Метод формирования проектных требований к системе управления информационной безопасностью

© Мохор В.В.
Институт проблем моделирования в энергетике им. Г.Е. Пухова
Национальной академии наук Украины, Киев, Украина
v.mokhor@gmail.com
© Богданов А.М. © Бакалинский А.О. © Цуркан В.В.
Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт имени Игоря Сикорского", Киев, Украина
a_m_bogdanov@inbox.ru baov@meta.ua v.v.tsurkan@gmail.com

Аннотация

Для современных организаций требованием времени является построение и использование систем управления информационной безопасностью. Это обусловлено такими аспектами как исключение неприемлемых рисков, эффективное использование имеющихся средств, повышение осознанности и управляемости процессов обеспечения информационной безопасности. Построение и использование систем управления информационной безопасностью рассматривается на основе риск-ориентированного подхода. Как следствие, за основу берется двухкомпонентная модель риска, которая представляется на плоскости. Благодаря этому определяется вероятностный критерий и его значение, задаваемое в качестве проектного требования при построении систем управления информационной безопасностью в виде «карты риска». Она позволяет «владельцам риска» задавать приемлемые уровни рисков и разделять их на приемлемые и неприемлемые. Однако, «карты рисков» оперируют единичными проявлениями событий и не учитывают их возможного повторного (многократного) проявления. Из этого, делается вывод о неконструктивности проектного требования к системе управления информационной безопасностью, основанного на концепте «обеспечить уровень риска не выше». Поэтому корректное проектное требование формулируется в контексте обеспечения системой управления информационной безопасностью обработки потока рисковых событий с уровнями риска и заданной вероятностью появления таких событий. То есть показывается возможность оценивания вероятности появления события с рисками для заданного уровня приемлемого риска. Или по заданному уровню приемлемого риска оценивается вероятность появления событий с рисками. Решение данной задачи осуществляется путем использования понятия и методов геометрической вероятности. Применение геометрического подхода к оцениванию вероятности попадания произвольных значений нормированного риска в зону приемлемого риска, дало возможность получить точную количественную оценку этой 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 проектные требования к созданию систем управления информационной безопасностью.

1 Постановка проблемы

Требованием времени для современных организаций является построение и использование систем управления информационной безопасностью, а особенно для тех, функционирование которых зависит от стабильной работы информационных технологий или иной критической инфраструктуры [1]. Это связано с тем, что построение и использование обозначенных систем обусловлено такими аспектами как исключение неприемлемых рисков, оптимизация затрат на обеспечение информационной безопасности за счет более эффективного использования имеющихся средств, повышение осознанности и управляемости процессов обеспечения информационной безопасности [1, 2].

При построении систем управления информационной безопасностью руководствуются требованиями международного стандарта ISO/IEC 27001:2013 «Информационные технологии. – Методы обеспечения безопасности. – Системы управления информационной безопасностью. – Требования» [3]. Этот стандарт предопределяет целесообразность использования риск-ориентированного подхода к управлению информационной безопасности [4-6]. С целью конкретизации требований по управлению рисками в рамках группы стандартов серии ISO/IEC 27k принят международный стандарт ISO/IEC 27005:2011 «Информационные технологии. – Методы и средства обеспечения безопасности. – Управление риском информационной безопасности» [6]. 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». Поэтому для формирования корректных и конструктивных требований к построению систем управления информационной безопасность 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. Трехмерный график этой зависимости представлен на рис.1.

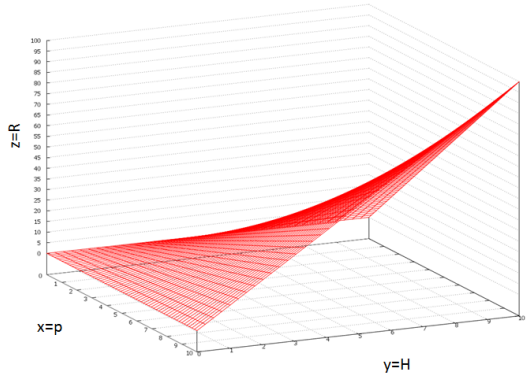

Рис. 1. Зависимость уровня риска R от вероятности его реализации p и оценки величины ущерба H

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 формирования проектных требований к системе управления информационной безопасностью может быть поставлена и в линейном виде. Рассмотрим это на простейшем примере двухкомпонентной модели риска представленного на плоскости (1).

В частности, 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 систем управления информационной безопасностью. Однако, 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 $R = R_0$ [3, 6].

