УДК 004.62

НЕЧЕТКАЯ МОДЕЛЬ ОЦЕНКИ РИСКОВ ВНЕДРЕНИЯ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ПРИ ФОРМИРОВАНИИ СИСТЕМЫ БЕЗОПАСНОСТИ

Разумников С.В.

Юргинский технологический институт (филиал) Национального исследовательского Томского политехнического университета, Юрга, e-mail: demolove7@inbox.ru

Каждый ответственный ИТ-руководитель в первую очередь интересуется безопасностью приложений и данных в облаке. Безопасность обеспечивается, если применяются соответствующие технологии и средства управления. Рассматриваются методы качественной и количественной оценки рисков при переходе к облачным технологиям. Выявлены главные составляющие при оценке рисков. В статье предлагается нечеткая модель оценки рисков внедрения облачных технологий. В работе подробно описана задача нечеткого оценивания, в основе которой лежит аппарат нечетких множеств. Обусловлено применение нечетких множеств тем, что риски приходится оценивать в условиях неопределенности и неточности информации, однако иметь представление о возможных рисках и их последствиях крайне важно. Это позволит увидеть наглядные последствия при заданных вероятностях рисков. В модели сформированы три важных лингвистических переменных: вероятность угрозы, вероятность уязвимости и размер ущерба, на основе которых определяется обобщенный интегральный риск использования облачного ИТ-сервиса по правилам дедуктивного логического вывода. Приводится подробный пример по расчету риска внедрения облачных технологий. Использование данной модели позволит выявить лучшие варианты использования проектов облачных вычислений с точки зрения рисков и информационной безопасности.

Ключевые слова: нечеткая модель, оценка, риски, информационная безопасность, облачные технологии

FUZZY MODEL OF EVALUATION OF RISKS OF INTRODUCING CLOUD TECHNOLOGIES WHEN FORMING A SECURITY SYSTEM

Razumnikov S.V.

Yurga Technological Institute (branch) of the National Research Tomsk Polytechnic University, Yurga, e-mail: demolove7@inbox.ru

Each responsible IT leader is primarily interested in the security of applications and data in the cloud. Safety is ensured if appropriate technologies and controls are used. Methods of qualitative and quantitative risk assessment during the transition to cloud technologies are considered. The main components in the risk assessment are identified. The article proposes a fuzzy model for assessing the risks of implementing cloud technologies. The paper describes in detail the fuzzy estimation problem, which is based on the apparatus of fuzzy sets. The use of fuzzy sets is due to the fact that risks have to be assessed in the conditions of uncertainty and inaccuracy of information, however, it is extremely important to have an idea of the possible risks and their consequences. This will allow you to see visual consequences for given risk probabilities. Three important linguistic variables are formed in the model: the probability of a threat, the probability of vulnerability, and the amount of damage, on the basis of which the generalized integral risk of using a cloud IT service is determined according to the rules of deductive inference. A detailed example is given of calculating the risk of implementing cloud technologies. Using this model will reveal the best options for using cloud computing projects in terms of risks and information security.

Keywords: fuzzy model, assessment, risks, information security, cloud technologies

Перенос приложений в облако – важная и серьезная задача, требующая изменения способа работы предприятия и ИТ-инфраструктуры [1]. Одной из главных составляющих переноса является безопасность приложений и данных в облаке.

Безопасность облака существенно отличается, например, от безопасности банка: владелец приложения и данных должен активно участвовать в ее обеспечении. В [2] рассмотрено, на что следует обратить внимание и для чего выделить ресурсы при формировании системы безопасности использования облачных вычислений.

Цель работы: создать модель оценки риска использования облачных ИТ с возможностью определить лучшие проекты с минимальным риском использования.

Оценка риска перехода к облачным ИТ

Для обеспечения оптимального размещения средств защиты информации необходимо провести оценку рисков перехода к облаку.

Для определения уровня риска необходимо комбинировать две величины: вероятность события и размер его последствия. Такое событие будет заключаться в осуществлении угрозы, которая использует уязвимости актива [3, 4].

