INFORMATION SECURITY RISK MANAGEMENT

UDK 004.056.5

VOLODYMYR MOKHOR,
VITALII BEZSHTANKO,
SERHII HONCHAR,
HRYHORII KRAVTSOV,
IHOR KOTSIUBA,
OLHA KRUK,
OLEKSANDER MAKAREVYCH,
YEVHEN MAKSYMENKO,
VASYL TSURKAN

ANALYTICAL GEOMETRY APPROACH FOR INFORMATION SECURITY RISKS ANALYSES

The main objective of the paper is to present new approach to assessment of complex risk in the process of creation of the information security management systems and design of systems of information protection. Main idea of the presented approach is based on the interpretation of properties of the plane equation in relevant three-dimensional space of primary probabilities. It opens up fresh opportunities for simple calculation of quantitative characteristics of complex risks and indicates the way of future investigations of complex risks reflected into analytic geometry models.

Keywords: equation of plane, complex risk, primary risks of information security, probability, harm.

Introduction. The risk analysis is one of the bases stages of planning and design of information security management systems [1]. The principles and guidelines of the risk management process are described in [2]. In common the direct problem of the risk analyses is an assessment of the risk on the base of evaluated probability and losses. However in the design of systems for information protection the inverse problem must be solved i.e. intervals of variation of probability or losses must be appointed on the base of known acceptable level of the boundary complex risk R.

It is known the complex risk security assessment includes risks associated with the losses of confidentiality, integrity and availability. That is to say the complex risk security assessment R is some combination of prime risks: boundary risk of confidentiality r_C, boundary risk of integrity r_I and boundary risk of availability r_A. If risks r_C, r_I and r_A are independent one from another then the equality

$$R = r_C + r_I + r_A. \tag{1}$$

For complex risk of information security is valid.

In the following H will denote value of harm (loses) and p will denote probability appropriated. Let us suppose that risk assessment is the product of value of harm H by appropriate probability p such as:

$$r = H \cdot p\,. \tag{2}$$

So three similar formulas for prime risks r_C, r_I and r_A can be written:

$$r_C = H_C \cdot p_C\,,$$

$$r_I = H_I \cdot p_I, \quad (3)$$
$$r_A = H_A \cdot p_A,$$

Therefore the equality (1) can be rewritten with right parts of formulas (3) instead of r_C, r_I and r_A correspondingly:

$$H_C \cdot p_C + H_I \cdot p_I + H_A \cdot p_A = R. \quad (4)$$

As is known from analytic geometry [3] every equation of the first degree in the next form

$$A \cdot x + B \cdot y + C \cdot z = D. \quad (5)$$

represents the plane in three-dimensional space. Comparison of two models (4) and (5) shows their equivalence up to notation. By this reason the attempt of analysis of the complex risk of information security on the base of interpretation of properties of the appropriate plane in three-dimensional space would be undertaken.

Two alternative variants exist in this connection. The first: probabilities p_C, p_I and p_A play roles of independent variables; and appropriate harms H_C, H_I and H_A play roles of constants in relevant equation of plane. The second: harms h_C, h_I and h_A will play roles of independent variables; and appropriate probabilities p_C, p_I and p_A will play roles of constants in relevant equation of plane.

We will consider only first of these variants on the assumption of the Cartesian coordinate system. Another variant will be just the same but probabilities and harms will change places only.

So, let us assume the plane of the information risk security is represented by means of equation

$$H_C \cdot p_C + H_I \cdot p_I + H_A \cdot p_A = R, \quad (6)$$

here p_C, p_I and p_A are independent variables; and H_C, H_I and H_A are fixed factors.

In this case and first of all it must be emphasized that the plane of risks is placed in the *space of probabilities* and all consequent transformation will have relation to this space. After that it should be noted that according to theorems of analytic geometry there [3] exists some another forms of the plane equation except of formula (6). For example two such forms of equations of the plane of information risks will be considered and analyzed: a) intercepts equation and b) normal equation.