Тем не менее, следует отметить, 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 системы управления информационной безопасностью. Иными словами, существующие в настоящее время методики ее построения не имеют возможности трансформировать уровень приемлемого риска, задаваемый собственником, в корректные формальные требования к построению системы управления информационной безопасностью. Из этого, следует вывод о неконструктивности проектного требования к системе управления информационной безопасностью, основанного на концепте «обеспечить уровень риска не выше R_0».

Поэтому корректное проектное требование следует сформулировать иначе, а именно так: система управления информационной безопасностью должна обеспечивать 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 возможность оценивания вероятности P_0 появления события с рисками $R \geq R_0$ для заданного уровня приемлемого риска $R = R_0$. Или по заданному уровню приемлемого риска $R = R_0$ оценить вероятность P_1, с которой могут появляться события с рисками $R < R_0$.

2 Формирование проектного требования к системе управления информационной безопасностью

Для оценки вероятности P_1 используем двумерную декартову систему координат, по горизонтальной оси которой будем откладывать значения вероятностей p, а по вертикальной оси – значения ущерба H [7]. 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 $0 \le p \le 1$. Поскольку длина каждой из сторон квадрата $OACE$ равна единице, то и площадь $S_{общ}$ квадрата $OACE$ равна 1.

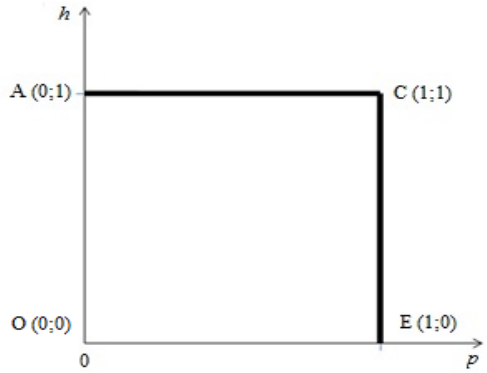

Рис. 2. Геометрическое место точек множества любых возможных значений нормированных рисков r

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 $r \ge r_0$.

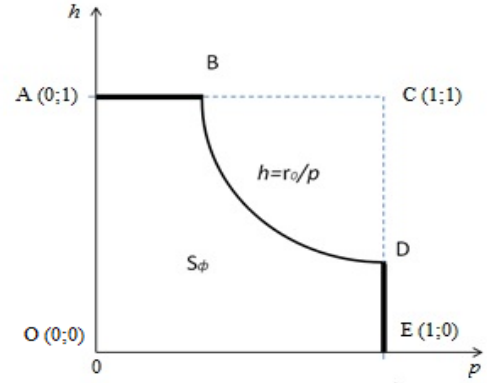

Рис. 3. Геометрическое место точек множества значений рисков, разделенное гиперболой $h = (1/p)$

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

$$S_ф = S_1 + S_1 \tag{6}$$

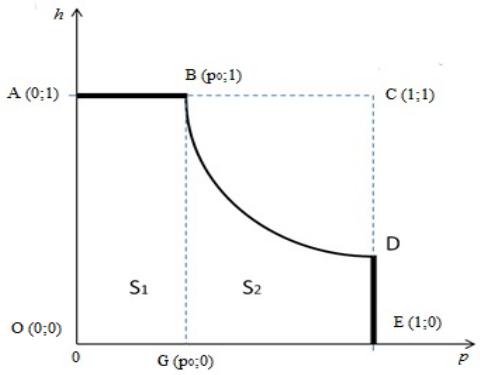

Рис.4. Разбиение фигуры $OABDE$ на две фигуры: прямоугольник $OABG$ и фигуру $GBDE$

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:

$$S_1 = 1 \cdot r_0 = r_0. \tag{7}$$

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:

$$S_2 = r_0 (\ln 1 - \ln r_0) = -r_0 \ln r_0. \tag{8}$$

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

$$S_ф = S_1 + S_2 = r_0 - r_0 \ln r_0 = r_0 (1 - \ln r_0). \tag{9}$$

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:

$$P_1 = r_0 (1 - \ln r_0). \tag{10}$$

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.5.

