УДК 004.056.53::519.212.3

ГЕОМЕТРИЧЕСКИЙ ПОДХОД К ОЦЕНИВАНИЮ ВЕРОЯТНОСТИ ПРИЕМЛЕМЫХ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Владимир Мохор, Александр Бакалинский, Василий Цуркан

Рассматривается построение и использование систем управления информационной безопасностью на основе риск-ориентированного подхода. При этом устанавливается не конструктивность проектного требования к построению таких систем путем «обеспечения уровня риска не выше приемлемого». Для преодоления установленного ограничения предлагается рассматривать функционирование системы управления информационной безопасностью как системы массового обслуживания с обработкой потока рисковых событий с уровнями риска выше приемлемого и заданной вероятностью появления таких событий. Решение данной задачи осуществляется путем использования понятия и методов геометрической вероятности. Благодаря такому подходу субъективный показатель риск-аппетита владельца риска, отображаемый в виде приемлемого уровня риска, трансформируется в формализованный вероятностный критерий, на основе которого можно сформулировать проверяемые требования к созданию систем управления информационной безопасностью.

Ключевые слова: *геометрическая вероятность, геометрический подход, риск информационной безопасности, приемлемый уровень риска, оценивание вероятности, риск-аппетит, владелец риска, система управления информационной безопасностью.*

Постановка проблемы

Построение и использование систем управления информационной безопасностью (далее – СУИБ) в современных компаниях, а особенно тех, функционирование которых зависит от стабильной работы информационных технологий или иной критической инфраструктуры (банки, компании-разработчики программного обеспечения и т.д.) – является требованием времени. Как утверждают компании, которые уже внедрили СУИБ, и имеют опыт ее эксплуатации не один год, а также консалтинговые компании, которые занимаются предоставлением услуг по построению СУИБ, преимущества организации, в которой функционирует эта система, значительны [1, 2]. Эти преимущества включают в себя такие аспекты, как исключение неприемлемых рисков, оптимизацию затрат на обеспечение информационной безопасности (ИБ) за счет более эффективного использования имеющихся средств, повышение осознанности и управляемости процессов обеспечения ИБ. Выгодами от внедрения СУИБ также являются [3]:

– понятность информационных активов для менеджмента компании;

– результативное выполнение политики безопасности (нахождение и исправление слабых мест в системе информационной безопасности);

– регулярное выявление угроз и уязвимостей безопасности для существующих бизнес-процессов;

– расчет рисков и принятие решений на основе бизнес-целей;

– эффективное управление предприятием в критичных ситуациях;

– демонстрация прозрачности и чистоты бизнеса перед законом благодаря соответствию стандарту;

– снижение и оптимизация стоимости поддержки системы безопасности;

– интеграция подсистемы информационной безопасности в общую систему менеджмента;

– демонстрация клиентам, партнерам, владельцам бизнеса своей приверженности к информационной безопасности;

– международное признание и повышение авторитета компании, как на внутреннем рынке, так и на внешних рынках.

Современные организации, строя у себя СУИБ, ориентируются, как правило, на требования международного стандарта ISO/IEC 27001:2013 «Информационные технологии. – Методы обеспечения безопасности. – Системы управления информационной безопасностью. – Требования» [4]. Этот стандарт предопределяет целесообразность использования риск-ориентированного подхода к управлению информационной безопасности в целом и, в частности, вытекающие из него требования к построению СУИБ. С целью конкретизации требований по риск-ме-

неджменту в контексте построения СУИБ в рамках группы стандартов серии ISO/IEC 27k принят международный стандарт ISO/IEC 27005:2011 «Информационные технологии. – Методы и средства обеспечения безопасности. – Менеджмент риска информационной безопасности» [5]. В нем, в частности, предопределено, что «риски должны быть идентифицированы, количественно определены или качественно описаны и расставлены в соответствии с приоритетами согласно критериям оценивания риска и уместным для организации целям».

Для формирования корректных и конструктивных требований к построению СУИБ важным является приведенное в этом стандарте определение риска: «Риск представляет собой комбинацию последствий, вытекающих из нежелательного события, и вероятности возникновения события». В частности, если такая комбинация принимает мультипликативную форму, то соотношение для вычисления уровня риска может быть записано в следующем виде:

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

где R – уровень (величина) риска, H – оценка величины последствий (ущерба), являющихся следствием нежелательного события, которые (речь идет о последствиях) в случае событий информационной безопасности принимают форму ущерба, p – вероятность возникновения события информационной безопасности. Иногда такую вероятность p называют вероятностью реализации угрозы информационной безопасности или просто вероятностью реализации угрозы.

