security (nanotechnologies, special types of printing, etc.).

However, for simpler printing products, such as alcohol labels, food products, perfume, drug packaging, often just a few simple security elements are enough to complicate the possibility of counterfeiting.

Such products are developed and printed in small enterprises, using common technologies and conventional equipment.

The effectiveness of security in this case is ensured by the complexity of the selected security elements, based on different physical principles. For example, microtext and microimages are based on the use of high-resolution equipment and can be falsified by the same counterfeiting technology. While a pair of security elements – microtext and pseudo-ireal printing in pantone color are based on different principles, and require greater efforts for falsification. However, when printing labels on offset equipment of good quality, both of these security elements in the original product are realized quite simply and do not require significant costs.

The choice of a security complex, that is, the selection of a small number of security elements that will provide a sufficient level of counterfeiting, requires certain knowledge in the field of secured printing. To solve this problem, within the framework of a small firm or design bureau, an automated information system will be a good help. This system in the conditions of a specific type of product and given financial constraints will help to make a list of security elements for inclusion in the developed original layout.

3. The aim and objectives of research

The aim of research is analysis of scientifically based models and methods for optimizing the selection of a complex of security printing technologies that ensures a sufficient level of security of a printed product from falsification.

To achieve this aim, the following tasks must be accomplished:

1. Analysis of information technologies used to protect printing products from unauthorized copying and falsification.

2. Development of an information model for the task of selecting a set of security printing technologies for a printed product (labels, packaging).

3. Statement of the mathematical problem of optimizing the selection of a complex of security printing technologies for a printed product.

4. Research of existing solutions of the problem

Development of quality systems that ensure the safety of products from attacks by counterfeiters has been going on for a long time. Various approaches are considered, both related to a comprehensive approach to the problem [1–3], and to the improvement of individual elements [4–6]. More promising authors consider integrated systems of security of printed products, when the original layout includes several security elements. A general description of elements of printing security includes hundreds of titles [2, 3, 7, 8].

In modern conditions of the development of computer technology, the theory of the development of information systems that can become a working tool of a designer of protected printed products becomes topical [9, 10]. In conditions of a variety of available security technologies, it is necessary to comprehensively assess the level of product security, to choose the optimal solution [9–12].

The main tasks of research are the following:

– evaluation of the security level of printed product. To do this, integral assessments are introduced, classification of types of security is carried out, weight coefficients are considered;

– selection of optimal parameters and security elements. A mathematical optimization model is constructed, which can be solved further within the framework of linear optimization or graph theory.

To assess the security level of a printed product in the literature, a weighted average integrated indicator is calculated based on the following criteria [7, 9]:

– the security degree provided by this technology;

– the cost of using this security element;

– a combination of these indicators.

In general, the integrated indicator is defined as:

$$R_{\text{int}} = \sum_{i=1}^{N} R_i x_i, \qquad (1)$$

где R_{int} – integrated indicator of security of a printed product; R_i –weight coefficient, taking into account the importance of security technology, based on its complexity, security properties; As a rule, in normalized systems $\sum_{i=1}^{N} R_i = 1$; x_i – a number of security elements that form a system of security products, usually represented in binary form $x \in \{0; 1\}$.

The level of importance of the security element is determined in [9] by the method of polling of ten experts with subsequent averaging. Similarly, the level of increase in the cost of the basic (unprotected) product is calculated. However, for a peer review, a limited set of security technologies is chosen, focused on a specific type of printing packaging.

Results of processing of expert estimations on much larger circle of security are resulted in [7]. Therefore, in subsequent studies, this list is taken as the basis, which was later refined and supplemented.