Под информационной безопасностью понимают определенные свойства информации, такие как доступность, конфиденциальность, целостность. Также к информационной безопасности относят еще аутентичность и неотказуемость.

Нарушение системы информационной безопасности наносит ущерб предприятию. Величина такого ущерба определяет ценность информационного актива для предприятия. Оценка рисков перехода к облачным вычислениям включает идентификацию и оценку значимости активов, последствий для бизнеса, идентификацию и оценку уязвимостей и угроз, комбинирование этих факторов для того, чтобы определить уровень риска в качественных и количественных величинах [5, 6].

Качественная оценка риска. В табл. 1 представлен пример матрицы, по которой можно определить значение риска. Она формируется по результатам изучения вероятности по развитию сценария инцидента, и рассматривается его влияние на бизнес. В этой матрице по горизонтали будем откладывать качественные показатели реализации угрозы (вероятности появления инцидента). По вертикали укажем качественный уровень ущерба, то есть влияние его на бизнес. Риск будем оценивать по шкале в заданном диапазоне от 0 до 8, и в соответствии с критериями риска, т.е. сравниваться с максимально допустимым уровнем риска. В качестве его может быть выбрано, например, значение 3. Значение риска, равное 0, будет соответствовать очень низкой вероятности инцидента, а также очень низкому влиянию этого инцидента на бизнес. Максимум, который будет равен 8, будет соответствовать очень высокой вероятности инцидента. И высокому влиянию на бизнес. Такую шкалу рисков сведем к общему рейтингу риска. К примеру, низкий риск будет соответствовать значениям от 0 до 2, средний – от 3 до 5, высокий – от 6 до 8 [7].

Вероятность сценария инцидента может быть представлена в свою очередь уровнем уязвимости и вероятностью осуществления угрозы. Комбинируя уязвимости и угрозу, можно получить сценарий инцидента. Чтобы определить значение вероятности инцидента, можно воспользоваться следующей матрицей (табл. 2) [7].

После нахождения величины риска важно проранжировать их для нахождения приоритетов по их обработке. Можно использовать таблицу для вероятности инцидента с возможным ущербом. Вероятностью будет являться причина инцидента, состоящая из угрозы и уязвимости. Вначале оценивается ущерб по определённой шкале, например от 1 до 5 по каждому анализируемому объекту (2-й столбец в табл. 1). Далее, на втором шаге оценивают вероятность наступления инцидента, также по определённой шкале, например от 1 до 5 (3-й столбец в табл. 1). На третьем шаге находим величину риска, перемножив 2-й и 3-й столбцы. В итоге инциденты могут быть проранжированы по критичности для бизнеса. За 1 приняты самая низкая вероятность и самый низкий ущерб. В табл. 3 представлено ранжирование инцидентов по величине рисков [7].

Данные способы качественной оценки рисков относятся к табличным методам. Настройкой соответствующих шкал должна заниматься сама организация. Любая качественная оценка, которая выражена числовыми значениями или словами «высокий», «средний», «низкий», должна соответствовать определенным диапазонам количественных оценочных величин.

Таблица 1

Шкала оценивания рисков

	Вероятность воздействия происшествия	Очень маловероятно (очень низкая)	Маловероятно (низкая)	Возможно (средняя)	Вероятно (высокая)	Часто (очень высокая)
Воздействие на работу	Очень низкое	0	1	2	3	4
	Низкое	1	2	3	4	5
	Среднее	2	3	4	5	6
	Высокое	3	4	5	6	7
	Очень высокое	4	5	6	7	8

Таблица 2

Шкала рисков

Вероятность угрозы	Низкая			Средняя			Высокая		
Уровни уязвимости	Низ.	Ср.	Выс.	Низ.	Ср.	Выс.	Низ.	Ср.	Выс.
Значение вероятности сценария инцидента	0	1	2	1	2	3	2	3	4

Таблица 3

Ранжирование происшествий по величине рисков

Происшествия	Стоимость ресурса (ущерб)	Вероятность появления	Величина риска	Категория происшествия
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	4

Количественная оценка риска. Количественно определить величину риска, связанного с конкретной угрозой информационной безопасности в отношении конкретного анализируемого объекта, можно по формуле

$$R = P_{соб} \times Y,$$

где R – величина риска, $P_{соб}$ – вероятность события, Y – размер ущерба.

$$P_{соб} = P_{угрозы} \times B_{уязв},$$

где $P_{угрозы}$ – вероятность угрозы, $B_{уязв}$ – величина уязвимости.