Очевидно, что на основе соотношения (1) можно сформировать тривиальный критерий ранжирования рисков. Но, кроме того, можно предположить, что опираясь на соотношение (1) и понятие приемлемого риска $R = R_0$ можно определить вероятностный критерий и его значение, задаваемое в качестве проектного требования при построении СУИБ (сразу оговоримся, что такой вероятностный критерий не может быть установлен очевидным соотношением $p = R_0/H$, поскольку величина H является неизвестной). Для этого применяется идея подхода, использующего так называемые «карты риска», которые позволяют «владельцам риска» задавать приемлемые уровни риска $R = R_0$ и разделять все риски на приемлемые и неприемлемые, проведя на «картах риска» линии, соответствующие $R = R_0$. Такой подход изложен в стандарте ISO/IEC 27005:2011 [5], где карта риска представляется в виде двумерной таблицы, ячейки которой на пересечениях соответствующих строк и столбцов содержат соответствующие значения риска. При этом, значения риска оцениваются, например, по шкале от 0 до 8.

Таблица 1

Пример шкалы рисков

Вероятность инцидентного сценария / Степень воздействия	Очень низкая	Низкая	Средняя	Высокая	Очень высокая
Очень высокая	4	5	6	7	8
Высокая	3	4	5	6	7
Средняя	2	3	4	5	6
Низкая	1	2	3	4	5
Очень низкая	0	1	2	3	4

Пример реализации этого похода наблюдается, в частности, в методических рекомендациях по созданию СУИБ и оцениванию рисков Национального банка Украины [6].

При этом в качестве очевидного посыла по умолчанию предполагается, что риски, которые отнесены к категории приемлемых, СУИБ должна обрабатывать в «автоматическом» режиме и без

применения организационно-административных мер и/или без привлечения дополнительных ресурсов. В подобных случаях оператор системы должен действовать по протоколу, так сказать «не включая интеллект» – достаточно плановой работы группы технической поддержки. И лишь в случае проявления событий, риск которых превышает заданный приемлемый уровень или когда проявляется эффект накопления рисков, должен вступать в работу риск-менеджер, а иногда и Группа реагирования на инциденты информационной безопасности [7], формируется план обработки рисков, привлекаются дополнительные ресурсы, как человеческие, так и финансовые, иногда, привлекаются сторонние организации.

Однако следует заметить, что «карты рисков» оперируют единичными проявлениями событий и не учитывают их возможного повторного (многократного) проявления. Накопление последствий совокупности событий, каждое из которых попадает в зону приемлемых, может привести к ущербу более высокому, чем тот, который ассоциирован с каждым из составляющих рисков заданного уровня, даже без учёта такого явления, как провокация одним риском появления другого. Все это приводит к осознанию того, что уровень приемлемого риска единичного события не может быть использован в качестве корректного проектного требования к построению СУИБ. Иными словами, существующие в настоящее время методики построения СУИБ не имеют возможности трансформировать уровень приемлемого риска, задаваемый собственником, в корректные формальные требования к построению СУИБ. И даже если такие требования формально выдвигаются, то нет ответа на вопрос, как убедиться в том, что СУИБ построенная исходя из требования обеспечения заданного уровня риска, обеспечивает выполнение этого требования.

Из тезиса, изложенного в предыдущем абзаце, следует вывод о неконструктивности проектного требования к СУИБ, основанного на концепте «обеспечить уровень риска не выше R_0». На наш взгляд, корректное проектное требование следует сформулировать иначе, а именно так: создаваемая СУИБ должна функционировать как система массового обслуживания, которая обеспечивает обработку потока рисковых событий с уровнями риска $R \geq R_0$ и заданной вероятностью P_0 появления таких событий.

Для обоснования корректности такого требования необходимо показать возможность определить по заданной величине приемлемого риска $R = R_0$ величину вероятности P_0, с которой проявляются события, ассоциированные с рисками $R \geq R_0$.

Иными словами, нужно показать разрешимость следующей задачи: для заданного уровня приемлемого риска $R = R_0$ необходимо оценить вероятность P_0 появления события с рисками $R \geq R_0$. Дуальная постановка этой же задачи: по заданному уровню приемлемого риска $R = R_0$ оценить вероятность P_1, с которой могут появляться события с рисками $R < R_0$. При этом очевидно, что $P_0 + P_1 = 1$.