A hierarchical scheme for assessing the quality of worn banknotes by using the hierarchy analysis method or using a complex indicator is developed in [10]. One of the criteria for assessing quality is the adoption of security, which includes as part of the group of material security, graphics, special types of printing, paints and post-printing [7]. On the basis of a generalized scheme for quality formation of banknote production, further production methods for improving technological processes are explored. The study developed a system for assessing the wear resistance of products obtained with the use of new solutions, as well as information tools that allow the implementation of new technological solutions and support feedback from users. The weight of the corresponding coefficients in the integrated indicator is calculated by statistical analysis of the results of the analysis of damaged banknotes. The degree of influence of partial criteria is taken into account by standardized indicators:

$$R_{\text{int}} = \begin{cases} \dfrac{x_{ij}}{x_{\max j}}, \ j = 1,k; \ x \in S, \\ \dfrac{x_{\min j}}{x_{ij}}, \ j = k+1,m; \ x \in D, \\ 1 - \dfrac{x_{ij}}{x_{\max j}}, \ j = m+1,k; \ x \in D^0. \end{cases} \quad (2)$$

The problem of optimization of a protected printed product is considered both for general cases [12], and for particular cases of packaging [8] or bank checks [4]. The method of linear optimization and graph theory is investigated.

The concept of «technological series» is introduced in [7] for a more accurate classification of technologies for printing security. As a definition, it is proposed the following: «the technological series unites types of printing security based on the same technological principle». In particular, the following technological series are distinguished (Table 1).

The security data are shown in Fig. 1 in more detail, taking into account the security properties and the economic coefficient.

In accordance with the table in Fig. 1, it is possible to develop a set of printing security, as well as avoid the repetition of the same type of security, while maintaining a sufficient level of product security.

In the developed table (Fig. 1), the vertical columns determine the reliability index of predictable security. Depending on the requirements for the printing product and, accordingly, the overall reliability index of the security complex, the elements can be classified according to their significance as follows:

1 – security, used only as auxiliary;
2 – security, which have satisfactory reliability;
3 – security of sufficient reliability;
4 – security by a high measure of reliability;
5 – dominant security;
6 – security of the highest measure of reliability.

Depending on the background conditions (controlled or uncontrolled), the significance of using security for a given range may vary. This particular protective technology can be highly resistant to falsification in itself, but if under these conditions such security can't be verified – the effectiveness of such security is reduced to zero.

On this basis, the integrated indicator of the security of a printed product can be calculated as:

$$R_{\text{int}} = \sum_{i=1}^{N} A_{ij} \sum_{j=1}^{M} R_{ij} x_{ij}, \quad (3)$$

where i – the serial number of the technological series; j – the serial number of the security technology in this technological series; A_i – coefficient of significance of this technological series in specific conditions for a specific type of printing products; R_{ij} – security coefficient of this technology of printing protection [7]; x_{ij} – set of security elements that form the system for security of a printed product is represented in a binary form $x \in \{0; \ 1\}$.

The problem of selecting a complex of security printing technologies for hampering unauthorized reproduction (falsification) has been repeatedly discussed in [3, 7, 9, 12]. As a rule, the creative nature of the solution of this problem and the need for cooperation with an expert in this field are emphasized.

Table 1

Classification of printing security by technological series

№ of series	Technological series	Principle of operation	Examples of security
1	Thin graphics in an uncontrolled environment	Using the minimum possible thickness of the element lines	Background tangry (anti-scanner) grid nets, guilloche elements, hidden images, microtext mm, microtext micron, micrographics
2	Thin graphics in a controlled environment	The manifestation of hidden images in thin graphics elements based on the use of a multicolor dot with a regular structure	Void Pantograph (a different dot with a regular structure), Copy ban + (a different dot with an irregular structure)
3	Dyes that glow in UV, IR radiation	Glow in UV/IR radiation	Colorless, colored, two-layered
4	Specialized dyes	Color change under the influence of physical and other influence	Metallized, oxidizing, penetrating, intumescent, color-shifting OVI, photosensitive, thermosensitive,double-layer thermosensitive
5	Water marks	Use of special paper	Tinting of paper cloth, figured silicone coating, one-level, two-level, halftone watermarks
6	Addition of visible inclusions into the material	Use of special paper	Fibers, heat-sensitive fibers, metallized threads, diving (stitch) metallized threads
7	The addition of inclusions visible in the UV and IR ranges into the material	Use of special paper	Invisible fibers, visible fibers, metallized threads – changing color in IR/UV radiation
8	Embossing	Special postpress operations	Stamping embossing, foil embossing
9	Die cutting	Special postpress operations	Figured die cutting
10	Holograms	Special postpress operations	Embossing with holographic foil, pressing of holograms
11	Machine-readable codes	Use of data scanning technologies	QR codes, bar codes, OCR codes, MICR codes, magnetic stripe, RFID identification
12	Numbering	Use of nonrepeating data	Numbering, numbering with perforation, numbering with control discharge, numbering with security paints
13	Printing technologies	Special types of printing	High, deep, pantone, pseudo-ire (pantone gradient), metallographic, iris (prismatic), Orlov printing

