INFORMATION SECURITY RISK MANAGEMENT

УДК 004.056.53

ВЛАДИМИР МОХОР,
АЛЕКСАНДР БАКАЛИНСКИЙ,
АЛЕКСАНДР БОГДАНОВ,
ВАСИЛИЙ ЦУРКАН

ИНТЕРПРЕТАЦИЯ ЗАВИСИМОСТИ УРОВНЯ ПРОСТОГО РИСКА ОТ ВЕРОЯТНОСТИ ЕГО РЕАЛИЗАЦИИ В ТЕРМИНАХ АНАЛИТИЧЕСКОЙ ГЕОМЕТРИИ

Рассматривается зависимость уровня простого риска от вероятности его реализации. Для интерпретации этой зависимости используется аналитическая геометрия. Показывается нелинейный характер этой зависимости, что приводит к сложности ее анализа на практике. Поэтому анализируется частный случай решения задачи анализа уровня рисков в линейном виде на примере двухкомпонентной модели риска, представленного на плоскости. Отмечается, что зависимость уровня риска от величины возможного ущерба аналогична зависимости уровня риска от величины вероятности его реализации и может быть выражена уравнением прямой. Определив аналогию между уравнением прямой и представлением соотношения риск-вероятность его реализации, проверяется соответствие данного утверждения другими способами задавания прямой на плоскости. Для этого рассматриваются известные варианты задания прямой в отрезках, с угловыми коэффициентами. То же касается и способов задания уравнения прямой по точке и направляющему вектору и нормальное уравнение прямой, в которых рассматриваются прямые, не выходящие из начала координат. Таким образом, показывается квазианалогия между представлением зависимости величины риска от вероятности его реализации и уравнением прямой на плоскости, которое выходит из начала координат и располагается в первом квадранте. Это позволяет исследовать риски с применением известных методов аналитической геометрии. Вместе с тем, при представлении риска в виде суммы двух и более составляющих сталкиваемся с необходимостью увеличения мерности системы координат до n, что приводит к необходимости дальнейших исследований в n-мерном пространстве.

Ключевые слова: простой риск, вероятность, ущерб, анализ рисков, аналитическая геометрия.

Постановка проблемы. Обеспечение информационной безопасности осуществляется путем внедрения системы управления информационной безопасностью, которая строятся, как правило, на основе требований, изложенных в международных стандартах серии ISO/IEC 27k. В частности, в стандарте ISO/IEC 27001:2013 “Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования” [1] - [6].

Сразу отметим [1] - [10], что ни один из существующих стандартов не содержит конкретных методик формирования проектных требований к системе управления информационной безопасностью (то есть, применительно к конкретной организации). Вместе с тем, часто речь идет о тех или иных аспектах информационной безопасности, которые должны быть внедрены во всей организации или по отношению к конкретному процессу. В таком случае, для того, чтобы понять, какие аспекты являются наиболее важными, какие характеристики должны быть реализованы при создании системы управления информационной безопасностью желательно иметь ее формальную модель. Исследование параметров такой модели может дать понимание того, на какие аспекты информационной

безопасности необходимо обращать пристальное внимание, а какие аспекты не являются принципиально важными. Для того, чтобы понять, какой именно вид может иметь формальная модель системы управления информационной безопасностью, какие из формальных методов применимы при ее моделировании, необходимо установить какому из видов формальных систем она аналогична. Если аналогии удастся выявить, то тогда можно предположить, что формальные методики проектирования, известные для систем-аналогов, удастся адаптировать к задачам создания системы управления информационной безопасностью [7].

Анализ последних исследований и публикаций. С целью выявления наиболее общих аналогий между системой управления информационной безопасностью и известными формальными системами рассмотрим более подробно основные ее качества. Согласно [5] система управления информационной безопасностью – это "та часть общей системы управления организации, которая основывается на оценке рисков [6]. Ею, как частью общей системы управления, создается, реализуется, эксплуатируется, осуществляется мониторинг, пересматривается, сопровождается и совершенствуется обеспечение информационной безопасности". Из этого определения следует, что все и любые системы управления информационной безопасностью можно рассматривать как класс систем, предназначенных для многоразового решения однотипных, в определенном смысле, задач. Такая трактовка наводит на мысль об аналогии между системой управления информационной безопасностью и системой массового обслуживания, в которой требования на выполняемые работы проявляются в виде событий информационной безопасности.