Information security risks appointment on the base of analyses of Intercepts equation

Let the equation (6) represent the plane of information risks. Left and right parts of that equation must be divided on the value of boundary complex risk R:

$$\frac{H_C}{R} \cdot p_C + \frac{H_I}{R} \cdot p_I + \frac{H_A}{R} \cdot p_A = 1.$$

Now this formula must be rewritten in such form:

$$\frac{p_C}{\left(\frac{R}{H_C}\right)} + \frac{p_I}{\left(\frac{R}{H_I}\right)} + \frac{p_A}{\left(\frac{R}{H_A}\right)} = 1. \quad (7)$$

So the plane of information risks that is represented by equation (7) will intercept interval R/H_C on the axis p_C, interval R/H_I on the axis p_I and interval R/H_A on the axis p_A. It is clear that values of probabilities must lie into interval 0 to 1. Therefore lengths of intervals intercepted on the each of the axis must not be more 1. In other words the system of such inequalities must be executable:

$$\frac{R}{H_C} \le 1;$$
$$\frac{R}{H_I} \le 1;$$
$$\frac{R}{H_A} \le 1.$$

On the base of this system we can write system of next conditions

$$\begin{aligned} R &\le H_C; \\ R &\le H_I; \\ R &\le H_A. \end{aligned} \tag{8}$$

that gives relations between complex risk of information security and evaluations of primary harms for confidentiality, integrity and availability.

Now let us select minimum from H_C, H_I and H_A:

$$H_{\min} = \min\{H_C, H_I, H_A\}.$$

After that the system of conditions (8) can be replaced to once equality:

$$R = H_{\min}. \tag{9}$$

It means that value of the complex risk of information security can be appointed as a minimum on set of harms acceptable for confidentiality, integrity and availability.

Information security risks appointment on the base of analyses of Normal equation

Let the equation (6) represent the plane of information risks. Let us multiply left and right parts of this equation (6) on the normalizing factor M:

$$M = \frac{1}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}. \tag{10}$$

So we obtain the equation (6) as next form:

$$M \cdot H_C \cdot p_C + M \cdot H_I \cdot p_I + M \cdot H_A \cdot p_A = M \cdot R \tag{11}$$

If the right part of the normalizing factor (10) insert to the formula (11) instead of symbol M such result will be obtained:

$$\frac{H_C}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|} \cdot p_C + \frac{H_I}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|} \cdot p_I + \frac{H_A}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|} \cdot p_A = \frac{R}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}. \tag{12}$$

It is known from the course of analytic geometry [1] that the term in the right part of the formula (12) is the minimum distance from the origin of coordinates to the plane that is defined by the appropriate normal equation. In future this term will be denoted with special label ρ and we can write:

$$\rho = \frac{R}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}. \tag{13}$$

Additionally it is known [1] that constants in left part of formula (12) are directional cosines of the normal of the plane that is defined by the appropriate normal equation. And formulas of those cosines are next:

$$\begin{aligned} \cos\alpha &= \frac{H_C}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}, \\ \cos\beta &= \frac{H_I}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}, \\ \cos\gamma &= \frac{H_A}{\left|\sqrt{H_C^2 + H_I^2 + H_A^2}\right|}. \end{aligned} \tag{14}$$

Thus the normal ρ can be considered as a diagonal of the rectangular parallelepiped; sides of this parallelepiped are projections of this normal ρ on axis p_C, p_I and p_A accordingly:

$$\rho\cos\alpha = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|}\frac{H_C}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|} = \frac{RH_C}{H_C^2+H_I^2+H_A^2};$$
$$\rho\cos\beta = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|}\frac{H_I}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|} = \frac{RH_I}{H_C^2+H_I^2+H_A^2}; \quad (15)$$
$$\rho\cos\gamma = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|}\frac{H_A}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|} = \frac{RH_A}{H_C^2+H_I^2+H_A^2}.$$

By this reason the next formulas can be written for calculation of evaluation of minimum probabilities p_C, p_I and p_A, are possible for the prescribed value of boundary risk of information security R under assumption that are known evaluations of acceptable harms of confidentiality H_C, integrity H_I and availability H_A:

$$p_C = \frac{RH_C}{H_C^2+H_I^2+H_A^2};$$
$$p_I = \frac{RH_I}{H_C^2+H_I^2+H_A^2}; \quad (16)$$
$$p_A = \frac{RH_A}{H_C^2+H_I^2+H_A^2}.$$

These formulas provide an opportunity to estimate probabilities p_C, p_I and p_A that are possible together for the given boundary of risk assessments R under allowable harms of confidentiality H_C, integrity H_I and availability H_A.

