УДК 004.056
DOI: 10.15827/0236-235X.123.565-568

Дата подачи статьи: 21.09.17
2018. Т. 31. № 3. С. 565–568

# *Алгоритм оценки значения остаточных рисков угроз информационной безопасности с учетом разделения механизмов защиты на типы*

*Д.А. Дерендяев* [1], *аспирант, od@mail.ifmo.ru*
*Ю.А. Гатчин* [1], *д.т.н., профессор, od@mail.ifmo.ru*
*В.А. Безруков* [1], *к.т.н., доцент, od@mail.ifmo.ru*

[1] *Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО), г. Санкт-Петербург, 197101, Россия*

На основе анализа современных подходов к оценке риска реализации угроз информационной безопасности можно сделать вывод, что большинство из них не рассматривают разделение механизмов защиты на типы, которое позволило бы более качественно проанализировать существующую систему защиты на предприятии.

Представленный алгоритм учитывает такое разделение и рассматривает каждый тип с упором на его особенности. Ввиду отсутствия четкого разграничения механизмов защиты предложено разделить их на две группы: технические и организационные. Для расчета остаточного риска учитываются дополнительные переменные, такие как вероятность корректной работы механизма защиты и вероятность преодоления механизма при реализации угрозы.

Для технических механизмов защиты необходимо учитывать вероятность перехода в неработоспособное состояние с течением времени. Рассматривая организационные меры, стоит принять во внимание истечение ее срока действия или изменение в связи с меняющимися условиями. Ввиду случайного характера таких процессов для определения их вероятностей используются математические аппараты скрытой марковской модели и случайных марковских процессов. Итоговый показатель остаточного риска определяется с помощью альтернативной математической модели, полученной на основе полного факторного эксперимента и позволяющей получить более корректные значения, рассматривая входные параметры на верхнем и нижнем уровнях.

В результате реализации алгоритма определяются значения остаточных рисков с учетом противодействия угрозе каждого из типов защитных мер, что дает возможность более четко определять недостатки системы защиты.

***Ключевые слова:*** *оценка остаточного риска, информационная безопасность, типы механизмов защиты, скрытые марковские модели, случайные марковские процессы.*

Существует большое количество нормативных документов, регламентирующих процесс оценки рисков (BSI, BS7799, ISO/IEC 27001), и методик, которые включают в себя определение значений остаточного риска (CRAMM, Risk Watch, ГРИФ и др. [1–4]). Проанализировав существующие подходы, можно сделать вывод об отсутствии в большинстве случаев разделения механизмов защиты на типы при расчете значений остаточных рисков. Представленный алгоритм исключает этот недостаток и рассматривает каждый тип с учетом его индивидуальных особенностей.

Разработанный алгоритм включает в себя определение вероятности корректной работы каждого из типов механизмов защиты, а также для более корректного определения значения остаточных рисков рассчитывается вероятность преодоления механизма защиты при реализации угрозы. Так как вероятность этих событий носит случайный характер, для их определения используются математические аппараты *скрытых марковских моделей* (СММ) и случайных марковских процессов [5].

Все механизмы защиты разделены на две группы – технические и организационные.

## Определение вероятности корректной работы механизмов защиты

Для каждого типа составляется ориентированный граф, на основании которого строится система уравнений Колмогорова и определяется значение вероятностей каждого состояния. При расчетах для технических механизмов защиты, как и для любого оборудования, необходимо учитывать вероятность перехода в неработоспособное состояние с течением времени. Пример графа для технических механизмов защиты представлен на рисунке 1.

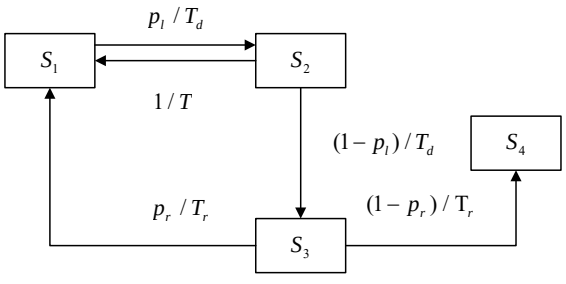


*Рис. 1. Ориентированный граф состояний технических механизмов защиты: $S_1$ – работоспособное состояние; $S_2$ – диагностика; $S_3$ – ремонт; $S_4$ – неработоспособное состояние механизма; $T$ – среднее время до проведения диагностики; $T_d$ – среднее время диагностики; $T_r$ – среднее время ремонта; $p_r$ – вероятность успешного ремонта; $p_l$ – вероятность корректного состояния механизма*

