INFORMATION SECURITY RISK MANAGEMENT

УДК 004.056.53

ВОЛОДИМИР МОХОР,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ОЛЕКСАНДР БОГДАНОВ,
ВАСИЛЬ ЦУРКАН

АНАЛІЗУВАННЯ ПРИЙНЯТНОСТІ СКЛАДНИХ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ МЕТОДАМИ АНАЛІТИЧНОЇ ГЕОМЕТРІЇ

Викладається підхід до аналізування прийнятності рівнів ризиків безпеки інформаційного активу при заданому їх граничному значенні. Для цього використовується математичний апарат аналітичної геометрії та припущення щодо аналогії між адитивною моделлю складного ризику з рівнянням прямої. Вона відображається у просторі та нею визначаються граничні, заздалегідь задані рівні ризиків. Розглядаються різні варіанти перетину ”граничної прямої” з іншими прямими. Виокремлюються форми представлення прямої, в тому числі рівняння прямої з кутовим коефіцієнтом. У залежності від взаємного розташування ”граничної” та інших прямих, з’являється можливість сформувати підходи до класифікування рекомендацій посадовим особам, які проектують комплексну систему захисту інформації та/або систему управління інформаційною безпекою. Це дозволяє спростити обчислення кількісних характеристик складних ризиків і відкриває можливості визначення напрямку подальших досліджень за допомогою аналітико-геометричних моделей.

Ключові слова: ризик інформаційної безпеки, ймовірність реалізації загрози, система управління інформаційною безпекою, комплексна система захисту інформації, рівняння прямої.

Постановка проблеми. Статтею 17 Конституції України визначається, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави, справою всього українського народу [1]. Ця норма знайшла свій подальший розвиток у ряді законів України, постанов Верховної ради, Кабінету Міністрів України та інших підзаконних актах органів, на які покладено повноваження забезпечення інформаційної безпеки держави. Одним з найважливіших аспектів цієї діяльності є захист інформації і тому, відповідно до Закону України “Про захист інформації в інформаційно-телекомунікаційних системах”, визначається, що інформація, яка є власністю держави або інформація з обмеженим доступом, вимоги до захисту якої визначені законом, повинна оброблятися з використанням комплексної системи захисту інформації (КСЗІ) [2] та/або системи управління інформаційною безпекою (СУІБ). Побудова означених систем регламентується, наприклад, такими нормативними документами як НД ТЗІ 1.1-002-99, НД ТЗІ 3.7-003-05, НД ТЗІ 2.6-001-11 та ДСТУ ISO/IEC 27001:2010. У них визначається, що при побудові КСЗІ та/або СУІБ необхідно визначати критерії прийнятності рівнів ризиків та встановити їх граничні значення. Це завдання покладено на власника або розпорядника інформаційного активу. Визначення граничних значень рівнів ризиків дозволяє провести межу між прийнятними та неприйнятними ризиками. Наявність такої межі дає можливість власнику або розпоряднику інформаційного активу, прийняти обґрунтоване рішення щодо необхідності обробляння ризиків, залучення необхідних для цього ресурсів, спираючись на математичне обґрунтування, а не на власне бажання. Такий підхід дозволяє суттєво знизити ризики корупційних проявів при прийнятті управлінських рішень.

Крім того, ст. 42 Кримінального кодексу України визначається, що виправданий ризик є обставиною, яка виключає злочинність діяння [3]. Безумовно, будь-якому керівнику, при прийнятті рішення, цікаво, а де ж знаходиться та межа, яка відокремлює його від негативних наслідків?

Нині існує багато визначень ризику, але найбільш прийнятним є визначення за міжнародним стандартом ISO/IEC 31000:2009, а саме: “Ризик – це вплив невизначеності на досягнення мети”. Що ж стосується ризиків інформаційної безпеки, то міжнародним стандартом ISO/IEC 27005:2011 “Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки” визначається ризик інформаційної безпеки як потенціальна можливість використання вразливості активу або групи активів конкретною загрозою для нанесення збитку організації. Ще одним документом ISO/Guide 73: 2009 ”Управління ризиками. Словник” дається визначення ризику, як поєднання наслідків події (включаючи зміни в обставинах) і пов’язаної з нею імовірності її виникнення [4-6].