Таким образом, величина риска равна

$$R = P_{угрозы} \times B_{уязв} \times Y.$$

Для определения риска используют количественные значения, которые получают экспертным путем, при помощи прогнозирования, а также с использованием статистических данных. Значение ущерба определяют в денежных единицах. Значение величины уязвимости определяют в диапазоне от 0 до 1. Значение вероятности угрозы выражают целым положительным числом, соответствующего количеству попыток появления угрозы за выбранный период времени.

Чтобы найти риск, хорошо и наглядно применять годовой период. Тогда значение риска будет соответствовать прогнозным среднегодовым потерям предприятия в результате появления инцидентов. Потери предприятия выражают в основном в денежном эквиваленте, так как это самый универсальный инструмент измерения ценности. Не важно, какой был ущерб, материальный или нематериальный, его желательно сопоставить денежной величине.

Оценку рисков желательно и можно проводить на конкретном уровне детализации. Для определения более точных оценок риска все его составляющие компоненты можно разложить на более мелкие. Это позволит более детально изучить состав риска. А также, наоборот, можно сгруппировать для нахождения обобщенной оценки.

Исходя от уровня детализации, для одного предприятия могут рассматриваться огромное количество рисков информационной безопасности при использовании облачных технологий. Сначала следует начинать с высокоуровневого оценивания рисков, который будет соответствовать наиболее низкому уровню детализации, постепенно повышая детализацию при необходимости. Более детализированная оценка рисков для принятия обоснованных решений по их обработке необходима, когда высокоуровневая оценка не предоставляет достаточно информации.

Разработка нечеткой модели оценки риска

Согласно порядку выполнения построения нечеткой модели [8] выполним необходимые шаги для построения нечеткой модели для каждой переменной.

Для начала опишем задачу нечеткого оценивания. В нашем примере объект исследования – переход на облачные технологии. Для данного объекта будут следующие свойства: Вероятность угрозы, Вероятность уязвимости, Размер ущерба. Базовое множество для размера ущерба – значение в рублях, для вероятностей – значение вероятности в диапазоне [0–1] или в %. Для всех трех свойств будут соответствующие лингвистические переменные со значениями («низкий», «средний», «высокий»).

Для каждого из значений лингвистических переменных построим функции принадлежности и представим в виде трапециевидного графика и затем зададим функции принадлежности в виде формул [9, 10].

Исходные данные показателей рисков для четырех вариантов использования облака приведены в табл. 4.

Таблица 4

Исходные данные для показателей рисков использования облака

Компоненты величина риска	Значения компонентов для расчета величины риска			
	I	II	III	IV
Вероятность угрозы	3	2	5	4
Вероятность уязвимости	0,1	0,3	0,15	0,2
Размер ущерба	255	320	170	560

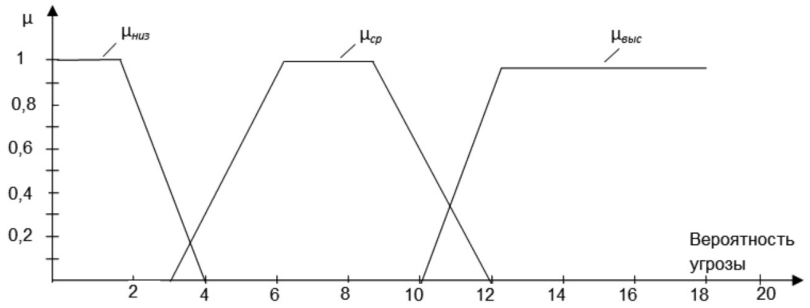

Рис. 1. График функции принадлежности для переменной «Вероятность угрозы»

Лингвистическая переменная «Вероятность угрозы». График функции принадлежности для переменной «Вероятность угрозы» («низкий», «средний», «высокий») представлен на рис. 1.