*Fig. 1. A oriented state graph of technical protection mechanisms*

На основе графа получим систему уравнений Колмогорова:

$$\begin{cases} P_1^{`}(t) = \dfrac{P_2(t)*p_l}{T_d} + \dfrac{P_3(t)*p_r}{T_r} - \dfrac{P_1(t)}{T}; \\ P_2^{`}(t) = \dfrac{P_1(t)}{T} - \dfrac{P_2(t)}{T_d}; \\ P_3^{`}(t) = \dfrac{(1-p_l)*P_2(t)}{T_d} - \dfrac{P_3(t)}{T_r}; \\ P_4^{`}(t) = \dfrac{(1-p_r)*P_3(t)}{T_r}. \end{cases}$$

Рассматривая организационные механизмы защиты, необходимо учитывать истечение срока действия механизма и его изменения в связи с меняющимися условиями. Пример графа для организационных механизмов защиты представлен на рисунке 2.

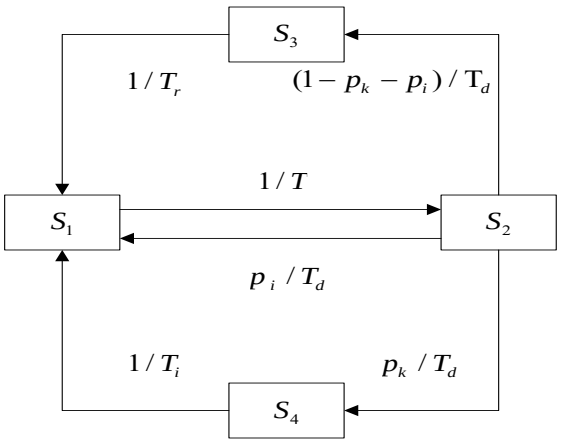


*Рис. 2. Ориентированный граф работоспособного состояния организационных механизмов защиты: $S_1$ – работоспособное состояние; $S_2$ – диагностика; $S_3$ – обновление существующего механизма; $S_4$ – доработка механизма; $T$ – среднее время до проведения диагностики; $T_d$ – среднее время диагностики; $T_r$ – среднее время обновления существующего механизма; $T_i$ – среднее время доработки механизма; $p_r$ – вероятность корректного состояния механизма; $p_l$ – вероятность необходимости доработки механизма*

*Fig. 2. An oriented graph of the operational state of organizational protection mechanisms*

Система уравнений Колмогорова на основе графа:

$$\begin{cases} P_1^{`}(t) = \dfrac{P_2(t)*p_l}{T_d} + \dfrac{P_3(t)}{T_r} + \dfrac{P_4(t)}{T_i} - \dfrac{P_1(t)}{T}; \\ P_2^{`}(t) = \dfrac{P_1(t)}{T} - \dfrac{P_2(t)}{T_d}; \\ P_3^{`}(t) = \dfrac{(1-p_l-p_k)*P_2(t)}{T_d} - \dfrac{P_3(t)}{T_r}; \\ P_4^{`}(t) = \dfrac{p_k*P_2(t)}{T_d} - \dfrac{P_4(t)}{T_i}. \end{cases}$$

## Определение вероятности преодоления механизма защиты конкретного типа

Вероятность преодоления механизма защиты конкретного типа определяется с помощью СММ. В этом случае модель будет состоять из двух состояний, соответствующих вероятности преодоления технических или организационных мер (рис. 3).

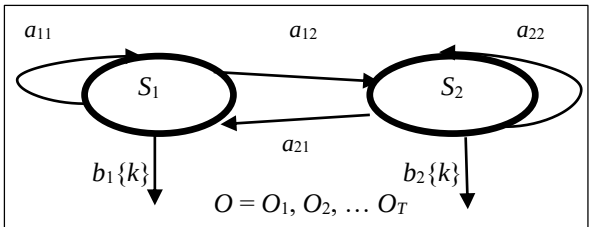


*Рис. 3. Графическое изображение СММ для двух состояний*

*Fig. 3. Graphical representation of hidden Markov models for two states*

Модель включает в себя $S_1/S_2$ – состояние модели (преодоление технических/организационных мер защиты); $O = O_1, O_2, \ldots O_T$ – наблюдаемая последовательность, генерируемая моделью, соответствующая инцидентам информационной безопасности; $b_j\{k\}$ – вероятность того, что в определенный момент времени система, находящаяся в $j$-м состоянии, выдаст $k$-й символ; $a_{ij}$ – вероятность состояний системы и переходов между ними.