ISSN 2226-3780

Konshin series	Principle of operation	1	1	2	2	3	3	4	4	5	5	6
1	Anti-scanner protection	–	Tangular grids	–	Guilloche elements	Latent Image	–	–	–	–	–	–
1	Microtext and micrographics	–	–	Microtext, mm	Microtext, mm	Micro-graphics	–	–	–	–	–	–
2	Anti-scanner protection with hidden image	–	–	–	–	Void Pantograph	** Latent Image (tilting effect)	Copy Ban +	–	–	–	–
3	Specialty dyes	–	Colorless UV	Colored UV	Current-carrying UV	Visible in IR	Double-layer visible in IR	–	–	–	–	–
4	Specialty dyes	Metallized	Oxidizing	Penetrating	Intumescent	Color-shifting OVI	Light sensitive	Thermo-sensitive	Double-layer thermo-sensitive	–	–	–
5	Water marks	–	Toning of the paper web	Figured silicone coating	–	One-level watermark	–	–	–	–	Two-level watermark	Halftone watermark
6	Fibers and inclusions	–	–	UV invisible fibers	–	UV visible fibers	Metallized fibers	Thermo-sensitive fibers	Metallized thread in the paper	Stitch metallized thread	–	–
7	Stamping and Die cutting	–	Figured die cutting	Stamping embossing	–	Foil stamping	–	Metallo-graphic ornament	Complex chemical protection	–	–	–
8	Embossing and holography	–	Protective gluing of self-copying forms	–	–	–	–	Embossing with holographic film	–	Pressing of holograms	–	–

Fig. 1. Classification of technologies of printing security according to technological series, taking into account the measure of security reliability

The formalization of the criteria for the selection of printing security, based on the level of product security and the increase in prime cost, is given in [3, 7, 12]. The future work on the construction of a model for the task of optimizing the parameters of a complex of printing security is considered promising, when the sufficiency in terms of the product's security (labels, packaging) and the commercial aspect of printing are the priorities.

5. Research results

5.1. Development of mathematical model. When solving a specific optimization problem, the researcher must first choose a mathematical method, with which it will be possible to obtain the final result with the least computational cost. The choice of this or that method is largely determined by the formulation of the optimization problem, and also by the mathematical model of the optimization object.

Let's formulate the problem of optimizing the parameters of a security printing complex as follows [12].

Let the values of the parameters of the security complex, i. e. the list of technologies used to protect the printing products against falsification, constitute a certain set X. Let's select from this set the subset x: $x \in X$, which represent the values of the parameters of the complex potentially applicable in this particular case. For example, the use of a microtext label with a normal resolution in a print, a high-resolution microtext, microimages are parameters of a complex that belong to a set of X, whereas Orlov or iris printings do not belong to this set.

In this case, the parameter of the complex corresponds to the presence (absence) of this or that technology of printing security and can be represented as:

$$\{x_i \geq 0;\ x_i \subset X;\ i = \{1, N\}\}. \quad (4)$$

This vector contains characteristics of a complex of printing security of arbitrary complexity.

Taking into account the significance of each parameter and, accordingly, the security level of the product, let's place the elements of the vector in correspondence with a certain weight characteristic R_{ij}: $\{R_{ij} \geq 0;\ i = \{1, N\};\ j = \{1, M\}\}$.

The weight characteristic R_{ij} is the coefficient, which in conventional units indicates the security degree of the printing product, provided that this security element is included in the security complex. Specific values of the weight characteristics R_{ij} are determined on the basis of statistical studies, taking into account the type of the protected printing product.