Формулы для трапециевидной функции принадлежности «Вероятность угрозы»:

$$\mu_{низ} = 1 \text{ при } x \le 2, \mu_{низ} = (4 - x)/(4 - 2) \text{ при } 2 < x \le 4, \mu_{низ} = 0 \text{ при } x \ge 4,$$

$$\mu_{ср} = 0 \text{ при } x \le 3 \text{ и при } x \ge 12, \mu_{ср} = (x - 3)/(6 - 3) \text{ при } 3 < x < 6,$$

$$\mu_{ср} = 1 \text{ при } 6 \le x \le 9, \mu_{ср} = (12 - x)/(12 - 9) \text{ при } 9 < x < 12,$$

$$\mu_{выс} = 0 \text{ при } x \le 10, \mu_{выс} = (x - 10)/(12 - 10) \text{ при } 10 < x < 12, \mu_{выс} = 1 \text{ при } x \ge 12.$$

Далее определим нечеткие значения лингвистической переменной для четырех вариантов сценария, подставив базовые значения в формулы функций принадлежности.

$$x_1 - A = 3 \text{ (I вариант)}; \mu_{низ} = (4 - 3) / (4 - 2) = 0{,}5; \mu_{ср} = 0. \mu_{выс} = 0.$$

$$x_2 - A = 2 \text{ (II вариант)}; \mu_{низ} = 1. \mu_{ср} = 0. \mu_{выс} = 0.$$

И так далее, результаты подстановки в формулы представлены в табл. 5.

Таблица 5

Результаты расчетов для лингвистической переменной

Варианты	Значения лингвистической переменной «Вероятность угрозы»		
	$\mu_{низ}$	$\mu_{ср}$	$\mu_{выс}$
I (3)	0,5	0	0
II (2)	1	0	0
III (5)	0	0,67	0
IV (4)	0	0,33	0

Лингвистическая переменная «Величина уязвимости». График функции принадлежности для переменной «Величина уязвимости» («низкий», «средний», «высокий») представлен на рис. 2.

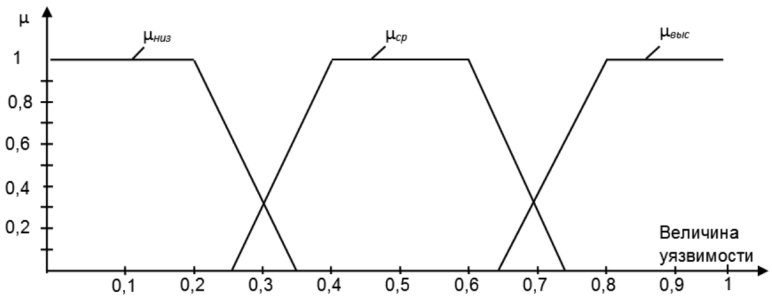

Рис. 2. График функции принадлежности для переменной «Вероятность уязвимости»

Формулы для трапециевидной функции принадлежности «Величина уязвимости»:

$\mu_{низ} = 1$ при $x \le 2$, $\mu_{низ} = (0{,}35 - x)/(0{,}35 - 0{,}2)$ при $0{,}2 < x \le 0{,}35$, $\mu_{низ} = 0$ при $x \ge 0{,}35$,

$\mu_{ср} = 0$ при $x \le 0{,}25$ и при $x \ge 0{,}75$, $\mu_{ср} = (x - 0{,}25)/(0{,}4 - 0{,}25)$ при $0{,}25 < x < 0{,}4$,

$\mu_{ср} = 1$ при $0{,}4 \le x \le 0{,}6$, $\mu_{ср} = (0{,}75 - x)/(0{,}75 - 0{,}6)$ при $0{,}6 < x < 0{,}75$,

$\mu_{выс} = 0$ при $x \le 0{,}65$, $\mu_{выс} = (x - 0{,}65)/(0{,}8 - 0{,}65)$ при $0{,}65 < x < 0{,}8$, $\mu_{выс} = 1$ при $x \ge 0{,}8$.