Изложение основного материала исследований

Оценку вероятности P_1 можно выполнить, используя понятие и методы геометрической вероятности [8]. Прежде всего, 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.1), как геометрическое место точек, соответствующих любым возможным значениям нормированного риска r:

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

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

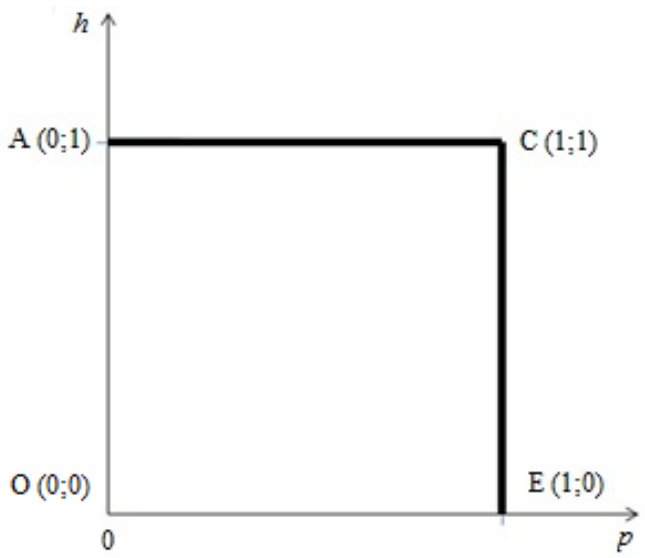

Рис. 1. Геометрическое место точек множества любых возможных значений нормированных рисков

$$r = h \cdot p$$

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. 2), 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 $r \geq r_0$.

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» $OACE$

$$P_1 = \frac{S_ф}{S_{общ}}, \qquad (4)$$

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:

$$P_1 = S_ф. \qquad (5)$$

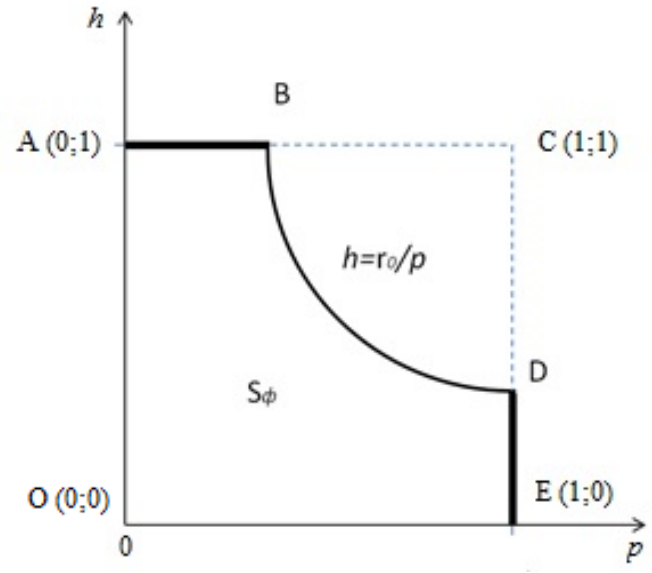

Рис. 2. Геометрическое место точек множества значений рисков, разделенное гиперболой $h = (1/p)$

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.3): часть первая – фигура $OABG$ с площадью S_1 и часть вторая – фигура $GBDE$ с площадью S_2.

Очевидно, что

$$S_ф = S_1 + S_1. \qquad (6)$$

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):

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

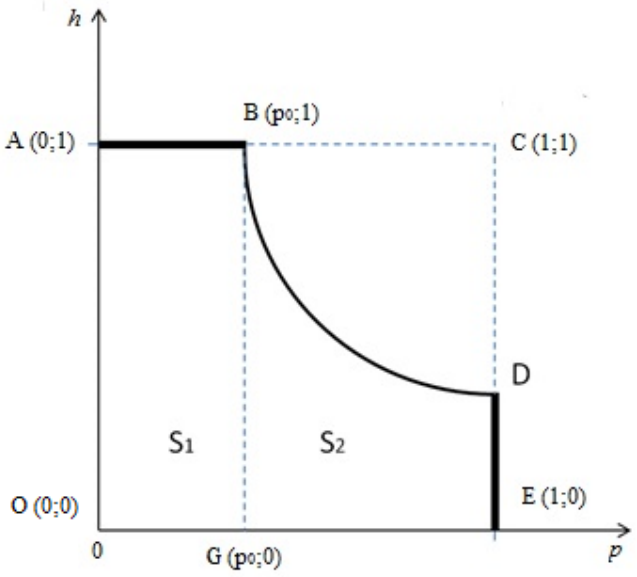

Рис. 3. Разбиение фигуры $OABDE$ на две фигуры: прямоугольник $OABG$ и фигуру $GBDE$

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:

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

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:

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

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

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

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:

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

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:

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

Пример положения графика этой функции относительно графика линии $P = r_0$ показано на рис. 4.