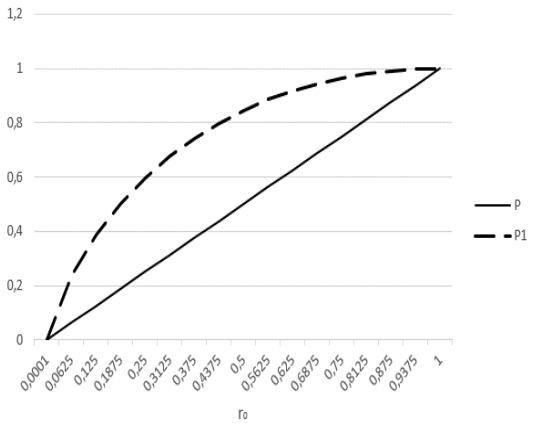

Рис.5. Положение графика функции $P_1 = r_0\left(1 + \ln\left(r_0^{-1}\right)\right)$ по отношению к графику функции $P = r_0$

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:

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

График функции, соответствующей такой разности, приведен на рис. 6 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.

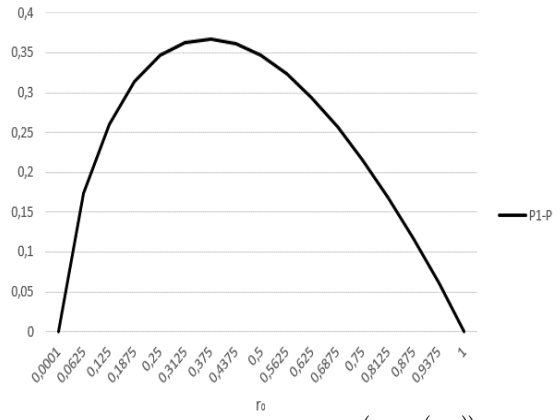

Рис.6. График разности функции $P_1 = r_0\left(1 + \ln\left(r_0^{-1}\right)\right)$ и $P = r_0$

3 Выводы

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%.

Благодаря этому стало возможным трансформировать субъективный показатель риск-аппетита владельца риска, отображаемый в виде приемлемого уровня риска, в формализованный вероятностный критерий, на основе которого можно сформулировать проверяемые проектные требования к построению систем управления информационной безопасностью.

Литература

1. 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.
2. 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 : сентябрь 2016. – Название с экрана.
3. Information technology. Security techniques. Information security management systems. Requirements : ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.
4. Information technology. Security techniques. Code of practice for information security controls : ISO/IEC 27002:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 80.
5. Risk management. Principles and guidelines : ISO 31000:2009. – First edition 2009-11-01. – Geneva, 2009. – P. 24.
6. Information technology. Security techniques. Information security risk management : ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – P. 68.
7. Кендалл М. Геометрические вероятности / М. Кендалл, П. Моран. – М. : Наука, 1972. – 192 с.

The Method of the Design Requirements Formation for Information Security Management System

© Vladimir V. Mokhor
Puchov IMEE NAS of Ukraine, Kiev, Ukraine
v.mokhor@gmail.com
© Aleksandr M. Bogdanov © Aleksandr O. Bakalinskii © Vasilii V. Tsurkan
Institute of Special Communication and Information Protection of National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kiev, Ukraine
a_m_bogdanov@inbox.ru baov@meta.ua v.v.tsurkan@gmail.com

Abstract

For modern organizations, the time requirement is the design and use of the information security management systems. This is due to aspects such as the exclusion of unacceptable risks, the effective use of available resources, increase of awareness and handling of information security processes. Design and use of information security management systems is considered on the basis of a risk-oriented approach. As a result, the basis of a two-component risk model, which is represented on a plane. This criterion is determined by the probability and its value, as defined in the project requirements in the design of a "risk map" for information security management systems. It allows you to "risk owners" to set acceptable risk levels and share them on acceptable and unacceptable. However, "risk map" operates on single events manifestations and do not consider their possible reuse (reusable) display. It concludes unconstructive design requirements for information security management system based on the concept "to provide the level of risk that is not higher than" Therefore, the correct design requirements formulated in the context of information security management system stream processing of risk events with a given level of risk and probability of occurrence of such events. That is shown the possibility of estimating the probability of event occurrence with the risk for a given level of acceptable risk. In other words, for a given level of acceptable risk is estimated the probability of event risks. The solution to this problem is solved by the use of concepts and methods of geometric probability. The use of the geometric approach to the estimation of the probability that the arbitrary values normalized risk acceptable risk zone, has made it possible to obtain accurate quantification of this probability. Through this approach, the subjective measure of "risk owner" risk appetite that is displayed in the form of an acceptable level of risk is transformed into a formal probabilistic criterion, based on which we can formulate verifiable design requirements for the establishment of information security management systems.