Далее определим нечеткие значения лингвистической переменной для четырех вариантов сценария, подставив базовые значения в формулы функций принадлежности. Результаты подстановки в формулы представлены в табл. 6.

Таблица 6

Результаты расчетов для лингвистической переменной

Варианты	Значения лингвистической переменной «Величина уязвимости»		
	$\mu_{низ}$	$\mu_{ср}$	$\mu_{выс}$
I (0,1)	1	0	0
II (0,3)	0,33	0,33	0
III (0,15)	1	0	0
IV (0,2)	1	0	0

Лингвистическая переменная «Размер ущерба». График функции принадлежности для переменной «Размер ущерба» («низкий», «средний», «высокий») представлен на рис. 3.

Формулы для трапециевидной функции принадлежности «Размер ущерба»:

$\mu_{низ} = 1$ при $x \le 150$, $\mu_{низ} = (300 - x)/(300 - 150)$ при $150 < x \le 300$, $\mu_{низ} = 0$ при $x \ge 300$,

$\mu_{ср} = 0$ при $x \le 250$ и при $x \ge 650$, $\mu_{ср} = (x - 250)/(400 - 250)$ при $250 < x < 400$,

$\mu_{ср} = 1$ при $400 \le x \le 500$, $\mu_{ср} = (650 - x)/(650 - 500)$ при $500 < x < 650$,

$\mu_{выс} = 0$ при $x \le 550$, $\mu_{выс} = (x - 550)/(700 - 550)$ при $550 < x < 700$, $\mu_{выс} = 1$ при $x \ge 700$.

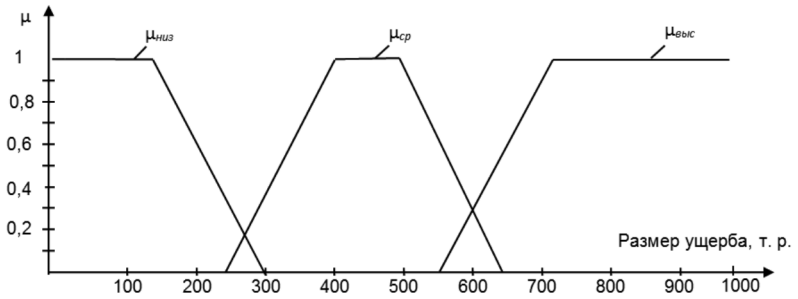

Рис. 3. График функции принадлежности для переменной «Размер ущерба»

Далее определим нечеткие значения лингвистической переменной для четырех вариантов сценария, подставив базовые значения в формулы функций принадлежности. Результаты подстановки в формулы представлены в табл. 7.

Таблица 7

Результаты расчетов для лингвистической переменной

Варианты	Значения лингвистической переменной «Размер ущерба»		
	$\mu_{низ}$	$\mu_{ср}$	$\mu_{выс}$
I (255)	0,33	0,03	0
II (320)	0	0,47	0
III (170)	0,87	0	0
IV (560)	0	0,6	0,07

Нечеткий вывод

X = {B1, B2, B3, B4} – варианты организации бизнес-процесса с использованием облачных ИТ-сервисов, характеризуемые лингвистическими переменными для расчета риска: *Вероятность угрозы ($Р_{угрозы}$), Вероятность уязвимости (Руязв), Размер ущерба*: <'н' (низкий), 'с' (средний), 'в' (высокий) >.

Исходные значения всех этих переменных рассчитываются. В табл. 8 приведены рассчитанные сходные данные для трех переменных.

Таблица 8

Результаты расчетов для лингвистических переменных

Переменные	Варианты			
	B1	B2	B3	B4
Вероятность угрозы ($Р_{угрозы}$)	н/0.5	н/1	с/0.67	с/33
Вероятность уязвимости ($Р_{уязв}$)	н/1	н/0.33	н/1	н/1
Размер ущерба	н/0,33	с/0,47	н/0,87	с/0,6

Значения переменной «Риск использования облачного ИТ-сервиса» выводятся по правилам-продукциям на основе предыдущих показателей:

П1: If «$Р_{угрозы}$» = 'н' & «$Р_{уязв}$» = 'н' & «Размер ущерба» = 'н' then «$Риск_{исп}$» = 'н';

П2: If «$Р_{угрозы}$» = 'н' & «$Р_{уязв}$» = 'н' & «Размер ущерба» = 'с' then «$Риск_{исп}$» = 'с';

П3: If «$Р_{угрозы}$» = 'с' & «$Р_{уязв}$» = 'н' & «Размер ущерба» = 'н' then «$Риск_{исп}$» = 'н';

П4: If «$Р_{угрозы}$» = 'с' & «$Р_{уязв}$» = 'н' & «Размер ущерба» = 'с' then «$Риск_{исп}$» = 'с';

П5: If «$Р_{угрозы}$» = 'с' & «$Р_{уязв}$» = 'в' & «Размер ущерба» = 'в' then «$Риск_{исп}$» = 'в'.

Для B1 по правилу П1 выводим «$Риск_{исп}$» = 'н', T = min (0.5, 1, 0.33) = 0.33.

Для B2 по правилу П2 выводим «$Риск_{исп}$» = 'с', T = min (1, 3.33, 0.47) = 0.33.

Для B3 по правилу П3 выводим «$Риск_{исп}$» = 'н', T = min (0.67, 1, 0.87) = 0.67.

Для B4 по правилу П4 выводим «$Риск_{исп}$» = 'с', T = min (0.33, 1, 0.06) = 0.33

Таким образом, Вариант под № 3 имеет наименьший риск использования облачного ИТ-сервиса, соответственно, он самый лучший. На втором место B1, далее B4 и B2.

Заключение

В статье представлена нечеткая модель оценки рисков при внедрении облачных технологий, которая является вспомогательным инструментом при формировании системы безопасности. Она позволит выявить лучшие варианты с наименьшим риском использования таких технологий с учетом вероятностей угроз и уязвимостей, а также ущерба в случае возникновения таких угроз.

Работа выполнена при финансовой поддержке гранта РФФИ № 18-07-00031 «Модели, алгоритмы и программное обеспечение системы поддержки принятия стратегических решений к переходу на облачные технологии».

Список литературы

1. Рахимбердиев А. Как создать облачный сервис и получить инвестиции // Infostart.ru [Электронный ресурс]. 2014. URL: http://infostart.ru/public/389683 (дата обращения: 11.09.2019).

2. Разумников С.В. Безопасность облака и управление им // Инновационные технологии в машиностроении: сборник трудов X Международной научно-практической конференции / ЮТИ. Томск: Изд-во ТПУ, 2019. С. 267–270.

3. Разумников С.В. Модель поддержки принятия решений о миграции корпоративных приложений в облачную среду // Научные труды Вольного экономического общества России. 2015. Т. 194. С. 490–502.

4. Разумников С.В. Оценка эффективности и рисков от внедрения облачных ИТ-сервисов // Фундаментальные исследования. 2014. № 11–1. С. 33–38.

5. Сафонов А. Практическое применение методов и средств анализа рисков // Information Security/Информационная безопасность. 2010. № 3. С. 42–43.

6. Одегов С.В. Методика снижения рисков информационной безопасности облачных сервисов на основе квантифицирования уровней защищенности и оптимизации состава ресурсов: дис. ... канд. тех. наук: 05.13.19. Санкт-Петербург, 2013. 107 с.

7. Астахов А.М. Искусство управления информационными рисками. [Электронный ресурс]. 2010. URL: http://xn----7sbab7afcqes2bn.xn--p1ai/content/soderzhanie (дата обращения: 11.09.2019).

8. Силич В.А., Силич М.П. Теория систем и системный анализ: учеб. пособие. Томск: Томский политехнический университет, 2010. 281 с.

9. Трофимова Л.А., Трофимов В.В. Методы принятия управленческих решений: учеб. пособие. СПб.: Изд-во СПбГУЭФ, 2012. 101 с.

10. Гладких Б.А. Методы оптимизации и исследование операций для бакалавров информатики. Ч. III. Теория решений: учеб. пособие. Томск: Изд-во НТЛ, 2012. 281 с.