КОРОТКІ ПОВІДОМЛЕННЯ

doi:https://doi.org/10.15407/emodel.41.02.121

UDC 004.056.53

V.M. Zvaritch, Dr. Sci. (Eng.)
Institute of Electrodynamics of the National Academy of Sciences of Ukraine
(56, Pobeda Av, Kyiv, 03680, Ukraine, tel.: 099 5017934,
e-mail: zvaritch@nas.gov.ua),
A.V. Davydiuk, Post-graduate
G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine
(15, General Naumov Str., 03164, Kiev, Ukraine,
tel. 098 0487954, e-mail: andrey19941904@gmail.com)

The Method of Color Formalization of the Level of Information Security Risk*

The method of color formalization of the level of information security risk is proposed. The main goal of this method is reflecting of the overall risk to ensure the confidentiality, integrity and availability of information in one color using the additive color RGB model. The approach to the formalized presentation of the level of information security risk consider the confidentiality, integrity, availability and observability of one color with help of four color CMYK. Auto-typing is also considered.

K e y w o r d s: information security risk, risk map, rating scale, RGB, CMYK.

This formalized presentation of information security risk assessments is carried out in the following ways: risk tree, rose (star) risk, helix risk, risk map, corridor of acceptable level of risk (corridor of tolerance of risks) [1—6]. The most obvious way to present a risk according to its quantitative assessment is a risk map [5]. The assessment of information security risks is displayed on the map as a result of multiplying the likelihood of the threat being implemented and the amount of losses. At the same time, the owner of the organization, at its own discretion, must determine the eligibility criteria. Frequently, not knowing what exactly this criterion determines, what kind of losses are acceptable for the activities of its organization, and which are already critical. Similar way to set require-

* This work was supported by the National Academy of Sciences of Ukraine under grants in the framework of RESURS-2 and «Support for the development of priority areas of scientific research (KPKVK 6541230).

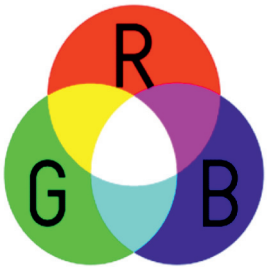

Fig. 1. Additive color model RGB

ments for the information security management system which is being designed has a number of drawbacks. Firstly, this is the discreteness of the step of risk values changes. In particular, it raises the complexity of interpreting the ranges of such changes, for example, from 12 to 20. This is due to the dependence of the choice of risk management measures and components of the information security management system from the subjective point of view of the expert, depending on the judgments of the experts, the absence of other formal requirements for the design of the indicated systems [7—10]. To solve this problem, in [11] proposed the use of continuous maps, but the question of criteria for displaying the level of risk in color was not resolved.

The basis of risk level interpretation of information security is the method of color discrepancies [12]. The method widely used in color television. The essence of this idea is to describe the risk of information security through the three properties of information: confidentiality, integrity and accessibility. Then the model of additive information security risk can be represented as follows:

$$H_c p_c + H_i p_i + H_a p_a = R, \qquad (1)$$

where $H_c p_c$ — the risk of confidentiality; $H_i p_i$ — the integrity risk; $H_a p_a$ — the accessibility risk; R — overall risk.

The interpretation of such a model is the indication of a single risk in one color. In television, the three concepts of accuracy of image reproduction are commonly used: physical accuracy (correspondence of the spectral components of the original and the image), physiological accuracy (visual non-differentiation of colors), psychological accuracy (high subjective evaluation of color reproduction quality). The concept of physical precision formulates the condition of reproduction not of color, but of the beam of radiation. Therefore, for color reproduction, a condition of physiological or colorimetric accuracy is necessary and sufficient, that is, the accuracy of reproduction of colors can be either colorimetric or psychological [13]. In order to assess color discrepancies, it is necessary that the distance in the color space between the points match two different colors corresponding to visually equal differences of these colors.

Existing methods and metrics for evaluating the quality of reproduction of color images do not fully take into account the specifics of human perception of differences in color. They are based on experimental data. Experimental data of threshold and ultra-high color differences are published in the works of Macadam [14], Brown [15], Vyshetsky [16]. The methodology for conducting these experiments was based on the technology of mixing three basic colors to

