Оценка информационных рисков на основе экспертной информации (на примере ГБУЗ АО «Центр медицинской профилактики»)

О.Н. Выборнова, Н.В. Давидюк, К.Л. Кравченко

Астраханский государственный технический университет

Аннотация: В настоящее время особенно актуальными, в том числе для медицинских учреждений, становятся риски, связанные с нарушением свойств безопасности информации. В данной работе описана методика оценки информационных рисков, включающая в себя: алгоритм оценки приемлемого риска, нечеткую когнитивную модель и алгоритм экспертной оценки текущих рисков. Предложенная модель и алгоритм оценки текущих рисков позволяют на координатной плоскости «ущерб-вероятность» определить множество точек, характеризующих текущий уровень информационных рисков. Основное отличие описанной методики от уже существующих – это учет значимости актива для деятельности организации, что в конечном итоге позволит принять обоснованные управленческие решения. Проведена апробация предложенной методики в ГБУЗ АО «Центр медицинской профилактики»: построена кривая приемлемого риска, оценены текущие (актуальные) информационные риски. Результаты оценки в дальнейшем были использованы для выработки управленческих решений по снижению рисков до приемлемых значений.

Ключевые слова: оценка информационных рисков, приемлемый риск, текущий риск, нечеткая когнитивная модель, информационный актив, экспертная информация, центр медицинской профилактики.

Введение

Любая деятельность в той или иной мере подвержена рискам. Поскольку информация является ценным активом практически в каждой организации, особенно актуальными в настоящее время становятся риски, связанные с нарушением свойств безопасности информации (конфиденциальности, целостности, доступности и т.д.) в процессе ее обработки – информационные риски [1, 2].

Это утверждение справедливо и для медицинских учреждений, в которых информационные технологии применяются для регистрации сведений о пациентах, а также используются в процессах диагностики и лечения.

От уровня информационной безопасности в значительной степени зависит нормальное функционирование любой организации, а случае

медицинских учреждений – часто даже жизнь пациента. Таким образом, необходима корректная оценка информационных рисков.

Исходя из этого, **цель данной работы**: предложить методику оценки информационных рисков в медицинских учреждениях и апробировать ее на примере ГБУЗ АО «Центр медицинской профилактики».

Описание методики оценки рисков

Оценка информационных рисков включает в себя: оценку приемлемого и текущих (актуальных) рисков и определение степени приемлемости текущих значений. В работе [3] был предложен алгоритм оценки приемлемого риска.

Для определения величины приемлемого риска экспертами организации задается массив значений «ущерб-вероятность» $\{(U_i;\ P_i^*)\}$ (опорные точки для построения кривой приемлемого риска (КПР)). Затем полученные значения аппроксимируются непрерывной функцией вида

$$P^* = a \cdot exp\,(-b \cdot (U - U^{нз}), \qquad (1)$$

где a и b – некоторые константы: a – соответствует вероятности, с которой допускается возникновение незначимого ущерба $U^{нз}$; b – определяет скорость падения допустимой вероятности принятия ущерба по мере приближения к критическому ущербу $U^{кр}$. После построения КПР суммарная величина приемлемого риска находится по формуле:

$$R^{пр} = \left[\int_{U^{нз}}^{U^{кр}} P^*(U)dU\right] / (U^{кр} - U^{нз}). \qquad (2)$$

Знаменатель в формуле (2) отражает площадь зоны толерантного риска (ЗТР) – предельного уровня риска, который организация может выдержать без значительного ущерба для своей финансовой и конкурентной позиции. Деление на площадь ЗТР позволяет нормировать степень риска по

отношению к критическому значению. Более подробное описание данной методики представлено в работе [3].