В общем случае последовательность требований на обслуживание, имеющих вид событий/рисков информационной безопасности, является случайной, как по времени проявления событий/рисков, так и по типу таких событий/рисков. Случайность последовательности событий/рисков, обслуживаемых системой управления информационной безопасностью, является еще одним аспектом аналогии с системой массового обслуживания.

Очевидно, что события информационной безопасности влекут за собой последствия в виде ущерба определенного размера H, возникновение которого связано с некоторой вероятностью p. Иногда такую вероятность p называют вероятностью реализации угрозы информационной безопасности, вероятностью реализации угрозы или вероятностью реализации риска.

В основу рассуждений возьмем то, что величина простого риска выражается с помощью следующего равенства:

$$R = H \cdot p, \qquad (1)$$

где R – уровень (величина) риска, H – стоимость ущерба, p – вероятность реализации угрозы. Кроме этого, необходимо выполнение условий: $R, H, p \geq 0$, а $p \leq 1$. Трехмерный график этой зависимости представлен на рисунке (см. рис.1).

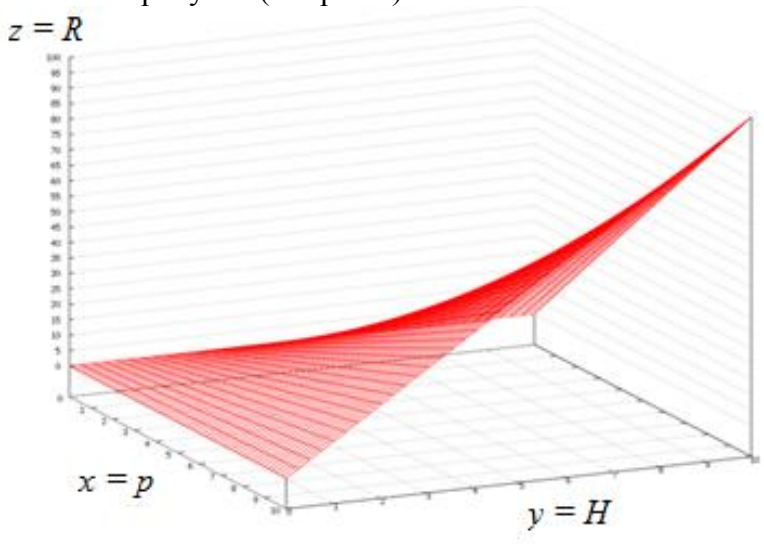

Рисунок 1 – Трехмерный армированный график зависимости уровня простого риска R

На рис.1 видно, что зависимости уровня риска R от вероятности его реализации p и стоимости ущерба H имеют нелинейный характер. Анализ систем с нелинейностями представляет большие сложности, а если представить, что на практике величина риска зависит от многих факторов (множеств H и p), то анализ подобных систем является исключительно сложным. С другой стороны, задача анализа уровня рисков может быть поставлена и в линейном виде. Рассмотрим это на простейшем примере двухкомпонентной модели риска представленного на плоскости (1).

Поэтому **целью работы** является интерпретация зависимости уровня простого риска от вероятности его реализации в терминах аналитической геометрии.

Представление риска в декартовой системе координат [7], [11]. Введем двумерную декартову систему координат, по горизонтальной оси которой будем откладывать значения вероятностей p, а по вертикальной оси – значения ущерба H. Очевидно, что значения вероятностей изменяются в диапазоне от $p=0$ до $p=1$, а значения ущерба в диапазоне от $H=0$ до некоторого $H=H_{\max}$. Для единообразия диапазона изменения величины ущерба с диапазоном изменения вероятностей введем в рассмотрение нормированную величину ущерба

$$h=\frac{H}{H_{\max}}.$$

Тогда нормированная величина ущерба будет изменяться в диапазоне от $h=0$ (при $H=0$) до $h=1$ при $H=H_{\max}$.

В декартовых координатах ($h0p$) определим “единичный квадрат” $OACE$ (см. рис.2), как геометрическое место точек, соответствующих любым возможным значениям нормированного риска r:

$$r=h\cdot p, \qquad (2)$$

где r подчиняется условию $0\le r\le 1$ вследствие выполнения условий $0\le h\le 1$ и $0\le p\le 1$.