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:

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

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:

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

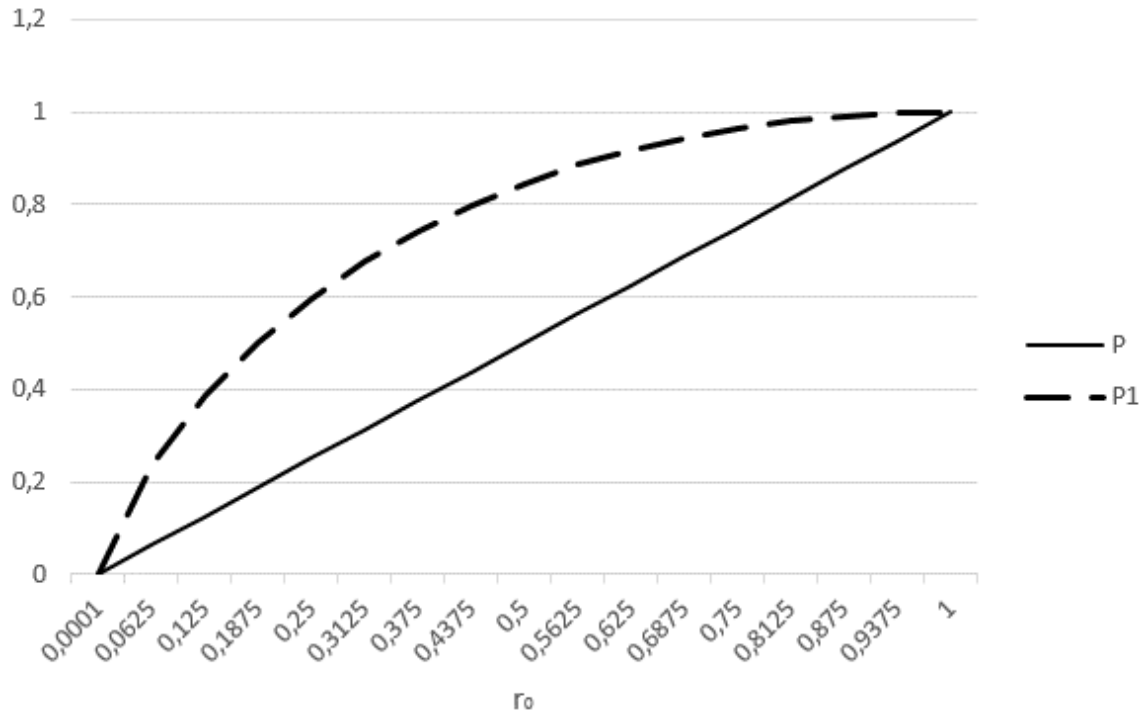

Рис. 4. Положение графика функции $P_1 = r_0\left(1+\ln\left(r_0^{-1}\right)\right)$ по отношению к графику функции $P = r_0$

График функции, соответствующей такой разности, приведен на рис. 5 и из него можно непосредственно получить, что:

1) максимальное значение погрешности оценивания вероятности ненамного превышает значение 0.36 (а если точно, то оно равно 0.3678) от единицы нормированного уровня риска;

2) максимальное значение погрешности достигается в окрестности значений нормированного риска $r_0 = 0.36$;

3) превышение уровня 10% погрешности оценивания вероятности может наблюдаться на 80% возможных значений r_0;

4) уровень погрешности, превышающий 36%, возможен более чем на 10% всех значений r_0.