Для оценки текущих информационных рисков предлагается построить нечеткую когнитивную модель (НКМ), представленную кортежем:

$$RSK = <G, QL, \{\alpha_{ij}\}, R, Def>, \quad (3)$$

где G – нечеткий когнитивный граф; QL = {*Низкий* (*Н*); *Ниже среднего* (*НС*); *Средний* (*С*); *Выше среднего* (*ВС*); *Высокий* (*В*)} – терм-множество лингвистических оценок значений параметров с нечетким классификатором {«*Н*» (0; 0; 0,15; 0,25); «*НС*» (0,15; 0,25; 0,35; 0,45); «*С*» (0,35; 0,45; 0,55; 0,65); «*ВС*» (0,55; 0,65; 0,75; 0,85); «*В*» (0,75; 0,85; 1; 1)}; $\{\alpha_{ij}\}$ – множество весов ребер графа G; R – множество правил агрегирования влияния различных концептов нижнего уровня на концепт верхнего уровня; $Def(A) = (a_2 + a_3) / 2$ – функция дефаззификации нечетких значений $A(a_1, a_2, a_3, a_4)$, полученных в результате вычислений по НКМ, a_2 и a_3 – абсциссы верхнего основания трапеции. При этом граф G включает в себя следующие уровни: нижний, 7-й – негативные события (НС); 6-й – угрозы активам, порождаемые НС; 5-й – защитные меры (ЗМ); 4-й – атаки (угрозы, прошедшие через ЗМ); 3-й – риски для информационных активов (ИА) (вероятное ухудшение состояния активов организации); 2-й – риски для подпроцессов (ПП) основных процессов организации; 1-й – риски для основных процессов (ОП) организации (вероятное снижение качества выполнения ОП); 0-й – риски для организации в целом [4, 5].

Формирование НКМ включает в себя следующие шаги:

1. Выявление ОП обработки информации организации и присвоение им весов.
2. Выделение (при необходимости) ПП в ОП и присвоение им весов.
3. Выявление перечня активов и присвоение им весов.

При определении весов ОП учитывается их вклад в деятельность организации (например, доля прибыли, приходящаяся на бизнес-процесс). Для присвоения весов подпроцессам используется предложенный в работах [4, 6] метод нестрого ранжирования, который позволяет находить искомые оценки в виде обобщенных весов Фишберна. Таким образом, веса ОП и ПП являются нормированными.

Веса активов в подпроцессе определяются как чувствительность ПП к выходу из строя данного актива и могут принимать значения от 0 до 1.

Вычисление рисков включает в себя следующие шаги:

1. Определение потенциальных НС.
2. Определение угроз, которые могут быть порождены НС, оценивание их интенсивности I_i и вероятности возникновения P_{I_i}. При этом под интенсивностью понимается потенциальный ущерб, который может быть вызван угрозой.
3. Оценивание эффективности воздействия защитных мер (ЗМ) на интенсивность Z_{I_i} и вероятность $Z_{P_{I_i}}$ возникновения угрозы.
4. Вычисление ущерба от воздействия атак (угроз, прошедших через ЗМ) на активы (рисков активам).
5. Для каждого ПП на основе значений, полученных на шаге 4, ущерб вычисляется по формуле:

$$U_i^{k,j} = \alpha_i^{k,j} U_i^{k+1,j}, \qquad (4)$$

где $U_i^{k,j}$ – i-й ущерб j-му концепту k-го уровня НКМ; $\alpha_i^{k,j}$ – весовой коэффициент, отражающий влияние i-го ущерба концепта (k+1)-го уровня на j-й концепт k-го уровня НКМ; $U_i^{k+1,j}$ – ущерб, нанесенный i-му концепту (k+1)-го уровня НКМ, влияющему на j-й концепт k-го уровня; $k \in \{0; 1; 2\}$.

6. Аналогично (по формуле (4) при $k = 1$) определяются уровни снижения качества основных процессов. При этом на этапах 5 и 6 вероятности атак остаются неизменными (вычисленными на шаге 4).

7. Вычисляются риски организации в целом по формуле (4) при $k = 0$. В результате получается множество точек, характеризующих текущие показатели риска для организации в целом, где $i = 1...N$; N – количество значений возможного ущерба.

Суммарное значение текущего риска находится по формуле:

$$R^{тек} = \left[\sum_{i=1}^{N}(\Delta U_i \cdot P_i)\right] / (U^{кр} - U^{из}), \quad (5)$$

где $\Delta U_i = U_i - U_{i\text{-}1}$; точки отсортированы по возрастанию величины ущерба; $U_0 = U^{из}$. Деление на площадь ЗТР и последующий перевод полученных значений $R^{тек}$ в вербальную оценку по шкале Харрингтона [7] позволяет классифицировать степень опасности текущих рисков.

