С. В. Запечников

МОДЕЛЬ МЕТОДИЧЕСКОЙ ОЦЕНКИ ВОЗМОЖНОГО УЩЕРБА В ИНФОРМАЦИОННОЙ СИСТЕМЕ ОТ РЕАЛИЗАЦИИ НЕБЛАГОПРИЯТНЫХ СОБЫТИЙ

Введение

Нарушение безопасности информации, циркулирующей в компьютерной системе, неизбежно ведет к потерям: финансовому, операционному, потребительскому ущербу, ущербу для персонала. Одним из важнейших показателей безопасности является риск.

Основанный на рисках подход к оценке потенциального ущерба от атак нарушителей и выбору мер для его минимизации нашел широкое применение в информационной безопасности и получил название *управления рисками*. Трактовка понятия управления рисками варьируется в различных источниках. Чаще всего под управлением рисками подразумевается полный комплекс из ряда выполняемых последовательно процессов, что соответствует существующим международным стандартам и практике управления рисками в организациях [1, 2]: определение контекста, идентификация рисков, анализ рисков и определение допустимых рисков, обработка рисков, принятие рисков, «коммуникация рисков», мониторинг и пересмотр. В существующих методиках управления рисками их идентификация осуществляется различными методами, такими как командные «мозговые штурмы», составление схем последовательности процессов и деревьев событий, анализ архитектуры системы, операционное моделирование, анализ сценариев, исследования HAZOP [3, 4]. При идентификации рисков часто используются вспомогательные понятия угрозы и уязвимости.

Задачи анализа рисков и управления рисками тесно взаимосвязаны [5]. Основанием для анализа рисков являются данные, собранные в процессе идентификации рисков, а результаты работы системного аналитика используются лицами, принимающими решения. В современных условиях системный аналитик, как правило, выполняет свою работу по заданию и в интересах менеджера рисков.

Модели анализа и оценки рисков исторически прошли три стадии развития [6].

В первых моделях, которые берут свое начало в 20-х годах XX в. и развивались вплоть до конца 70-х, использовались сравнительно простые способы оценки рисков переборного характера (путем эвристической оценки всех возможных угроз). Однако в конечном счете стала очевидной непрактичность такого подхода из-за крайне больших размерностей переборных задач и высокой вероятности недоучета важных факторов, влияющих на конечное решение.

Следующее поколение моделей (80—90-е годы XX в.) включает в себя четыре основных подхода (укажем их применительно к сфере информационных технологий): 1) риск в области ИТ рассматривается как частный случай общего риска деловой деятельности; 2) оценка рисков исходит из стоимостной оценки информационных ресурсов; 3) используются подходы, основанные на анализе сценариев реализации событий; 4) используются подходы, основанные на «лучших практиках» (best practices).

Третье поколение моделей, которым уделяется основное внимание в настоящее время, рассматривает управление рисками как принятие решений в условиях неопределенности, а количественные показатели риска — как критерии принятия альтернативных или взаимодополняющих решений в процессе какой-либо деятельности. Неопределенность, учитываемая в моделях третьего поколения, объясняется недостаточными субъективными знаниями о предмете или ситуации, в отличие от вероятности, которая является объективной мерой возможности реализации событий, учитывавшейся в моделях второго поколения. Каждая альтернатива характеризуется «профилем

риска», который может быть изменен в результате принятия тех или иных мер, составляющих процесс управления рисками: избежания риска, снижения риска, отказа от мер по снижению риска, отказа от определенного вида деятельности и др. [7]. Риск и выгода от какой-либо деятельности, от какого-либо принятого решения в этом случае понимаются как противоположности.

Указанный подход имеет непосредственное приложение к решению задач обеспечения безопасности информационных ресурсов, а количественные показатели рисков в такого рода задачах становятся количественными показателями безопасности информационных ресурсов.

1. Параметры, характеризующие риски нарушения безопасности информационных ресурсов

Как отмечалось выше, риск является одним из основополагающих понятий системного анализа. Следуя подходу Кумамото и Хенли [7], примем следующее формальное определение.

Риск — это множество, состоящее из кортежей:

$Risk \equiv \{(O_i,\ L_i,\ U_i,\ CS_i,\ PO_i) | i=1,...,\ n\}$,

где O_i, $i=1,...,\ n$ — множество исходов;

L_i — вероятности их реализации, оцениваемые качественно или количественно;

U_i — оценка значимости i-го исхода при помощи выбранного критериального показателя риска;

CS_i — сценарий реализации i-го исхода, указывающий причинно-следственные связи между событиями, предшествующими данному исходу и следующими за ним;

PO_i — группа населения, на которую влияют события, составляющие исход O_i.