Виклад основного матеріалу дослідження. У зв’язку з необхідністю проведення обчислень рівнів ризиків, за загальним правилом використовується бінарна модель, яка оперує двома складовими – рівнем нанесених втрат організації у випадку реалізації загрози та ймовірністю настання такої події:

$$R = S \cdot p \tag{1}$$

де R – рівень ризику,

S – величина нанесених втрат,

p – імовірність реалізації загрози.

До того ж, повинні виконуватись умови R, $S \geq 0$, $0 \leq p \leq 1$.

Зазвичай, визначення імовірності є складною задачею та вимагає, як правило, великого обсягу статистичних даних. Проте власники або розпорядники активів здебільшого приховують статистику з метою мінімізації іміджевих ризиків. Крім статистичних методів можуть використовуватись й інші, наприклад [7]: імовірнісно-статистичні, теоретико-ймовірнісні, евристично-аналітичні. Однак, для цих методів теж характерні обмеження, що пов’язані з коректністю застосування статистичних даних про реалізації загроз. До того ж характерними обмеженнями є відсутність стаціонарності спостережень за реалізаціями загроз, складність формування експертних груп (особливо в організаціях з невеликою кількістю персоналу). В кінцевому випадку отримання імовірнісних характеристик граничних ризиків здійснюється за недостатності статистичних даних про реалізації загроз безпеці інформаційних активів, зокрема, – державних інформаційних ресурсів.

Отже, виникає необхідність формування підходу до визначення прийнятних рівнів ризиків інформаційної безпеки при заданих граничних значеннях для прийняття обґрунтованого рішення щодо необхідності обробляння ризиків у комплексній системі захисту інформації та/або системі управління інформаційною безпекою.

Здебільшого на безпеку інформаційного активу впливає декілька загроз. Більш того, вони можуть бути спрямовані на різні його властивості, наприклад, конфіденційність, цілісність, доступність або спостережність. Тобто ризик є складним.

У випадку існування двох загроз безпеці інформаційного активу, (не принципово до якої властивості), визначимо, що:

$$R = R_1 + R_2, \tag{2}$$

де R_1 – ризик реалізації першої загрози, який представляється добутком:

$$R_1 = S_1 \cdot p_1, \tag{3}$$

R_2 – ризик реалізації другої загрози:

$$R_2 = S_2 \cdot p_2, \tag{4}$$

Шляхом підстановки (3) та (4) в (2) отримаємо наступне співвідношення:

$$R = S_1 \cdot p_1 + S_2 \cdot p_2, \tag{5}$$

в якому $0 \leq p_1 \leq 1$ та $0 \leq p_2 \leq 1$.

Якщо ми перенесемо R у праву частину, то отримаємо:

$$S_1 \cdot p_1 + S_2 \cdot p_2 - R = 0. \tag{6}$$

Порівнюючи це співвідношення з загальним рівнянням прямої на площині:

$$Ax + By + C = 0,$$

можемо констатувати їх збіг з точністю до позначень. Тоді співвідношення (6) можна проінтерпретувати як загальне рівняння прямої з негативним вільним членом R [8]. Як наслідок, пряма зображується в межах координат з осями, що визначають імовірності p_1 та p_2 реалізації першої та другої загрози відповідно. Тоді як точки перетину прямої (6) з осями можна визначити за допомогою рівняння прямої в відрізках на осях:

$$\frac{S_1 \cdot p_1}{R} + \frac{S_2 \cdot p_2}{R} = 1 \Rightarrow \frac{p_1}{\frac{R}{S_1}} + \frac{p_2}{\frac{R}{S_2}} = 1 \Rightarrow p_1 = M_1\left(\frac{R}{S_1}; 0\right),\ p_2 = M_2\left(0; \frac{R}{S_2}\right), \quad (7)$$

де M_1 та M_2 – точки перетину осей $0p_1$ та $0p_2$ відповідно. За умови (5) є крайніми, що нас задовольняють $p_1 = M_1(1;0)$ та $p_2 = M_2(0;1)$ (див. рис. 1). Таким чином, пряма M_1M_2 характеризує гранично можливий (або прийнятний) рівень ризику безпеці інформаційному активу у випадку реалізації двох загроз.