При этом если хотя бы одна из точек, описывающих текущее состояние риска, находится выше КПР, необходимо принять меры по снижению риска до приемлемого уровня.

Апробация методики

Описанная выше методика была апробирована в государственном бюджетном учреждении здравоохранения Астраханской области «Центр медицинской профилактики» (ГБУЗ АО «ЦМП»).

Деятельность ГБУЗ АО «ЦМП» включают в себя следующие направления [8]:

– формирование здорового образа жизни;

– совершенствование медицинских мер профилактики неинфекционных заболеваний, организация и методическое сопровождение диспансеризации и профилактических медицинских осмотров населения Астраханской области;

– лечебно-оздоровительную деятельность.

В организации были выделены три основных процесса: «Лечение», «Диагностика» и «Профилактика». В рамках этих ОП были рассмотрены процессы обработки информации, выявлены информационные активы, обеспечивающие их функционирование. Была построена кривая приемлемого риска и в соответствии с построенной НКМ оценены текущие (актуальные) информационные риски.

В качестве примера оценки текущих рисков рассмотрим информационный актив «Сервер регистратуры», участвующий в процессе обработки данных о пациентах в рамках всех трёх ОП организации.

Эксперты составили перечень НС, которые могут породить угрозы данному активу: перепады напряжения, заражение вредоносным программным обеспечением (ПО) и т.д. При этом заданным лингвистически значениям ущерба были поставлены в соответствие трапециевидные числа, а для перехода от вербальных оценок вероятностей к численным значениям использована шкала Харрингтона (ШХ) [7]. Вероятность возникновения НС «Заражение вредоносным ПО» была оценена экспертами нечетким числом (НЧ) «выше среднего». Согласно ШХ данному значению была поставлена в соответствие вероятность 0,71.

Указанное НС порождает: угрозу утраты данных на сервере регистратуры (угроза 1), интенсивность которой была оценена как «высокая» (ей поставлено в соответствие трапециевидное число (0,75; 0,85; 1,0; 1,0)), вероятность была оценена как «средняя» (согласно шкале Харрингтона – 0,51); угрозу утраты доступа к данным на сервере регистратуры (угроза 2) с интенсивностью – «высокая» и вероятностью – «выше среднего» (согласно ШХ – 0,71). С учетов вероятности возникновения НС вероятность возникновения указанных угроз составляет 0,36 (0,71·0,51) и 0,5 (0,71·0,71) соответственно. Аналогичные оценки были получены для других угроз, а

также для других информационных активов (ИА), обеспечивающих процессы обработки информации в организации.

Против угрозы 1 не применено никаких защитных мер (ЗМ). Против угрозы 2 применена, в частности, защитная мера «Антивирусное ПО», эффективность которой по снижению вероятности угрозы 2 была оценена экспертами как «средняя» (0,51 по ШХ), т.е. применение данной ЗМ позволяет уменьшить вероятность утраты доступа к данным на сервере до величины $0,5 \cdot (1 – 0,51) = 0,25$. Эффективность рассматриваемой ЗМ по снижению интенсивности угрозы 2 была оценена как «выше среднего», т.е. применение этой ЗМ снижает ущерб от утраты доступа к данным на сервере до величины В · (1 – ВС) = НЧ (0,11; 0,21; 0,35; 0,45). Таким образом, риск активу «сервер регистратуры» в результате воздействия угрозы 1 оценивается ущербом, представленным трапециевидным числом (0,75; 0,85; 1,0; 1,0) и вероятностью 0,36; в результате воздействия угрозы 2 – ущербом (0,11; 0,21; 0,35; 0,45) и вероятностью 0,25. Эти значения были переданы на следующий уровень.

В результате, после аналогичных оценок влияния всех информационных активов, поддерживающих основные процессы обработки информации, было получено множество пар (трапециевидное НЧ; вероятность), характеризующих риски для организации. Далее была осуществлена дефаззификация полученных НЧ методом «центра тяжести» [9, 10]. Некоторые из полученных значений приведены на рисунке 1.

При этом, поскольку некоторые информационные активы задействованы в более чем одном ОП, риски для ИА повторно учитываются с учетом их весов в ОП (в этом случае каждой такой угрозе на координатной плоскости «ущерб – вероятность» соответствует более одной точки).