При анализе задач обеспечения безопасности, возникающих в сфере информационных технологий, обычно принимается «усеченное» определение риска без двух последних составляющих:

$Risk \equiv \{(O_i,\ L_i,\ U_i) | i=1,...,\ n\}$.

Таким образом, основные параметры, характеризующие риск нарушения безопасности информационных ресурсов, — это перечень исходов, оценка вероятностей их реализации и оценка их влияния на рассматриваемый вид деятельности, которое выражается принятыми критериальными показателями риска: стоимостью потерь, временем задержки процесса, изменением качества выпускаемой продукции или оказываемых услуг и др.

2. Оценка критериального показателя риска

Пусть $\{O_1,...,\ O_m\}$ — множество всех неблагоприятных событий (НС), приводящих к снижению системной эффективности информационной системы (ИС), $\mathbf{O} = \{O_{i_1},...,\ O_{i_n}\} \subseteq \{O_1,...,\ O_m\}$ — подмножество НС, приводящих к нарушению безопасности информации в ИС. Математическое ожидание ущерба, вызываемого i-м неблагоприятным событием за время ΔT, выражается формулой:

$$e(O_i, \Delta T) = \mathbf{M}[e(O_i) \cdot f_i],$$

где $e(O_i)$ — случайная величина ущерба при единичном наступлении НС,

f_i — случайная величина количества событий за время ΔT.

Если НС не имеют последействия в том смысле, что ущерб от каждого НС независим, то

$$e(O_i, \Delta T) = \mathbf{M}[e(O_i)] \cdot \mathbf{M}[f_i],$$

$$E(\mathbf{O}, \Delta T) = \sum_{i=1}^{n} e(O_i, \Delta T) = \sum_{i=1}^{n} \mathbf{M}[e(O_i)] \cdot \mathbf{M}[f_i].$$

Если поток НС — простейший, то вероятность того, что за время ΔT произойдет ровно m событий, равна:

$$P(f_i = m, \Delta T) = \frac{(\lambda_i \cdot \Delta T)^m \cdot e^{-\lambda_i \cdot \Delta T}}{m!},$$

а математическое ожидание количества НС равно:

$\mathbf{M}[f_i] = \lambda_i \cdot \Delta T$,

где λ_i — интенсивность потока НС.

$\mathbf{M}[f_i]$ можно выразить через вероятность наступления хотя бы одного НС:

$P_i(\Delta T) = 1 - P(f_i = 0, \Delta T) = 1 - e^{-\lambda_i \cdot \Delta T}$,

$e^{-\lambda_i \cdot \Delta T} = 1 - P_i(\Delta T)$,

$\lambda_i \cdot \Delta T = -\ln(1 - P_i(\Delta T))$,

$\mathbf{M}[f_i] = -\ln(1 - P_i(\Delta T))$.

Если принять предположение о том, что ожидаемый ущерб прямо пропорционален ожидаемому числу событий, то

$e(O_i, \Delta T) = \mathbf{M}[e(O_i)] \cdot \mathbf{M}[f_i] = -E(O_i) \cdot \ln(1 - P_i(\Delta T))$,

$E(\mathbf{O}, \Delta T) = -\sum_{i=1}^{n} E(O_i) \cdot \ln(1 - P_i(\Delta T))|_{\Delta T}$.

При малых значениях $P_i(\Delta T)$ имеем:

$E(\mathbf{O}, \Delta T) \approx \sum_{i=1}^{n} E(O_i) \cdot P_i(\Delta T)_{\Delta T}$.

Если поток НС не является простейшим, а имеет другой характер, то распределение вероятностей реализации заданного количества НС будет иным и потребует дополнительного исследования.

Вероятности НС для различных структурных составляющих информационных ресурсов определяются на основании процессов методической оценки вероятностей реализации НС, что представляет собой самостоятельную научную задачу.