Let's compose the function of integrated security of the product (the objective function) for the task. In this case, x_{ij} will be parameters that need to be determined based on the maximization of the aggregate security level. The correctness of such premise is shown in [10] and is based on the fact that the logical function of the conjunction can be interpreted as the sum of the corresponding components in the arithmetic sense:

$$R_{\text{int}} = R_1 x_1 + R_2 x_2 + \ldots + R_n x_n = \sum_{i=1}^{N} R_i x_i \to \max,$$

$$R_{\text{int}} = \sum_{i=1}^{N} A_i \sum_{j=1}^{M} R_{ij} x_{ij} \to \max. \quad (5)$$

It should be noted that the conditions under which this approach can lead to a reassessment of the actual security level of the product. The authors of [3, 10] show the necessity of taking into account the complexity of the algorithm of forming the function of the security level, which they relate to the level of costs for the implementation of this algorithm.

The conditions that apply to the parameters of the protective complex are mainly of economic origin – a reduction in the cost of the product. However, indirectly, the diversity of the principles used to counter counterfeiters is taken into account here.

Formalization of such requirements is not an easy task, and in practice the generalized data given in [7] are often used, where the level of rise in cost of production with respect to the base product is displayed by cost indices (Table 2).

Table 2

Correspondence of level of rise in price of the cost price in relation to a base product

Value index	Rise in price in relation to the base product, %
1	0–5
2	5–30
3	30–50
4	50–100
5	100–200
6	200–300
7	300–400
8	400–500

A conditional base product is understood as an unsecured polygraph product corresponding to this security. That is, the masking meshes for mailers and mailings correspond to a basic unprotected mailer or mailing. Contour silicone coating with toning of silicone mass corresponds to an unprotected printing self-adhesive product. Paper with a watermark corresponds to the product on unsecured offset paper. UV, IR and heat-sensitive paints correspond to an unsecured product made with conventional printing inks.

The best relation between the value index and the rise in price is described by a polynomial dependence, as shown in the graph of Fig. 2.

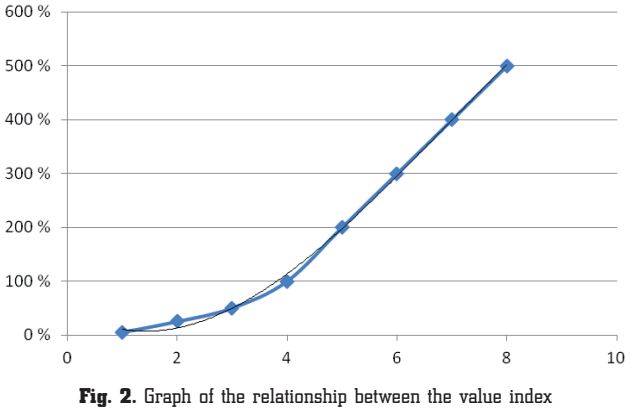

Fig. 2. Graph of the relationship between the value index and the rise in price

The aggregated rise in price of the base product can be defined as a first approximation as the total index of the rise in price of the prime cost, determined by all applied security technologies.

Thus, the cumulative increase in the cost price of a printed product in comparison with the base product can be defined as:

$$C_{\text{int}} = c_1x_1 + c_2x_2 + ... + c_nx_n = \sum_{i=1}^{N} c_ix_i \le C_0. \quad (6)$$

In this case, as a rule, the maximum rise in price is limited by a certain level of C_0.

As a result, the general problem of linear programming for selecting parameters that define a complex of printing security may look like:

$$R_{\text{int}} = \sum_{i=1}^{N} A_i \sum_{j=1}^{M} R_{ij}x_{ij} \to \max,$$
$$C_{\text{int}} = \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij}x_{ij} \le C_0. \quad (7)$$

An important tool for increasing the effectiveness of numerical methods of linear programming, as in other fields of mathematics, is the consideration of the additional specificity of the solving problem. Due to the complexity of the logical structure of the general method, it is often possible to reduce its complexity and simplify the requirements for the power of computer technology.