Изначальные характеристики модели определяются экспертным путем, для корректности которого в методе добавлены определение наиболее критичного фактора и расчет коэффициента его влияния [6–9]. При этом полученные факторы проходят проверку в соответствии с алгоритмом, представленным на рисунке 4.

Идея алгоритма заключается в определении коэффициентов математической модели остаточного риска от угрозы в целом, под действием наиболее критичного фактора и под действием остальных факторов. Сами коэффициенты рассчитываются с помощью математического аппарата полного факторного эксперимента [10]. Фактор проходит проверку в случае выполнения условия $a_i < a_{i_c} < a_{i_o}$, где $a_i$ – коэффициенты модели остаточного риска от угрозы в целом; $a_{i_c}$ – коэффициенты модели остаточного риска под действием наиболее критичного фактора; $a_{i_o}$ – коэффициенты модели остаточного риска под действием остальных факторов.

Для получения более точных значений вероятностей с помощью СММ необходимо решить задачу обучения, которая заключается в подстройке параметров модели, для получения значений вероятности наиболее соответствующих наблюдаемой последовательности. Для ее решения используется алгоритм Баума–Уэлча [5].

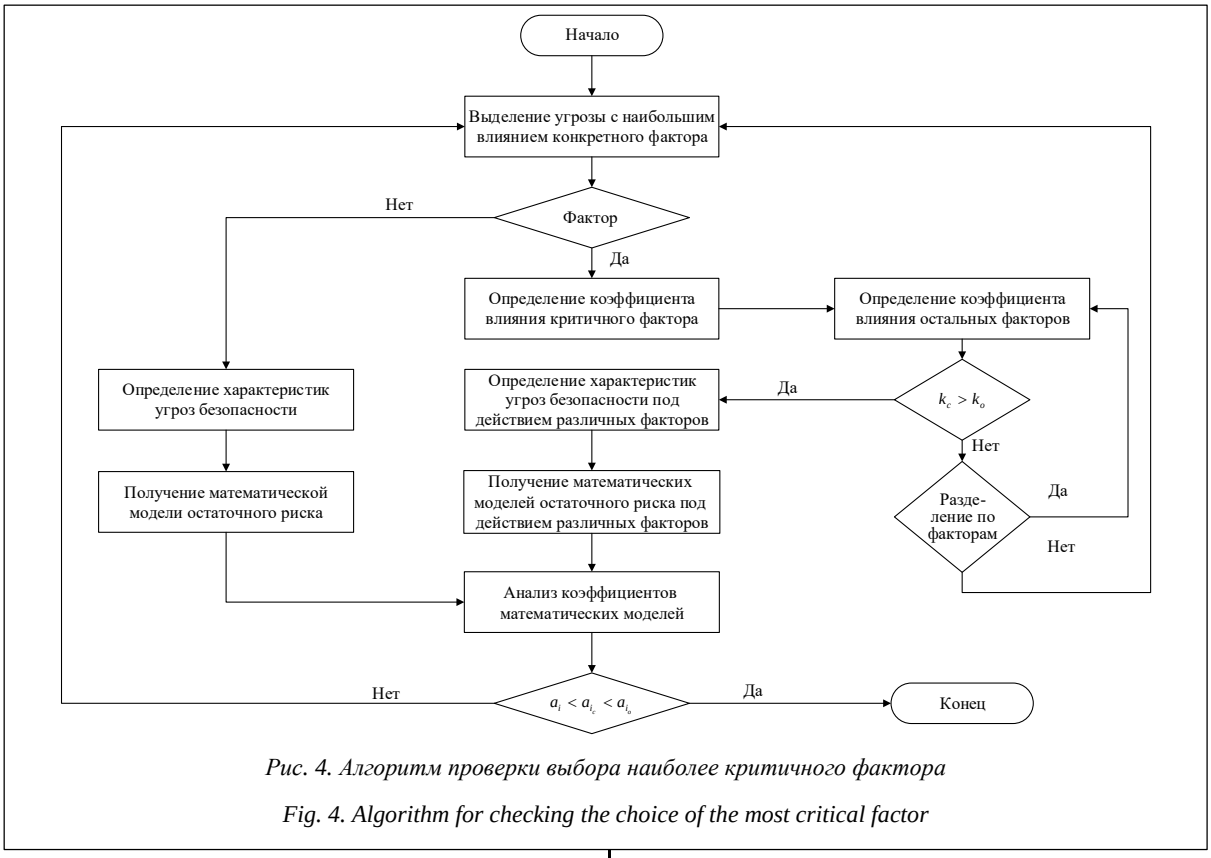


*Рис. 4. Алгоритм проверки выбора наиболее критичного фактора*

*Fig. 4. Algorithm for checking the choice of the most critical factor*

Переоценка параметров модели происходит по следующим формулам: $\overline{\pi} = \gamma_t(i)$, $\overline{a_{ij}} = \frac{\sum_{t=1}^{T-1} \xi_t(i, j)}{\sum_{t=1}^{T-1} \gamma_t(i)}$, $\overline{\beta}_j(k) = \frac{\sum_{t=1}^{T} \gamma_t(j) \text{ при } O_1 = v_k}{\sum_{t=1}^{T} \gamma_t(j)}$, где $\xi_t(i, j)$ – вероятность того, что при заданной последовательности наблюдений в моменты времени $t$ и $t + 1$ система будет находиться в состояниях $S_i$ и $S_j$ соответственно; $\gamma_t(i)$ – вероятность пребывания модели в момент $t$ в состоянии $S_i$ при заданной последовательности наблюдений.

После определения необходимых параметров рассчитывается значение остаточного риска с помощью математической модели, полученной на основе полного факторного эксперимента, который позволяет учесть входные параметры на верхнем и нижнем уровнях, что дает возможность уменьшить вероятность ошибки экспертной оценки [11–14].