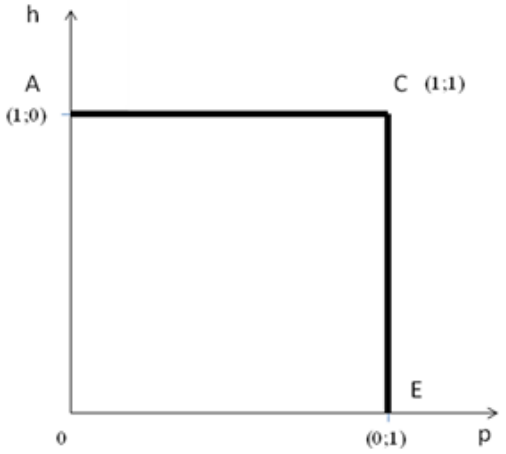

Рисунок 2 – Геометрическое место точек множества любых возможных значений нормированных рисков $r=h\cdot p$

Поскольку длина каждой из сторон квадрата $OACE$ равна единице, то и площадь $S_{общ}$ квадрата $OACE$ равна 1:

$$S_{общ}=1\cdot 1=1.$$

Зададим уровень приемлемого нормированного риска $r=r_0$. Тогда из соотношения (2) очевидно следует функциональная зависимость

$$h=r_0\cdot\frac{1}{p}, \qquad (3)$$

графиком которой является гипербола $h=(1/p)$, сдвигаемая коэффициентом r_0 от начала координат $(0,0)$ по направлению к точке с координатами $(1,1)$. Если наложить гиперболу

$h=(1/p)$ на единичный квадрат $OACE$, геометрическое место точек множества всех рисков разделяется на два подмножества (см. рис. 3), а именно: фигура $OABDE$ определяет геометрическое место точек множества значений рисков, для которых выполняется соотношение $r<r_0$, а фигура BCD определяет геометрическое место точек множества значений рисков, для которых выполняется соотношение $r \geq r_0$.

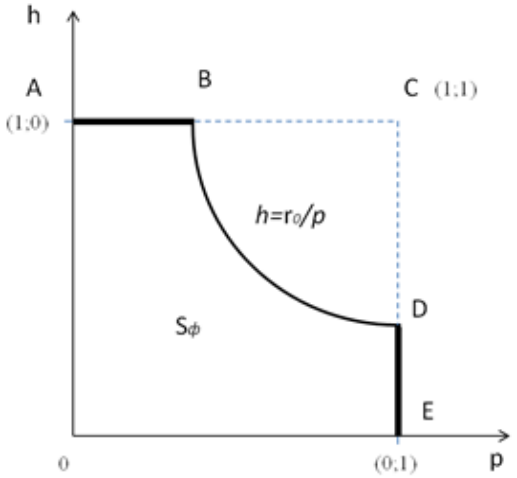

Рисунок 3 – Геометрическое место точек множества значений рисков, разделенное гиперболой $h=(1/p)$

В таком случае вероятность P_1 того, что значение произвольного нормированного риска r не будет превышать значения заданного уровня нормированного риска $r=r_0$, определяется отношением площади фигуры $OABDE$ к площади «единичного квадрата» $OACE$

$$P_1=\frac{S_ф}{S_{общ}}, \tag{4}$$

где $S_ф$ – площадь фигуры $OABDE$, а $S_{общ}$ – площадь «единичного квадрата». Так как ранее было показано, что $S_{общ}=1$, то соотношении (4) принимает вид:

$$P_1=S_ф. \tag{5}$$

Таким образом, вероятность P_1 того, что для произвольного риска будет выполняться условие $R>R_0$ равна площади фигуры $OABDE$. Остаётся рассчитать площадь этой фигуры.

Для этого разобьём фигуру $OABDE$ на две части (см. рис. 4): часть первая – фигура $OABG$ с площадью S_1 и часть вторая – фигура $GBDE$ с площадью S_2. Очевидно, что

$$S_ф=S_1+S_1 \tag{6}$$

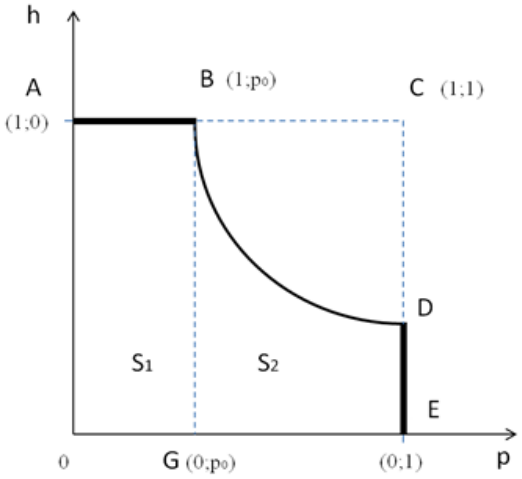

Рисунок 4 – Разбиение фигуры $OABDE$ на две фигуры

Площадь S_1 рассчитывается как площадь прямоугольника со сторонами OA и AB. Длина стороны OA, как было ранее обусловлено, равна 1. А длина стороны AB определяется численным значением вероятностной координаты точки B. Точка B есть точка пересечения прямой $b=1$ с гиперболой, определяемой соотношением (3). Тогда численное значение вероятностной координаты точки B можно определить, подставляя значение $h=1$ в левую часть соотношения (3):