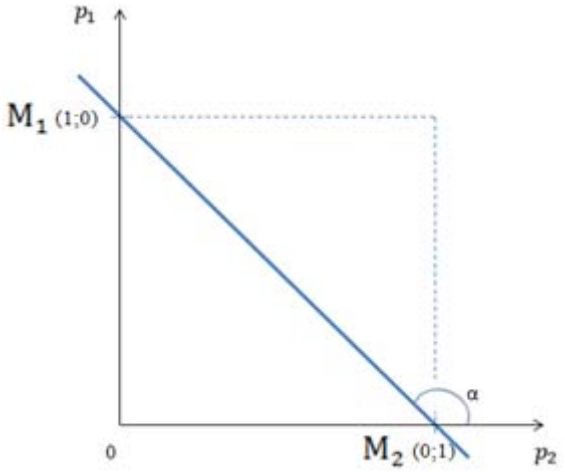

Рисунок 1 – Межа прийнятності рівня ризику інформаційної безпеки

Це означає, що результати будь-яких комбінацій $S_1 \cdot p_1$ та $S_2 \cdot p_2$, або їх сума повинні знаходитись на прямій M_1, M_2 або нижче, зважаючи на те, що $R = const$, тобто, рівень прийнятного ризику чітко задано власником або ропорядником активу.

Ідея представлення ризиків інформаційної безпеки у вигляді рівняння прямої у *n*-мірному просторі ймовірностей відома з [8]. Проте, просторовий підхід не дає можливості проаналізувати та з'ясувати особливості взаємного розташування множини точок гранично прийнятних ризиків та множини точок, які задовольняють рівнянню (5). Внаслідок цього, до множини прийнятних значень необґрунтовано можуть бути включені підмножини принципово не прийнятних рішень.

Якщо ж представлення ризиків у графічному вигляді відобразити рівнянням прямої з кутовим коефіцієнтом (див. рис. 2), то подальша аналогія стає ще більш очевидною [8]

$$y = kx + b, \quad (8)$$

де коефіцієнт $k = tg\alpha$ визначає ступінь нахилу прямої до осі $0p_1$.

Шляхом перетворення (8) отримаємо

$$p_2 = \frac{S_1}{S_2} \cdot p_1 - \frac{R}{S_2}. \quad (9)$$

Тоді як порівнюючи (8) та (9), можна стверджувати про їх співпадання до позначень

$$k = \frac{S_1}{S_2} = tg\alpha, \quad b = \frac{R}{S_2}.$$

Пряма, що проходить через точки з координатами *(1;0)* та *(0;1)* називається "граничною прямою". Вона визначається рівнянням $y = -x + 1$. З огляду на це множина прийнятних імовірностей обмежується трикутником, вершини якого мають координати *(1;0), (0;0)*, *(0;1)*.

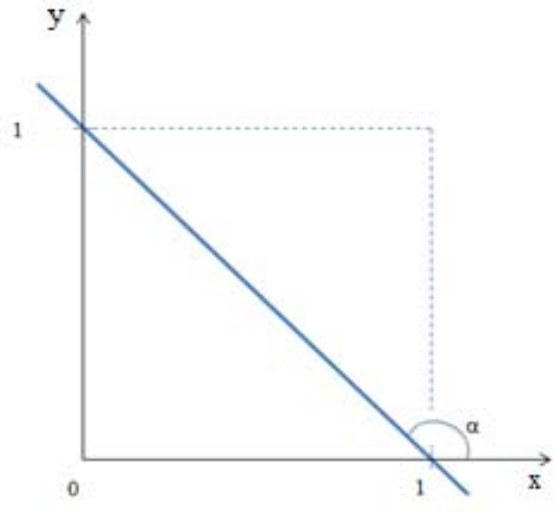

Рисунок 2 – Графік рівняння прямої з кутовим коефіцієнтом

Таким чином, прямі, якими відображається сукупність прийнятних ризиків, повинні знаходитись під ”граничною прямою” (коефіцієнт $k < 0$). Тобто максимально допустимою є ситуація, коли ці прямі знаходяться під прямою M_1M_2 та мають кут $\alpha = 135^o$ (інакше кажучи, паралельні M_1M_2).