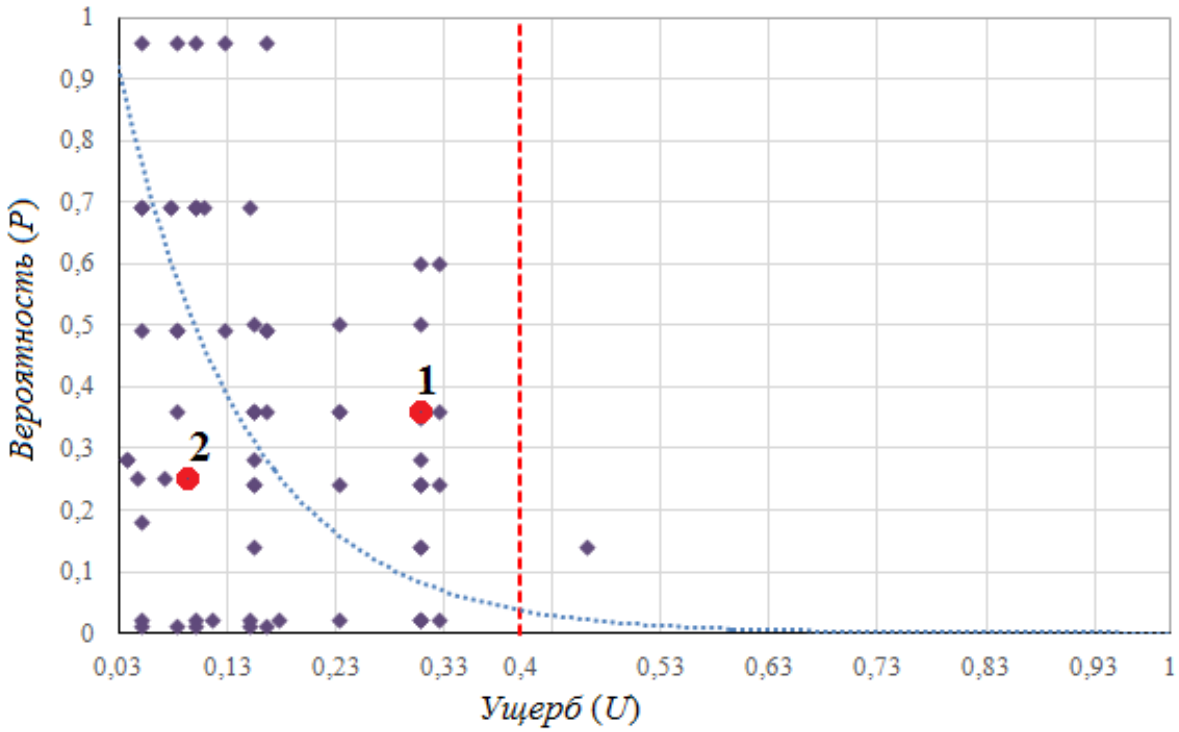

Рис. 1. – Результаты оценки текущих информационных рисков в ГБУЗ АО «Центр медицинской профилактики»

Точке 2 на рисунке 1 соответствует риск, связанный с угрозой 2. Точка лежит в зоне приемлемого риска. Точке 1 соответствует риск, связанный с угрозой 1. Точка лежит выше КПР – риск неприемлем.

Заключение

Таким образом, для оценки информационных рисков предложена методика, включающая в себя алгоритм определения приемлемого риска, нечеткую когнитивную модель и алгоритм оценки текущих (актуальных рисков) на основе экспертной информации.

В результате применения методики в ГБУЗ АО «ЦМП» выявлены актуальные риски. Полученные значения в дальнейшем были использованы для выработки управленческих решений по снижению рисков до приемлемых значений.

Литература

1. Абрамова Н. А. О проблеме рисков из-за человеческого фактора в экспертных методах и информационных технологиях. // Проблемы управления. 2007. №2 С. 11-21.

2. Why Information Risk is a Board-level Issue. URL: iaac.org.uk/media/1066/why-information-risk.pdf

3. Ажмухамедов И. М., Выборнова О. Н. Формализация понятий приемлемого и толерантного рисков. // Инженерный вестник Дона, 2015, № 3 URL: ivdon.ru/ru/magazine/archive/ n3y2015/3240.