When solving this problem for specific cases, the obtained results will reflect the values of the vector of technologies applied in the protective complex, expressed by binary values («1» – technology is enabled, «0» – technology is disabled). However, the analysis of the algorithm for solving the linear programming problem points to the one-sided nature of such optimization method with respect to the chosen direction of its application – the process of selecting elements of complex printing security. The essence of this shortcoming is in the above formulation of the problem, a number of inexpensive, one-type protective technologies can be chosen, which are based on the same technological principle.

Thus, let's consider it expedient to supplement the task of optimizing the parameters for selecting complex printing security by taking into account the technological series, introducing an additional condition – each technological series must be represented by only one security technology.

The statement of the problem will remain the same for all types of printing products, but it is supplemented by a condition of the form:

$$\sum_{j=1}^{N} x_{ij} = 1, \quad (8)$$

for each i-th technological series.

As a result, the general problem of linear programming for selecting parameters that define a complex of printing security may look like:

$$R_{\text{int}} = \sum_{i=1}^{N} A_i \sum_{j=1}^{M} R_{ij}x_{ij} \to \max,$$
$$C_{\text{int}} = \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij}x_{ij} \le C_0,$$
$$\sum_{j=1}^{M} x_{ij} = 1 \,|\, \forall i = 1, N. \quad (9)$$

The result will be a set of recommended security elements that provides the highest possible security rating with a given limitation of the level of increase in prime cost.

ISSN 2226-3780

5.2. Development of a system of indicators and methods for assessing the security level of printing products. To determine the importance of accounting for various technological series, an experimental account of the frequency of use of protective technologies in labels of alcoholic beverages, food products, drugs produced by printing enterprises in Kharkov (Ukraine) is taken. The possibility of combining various security elements to counter falsification is analyzed.

Samples of secured printed production are analyzed for this purpose, the main elements of security are identified, the frequency of occurrence of this element is calculated (Table 3).

Based on the results of the generalized analysis, the weight coefficient is calculated with which this security element will be taken into account in the integrated evaluation of the product's security. This weight coefficient takes into account the frequency of occurrence of this element in the totality of the considered samples, as well as the belonging of the element to a certain technological series. For example, the use of metallic paints or pantone inks as a security element is found in very many labels, they are taken into account within the same technological series and are interchangeable elements. Figured die cutting is much less common than metallic ones, but within its technological range is the predominant security element.

Table 3

Analysis of the applicability of security technologies

Frequency of occurrence,%	Weight coefficient, %	Security element	Kazatska Rada label	Bud'mo label	Hamilton label	Syabrovka label	Rusalka Maiak label	Rusalka-Volna label	Rusalka-Ryby label	Sretenka vodka label	Smirnoff label	Finlandia label	Stolichnaya label	Set of labels for cognac, Dovgan-Ukraine company (Kharkov)	Sausage label Flexoprint
69	31	Figured Die Cutting	–	+	+	+	–	+	+	+	–	+	–	+	+
92	43	Metallic paint	+	+	+	+	+	+	+	+	+	+	+	+	–
77	42	Pantone color	–	–	–	+	+	+	+	+	+	+	+	+	+
85	33	Barcode	+	+	+	+	+	+	+	+	+	+	–	+	–
62	24	Microtext 2pt	–	–	+	+	–	–	–	+	+	+	+	+	+
23	9	Microtext 2pt swath	–	–	+	–	–	–	–	–	+	–	–	–	+
8	3	Microimage	–	–	–	–	–	–	–	–	–	–	–	–	+
38	15	Ornamental microfiber	–	+	+	+	–	–	–	+	–	–	–	–	+
38	15	Anti-scanner background grid	–	–	–	+	+	+	+	+	–	–	–	–	–
38	83	Transparent glue	+	–	–	–	–	+	+	–	+	+	–	–	–
38	69	Base transparent film	+	–	–	–	–	+	+	–	+	+	–	–	–
15	8	Base metallic color	–	–	–	+	–	–	–	–	–	–	–	+	–
8	17	Printing on the adhesive side	–	–	–	+	–	–	–	–	–	–	–	–	–

5.3. Estimation of the significance of the used statistical data. In selective observation, the concepts of «general set» are used – the studied set of units that is to be studied on the basis of characteristics of interest to the researcher, and «sample set» is a randomly selected part of the general set. This sample is presented with the requirement of representativeness, that is, when studying only a part of the general set, the conclusions can be applied to the whole set. Characteristics of the general and sample collections can be the average values of the studied features, their variances and the mean square deviations, mode and median, etc.