So as the normal ρ is the diagonal of the rectangular parallelepiped and three sides of that parallelepiped are probabilities p_C, p_I and p_A of harms of confidentiality, integrity and availability correspondently we can write formulas for complex probability:

$$p = \left|\sqrt{p_C^2+p_I^2+p_A^2}\right|. \quad (17)$$

Probabilities p_C, p_I and p_A in this formula can be changed by right parts of relations (16) correspondently. In result we will obtain:

$$p = \sqrt{\left(\frac{RH_C}{H_C^2+H_I^2+H_A^2}\right)^2+\left(\frac{RH_I}{H_C^2+H_I^2+H_A^2}\right)^2+\left(\frac{RH_A}{H_C^2+H_I^2+H_A^2}\right)^2}. \quad (18)$$

In the right part of this formula (18) we can perform next transformations:

$$\sqrt{\left(\frac{RH_C}{H_C^2+H_I^2+H_A^2}\right)^2+\left(\frac{RH_I}{H_C^2+H_I^2+H_A^2}\right)^2+\left(\frac{RH_A}{H_C^2+H_I^2+H_A^2}\right)^2} =$$
$$= \frac{R}{H_C^2+H_I^2+H_A^2}\sqrt{H_C^2+H_I^2+H_A^2} = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|}.$$

Therefore next formula can be written for complex probability in the result:

$$p = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|}. \quad (19)$$

Just us $p \le 1$ so

$$p = \frac{R}{\left|\sqrt{H_C^2+H_I^2+H_A^2}\right|} \le 1, \quad (20)$$

and it follows that

$$R \le \left| \sqrt{H_C^2 + H_I^2 + H_A^2} \right|. \quad (21)$$

This inequality gives upper-bound estimation for acceptable complex risk of information security.

Let's take minimum harm value

$$H_{\min} = \min\{H_C, H_I, H_A\}.$$

On the base of practical considerations and according of formula (9) we should not to accept the risk estimation less the minimum permissible harm. Therefore the one-sided in equation (21) could be brought up to the two-sided in equation:

$$\min\{H_C, H_I, H_A\} \le R \le \left| \sqrt{H_C^2 + H_I^2 + H_A^2} \right|. \quad (22)$$

Let us assume

$$H_{\min} = H_C = H_I = H_A,$$

and then the two-sided in equation (22) could be rewritten as follow:

$$H_{\min} \le R \le \sqrt{3} \cdot H_{\min}, \quad (23)$$

Divided all parts of this in equation by $H_{\min}$ we are obtaining ratio

$$1 \le \left(\frac{R}{H_{\min}} \right) \le \left| \sqrt{3} \right|, \quad (24)$$

following conclusion than relation of complex risk of information security to minimum acceptable hart should be from 1 to $\left|\sqrt{3}\right|$.

Relations (22)-(24) provide a way in order to obtain the quantity express-estimation of the interval of variations of the complex risk value of information security on the base of sufficiently general perception about primary harms of vulnerabilities of confidentiality, integrity and availability.

Conclusion. Interpretation of analytical representation of complex information security risks in the form of a plane in the corresponding three-dimensional space allows to obtain quantitative estimates of acceptable values of probability of acceptable risks needed to justify decisions taken in the creation of information security management systems and building information security tools.

The further research in the tideway of outlined analytic-geometry approach can be directed towards the development of understanding of analogies between complex risk and other types of equations of the plane in three-dimension space, the migration to multidimensional spaces and the passing from plane to nonlinear surfaces.

REFERENCES

1. International Organization for Standardization (2013), ISO/IEC 27001:2013, *Information technology. Security techniques. Information security management. Requirements*, Geneva, 23 p.

2. International Organization for Standardization (2009), ISO 31000:2009, *Risk management. Principles and guidelines*, Geneva, 24 p.

3. *Siceloff, L., Wentworth, G., Smith, D. (1922), Analytic geometry (Wentworth-Smith Mathematical series)*, Ginn and Company, New York, 296 p.

The article was received 10.03.2015.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Information technology. Security techniques. Information security management. Requirements : ISO/IEC 27001:2013. – [Published on 2013-10-01]. – Geneva, 2013. – 23 p.

2. Risk management. Principles and guidelines : ISO 31000:2009. – [Published on 2013-11-15]. – Geneva, 2009. – 24 p.

3. Siceloff L. Analytic geometry (Wentworth-Smith Mathematical series) / L. Siceloff, G. Wentworth, D. Smith. – New York : Ginn and Company, 1922. – 296 p.