$$1 = r_0 \cdot \frac{1}{p}.$$

Из этого соотношения следует, что численное значение вероятностной координаты $p = p_0$ точки B есть:

$$p_0 = r_0.$$

Тогда площадь S_1 может быть выражена следующим соотношением:

$$S_1 = 1 \cdot r_0 = r_0. \quad (7)$$

Площадь S_2 второй фигуры $GBDE$, которая образована гиперболой, заданной соотношением (3) и тремя прямыми: $h=0$, $p = p_0 = r_0$ и $p=1$, вычисляется как определенный интеграл по следующей формуле:

$$S_2 = \int_{r_0}^{1} \frac{r_0}{p} dp = r_0 \int_{r_0}^{1} \frac{1}{p} dp = r_0 \ln p \Big|_{r_0}^{1} = r_0 (\ln 1 - \ln r_0).$$

Поскольку $\ln 1 = 0$, то формула для вычисления площади S_2 принимает следующий вид:

$$S_2 = r_0 (\ln 1 - \ln r_0) = -r_0 \ln r_0. \quad (8)$$

Тогда для вычисления площади фигуры $OABDE$ подставим в (6) значения (7) и (8) и получим:

$$S_{\phi} = S_1 + S_2 = r_0 - r_0 \ln r_0 = r_0 (1 - \ln r_0). \quad (9)$$

Итак, с учетом (5) получается формула для оценки вероятности P_1 того, что нормированные значения величины возможных рисков не будут превышать заданной величины приемлемого риска r_0:

$$P_1 = r_0 (1 - \ln r_0). \quad (10)$$

Проанализируем полученное соотношение.

Во-первых, поскольку для значений r_0 выполняется условие $0 \le r_0 \le 1$, постольку функция $\ln r_0$ в формуле (10) принимает отрицательные значения $\ln r_0 < 0$. За счет этого вычитаемая величина $(-r_0 \ln r_0)$ в формуле (10) превращается в положительное слагаемое. Для того, чтобы этот факт отразить явным образом, формулу (10) представим в следующем виде:

$$P_1 = r_0 (1 + \ln (r_0^{-1})). \quad (11)$$

Из соотношения (11) следует, что вероятность P_1, с которой могут возникать нормированные риски $r < r_0$, почти всегда превышает значение заданной величины этого приемлемого нормированного риска r_0, за исключением единственного случая $r_0 = 1$. В этом крайнем случае $\ln r_0 = 0$ и соотношение (11) принимает вид

$$P_1 = r_0 (1 + \ln (r_0^{-1})) = 1 \cdot (1 + \ln 1) = 1 \cdot (1 + 0) = 1,$$

и это является формальным отражением того тривиального факта, что если максимальную величину ущерба $H = H_{\max}$ задавать в качестве приемлемой, то тогда любые значения рисков являются допустимыми.

Во-вторых, можно определить максимальную погрешность замены вероятности P_1 риском r_0 (т.е. вероятностью $P = r_0$), как отклонение функции, заданной соотношением (11), от линии $P = r_0$, взяв следующую разность:

$$P_1 - P = r_0\left(1 + \ln\left(r_0^{-1}\right)\right) - r_0 = r_0 \ln\left(r_0^{-1}\right).$$

Итак [7], применение геометрического подхода к оцениванию вероятности P_1 того, что произвольные значения нормированного риска r угроз безопасности информации будут попадать в зону $r < r_0$, дало возможность получить точную количественную оценку этой вероятности в виде формулы (11). Как следствие, установлено, что такая вероятность P_1 практически всегда превышает уровень r_0. При этом в большинстве случаев это отличие достигает 30%, а более чем на 10% всех случаев различие даже слегка превышает 36%.