Researchers may also be interested in the distribution of units according to the characteristics studied in the general and sample collections. In this case, frequencies are called general and selective, respectively.

The system of selection rules and methods for characterizing the units of the studied set is the content of the sampling method. The essence of the method consists in obtaining primary data when observing the sample with subsequent generalization and analysis. The received data extend to the general set, assuming that the conclusions obtained in the sample set will be true for the general set.

The representativeness of the sample is ensured by observing the principle of randomness of selection of objects in the set. If the set is qualitatively homogeneous, then the randomness principle is realized by a simple random selection of sampling objects. A simple random selection is a sampling procedure that provides for each unit of the set the same probability of being selected for observation, for any sample of a given volume.

Thus, the purpose of the sampling method is to draw a conclusion about the significance of the characteristics of the set on the basis of random sampling information from this set.

The power of the criterion is the ability of the criterion to detect statistically significant differences, if they really exist. When planning a study, it is necessary to know the power of the used criterion. It makes sense to begin the study when there is a good chance to detect clinically significant differences. And it makes no sense to spend resources on 40 % the probability of confirming the effect of a new remedy. Usually, the power is selected at the level of 70–80 % (β = 0.2–0.3). The significance level α is given by the researcher himself. Currently, for clinical trials, it is recommended to choose alpha 0.01 or even 0.001:

$$n = \frac{pqZ_\alpha^2}{\Delta^2} = \frac{0{,}75 \cdot 0{,}25 \cdot 2{,}3^2}{0{,}05^2} \approx 400. \quad (10)$$

In this case, let's consider the type of sample as a simple random sample (simple randomized selection). In this case, any sample unit has equal chances to be selected.

For quantitative characteristics:

$$n = \frac{s^2 Z_\alpha^2 N}{\Delta^2 N + s^2 Z_\alpha^2}, \quad (11)$$

where N – the volume of the general set; Δ – sampling error is an objectively discrepancy between the characteristics of the sample and the general population, as well as the level of significance, the sampling error is set by the researcher himself. Its preliminary evaluation (the preferred value before substitution into the formula) is often arbitrary. As a rule, it is not recommended to accept a sampling error above 5 %.

For nominal and ordinal attributes (the proportion of objects with a given characteristic):

$$n = \frac{pqZ_\alpha^2 N}{\Delta^2 N + pqZ_\alpha^2}. \quad (12)$$

The representativeness of the sample is confirmed by statistical calculations. To estimate the required range of a representative sample n, the following formula is used:

$$n = \frac{pqZ_\alpha^2 N}{\Delta^2 N + pqZ_\alpha^2} = \frac{0{,}75 \cdot 0{,}25 \cdot 2{,}3^2 \cdot 2500}{0{,}05^2 \cdot 2500 + 0{,}75 \cdot 0{,}25 \cdot 2{,}3^2} \approx 345, \quad (13)$$

where N – the volume of the general set, for the Kharkov region (Ukraine), numbering about 500 printing enterprises, it was decided to consider a total range of issued labels in 2500 titles; Δ – sampling error, in accordance with the recommendations was adopted at 5 %.

The significance level α was chosen in accordance with the recommendations $\alpha = 0.015$, which corresponds to the critical Z value of the standard normal distribution $Z = 0.25$.

The probabilistic values $q = 1-p$, p were chosen empirically, in the paper $p = 0.75$ and $q = 0.25$.

For an unknown number of the general population for quantitative characteristics, the formula is somewhat simplified, but it gives a calculated result of the same order:

$$n = \frac{pqZ_\alpha^2}{\Delta^2} = \frac{0{,}75 \cdot 0{,}25 \cdot 2{,}3^2}{0{,}05^2} \approx 400. \quad (14)$$

Thus, the analysis of more than 500 labels (printed products) carried out during the study can be considered sufficient from the point of view of statistical certainty.