ВОЛОДИМИР МОХОР,
ВІТАЛІЙ БЕЗШТАНЬКО,
СЕРГІЙ ГОНЧАР,
ГРИГОРІЙ КРАВЦОВ,
ІГОР КОЦЮБА,
ОЛЬГА КРУК,
ОЛЕКСАНДЕР МАКАРЕВИЧ,
ЄВГЕН МАКСИМЕНКО,
ВАСИЛЬ ЦУРКАН

АНАЛІТИКО-ГЕОМЕТРИЧНИЙ ПІДХІД ДО АНАЛІЗУВАННЯ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

Основною метою роботи є представлення нового підходу до оцінювання складного ризику в процесі створення систем управління безпекою інформації та проектування систем захисту інформації. Основна ідея представленого підходу полягає в інтерпретації властивостей рівняння площині у відповідному тривимірному просторі простих імовірностей. Це дозволило спростити обчислення кількісних характеристик складних ризиків і визначити напрямок їх подальших досліджень за допомогою аналітико-геометричних моделей.

Ключові слова: рівняння площини, складний ризик, прості ризики безпеки інформації, ймовірність, втрати.

ВЛАДИМИР МОХОР,
ВИТАЛИЙ БЕЗШТАНЬКО,
СЕРГЕЙ ГОНЧАР,
ГРИГОРИЙ КРАВЦОВ,
ИГОРЬ КОЦЮБА,
ОЛЬГА КРУК,
АЛЕКСАНДЕР МАКАРЕВИЧ,
ЕВГЕН МАКСИМЕНКО,
ВАСИЛИЙ ЦУРКАН

АНАЛИТИКО-ГЕОМЕТРИЧЕСКИЙ ПОДХОД К АНАЛИЗУ РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основной целью работы является представление нового подхода к оценке сложного риска в процессе создания систем управления безопасностью информации и проектирования систем защиты информации. Основная идея представленного подхода состоит в интерпретации свойств уравнения площади в соответствующем трехмерном пространстве простых вероятностей. Это позволило упростить вычисление количественных характеристик сложных рисков и определить направление дальнейших исследований с помощью аналитико-геометрических моделей.

Ключові слова: уравнение площади, сложный риск, простые риски безопасности информации, вероятность, потери.

Volodymyr Mokhor, doctor of technical sciences, professor, head of department, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.
E-mail: v.mokhor@gmail.com.

Vitalii Bezshtanko, head of laboratory, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.
E-mail: v.bezshtanko@gmail.com.

Serhii Honchar, candidate of technical sciences, doctoral student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
E-mail: sfgonchar@gmail.com.

Hryhorii Kravtsov, candidate of technical sciences, doctoral student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
E-mail: java_dev@i.ua.

Ihor Kotsiuba, postgraduate student, Pukhov Institute for modeling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine.
E-mail: i.kotsiuba@gmail.com.

Olha Kruk, junior researcher, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
E-mail: onk@conferen.ru.

Oleksander Makarevych, postgraduate student, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.
E-mail: amakarevich20@gmail.com.

Yevhen Maksymenko, deputy head of department, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.
E-mail: iszzi@i.ua.

Vasyl Tsurkan, candidate of technical sciences, leading researcher, Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute», Kyiv, Ukraine.
E-mail: v.v.tsurkan@gmail.com.

Володимир Володимирович Мохор, доктор технічних наук, професор, завідувач кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Віталій Михайлович Безштанько, начальник лабораторії, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Сергій Феодосійович Гончар, кандидат технічних наук, докторант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Григорій Олексійович Кравцов, кандидат технічних наук, докторант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Ігор Васильович Коцюба, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Ольга Миколаївна Крук, молодший науковий співробітник, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Олександр Євгенович Макаревич, аспірант, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Євген Васильович Максименко, заступник завідувача кафедри, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Василь Васильович Цуркан, кандидат технічних наук, провідний науковий співробітник, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут», Київ, Україна.

Владимир Владимирович Мохор, доктор технических наук, профессор, заведующий кафедрой, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Виталий Михайлович Безштанько, начальник лаборатории, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Сергей Феодосиевич Гончар, кандидат технических наук, докторант, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Григорий Алексеевич Кравцов, кандидат технических наук, докторант, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Игорь Васильевич Коцюба, аспирант, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Ольга Николаевна Крук, младший научный сотрудник, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Александр Евгеньевич Макаревич, аспирант, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Евгений Васильевич Максименко, заместитель заведующего кафедрой, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, ведущий научный сотрудник, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт», Киев, Украина.