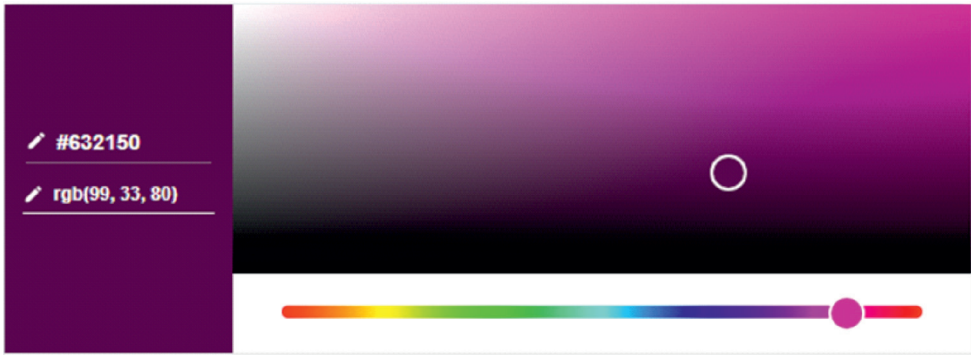

Fig. 2. Gradient

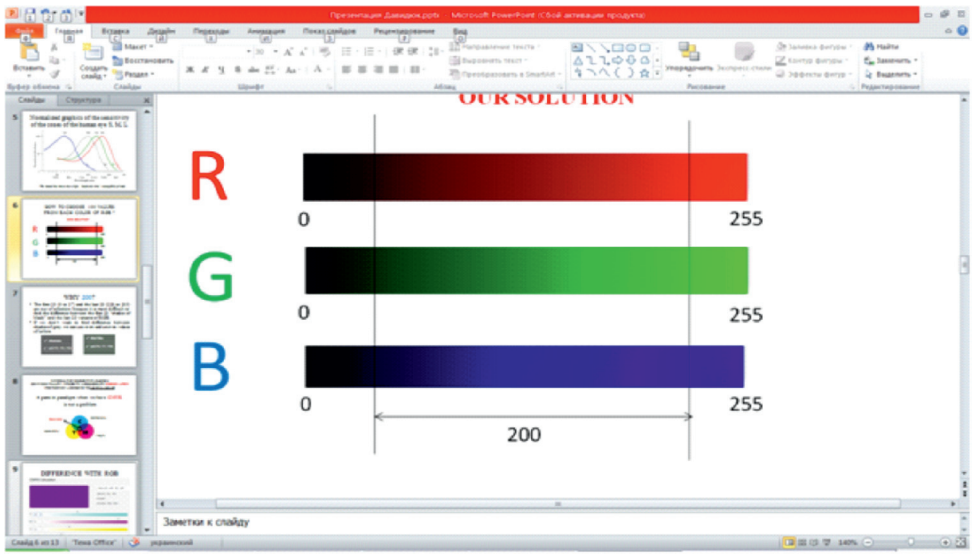

Fig. 3. Gradient boundaries

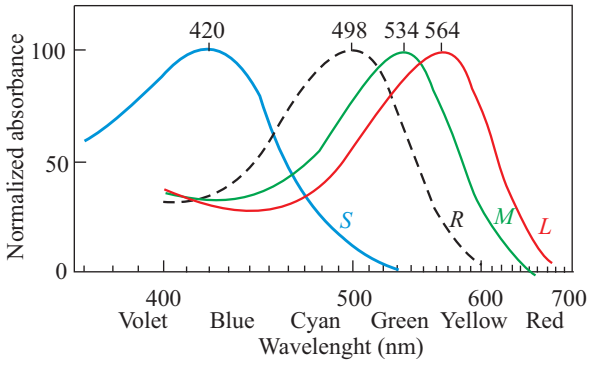

Fig. 4. Normalized graph of the sensitivity of cones of the human eye (*S*, *M*, *L*): *R* — tone perception

a *b*

Fig. 5. Gray tint with the same color values (*a*) color with two identical color values (*b*)

obtain the desired color for the comparison with a fixed color stimulus in computer technology, color transfer occurs in accordance with color representation models RGB and CMYK. The idea of using color representation RGB and CMYK models to formalize the level of information securty risk was developed with participation of prof. V.V. Mokhor. As part of the existing paradigm of information protection, which is to ensure confidentiality, integrity and availability, it is expedient to use an additive RGB model (Fig. 1). It should be noted that each of the RGB colors (red, green, blue) has 256 values (from 0 to 255), in turn, the scale of risk assessment has 100 values. Given the above, the question aris about the choice of a set of color values that will be used to indicate the level of information security risk.

In order to eliminate the uncertainties in the subsequent presentation of the material, it is expedient to determine the term gradient — an orderly set of color values (Fig. 2). To indicate the level of information security risk, we set the following limits of the gradient — from 28 to 227 (200 values) (Fig. 3).

The choice of 200 values is based on the fact that the colors at the beginning and at the end of the gradient are difficult to distinguish by human (Fig. 4), also when applying a scale of 100.

It is possble that we will observe shades of gray at the same risk values (Fig. 5, *a*). From the pool of 200 values for each color it becomes possible to avoid the above situation by alternating pair and non-even values for each color. For example: R = {28, 30, 32...226}, G = {29, 31, 32...227}, B = {28, 30, 32...226}. With this approach we get the following result (Fig. 5, *b*).

Taking into account the requirements of current legislation of Ukraine and normative documents in the field of information protection, in particular ND TPI 2.5-004-99, the paradigm of information security in our state contains four following components: confidentiality, integrity, accessibility, observation.

To determine the overall risk *R*, we use the following model:

$$H_c p_c + H_i p_i + H_a p_a + H_o p_o = R, \qquad (2)$$

where $H_o p_o$ — risk of observation.