$E(\mathbf{O}, \Delta T)$ можно принять в качестве критериального показателя риска. Тогда в соответствии с ранее принятым определением:

$R(\Delta T) = \{(O_{i_1}, P_{i_1}(\Delta T), E(O_{i_1})), ..., (O_{i_n}, P_{i_n}(\Delta T), E(O_{i_n}))\}$ — риск, обусловленный существованием множества НС;

$R_i(\Delta T) = \{O_i, P_i(\Delta T), E(O_i)\}$ — «элементарный» риск, обусловленный одним видом НС.

Здесь $\mathbf{O} = \{O_{i_1}, ..., O_{i_n}\}$ — множество НС, $P_i(\Delta T)$ — вероятности реализации НС, $E(O_i)$ — математическое ожидание ущерба от реализации НС.

Таким образом, для расчета принятого критериального показателя риска необходимо предложить способ нахождения величин $E(O_i)$.

Пусть:

X — множество функциональных задач, решаемых ИС, каждая из которых связана с определенным процессом обработки данных или реализацией какого-либо процесса деловой деятельности;

$x \in X$ — единичная функциональная задача, которая описывается следующими числовыми характеристиками:

$c_i^{\mathbf{Z}}(x, \Delta T) = c_i^{\mathbf{Z}}(x) \cdot \Delta T$ — ущерб от простоя процесса обработки данных (процесса деловой деятельности) в течение времени ΔT вследствие утраты доступности, целостности или конфиденциальности информационных ресурсов, где $\mathbf{Z} = \{\text{Д}, \text{Ц}, \text{К}\}$;

$c_i^{\mathbf{Z}}(x, \Delta T, d^{\mathbf{Z}}) = d^{\mathbf{Z}} \cdot c_i^{\mathbf{Z}}(x) \cdot \Delta T$ — ущерб от деградации процесса обработки данных (процесса деловой деятельности), т. е. от снижения эффективности функционирования системы, в течение времени ΔT вследствие утраты доступности, целостности или конфиденциальности информационных ресурсов, где $\mathbf{Z} = \{\text{Д}, \text{Ц}, \text{К}\}$, $d^{\mathbf{Z}} \in [0;1]$ — коэффициент деградации.

Ущерб от i-го НС, если оно приводит к нарушению одного из аспектов безопасности информационных ресурсов: доступности, целостности либо конфиденциальности, выражается формулой:

$$e_i^{\mathbf{Z}}(x) = p^{\mathbf{Z}} \cdot \lim_{\Delta T \to \infty} c_i^{\mathbf{Z}}\left(x, \Delta T, d^{\mathbf{Z}}\right) + \left(1 - p^{\mathbf{Z}}\right) c_i^{\mathbf{Z}}\left(x, \Delta T_{\to}^{\mathbf{Z}}, d^{\mathbf{Z}}\right),$$

где $\rho^{\mathbf{Z}}$ — вероятность, с которой наступает перманентный простой процесса, $1 - \rho^{\mathbf{Z}}$ — вероятность временного простоя процесса, $T_{\to}^{\mathbf{Z}}$ — период последействия НС, вызвавшего утрату одного из аспектов безопасности информационных ресурсов, $\mathbf{Z} = \{\text{Д}, \text{Ц}, \text{К}\}$.

Суммарный ущерб процессу обработки данных от i-го НС:

$$e_i(x) = e_i^{\text{Д}}(x) + e_i^{\text{Ц}}(x) + e_i^{\text{К}}(x).$$

Полный ущерб от i-го НС всем процессам обработки данных (процессам деловой деятельности), реализованным в ИС:

$$e(O_i) = \sum_{x \in X} e_i^{\text{Д}}(x) + e_i^{\text{Ц}}(x) + e_i^{\text{К}}(x).$$

Математическое ожидание ущерба от i-го НС:

$$E(O_i) = \mathbf{M}[e(O_i)] = \sum_{x \in X} \mathbf{M}\left[e_i^{\text{Д}}(x)\right] + \mathbf{M}\left[e_i^{\text{Ц}}(x)\right] + \mathbf{M}\left[e_i^{\text{К}}(x)\right].$$

3. Оценка возможного ущерба с учетом структуры информационных ресурсов

Предложенная математическая модель может быть уточнена с учетом того факта, что информационные ресурсы ИС структурированы.

Пусть R — множество информационных ресурсов ИС, R^x — подмножество информационных ресурсов, задействованных в функциональной задаче x, $r \in R$ — отдельный информационный ресурс, идентифицируемый в ИС.