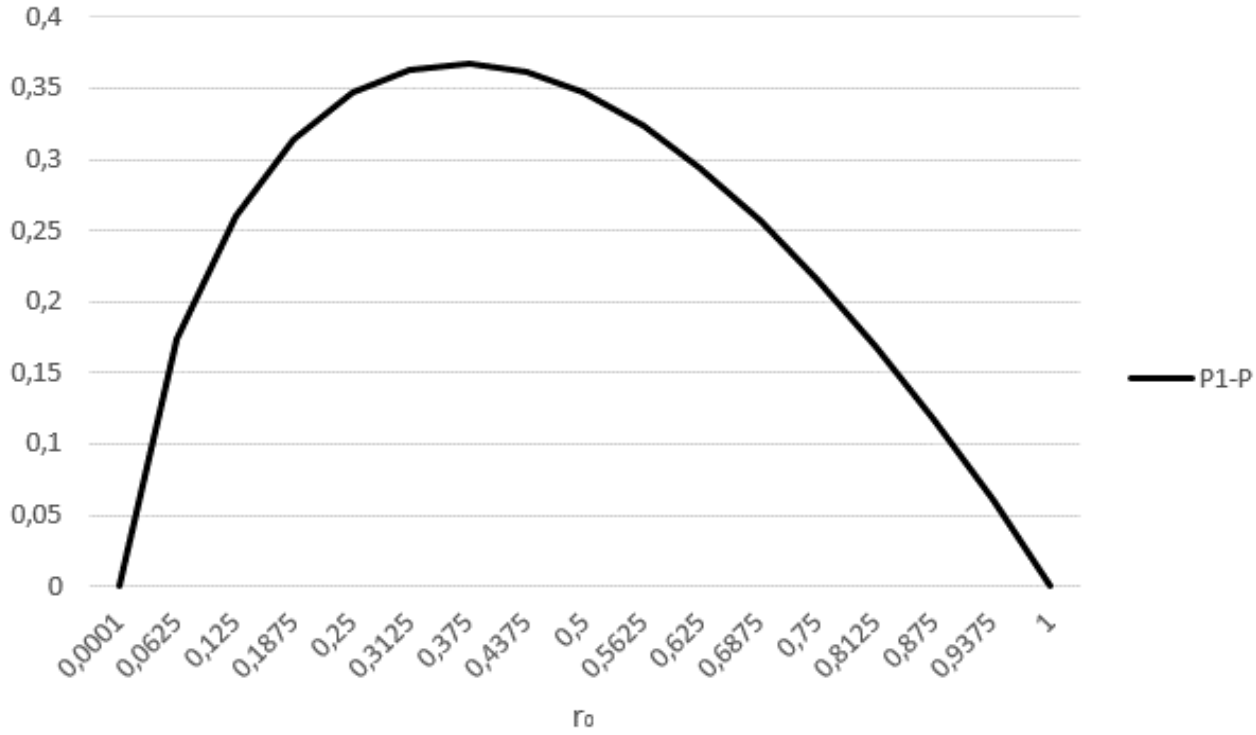

Рис. 5. График разности функции $P_1 = r_0\left(1+\ln\left(r_0^{-1}\right)\right)$ и $P = r_0$

Итак, 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%.

Выводы

Таким образом, применение геометрического подхода дает возможность трансформировать субъективный показатель риск-аппетита владельца риска, отображаемый в виде приемлемого уровня риска, в формализованный вероятностный критерий, на основе которого можно сформулировать проверяемые требования к созданию систем управления информационной безопасностью.

ЛИТЕРАТУРА

[1]. Компания «Инфосистемы Джет» построила СУИБ «Эльдорадо» [Электронный ресурс]. – Режим доступа : http://www.osp.ru/osp-new/public/resources/releases/?rid=7954. – Дата доступа : июнь 2016. – Название с экрана.

[2]. ISO 27001 – Information Management Security System [Electronic resource]. – Access mode : http://www.enhancequality.com/iso-standards/iso-27001-information-security-management-system/. – Access data : June 2016. – The title of the screen.

[3]. Дмитриев А. Менеджмент информационной безопасности [Электронный ресурс] / А. Дмитриев. – Режим доступа : http://www.comizdat.com/index_.php?in=ksks_articles_id&id=568. – Дата доступа : июнь 2016. – Название с экрана.

[4]. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.

[5]. Information technology. Security techniques. Information security risk management : ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – P. 68.

[6]. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/v0365500-11/page. – Дата доступу : червень 2016. – Назва з екрану.

[7]. Information technology. Security techniques. Information security incident management : ISO/IEC 27035:2011. – First edition 2011-09-01. – Geneva, 2011. – P. 78.

[8]. Кендалл М. Геометрические вероятности / М. Кендалл, П. Моран. – М. : Наука, 1972. – 192 с.