4. Выборнова О. Н., Кравченко К. Л. Оценка рисков на основе экспертной информации. // Математические методы в технике и технологиях – ММТТ-29: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т. 4. / под общ. ред. А. А. Большакова. – Саратов: Саратов. гос. техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. С. 105-109.

5. Выборнова О. Н., Ажмухамедов И. М. Нечеткая когнитивная модель оценки актуальных рисков // Математические методы в технике и технологиях – ММТТ-29: сб. трудов XXIX Междунар. науч. конф.: в 12 т. Т. 2. / под общ. ред. А. А. Большакова. – Саратов: Саратов. гос. техн. ун-т; Санкт-Петербург: СПбГТИ(ТУ), СПбПУ, СПИИРАН; Самара: Самарск. гос. техн. ун-т, 2016. С. 182-186.

6. Проталинский О. М., Ажмухамедов И. М. Системный анализ и моделирование слабо структурированных и плохо формализуемых процессов в социотехнических системах // Инженерный вестник Дона, 2012, №3, URL: ivdon.ru/ru/magazine/archive/n3y2012/916.

7. Harrington E.C. The desirable function // Industrial Quality Control. 1965. V.21. №10. pp. 494-498.

8. Сайт ГБУЗ АО «Центр медицинской профилактики». URL: гбуз-ао-цмп.рф

9. Ротштейн А. П., Штовба С. Д. Влияние методов деффазификации на скорость настройки нечеткой модели // Кибернетика и системный анализ. 2002. № 1. С. 28-35.

10. Kosko B. Fuzzy systems as universal approximators // IEEE Transactions on Computers. November 1994. vol. 43, No. 11. pp. 1329-1333.

References

1. Abramova N. A. Problemy upravlenija. 2007. №2. pp. 11-21.

2. Why Information Risk is a Board-level Issue. URL: iaac.org.uk/media/1066/why-information-risk.pdf

3. Azhmuhamedov I. M., Vybornova O. N. Inženernyj vestnik Dona (Rus). 2015, №3 URL: ivdon.ru/ru/magazine/archive/ n3y2015/3240.

4. Vybornova O. N., Kravchenko K. L. Matematicheskie metody v tehnike i tehnologijah – MMTT-29: sb. trudov XXIX Mezhdunar. nauch. konf. (XXIX - International Scientific Conference on Mathematical Methods in Technics and Technologies - MMTT-29): v 12 t. T. 4. Pod obshh. red. A. A. Bol'shakova. Saratov: Saratov. gos. tehn. un-t; Sankt-Peterburg: SPbGTI(TU), SPbPU, SPIIRAN; Samara: Samarsk. gos. tehn. un-t, 2016. pp. 105-109.

5. Vybornova O. N., Azhmuhamedov I. M. Matematicheskie metody v tehnike i tehnologijah – MMTT-29: sb. trudov XXIX Mezhdunar. nauch. konf. (XXIX - International Scientific Conference on Mathematical Methods in Technics and Technologies - MMTT-29): v 12 t. T. 2. Pod obshh. red. A. A. Bol'shakova. Saratov: Saratov. gos. tehn. un-t; Sankt-Peterburg: SPbGTI(TU), SPbPU, SPIIRAN; Samara: Samarsk. gos. tehn. un-t, 2016. pp. 182-186.

6. Protalinskij O. M., Azhmuhamedov I. M. Inženernyj vestnik Dona, 2012, №3 URL: ivdon.ru/ru/magazine/archive/n3y2012/916.

7. Harrington E.C. The desirable function. Industrial Quality Control. 1965. V.21. №10. pp. 494-498.

8. Sajt GBUZ AO «Centr medicinskoj profilaktiki» (Website SBHI AR "Medical Prevention Center"). URL: гбуз-ао-цмп.рф

9. Rotshteyn A. P., Shtovba S. D. Kibernetika i sistemnyj analiz. 2002. № 1. pp. 28-35.

10. Kosko B. Fuzzy systems as universal approximators. IEEE Transactions on Computers. November 1994. vol. 43, No. 11. pp. 1329-1333.