Водночас доцільно зазначити, що в інших випадках прямі матимуть точки перетину з прямою M_1M_2 або з осями координат $0p_1\,0p_2$. Кожен з цих випадків розглядається окремо. Приклад графічного відображення множини варіантів перетину прямої M_1M_2 та осей координат $0p_1\,0p_2$ показано на рис. 3.

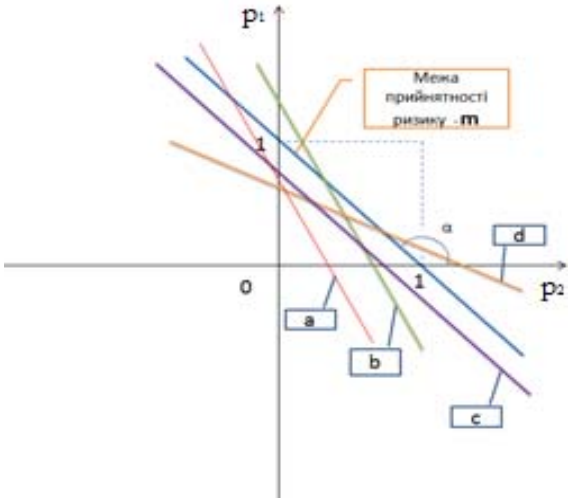

Рисунок 3 – Варіанти перетинів “граничної прямої” та осей координат $0p_1\,0p_2$

Розглянемо кожен з варіантів (див. рис. 3) детально. Зокрема, для них характерні загальні ознаки, що, з точки зору ризик-менеджменту, можуть сприяти формуванню загальних рекомендацій дій менеджера або посадової особи при плануванні або розроблянні КСЗІ та/або СУІБ.

На рис. 4-7 зображені варіанти перетину прямих, які мають різні ознаки порівняно з “граничною прямою”, а саме:

”1” – точку перетину двох прямих;

”2” – точку перетину прямої з віссю $0p_1$;

”3” – точку перетину прямої з віссю $0p_2$;

”4” – точку перетину межі ”одиничного квадрату”.