Пусть:

$c_i^{\mathbf{Z}}(x, r, \Delta T) = c_i^{\mathbf{Z}}(x, r) \cdot \Delta T$ — ущерб от простоя процесса обработки данных (процесса деловой деятельности), связанного с функциональной задачей x, вследствие нарушения безопасности информационного ресурса r в течение времени ΔT;

$c_i^{\mathbf{Z}}\left(x, r, \Delta T, d^{\mathbf{Z}}\right) = d^{\mathbf{Z}} \cdot c_i^{\mathbf{Z}}(x, r) \cdot \Delta T$ — ущерб от деградации процесса обработки данных (процесса деловой деятельности), связанного с функциональной задачей x, вследствие нарушения безопасности информационного ресурса r в течение времени ΔT.

Тогда ущерб для процесса, связанного с функциональной задачей x, от нарушения доступности, целостности и конфиденциальности информационного ресурса r вследствие i-го НС выражается следующим образом:

$$e_i^{\text{Д}}(x, r) = p^{\text{Д}} \cdot \lim_{\Delta T \to \infty} c_i^{\text{Д}}\left(x, r, \Delta T, d^{\text{Д}}\right) + \left(1 - p^{\text{Д}}\right) c_i^{\text{Д}}\left(x, r, \Delta T_{\to}^{\text{Д}}, d^{\text{Д}}\right),$$

$$e_i^{\text{Ц}}(x, r) = p^{\text{Ц}} \cdot \lim_{\Delta T \to \infty} c_i^{\text{Ц}}\left(x, r, \Delta T, d^{\text{Ц}}\right) + \left(1 - p^{\text{Ц}}\right) c_i^{\text{Ц}}\left(x, r, \Delta T_{\to}^{\text{Ц}}, d^{\text{Ц}}\right),$$

$$e_i^{\text{К}}(x, r) = p^{\text{К}} \cdot \lim_{\Delta T \to \infty} c_i^{\text{К}}\left(x, r, \Delta T, d^{\text{К}}\right) + \left(1 - p^{\text{К}}\right) c_i^{\text{К}}\left(x, r, \Delta T_{\to}^{\text{К}}, d^{\text{К}}\right),$$

при тех же обозначениях для входящих в формулы величин, что и ранее.

Полный ущерб для процесса, связанного с функциональной задачей x, от нарушения безопасности информационного ресурса r вследствие i-го НС выражается формулой:

$$e_i(x, r) = e_i^{\text{Д}}(x, r) + e_i^{\text{Ц}}(x, r) + e_i^{\text{К}}(x, r).$$

Полный ущерб для процесса, связанного с функциональной задачей x, от нарушения безопасности всех задействованных в нем информационных ресурсов вследствие i-го НС выражается формулой:

$$e_i(x) = \sum_{r \in R^x} e_i(x, r).$$

Полный ущерб для всех процессов, связанных с решаемыми ИС функциональными задачами, от реализации i-го НС:

$$e(O_i)=\sum_{x\in X}\sum_{r\in R^x} e_i(x,r).$$

Математическое ожидание полного ущерба от i-го НС:

$$E(O_i)=\mathbf{M}[e(O_i)]=\sum_{x\in X}\sum_{r\in R^x}\mathbf{M}\left[e_i^{\text{Д}}(x,r)\right]+\mathbf{M}\left[e_i^{\text{Ц}}(x,r)\right]+\mathbf{M}\left[e_i^{\text{К}}(x,r)\right].$$

Математическое ожидание полного ущерба от множества НС за время ΔT:

$$E(\mathbf{O},\Delta T)=-\sum_{i=1}^{n}\sum_{x\in X}\sum_{r\in R^x}\left(\mathbf{M}\left[e_i^{\text{Д}}(x,r)\right]+\mathbf{M}\left[e_i^{\text{Ц}}(x,r)\right]+\mathbf{M}\left[e_i^{\text{К}}(x,r)\right]\right)\cdot\ln(1-P_i(\Delta T)).$$

Для применения предложенной математической модели необходимо построение в том или ином виде:

1) каталога решаемых ИС функциональных задач, в котором должна содержаться информация об использовании всех идентифицируемых в ИС информационных ресурсов решаемыми в ней функциональными задачами либо для каждой функциональной задачи должен быть дан перечень используемых ею ресурсов;