## Заключение

Разработанный алгоритм позволяет определять значение остаточного риска для угроз информационной безопасности с учетом разделения механизмов защиты на типы, что в дальнейшем может помочь более качественно анализировать существующую систему защиты на предприятии и, возможно, позволит более качественно определять комплекс мер защиты конкретного типа при противодействии угрозам.

### *Литература*

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. ISO, 2013, 30 p.

2. BS 7799-2:2002. Information security management. Specification with guidance for use. BSI, 2002, 38 p.

3. BSI Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz. BSI, 2008, 23 p.

4. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. № 1. С. 73–79.

5. Rabiner L. A tutorial on hidden markov models and selected applications in speech recognition. Proc. of IEEE, 1989. Т. 77. № 2. С. 86–120.

6. Дерендяев Д.А., Гатчин Ю.А., Безруков В.А. Математическая модель оценки коэффициента влияния отдельно взятого фактора на угрозы информационной безопасности // Кибернетика и программирование. 2016. № 5. С. 222–227.

7. Гатчин Ю.А., Жаринов И.О., Коробейников А.Г. Математические модели оценки инфраструктуры системы защиты информации на предприятии // Науч.-технич. вестн. информ. технологий, механики и оптики. 2012. № 2. С. 92–95.

8. Гришина Н.В. Организация комплексной системы защиты информации. М.: Гелиос АРВ, 2007. 256 с.

9. Berr J. Computer security's weak link: Humans. 2015. URL: http://www.cbsnews.com/news/the-human-element-and-computer-security (дата обращения: 19.09.17).

10. Дерендяев Д.А., Безруков В.А. Алгоритм определения фактора, оказывающего наиболее критичное влияние на угрозы

информационной безопасности // XVII Междунар. науч.-практич. конф.: сб. стат. М.: Интернаука, 2016. № 15. С. 97–102.

11. Дерендяев Д.А., Гатчин Ю.А., Безруков В.А. Алгоритм представления математической модели остаточного риска // Кибернетика и программирование. 2016. № 4. С. 81–85.

12. Goel S., Chen V. Information security risk analysis – a matrix-based approach. 2005. URL: http://www.albany.edu/~goel/publications/goelchen2005.pdf (дата обращения: 19.09.17).

13. Lee M.C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. IJCSIT, 2014, vol. 6, no. 1. URL: http://www.airccse.org/journal/jcsit/6114ijcsit03.pdf (дата обращения: 19.09.17).

14. Варфоломеев А.А. Управление информационными рисками. М.: РУДН, 2008. 158 с.