The research shows that the most common in modern labels is the use of non-traditional printing inks – pantone colors, metallized paints. Figured die cutting is often occurred. The printing of protective anti-scanner grids and micro-text inscriptions with font size less than 2 pt, which is dictated by the fight against digital falsification, are popular.

6. SWOT analysis of research results

Strengths. The proposed methodology makes it possible to facilitate and improve the work of the designer and developer of printing products (labels, packages) that require the use of anti-counterfeiting elements. The main principles on which the methodology is based are:

– a comprehensive security system is preferable to the use of separate elements;

– the main factor controlled the falsifier is an economic factor. If the increase in the cost price of a product with security technology from a counterfeiter is higher than that of a developer, such security is deemed satisfactory.

The strengths of the proposed methodology include:

– ease of implementation of mathematical calculations, in the form of Excel spreadsheets or a simple software product;

– ease of use for a user who is not sufficiently trained in the field of secured printing. The user (designer) operates with the usual terms for himself (label, rise in price);

– the methodology is based on the classification series, which ensures the use in each specific product of various security elements.

ISSN 2226-3780

Weaknesses. To the weaknesses of the proposed methodology, one can attribute the general lack of problems solved by the method of linear programming. In particular, the selection of the complex begins with an element that gives maximum security with minimal cost increase. At the same time, an equivalent combination of less effective, but less expensive technologies can be lost.

Opportunities. Improvement of the proposed methodology may be associated with research and identification of the importance of secured printing technologies for specific types of products. The introduction of additional subcategories (wine label or low-alcohol label in the category «alcohol label») will allow more accurate consideration of the applicability of secured technologies in individual cases.

Another area of promising research is the use of more complex mathematical methods, for example, formal graph theory.

The main area of application of the proposed methodology are small design firms of printing orientation, developing inexpensive printed products of medium and small print runs. To introduce elements of printing protection against falsification in these cases, often it does not require the participation of an experienced expert. However, the selection of the optimal set of protective equipment is an important task.

Threats. The methodology assumes constant monitoring of security technologies, means of a press and postpress processing. New means of printing security appear quickly enough. The improvement of equipment leads to a reduction in the cost of security technologies. Thus, there is a need for constant updating and refinement of weight coefficients.

A software solution that allows to choose the optimal security complex, recommends only a set of security elements, but not their size and location on the secured product. Placement of security elements on the original layout is shifted to the designer-developer.

7. Conclusions

1. The analysis of information technologies used to protect printing products from unauthorized copying and falsification is performed, and a promising research direction is identified, namely, a comprehensive integrated assessment of the level of product security. There are 104 elements that can be considered as preventing falsification. Six characteristic profiles (wine label, perfume label, etc.) are distinguished. Lists of acceptable protective elements are made for them. In the optimization problem, from this list, the best ones are chosen according to the security properties within the constraints.

2. The application of the methodology of integrated indicators for evaluating the security of a printed product against falsification is proposed. The peculiarity of the technique consists in determining the weight coefficients taking into account 15 technological series to exclude the use of the same type of security elements. The significance of each element in the integral evaluation is determined by the analysis of 500 labels (printed products).

3. The mathematical problem of selection of a complex of security printing technologies by the method of linear optimization is set. The optimized value is an integrated assessment of the security level of a printed product against falsification, and the main limitation is the level of increase in the cost of a product due to the use of security elements.