REFERENCES

[1]. '«Jet Infosystems» company has built ISMS «Eldorado»', viewed 15 June 2016, http://www.osp.ru/osp-new/public/resources/releases/?rid=7954.

[2]. 'ISO 27001 – Information Management Security System', viewed 15 June 2016, http://www.enhancequality.com/iso-standards/iso-27001-information-security-management-system/.

[3]. Dmitriev A. (2007), 'Information security management', viewed 15 June 2016, http://www.comizdat.com/index_.php?in=ksks_articles_id&id=568.

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

[5]. International Organization for Standardization (2011), ISO/IEC 27005: *Information technology. Security techniques. Information security risk management*, Geneva, 68 p.

[6]. Guidelines for the implementation of information security management systems and risk assessment methodology in accordance with the standards of the National Bank of Ukraine, viewed 15 June 2016, http://zakon3.rada.gov.ua/laws/show/v0365500-11/page.

[7]. International Organization for Standardization (2011), ISO/IEC 27035 : Information technology. Security techniques. Information security incident management, Geneva, 78 p.

[8]. Kendall M., Moran P. (1972), 'Geometrical probabilities', Nauka, Moscow, 192 p.

ГЕОМЕТРИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ІМОВІРНОСТІ ПРИЙНЯТНИХ РИЗИКІВ БЕЗПЕКИ ІНФОРМАЦІЇ

Розглядається побудова та використання системи керування безпекою інформації на основі ризик-орієнтованого підходу. При цьому встановлюється не конструктивність проектної вимоги до побудови таких систем шляхом «забезпечення рівня ризику не вище прийнятного». Для подолання встановленого

обмеження пропонується розглядати функціонування системи керування безпекою інформації як системи масового обслуговування з обробляннням потоку ризикових подій з рівнями ризику вище прийнятного та заданою імовірністю появлення таких подій. Розв'язання цього завдання здійснюється шляхом використання поняття та методів геометричної імовірності. Завдяки такому підходу суб'єктивний показник ризик-апетиту власника ризику, що відображається прийнятним рівнем ризику, трансформується в формалізований імовірнісний критерій, на основі якого можна сформулювати вимоги до побудови систем керування безпекою інформації, що перевіряються.

Ключові слова: геометрична ймовірність, геометричний підхід, ризик безпеки інформації, прийнятний рівень ризику, оцінювання імовірності, ризик-апетит, власник ризику, система керування безпекою інформації.

A GEOMETRIC APPROACH TO THE ACCEPTABLE RISK PROBABILITIES ESTIMATION OF INFORMATION SECURITY

Construction and usage of the information security management system based on a risk-oriented approach is considered. At the same time nonconstructivity of project requirements for the construction of such systems by «ensuring the level of risk no higher than acceptable» is defined. In order to overcome this limit proposed to review the functioning of an information security management system as a queuing system with processing the flow of risk events with levels of risk that higher than acceptable and a defined probability of such events occurrence. The solution to this problem is realized by the use of concepts and methods of geometrical probability. With this approach the subjective indicator of risk owner risk-appetite, displayed in the form of acceptable level of risk is transformed into a formalized probabilistic criterion, on which is possible to formulate verifiable requirements for the establishment of information security management systems.

Keywords: geometric probability, geometric approach, information security risk, acceptable risk, probability estimation, risk-appetite, risk owner, information security risk management system.

Мохор Владимир Владимирович, доктор технических наук, профессор, Директор Института проблем моделирования в энергетике им. Г.Е. Пухова Национальной академии наук Украины.
E-mail: v.mokhor@gmail.com.

Мохор Володимир Володимирович, доктор технічних наук, професор, Директор Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

Mokhor Volodymyr, doctor of engineering science, professor, Director of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine.

Бакалинский Александр Олегович, заместитель заведующего кафедрой Государственного учреждения «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт».
E-mail: baov@meta.ua.

Бакалинский Олександр Олегович, заступник завідувача кафедри Державного закладу «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут».

Bakalynskyi Oleksandr, deputy head of department, State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute».

Цуркан Василий Васильевич, кандидат технических наук, ведущий научный сотрудник научно-исследовательского центра Государственного учреждения «Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт».
E-mail: v.v.tsurkan@gmail.com.

Цуркан Василь Васильович, кандидат технічних наук, провідний науковий співробітник науково-дослідного центру Державного закладу «Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут».

Tsurkan Vasyl, candidate of engineering science, leading researcher of State institution «Institute of special communications and information security National technical university of Ukraine «Kyiv polytechnic institute».