Интерпретация зависимости уровня простого риска от вероятности его реализации. Определим стоимость ущерба, который может быть нанесен активу *H*. Примем, что нанесенным ущербом актив не уничтожается полностью, и тогда, стоимость ущерба может быть определена, как стоимость полного восстановления актива до исходного состояния. Или стоимость ущерба равна полной стоимости актива A, которая понижается на ту часть стоимости H_1, которая соответствует поврежденной части актива. Выразим это в виде:

$$H = A - H_1\,, \tag{12}$$

где A – полная стоимость актива, H – стоимость ущерба, а H_1 – стоимость неповрежденной части актива. Тогда, умножив и поделив правую часть (12) на A мы получим представление стоимости ущерба H, как:

$$H = A\frac{1}{B}. \tag{13}$$

где

$$B = \frac{A}{A - H_1} = \frac{A}{H}. \tag{14}$$

Иными словами, B – это отношение полной стоимости актива к стоимости поврежденной части (стоимости ущерба), а величина обратная B выражает процент повреждения актива.

С другой стороны, из (1) следует, что стоимость ущерба H можно представить, как отношение величины риска к вероятности его реализации:

$$H = \frac{R}{p}. \tag{15}$$

Заменяя значение H, равное из (13) получим следующее соотношение:

$$\frac{R}{p} = \frac{A}{B}. \tag{16}$$

что в свою очередь приводит к следующему выражению:

$$R \cdot B = A \cdot p. \tag{17}$$

Перенеся все слагаемые в левую часть, получим:

$$B \cdot R - A \cdot p = 0. \tag{18}$$

Поставим слагаемое с p на первое место, и, по правилам математического этикета, коэффициент первого слагаемого (в данном случае A) должен быть положительным. Меняем знаки:

$$A \cdot p + (-B) \cdot R = 0. \tag{19}$$

Если сравнить выражение (19) с уравнением прямой

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

известной из курса аналитической геометрии, то можно увидеть их полное совпадение с точностью до обозначения, в случае, если $C = 0$. В этом случае прямая, которая отражает зависимость уровня риска R от вероятности его реализации p, всегда проходит через начало координат и, при ее представлении в виде общего уравнения прямой, имеет вид (см. рис. 5):

$$Ax + By = 0.$$

Тогда прямая, описывающая соотношение величины риска с вероятностью его реализации выглядит на графике аналогично (см. рис. 6).

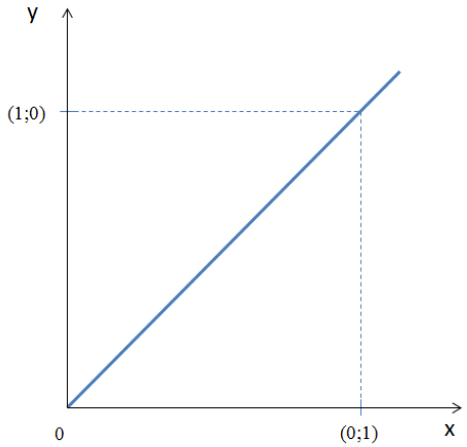

Рисунок 5 – График прямой, которая проходит через начало координат.

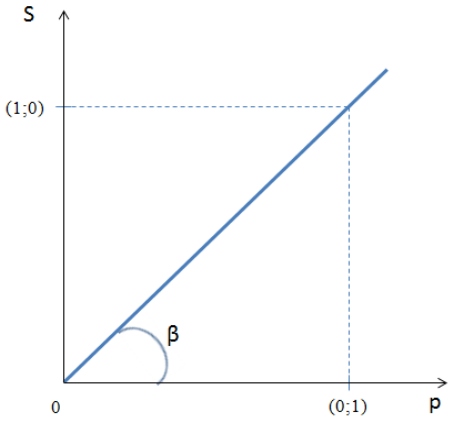

Рисунок 6 – График зависимости величины риска от вероятности его реализации.

А вот вариантов прохождения этой прямой может быть несколько, что отражено на рис. 7.

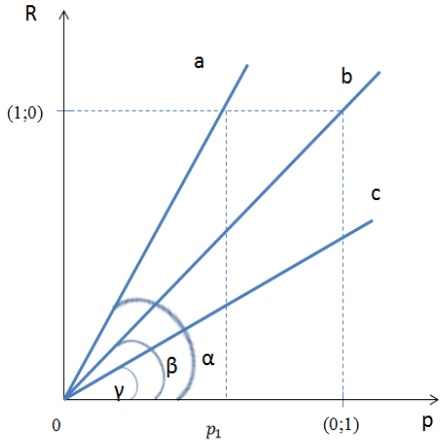

Рисунок 7 – Варианты прохождения прямой, задающей уровень рисков.

Причем для прямой a видно, что при вероятности реализации риска ниже единицы, наступает максимально возможный ущерб (уничтожение актива), угол наклона прямой $\alpha > 45°$, в случае же прямой b мы имеем дело с «идеальным соотношением» риск-вероятность, при котором угол равен 45°.