2) каталога информационных ресурсов ИС, в котором должна быть указана следующая информация: для каждого информационного ресурса r и для каждой функциональной задачи, в которой он используется, должны быть приведены оценки величины ущерба от нарушения его безопасности: $e_i^{\text{Д}}(x,r)$, $e_i^{\text{Ц}}(x,r)$, $e_i^{\text{К}}(x,r)$, а также полная стоимость информационного ресурса r для функциональной задачи x, т. е. $e(x,r)=\max\limits_{\mathbf{Z}=\{\text{Д},\text{Ц},\text{К}\}}\lim\limits_{\Delta T\to\infty} e_i^{\mathbf{Z}}(x,r,\Delta T,d^{\mathbf{Z}})$. В целях упрощения процедур оценки возможного ущерба оценки ущерба и стоимости информационных ресурсов могут совпадать как для различных (или даже для всех) функциональных задач, так и для различных аспектов безопасности.

4. Условие снижения величины ожидаемого ущерба

Из предложенной модели оценки возможного ущерба от реализации НС выводится условие снижения ожидаемого ущерба от нарушений информационной безопасности на этапе эксплуатации ИС.

Ожидаемый ущерб от нарушения безопасности информационных ресурсов ИС для множества НС $\mathbf{O}^*$, множества функциональных задач X^* и множества используемых ими информационных ресурсов R^* будет ниже ожидаемого ущерба от нарушения безопасности информационных ресурсов ИС для множества НС $\mathbf{O}$, множества функциональных задач X и множества используемых ими информационных ресурсов R, если

$$-\sum_{i\in\mathbf{O}^*}\sum_{x^*\in X^*}\sum_{r\in R^{x^*}}\left(\mathbf{M}\left[e_i\left(x^*,r\right)\right]\ln(1-P_i(\Delta T))\right)<-\sum_{i\in\mathbf{O}}\sum_{x\in X}\sum_{r\in R^x}\left(\mathbf{M}[e_i(x,r)]\cdot\ln(1-P_i(\Delta T))\right),$$

где $R^{x^*}\subseteq R^*$ — множества информационных ресурсов, используемые функциональными задачами x^*, $R^x\subseteq R$ — множества информационных ресурсов, используемые функциональными задачами x.

Обозначим $S_i=-\ln(1-P_i(\Delta T))$. Всегда выполняется условие:

$$S_i=-\ln(1-P_i(\Delta T))=\ln\frac{1}{1-P_i(\Delta T)}\geq 0$$

и, кроме того, $e_i(x,r)\geq 0$, $e_i\left(x^*,r\right)\geq 0$.

Поэтому

$$\sum_{i\in\mathbf{O}^*}S_i\sum_{x^*\in X^*}\sum_{r\in R^{x^*}}\mathbf{M}\left[e_i\left(x^*,r\right)\right]<\sum_{i\in\mathbf{O}}S_i\sum_{x\in X}\sum_{r\in R^x}\mathbf{M}[e_i(x,r)] \qquad (1)$$

что и является условием снижения величины ожидаемого ущерба.

5. Пути реализации условия снижения ожидаемого ущерба

Рассмотрим возможные пути реализации полученного условия.

1. Выполнение условия (1) будет, в частности, обеспечено, если

$$\sum_{x^* \in X^*} \sum_{r \in R^{x^*}} \mathbf{M}\left[e_i(x^*, r)\right] < \sum_{x \in X} \sum_{r \in R^x} \mathbf{M}\left[e_i(x, r)\right]$$

для $i \in I^* = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\} = I$ и

$$\sum_{x^* \in X^*} \sum_{r \in R^{x^*}} \mathbf{M}\left[e_i(x^*, r)\right] = \sum_{x \in X} \sum_{r \in R^x} \mathbf{M}\left[e_i(x, r)\right]$$

для $i \in I \setminus I^*$, т. е. для некоторого подмножества угроз должны быть приняты меры, позволяющие уменьшить суммарный размер ожидаемого ущерба для нового множества функциональных задач X^* по сравнению с множеством функциональных задач X, а для остальных меры обеспечения безопасности могут быть оставлены без изменений.