References

1. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems [Text] / R. Anderson. – John Wiley & Sons, 2001. – 640 p.
2. Lampert, C. Printing Technique Classification for Document Counterfeit Detection [Text] / C. Lampert, L. Mei, T. Breuel // 2006 International Conference on Computational Intelligence and Security. – 2006. – P. 1–6. doi:10.1109/iccias.2006.294214
3. Kyrychok, P. O. Zakhyst tsinnykh paperiv ta dokumentiv suvoroho obliku [Text]: Monograph / P. O. Kyrychok, Yu. M. Korostil, A. V. Shevchuk. – Kyiv: NTUU «KPI», 2008. – 368 p.
4. Cerulli, R. Finding Pattern Configurations for Bank Cheque Printing [Text] / R. Cerulli, R. De Leone, M. Gentili // Procedia – Social and Behavioral Sciences. – 2014. – Vol. 108. – P. 219–234. doi:10.1016/j.sbspro.2013.12.833
5. Seto, A. Ensuring document security and privacy in transpromo printing [Text] / A. Seto, J. Lisi, M. K. Ahmed // 2009 IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH). – 2009. doi:10.1109/tic-sth.2009.5444488
6. Simske, S. J. Qualification of security printing features [Text] / S. J. Simske, J. S. Aronoff, J. Arnabat // Optical Security and Counterfeit Deterrence Techniques VI. – 2006. – P. 1–12. doi:10.1117/12.641762
7. Konshin, A. A. Zashchita poligraficheskoi produktsii ot fal'sifikatsii [Text] / A. A. Konshin. – Moscow: Sinus, 1999. – 160 p.
8. Warner, R. D. Introduction to Security Printing [Text] / R. D. Warner, R. M. Adams II. –Ed. 2. – USA, Pittsburgh, PA: Printing Industries of America (PIA) Press, 2016. – 240 p.
9. Krestianpol, O. A. Informatsiini tekhnolohii v proektuvanni systemy zakhystu pakovanoi produktsii [Text]: Monograph / O. A. Krestianpol, L. Yu. Krestianpol, B. O. Palchevsky; ed. by B. O. Palchevsky. – Lutsk: Vezha-Druk, 2015. – 160 p.
10. Kyrychok, T. Yu. Naukovi osnovy zabezpechennia znosostiikosti banknotnoi produktsii [Text]: Thesis of the Doctor of Technical Sciences / T. Yu. Kyrychok. – Lviv, 2014. – 450 p.
11. Hampden-Smith, M. Overt security features through digital printing [Text] / M. Hampden-Smith, S. Haubrich, R. Kornbrekke, J. Shah, R. Bhatia, N. Hardman, R. Einhorn // Optical Security and Counterfeit Deterrence Techniques VI. – 2006. – P. 1–10. doi:10.1117/12.641882
12. Biziuk, A. V. Raschet obobshchennogo pokazatelia zashchishchennosti poligraficheskogo izdeliia dlia informatsionnoi sistemy [Text] / A. V. Biziuk, P. E. Zhernova // Bionica Intellecta. – 2016. – № 1 (86). – P. 63–67.

РАЗРАБОТКА МЕТОДОВ И МОДЕЛЕЙ КОМПЛЕКСА ЗАЩИТНЫХ ТЕХНОЛОГИЙ ДЛЯ ПОЛИГРАФИЧЕСКИХ ИЗДЕЛИЙ

Проведен анализ существующей технологии описания уровня защищенности полиграфического изделия от фальсификации с последующим выявлением ее недостатков. Разработана математическая модель, позволяющая вычислить интегрированный показатель защищенности изделия. Особенностью модели является использование понятия «технологический ряд», чтобы исключить применение однотипных защитных элементов. Результатами проведенного исследования являются рекомендации по оптимизации выбора защитного комплекса.

Ключевые слова: защищенность полиграфического изделия от фальсификации, технологический ряд, защитный комплекс, защитный элемент.

Biziuk Andrii, *PhD, Associate Professor, Department of Media Systems and Technologies, Kharkiv National University of Radio Electronics, Ukraine, e-mail: andrii.biziuk@nure.ua, ORCID: http://orcid.org/0000-0001-9830-9206*

Tkachenko Volodymyr, *PhD, Professor, Department of Media Systems and Technologies, Kharkiv National University of Radio Electronics, Ukraine, e-mail: volodymyr.tkachenko@nure.ua, ORCID: http://orcid.org/0000-0002-5076-0724*

Vovk Aleksandr, *PhD, Associate Professor, Department of Media Systems and Technologies, Kharkiv National University of Radio Electronics, Ukraine, e-mail: oleksandr.vovk@nure.ua, ORCID: http://orcid.org/0000-0001-9072-1634*