Это же видно и из следующих преобразований:

$$A \cdot p - B \cdot R = 0 \Rightarrow p = \frac{B}{A} \cdot R \Rightarrow p = tg\beta \cdot R \Rightarrow tg\beta = \frac{B}{A} \quad (20)$$

Если в (20) подставить значение B из (14), то получим:

$$tg\beta = \frac{1}{H} \quad (21)$$

Зная, что $H=1$ в случае $R= p$=1, то есть когда максимальный ущерб наступает при сочетании максимальной вероятности реализации риска p и максимального уровня риска R и приводит к полной потере актива, определим, что $tg\beta = 1$, что в свою очередь соответствует углу, равному 45°. Что и требовалось доказать. Для прямой c видно, что угол её наклона $\gamma < 45°$, что не превышает максимально возможный риск, а наоборот, на ней лежит множество рисков, уровень которых не достигает максимума при максимальной вероятности его реализации.

Определив аналогию между уравнением прямой и представлением соотношения риск-вероятность его реализации, проверим соответствие нашего утверждения другим способам задавания прямой на плоскости. Для этого рассмотрим другие известные варианты.

Уравнение прямой с угловым коэффициентом рассмотрено на рис. 6. Из его графического представления видно, что при необходимости достижения прямой рисков a положения "идеальной прямой" b, необходимо снижать величину угла α до величины угла β, или, другими словами, необходимо понижать стоимость актива A (дублировать актив, увеличивать количество подобных активов), или увеличивать B – соотношение полной стоимости актива к стоимости поврежденной части.

$$y = kx + b,$$

где $k = tg\beta$, а $b = 0$.

Зная, что $tg\beta = 1$, можем сделать вывод, что на прямой (12) уровень риска R всегда равен p, то есть она "идеальна".

При рассмотрении рисков, которые лежат на прямой c видно, что их уровень ниже "идеальной прямой", а значит, дополнительные действия по обработке рисков не требуется.

Способ задания уравнения прямой в отрезках не имеет смысла, так как он описывает варианты пересечения прямой с осями, в нашем случае это пересечение происходит в начале координат.

То же касается и способов задания уравнения прямой по точке и направляющему вектору и нормальное уравнение прямой в которых рассматриваются прямые, которые не выходят из начала координат и пересекают обе оси.

В случае представления уравнения прямой, которая проходит через две точки получаем равенство $R= p$.

Рассмотрим подробнее:

Если есть две точки $M_1(0;0)$ и $M_2(1;1)$, то уравнение прямой будет выглядеть как:

$$\frac{x - x_1}{x_2 - x_1} = \frac{y - y_1}{y_2 - y_1} \Rightarrow x = y \Rightarrow R = p,$$

что и требовалось доказать.

Уравнение прямой в полярной системе координат рассматривать нет смысла, так как оно определяет положение прямой, которая не выходит из начала координат, что противоречит нашим рассуждениям о том, когда вероятность реализации риска равна нулю и стоимость ущерба нулевая.

Можно отметить, что зависимость уровня риска от величины возможного ущерба аналогична зависимости уровня риска от величины вероятности его реализации и тоже может быть выражена через уравнение прямой.

Выводы. В результате проведенного исследования была показана квазианалогия между представлением зависимости величины риска от вероятности его реализации и уравнением прямой на плоскости, которое выходит из начала координат и располагается в первом квадранте. Таким образом, исследование рисков возможно с применением известных методов аналитической геометрии. При представлении риска в виде суммы двух и более составляющих мы сталкиваемся с необходимостью увеличивать мерность системы координат до n, что приводит к необходимости дальнейших исследований в n-мерном пространстве.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

[1]. “Компания “Инфосистемы Джет” построила СУИБ “Эльдорадо” [Электронный ресурс]. Доступно: http://www.osp.ru/osp-new/public/resources/releases/?rid=7954. Дата обращения: Февр. 6, 2017.

[2]. “ISO 27001 – Information Management Security System”. [Online]. Available: http://www.enhancequality.com/iso-standards/iso-27001-information-security-management-system/. Accessed on: Febr. 6, 2017.

[3]. А. Дмитриев, “Менеджмент информационной безопасности”. [Электронный ресурс]. Доступно: http://www.comizdat.com/index_.php?in=ksks_articles_id&id=568. Дата обращения: Февр. 6, 2017.

[4]. International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Febr. 6, 2017.

[5]. International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html. Accessed on: Febr. 6, 2017.

[6]. International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html. Accessed on: Febr. 6, 2017.