2. Выполнение условия (1) также может быть обеспечено, если

$$\sum_{y^* \in Y^*} \sum_{r \in R^{y^*}} \mathbf{M}\left[e_i^{\text{Д}}(y^*, r)\right] < \sum_{y \in Y} \sum_{r \in R^y} \mathbf{M}\left[e_i^{\text{Д}}(y, r)\right],$$

или

$$\sum_{y^* \in Y^*} \sum_{r \in R^{y^*}} \mathbf{M}\left[e_i^{\text{Ц}}(y^*, r)\right] < \sum_{y \in Y} \sum_{r \in R^y} \mathbf{M}\left[e_i^{\text{Ц}}(y, r)\right],$$

или

$$\sum_{y^* \in Y^*} \sum_{r \in R^{y^*}} \mathbf{M}\left[e_i^{\text{К}}(y^*, r)\right] < \sum_{y \in Y} \sum_{r \in R^y} \mathbf{M}\left[e_i^{\text{К}}(y, r)\right]$$

для $y \in Y \subseteq X$, $y^* \in Y^* \subseteq X^*$, т. е. для некоторого подмножества функциональных задач должны быть приняты меры, позволяющие уменьшить размер ожидаемого ущерба от НС, приводящих к утрате доступности и (или) целостности и (или) конфиденциальности.

3. Выполнение условия (1) будет обеспечено, если

$$\sum_{r \in R'} \mathbf{M}\left[e_i(x', r)\right] < \sum_{x \in X} \sum_{r \in R^x} \mathbf{M}\left[e_i(x, r)\right]$$

для $i \in I^* \subseteq I$, $R' \subseteq R^x$ и

$$\sum_{r \in R'} \mathbf{M}\left[e_i(x', r)\right] = \sum_{x \in X} \sum_{r \in R^x} \mathbf{M}\left[e_i(x, r)\right]$$

для $i \in I \setminus I^*$, $R' \subseteq R^x$, т. е. если множество X функциональных задач заменяется одной функциональной задачей x', иными словами, происходит интеграция процессов обработки данных при условии, что величина возможного ущерба и полная стоимость информационных ресурсов для интегрированного процесса не превышают суммарной величины ущерба и полной стоимости информационных ресурсов для совокупности исходных функциональных задач.

4. Возможна комбинация трех перечисленных выше путей.

Таким образом, намечаются пути снижения величины возможного ущерба от реализации угроз:

· введение в ИС средств повышения доступности, позволяющих снизить ущерб от НС, которые приводят к утрате доступности информационных ресурсов, либо уменьшить вероятность реализации НС, либо сократить множество таких НС;

· введение в ИС средств, позволяющих достичь аналогичного результата в отношении целостности информационных ресурсов;

· введение в ИС средств, позволяющих достичь аналогичного результата в отношении конфиденциальности информационных ресурсов;

· сокращение множества угроз за счет реализации дополнительных мер и механизмов защиты;

· перестройка процессов обработки данных, реализующих множество решаемых системой функциональных задач, в частности их интеграция при принятии мер, гарантирующих, что величина

возможного ущерба и полная стоимость информационных ресурсов для интегрированного процесса не превышают суммарной величины ущерба и полной стоимости информационных ресурсов для совокупности исходных функциональных задач.

Заключение

В работе обоснована и предложена модель методической оценки возможного ущерба при реализации неблагоприятных событий для информационных ресурсов компьютерных систем, что позволило выявить условия снижения возможного ущерба и определить пути реализации этих условий, в частности, за счет применения специальных стратегий управления информационными ресурсами и специальных методов обеспечения безопасности информационных ресурсов в условиях частичного разрушения системы. Полученные результаты представляют интерес для системных аналитиков и архитекторов, решающих задачи анализа, структурно-параметрического синтеза и оптимизации компьютерных систем в части обеспечения безопасности их информационных ресурсов.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. 2008.
2. Risk management: Implementation principles and inventories for risk management / risk assessment methods and tools. ENISA (European Network and Information Security Agency). 2006.
3. IEC 61882:2001. Hazard and operability studies (HAZOP studies). Application guide. 2001.
4. ГОСТ Р 51901.11-2005 (МЭК 61882:2001). Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство. М.: Стандартинформ, 2006.
5. *Vose D*. Risk analysis: a quantitative guide. 3rd edition. John Wiley & Sons, 2008. — 752 p.
6. *Soo Hoo K*. How much is enough? A risk-management approach to computer security [электронный ресурс]. PhD thesis. Stanford University, 2001. — 99 p. Режим доступа: http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.
7. *Kumamoto H., Henley E*. Probabilistic risk assessment and management for engineers and scientists. 2nd edition. Institute of Electrical and Electronics Engineers. Inc. New York, 1996. — 620 p.