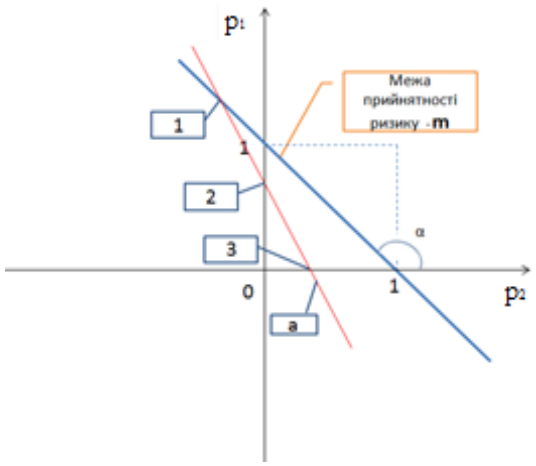

Рисунок 4 – Варіант 1

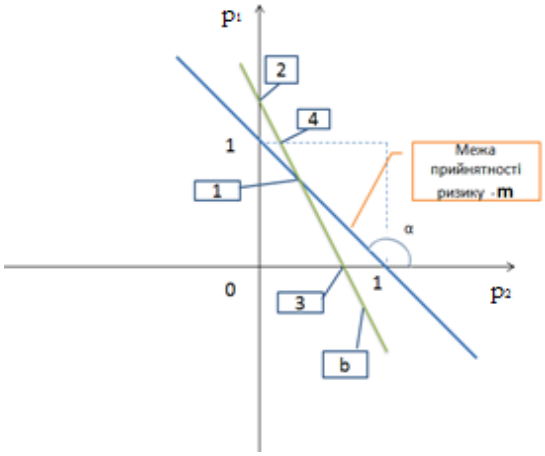

Рисунок 5 – Варіант 2

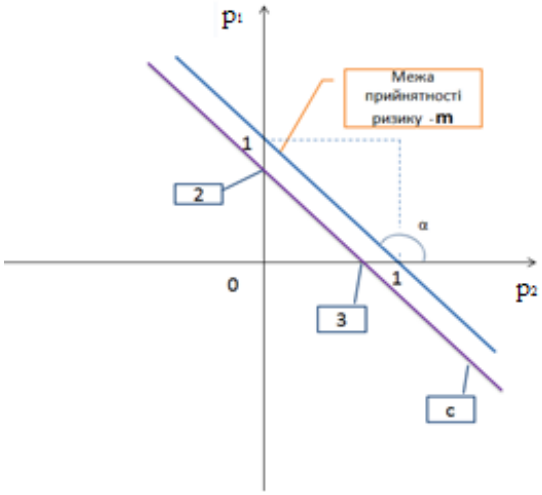

Рисунок 6 – Варіант 3

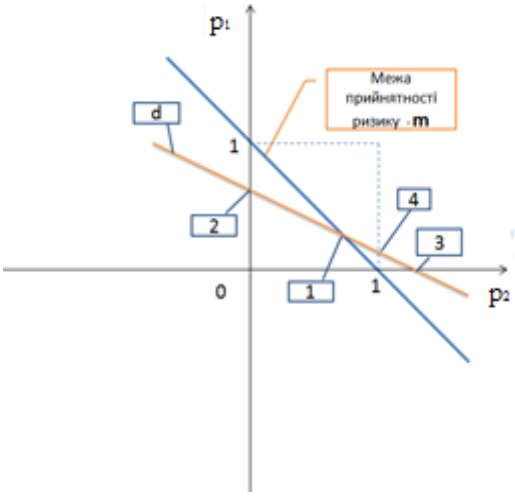

Рисунок 7 – Варіант 4

За результатами аналізування рис. 4-7 можна згрупувати варіанти ”поведінки” прямих у наступні групи:

1. Пряма у першому квадранті знаходиться у заданих межах, нижче “граничної прямої”, хоча в інших квадрантах вона має точку перетину (див., наприклад, рис. 4). Проте у всіх інших квадрантах значення імовірності від’ємне, що не коректно з точки зору її визначення. У цьому випадку ризик-менеджеру доцільно прийняти рішення про відповідність вірогідних ризиків умовам їх прийнятності.

2. ”Гранична” та прямі, що досліджуються, мають точку перетину 1. Вона розглядається як граничний варіант прийнятного рівня ризику (див., наприклад, рис. 5 і 7). Водночас пряма знаходиться в межах одиничного квадрату до точки 4, імовірності реалізації загроз у допустимих межах, але втрати сумарно вже неприйнятні. Тому доцільно приймати управлінські рішення щодо обробляння ризиків. Тоді як за точками 4, 2 (див., наприклад, рис. 2), або 3 (див., наприклад, рис. 7) спостерігається невідповідність імовірності вимогам $0 \le p_1 \le 1$ та $0 \le p_2 \le 1$. Тому ризик-менеджеру доцільно приймати рішення щодо змінювання співвідношення імовірних втрат. Відмінність між цими двома варіантами полягає у значені кута нахилу α.

3. Дві прямі не мають точок перетину та пряма, яку ми досліджуємо, знаходиться нижче заданого максимально прийнятного рівня ризику (див., наприклад, рис. 6). Тобто ця інформація корисна для проектувальника при дослідженні різних варіантів та комбінацій рішень щодо засобів і заходів забезпечення безпеки інформаційних активів. Цей варіант задовольняє ризик-менеджера та є для нього прийнятним.

Висновки. Показано аналогію рівняння прямої з адитивною моделлю обчислення складних ризиків реалізації загроз безпеці інформативного активу при заданому сумарному,

кінцевому рівні ризику. Визначено умови використання рівняння прямої для оцінювання ризиків при двох загрозах та можливі варіанти дій ризик-менеджера та посадових осіб при плануванні та розроблянні КСЗІ (та/або СУІБ).

Перспективи подальших досліджень пов'язані з використанням запропонованого підходу в *n*-мірному просторі ризиків.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Верховна рада України. 5 сесія. (1996, Черв. 26). *Конституція України*. [Електронний ресурс]. Доступно: http://zakon5.rada.gov.ua/laws/ show/254%D0%BA/96%D0%B2%D1% 80. Дата звернення: Листоп. 19, 2015.