[7]. В. Мохор, А. Бакалинский, и В. Цуркан, “Геометрический подход к оцениванию вероятности приемлемых рисков информационной безопасности”, Захист інформації, том 18, № 3, С. 210-217, 2016.
doi: 10.18372/2410-7840.18.10850.

[8] “Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/v0365500-11/page. Дата звернення: Лют. 6, 2017.

[9]. International Organization for Standardization. (2016, Nov. 01). *ISO/IEC 27035-1. Information technology. Security techniques. Information security incident management. Part 1: Principles of incident management.* [Online]. Available: https://www.iso.org/standard/60803.html. Accessed on: Febr. 6, 2017.

[10]. International Organization for Standardization. (2016, Nov. 01). *ISO/IEC 27035-2. Information technology. Security techniques. Information security incident management. Part 2*: Guidelines to plan and prepare for incident response. [Online]. Available: https://www.iso.org/standard/62071.html. Accessed on: Febr. 6, 2017.

[11]. М. Кендалл, та П. Моран, Геометрические вероятности. Москва, Россия: Издательство “Наука”, 1972.

Статья поступила в редакцию 16 февраля 2017 года.

REFERENCE

[1]. “Jet Infosystems” company has built ISMS “Eldorado” [Online]. Available: http://www.osp.ru/osp-new/public/resources/releases/?rid=7954. Accessed on: Febr. 6, 2017.

[2]. “ISO 27001 – Information Management Security System”. [Online]. Available: http://www.enhancequality.com/iso-standards/iso-27001-information-security-management-system/. Accessed on: Febr. 6, 2017.

[3]. A. Dmitriev, “Information security management”. [Online]. Available: http://www.comizdat.com/index_.php?in=ksks_articles_id&id=568. Accessed on: Febr. 6, 2017.

[4]. International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Febr. 6, 2017.

[5]. International Organization for Standardization. (2013, Oct. 01). *ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security controls*. [Online]. Available: https://www.iso.org/standard/54533.html. Accessed on: Febr. 6, 2017.
[6]. International Organization for Standardization. (2011, June 10). *ISO/IEC 27005. Information technology. Security techniques. Information security risk management.* [Online]. Available: https://www.iso.org/standard/56742.html. Accessed on: Febr. 6, 2017.
[6]. V. Mokhor, O. Bakalynskyi, and V. Tsurkan, "A geometric approach to the acceptable risk probabilities estimation of information security", *Ukrainian Information Security Research Journal*, vol. 18, no. 3, pp. 210-217, 2016.
doi: 10.18372/2410-7840.18.10850.
[7] "Guidelines for the implementation of information security management systems and risk assessment methodology in accordance with the standards of the National Bank of Ukraine". [Online]. Available: http://zakon3.rada.gov.ua/laws/show/ v0365500-11/page. Accessed on: Febr. 6, 2017.
[7]. International Organization for Standardization. (2016, Nov. 01). *ISO/IEC 27035-1. Information technology. Security techniques. Information security incident management. Part 1: Principles of incident management*. [Online]. Available: https://www.iso.org/standard/60803.html. Accessed on: Febr. 6, 2017.
[8]. International Organization for Standardization. (2016, Nov. 01). *ISO/IEC 27035-2. Information technology. Security techniques. Information security incident management. Part 2: Guidelines to plan and prepare for incident response*. [Online]. Available: https://www.iso.org/ standard/62071.html. Accessed on: Febr. 6, 2017.
[9]. M. Kendall, and P. Moran, Geometrical probabilities. Moscow, Russia: Publishing "Nauka", 1972.