Software & Systems
DOI: 10.15827/0236-235X.123.565-568

Received 21.09.17
2018, vol. 31, no. 3, pp. 565–568

## An algorithm of information security residual risk assessment taking into account a protection mechanisms separation by types

***D.A. Derendyaev*** [1], *Postgraduate Student, od@mail.ifmo.ru*
***Yu.A. Gatchin*** [1], *Dr.Sc. (Engineering), Professor, od@mail.ifmo.ru*
***V.A. Bezrukov*** [1], *Ph.D. (Engineering), Associate Professor, od@mail.ifmo.ru*

[1] *The National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, 197101, Russian Federation*

**Abstract.** Analyzing modern approaches to assessing the risk of information security threats, the authors conclude that most of these approaches do not consider protection mechanisms separation by types, which would allow a better analysis of the existing protection system in an enterprise.

The presented algorithm takes into account such separation and considers each type with an emphasis on its features. Due to the absence of clear separation of protection mechanisms, it is proposed to divide them into two groups: technical and organizational. To calculate residual risk, the authors taken into account additional variables, such as a possibility of the correct operation of the protection mechanism and the possibility of overcoming the mechanism in threat materializing.

Technical protection mechanisms reqiire taking into account the probability of transition to an inoperative state over time. Considering organizational measures, it is worth considering an expiration of its validity or its changing due to changing conditions. Such processes have random nature, therefore the mathematical apparatuses of the hidden Markov model and random Markov processes are used to determine their probabilities. The final indicator of residual risk is determined using an alternative mathematical model obtained after a full factorial experiment. This model allows obtaining more correct values as it considers input parameters at upper and lower levels.

As a result of the algorithm implementation, the values of residual risks are determined taking into account counteraction to the threat of each type of protective measures, which allows identifying the disadvantages of the protection system more precisely.

**Keywords:** residual risk assessment, information security, types of protection mechanisms, hidden Markov models, random Markov processes.

***References***

1. *ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems*. Requirements. 2013, 30 p.

2. *BS 7799-2:2002. Information security management. Specification with guidance for use*. BSI Publ., 2002, 38 p.

3. *BSI Standard 100-3. Risikoanalyse auf der Basis von IT-Grundschutz*. BSI Publ., 2008, 23 p.

4. Baranova E.K. Methods of analysis and assessment of information security risks. *Educational Resources and Technologies*. 2015, no. 1, pp. 73–79 (in Russ.).

5. Rabiner L. A tutorial on hidden markov models and selected applications in speech recognition. *Proc. of IEEE*. 1989, vol. 77, no. 2, pp. 86–120

6. Derendyaev D.A., Gatchin Yu.A., Bezrukov V.A. A mathematical model for estimating the coefficient of an individual factor influence on information security threats. *Cybernetics and Programming*. 2016, no. 5, pp. 222–227 (in Russ.).

7. Gatchin Yu.A., Zharinov I.O., Korobeynikov A.G. Mathematical models of an estimation of an infrastructure of an information security system at the enterprise. *Sci. and Tech. J. of Information Technologies, Mechanics and Optics*. 2012, no. 2, pp. 92–95 (in Russ.).

8. Grishina N.V. *Organization of a Comprehensive Information Security System*. Moscow, Gelios ARV Publ., 2007, 256 p.

9. Berr J. Computer security's weak link: Humans. J. Berr. *CBS News*. 2015, no. 04. Available at: http://www.cbsnews.com/news/the-human-element-and-computer-security (accessed September 19, 2017).

10. Derendyaev D.A., Bezrukov V.A. An algorithm for determining the factor that has the most critical impact on information security threats. *Proc. 17th Intern. Sci. and Pract. Conf*. Moscow, Internauka Publ., 2016, no. 15, pp. 97–102 (in Russ.).

11. Derendyaev D.A., Gatchin Ya.A., Bezrukov V.A. An algorithm for representing the mathematical model of residual risk. *Cybernetics and Programming*. 2016, no. 4, pp. 81–85 (in Russ.).

12. Goel S., Chen V. *Information Security Risk Analysis – a Matrix-Based Approach*. 2005. Available at: http://www.albany.edu/~goel/publications/goelchen2005.pdf (accessed September 19, 2017).

13. Lee M.C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *IJCSIT*. 2014, vol. 6, no. 1. Available at: http://www.airccse.org/journal/jcsit/6114ijcsit03.pdf (accessed September 19, 2017).

14. Varfolomeev A.A. *Information Risk Management*. Moscow, RUDN Publ., 2008, 158 p.