[2] Верховна рада України. 1 сесія. (1994, Лип. 05). Закон України "Про захист інформації в інформаційно-телекомунікаційних системах". [Електронний ресурс]. Доступно: http://zakon5.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80. Дата звернення: Листоп. 19, 2015.

[3] Верховна рада України. 7 сесія. (2001, Квіт. 5). *Кримінальний кодекс України*. [Електронний ресурс]. Доступно: http://zakon5.rada.gov.ua/laws/show/2341-14. Дата звернення: Листоп. 19, 2015.

[4] International Organization for Standardization. 2009. *ISO/IEC 31000, Risk management. Principles and guidelines.* [Online]. Available: http://www.iso.org/iso/iso31000. Accessed on: Nov. 19, 2015.

[5] International Organization for Standardization. 2011. *ISO/IEC 27005, Information technology. Security techniques. Information security risk management*. [Online]. Available: http://www.iso.org/iso/iso27005. Accessed on: Nov. 19, 2015.

[6] International Organization for Standardization. 2009. *ISO Guide 73, Risk management. Vocabulary.* [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en. Accessed on: Nov. 19, 2015.

[7] В.С. Зарубин, А.Н. Канатников, и А.П. Крищенко, *Аналитическая геометрия.* Москва, Россия: МГТУ им. Н.Э. Баумана, 2000.

[8] V. Mokhor et al., "Analytical geometry approach for information security risks analyses", *Information Technology and Security*, vol. 3. iss. 1 (4), pp. 60-67, January-June 2015.

Стаття надійшла до редакції 26 грудня 2015 року.

REFERENCE

[1] Verkhovna Rada of Ukraine. 5th Session. (1996, June 26). *Constitution of Ukraine.* [Online]. Available: http://zakon5.rada.gov.ua/laws/show/254% D0%BA/96-%D0%B2%D1%80. Accessed on: Nov. 19, 2015.

[2] Verkhovna Rada of Ukraine. 1st Session. (1994, July. 05). *Law of Ukraine "About information protection in telecommunication".* [Online]. Available: http://zakon5.rada.gov.ua/laws/show/ 80/94-%D0%B2%D1%80. Accessed on: Nov. 19, 2015.

[3] Verkhovna Rada of Ukraine. 7th Session. (2001, Apr. 5). *Criminal codex of Ukraine*. [Online]. Available: http://zakon5.rada.gov.ua/laws/show/2341-14. Accessed on: Nov. 19, 2015.

[4] International Organization for Standardization. 2009. *ISO/IEC 31000, Risk management. Principles and guidelines.* [Online]. Available: http://www.iso.org/iso/iso31000. Accessed on: Nov. 19, 2015.

[5] International Organization for Standardization. 2011. *ISO/IEC 27005, Information technology. Security techniques. Information security risk management*. [Online]. Available: http://www.iso.org/iso/iso27005. Accessed on: Nov. 19, 2015.

[6] International Organization for Standardization. 2009. *ISO Guide 73, Risk management. Vocabulary.* [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en. Accessed on: Nov. 19, 2015.

[7] V.S. Zarubin, A.N. Kanatnikov, and A.P. Krishchenko, *Analytical geometry*. Moskow, Russia: Bauman MSTU, 2000.
[8] V. Mokhor et al., "Analytical geometry approach for information security risks analyses", *Information Technology and Security*, vol. 3. iss. 1 (4), pp. 60-67, January-June 2015.