ВОЛОДИМИР МОХОР,
ОЛЕКСАНДР БАКАЛИНСЬКИЙ,
ОЛЕКСАНДР БОГДАНОВ,
ВАСИЛЬ ЦУРКАН

ІНТЕРПРЕТУВАННЯ ЗАЛЕЖНОСТІ РІВНЯ ПРОСТОГО РИЗИКУ ВІД ІМОВІРНОСТІ ЙОГО РЕАЛІЗУВАННЯ В ТЕРМІНАХ АНАЛІТИЧНОЇ ГЕОМЕТРІЇ

Розглядається залежність рівня простого ризику від імовірності його реалізування. Для інтерпретування цієї залежності використовується аналітична геометрія. Показується нелінійних характер означеної залежності, що призводить до складнощів її аналізування на практиці. Тому аналізується окремий випадок вирішення завдання з аналізування рівня ризиків у лінійному виді на прикладі двохкомпонентної моделі ризику, що відображається на площині. Відмічається, що залежність рівня ризику від величини вірогідних збитків аналогічна залежності рівня ризику від величини імовірності його реалізування і може бути виражена рівнянням прямої. Визначення аналогії між рівнянням прямої і відображення співвідношення ризик-імовірність його реалізування, перевіряється відповідність даного твердження іншими способами задання прямої на площині. Для цього розглядаються відомі варіанти задання прямої у відрізках, з кутовими коефіцієнтами. Те ж стосується і способів задання прямої за точкою і напрямним вектором і номальне рівняння прямої, у яких розглядаються прямі, що не виходять з початку координат. Таким чином, показується квазіаналогія між представленням залежності величини ризику від імовірності його реалізації і рівняням прямої на площині, що виходить з початку координат і розміщується у першому квадрантів. Це дозволяє досліджувати ризики шляхом використання відомих методів аналітичної геометрії. Разом з тим, при представленні ризику сумою двох і більше складових виникає потреба зменшення мірності системи координат до *n*, Це призводить до необхідності проведення подальших досліджень в *n*-мірному просторі.

Ключові слова: простий ризик, імовірність, збитки, аналізування ризиків, аналітична геометрія.

VOLODYMYR MOKHOR,
OLEKSANDR BAKALYNSKYI,
OLEKSANDR BOHDANOV,
VASYL TSURKAN

INTERPRETATION OF THE SIMPLE RISK LEVEL DEPENDENCE OF ITS IMPLEMENTATION IN THE TERMS OF ANALYTIC GEOMETRY

It is considered the dependence of the level of simple risk on the likelihood of its implementation. Analytical geometry is used to interpret this dependence. It is shown the nonlinear character of its dependence, which leads to the complexity of its analysis in practice. Therefore, a special case of solving the problem of risk level analysis in a linear form is analyzed on the example of a two-component risk model presented on a plane. It is noted that the dependence of the level of risk on the magnitude of possible damage is analogous to the dependence of the level of risk on the magnitude of the probability of its realization and can be expressed by the direct equation. Defining the analogy between the equation of a straight line and the representation of the risk-probability relation for its realization, it is verified the correspondence of this assertion to other methods of specifying a line in the plane. It is considered known variants of specifying a straight line in a segment, with angular coefficients to solve that. The same applies to the methods of specifying the equation of a straight line with respect to a point and a guiding vector and the normal equation of a straight line in which straight lines not leaving the origin of coordinates are considered. Thus, a quasi-analogy is shown between the representation of the dependence of the risk value on the probability of its realization and the equation of the straight line on the plane that leaves the origin and is located in the first quadrant. This allows to investigate risks using known methods of analytical geometry. At the same time, while representing the risk as a sum of two or more components, encountered the need to increase the dimensionality of the coordinate system to n, which leads to the need for further studies in n-dimensional space.

Keywords: simple risk, probability, damage, risk analysis, analytical geometry.

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

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

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.

E-mail: baov@meta.ua.

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.

E-mail: bodya1949@gmail.com.

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.

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

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

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.

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.

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.

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.

УДК 004.056.5

ЮЛІЯ КОЖЕДУБ

АНАЛІЗ ДОКУМЕНТІВ З КЕРУВАННЯ РИЗИКОМ КІБЕРБЕЗПЕКИ

У статті подано аналіз новітніх документів щодо менеджменту ризиків в сфері забезпечення інформаційної безпеки та кібербезпеки. Дослідження сучасних стандартів показують, що їхню увагу зосереджено на ризиках, як це було започатковано в стандартах на системи менеджменту Міжнародної організації зі стандартизації. У статті показано, що проблемою дослідження ризиків інформаційної безпеки та кібербезпеки займаються організації різного статусу, підпорядкованості й форми власності. Зазначені організації набули великого досвіду у питаннях, пов'язаних з процесом керування ризиками інформаційної безпеки та кібербезпеки. Значення їхньої роботи має планетарний характер, оскільки розробки у цій сфері діяльності було покладено як основа створення документів різного виду, що вони їх пропонують різним країнам і організаціям для упровадження в діяльність щодо забезпечення інформаційної безпеки та кібербезпеки. У статті запропоновано розглядати комплексно документи, розроблені для роботи ризик-менеджера з інформаційної безпеки та кібербезпеки. Модель інструментарію побудовано на центральному ядрі, який визначено нормативними документами як процес управління ризиками. Нормативні документи, що визначають процес управління ризиками – це основоположні стандарти, що застандартизовують поняття «ризик» і це є відправною точкою для менеджерів усіх ланок, які