Fig. 6. Model CMYK

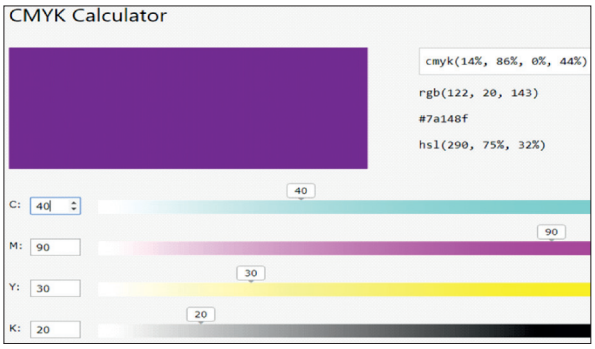

Fig. 7. Characteristics of the CMYK model

The CMYK four-color model (Fig. 6) will be useful for formalizing this model. The CMYK model has some differences from the RGB model, in terms of the number of values that describe each color (Fig. 7).

In the CMYK model, each color is described by 100 values that can be correlated with RGB colors, but it is worth noting that non-RGB colors have a conformity in CMYK.

Conclusions

The formalization of the values of risk for the information asset using color is easier to perceive from the methods described earlier in the study. It facilitates a quick, objective decision-making by the manager and helps to provide a more fully assess of the information security of organization, which makes the use of color models RGB and CMYK a promising field of research in risk management.

REFERENCES

1. International Organization for Standartization. (2013, October 01). ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements, available at: https://www.iso.org/standard/54534.html.
2. International Organization for Standartization. (2013, October 01). ISO/IEC 27002. Informationtechnology. Security techniques. Code of practice for information security controls, available at: https://www.iso.org/standard/54533.html.
3. International Organization for Standartization. (2011, June 10). ISO/IEC 27005. Informationtechnology. Security techniques. Information security risk management, available at:https://www.iso.org/standard/56742.html.
4. International Organization for Standartization. (2018, Febr. 15). ISO 31000. Risk management. Guidelines, available at: https://www.iso.org/standard/65694.html.
5. International Organization for Standartization. (2009, November 27). IEC 31010. Risk management. Risk assessment techniques, available at: https://www.iso.org/standard/51073.html.

6. Badalova, A.G. and Panteleev, A.V. (2016), Risk management of the enterprise, Vuzovskaia knika, Moscow, Russia.
7. Mokhor, V., Bakalynskyi, O. and Tsurkan, V. (2018), "Analysis of information security risk assessment representation methods", *Information Technology and Technology*, Vol. 6, no. 1, DOI: 10.20535/2411-1031.2018.6.1.153189.
8. Petrenko, S.A. and Simonov, S.V. (2004), Information risk management. Cost-effective security, DMK Press, Moscow, Russia.
9. Vishniakov, I.D. and Radaev, N.N. (2007), General risk theory, Akademiia, Moscow, Russia.
10. Astakhov, A.M. (2010), The art of information risk management, DMK Press, Moscow, Russia.
11. Mokhor, V.V., Bakalinskiy, O.O. and Tsurkan, V.V. (2018), "Presentation of information security risk assessments by a risk map", *Information Technology and Security*, pp. 94-100.
12. Mokhor, V., Zvaritch, V. and Davydiuk, A. Formalized presentation of information security risk level. Presentation in Governance for Cyber Security and Resilience in the Arctic. Advanced Research Workshop in the NATO Science Peace and Security Programme Framework, January 27-30, 2019, Rovaniemi, Finland.
13. Pevzner, B.M. (1998), *Kachestvo tsvetnykh televizionnykh zobrazheniy* [The quality of color television images], Radio i svyaz, Moscow, Russia.
14. MacAdam, D. (1943), "Visual sensitivities to color differences in daylight", *Journal of the Optical Society of America*, Vol. 32, pp. 247-274.
15. Brown, W. (1957), "Color Discrimination of twelve observers", *Journal of the Optical Society of America*, Vol. 47, pp. 137-143.
16. Wyszecki, G. and Stiles, W.S. (2000), Color Science, second edition, Wiley Classics Library Edition, USA.

Received 13.03.19

ZVARICH Valerii Mykolayovych, Doctor of sciences (engineering), leading scientific worker of the Institute of Electrodynamics of the National Academy of Sciences of Ukraine, graduated from the National Technical University of Ukraine Kiev Polytechnic Institute in 1982. Sphere of scientific research: modeling of information signals with the use of statistical approach, development of computer systems of vibrodiagnostics, cybersecurity in energy.

DAVYDIUK Andriy Viktorovych, post-graduate, G.E. Pukhov Institute for Modelling in Energy Engineering National Academy of Sciences of Ukraine, graduated from the National Technical University of Ukraine Kiev Polytechnic Institute in 2018. Sphere of scientific research: cybersecurity, risk theory and cybersecurity risk management.