ВЛАДИМИР МОХОР,
АЛЕКСАНДР БАКАЛИНСКИЙ,
АЛЕКСАНДР БОГДАНОВ,
ВАСИЛИЙ ЦУРКАН

АНАЛИЗ ПРИЕМЛЕМОСТИ СЛОЖНЫХ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДАМИ АНАЛИТИЧЕСКОЙ ГЕОМЕТРИИ

Излагается подход к анализу приемлемости уровней рисков безопасности информационного актива при заданном их граничном значении. Для этого используется математический аппарат аналитической геометрии и допущение относительно аналогии между аддитивной моделью сложного риска с уравнением прямой. Она отображается в пространстве и ею определяются граничные, заблаговременно заданные уровни рисков. Рассматриваются различные варианты пересечения "граничной прямой" с другими прямыми. Выделяются формы представления прямой, в том числе уравнения прямой с угловым коэффициентом. В зависимости от взаимного размещения "граничной" и других прямых, появляется возможность формирования подходов к классификации рекомендаций должностным лицам, которые проектируют комплексную систему защиты информации и/или систему управления информационной безопасностью. Это позволяет упростить вычисления количественных характеристик сложных рисков и открывает возможность определения дальнейшего направления исследований с помощью аналитико-геометрический моделей.

Ключевые слова: риск информационной безопасности, вероятность реализации угрозы, система управления информационной безопасностью, комплексная система защиты информации, уравнение прямой.

VOLODYMYR MOKHOR,
OLEKSANDR BAKALYNSKYI,
OLEKSANDR BOHDANOV,
VASYL TSURKAN

ANALYZING OF ELIGIBILITY OF COMPLEX RISKS OF INFORMATION SECURITY BY ANALYTICAL GEOMETRY METHODS

Requirement for the protection state information resources is determined by the law Ukraine. Complex systems of information protection or information security management system is rooted for this. It is necessary to determine eligibility of criteria risk levels and set their limit values during development of such systems. This task is assigned to the owner or manager of information asset. Determination of limit values of risk levels allows to draw the line between acceptable and unacceptable risk. Presence of such limits provides an opportunity to make informed decisions about necessary risks processing and attracting the necessary resources. Therefore, the main purpose is presenting the approach to analyzing the levels acceptability of complex information security risks using mathematical tools of analytical geometry and assumptions concerning the analogy between the additive model of complex risk with equation of line. This line is reflected in the area and defines the boundary, predefined risk levels. The analogy equation of the line with the equation of finding two risk values of threats to security informative asset for a given level of total risk shows as an example. The location of "boundary line" is defined and proven, also considered various options for its intersection with other direct. Depending on their relative position became possible the formation of approaches to the definition and classification of officials recommendations who are developing a complex information protection system or the system of information security management. It is allowed to simplify and justify determination of quantitative characteristics of complex risks and contributed to the formulation of further research in *n*-dimensional area by using the analytical and geometric models.

Keywords: information security risk, probability of threats, information security management system, complex information protection system, analytic geometry, line equation.

Володимир Володимирович Мохор, доктор технічних наук, професор, директор, Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

E-mail: v.mokhor@gmail.com.

Олександр Олегович Бакалинський, заступник завідувача кафедри управління та тактико-спеціальної підготовки, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

E-mail: baov@meta.ua.

Олександр Михайлович Богданов, доктор технічних наук, професор, завідувач кафедри управління та тактико-спеціальної підготовки, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

E-mail: a_m_bogdanov@inbox.ru.

Василь Васильович Цуркан, кандидат технічних наук, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Державний заклад "Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут", Київ, Україна.

E-mail: v.v.tsurkan@gmail.com.

Владимир Владимирович Мохор, доктор технических наук, профессор, директор, Институт проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины, Киев, Украина.

Александр Олегович Бакалинський, заместитель заведующего кафедрой управления и тактико-специальной подготовки, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Александр Михайлович Богданов, доктор технических наук, профессор, заведующий кафедрой управления и тактико-специальной подготовки, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Василий Васильевич Цуркан, кандидат технических наук, доцент кафедры кибербезопасности и применения автоматизированных информационных систем и технологий, Государственное учреждение "Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт", Киев, Украина.

Volodymyr Mokhor, doctor of technical sciences, professor, director, Pukhov institute for modeling in energy engineering of National academy of sciences of Ukraine, Kyiv, Ukraine.

Oleksandr Bakalynskyi, deputy head of management and tactical and special training academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Oleksandr Bohdanov, doctor of technical sciences, professor, head of management and tactical and special training academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.

Vasyl Tsurkan, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, State institution "Institute of special communications and information protection National technical university of Ukraine "Kyiv polytechnic institute", Kyiv, Ukraine.