Раздел I. Управление рисками информационной безопасности

УДК 004.056.5

А.Ю. Сенцова, И.В. Машкина

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ОЦЕНКИ ОПЕРАТИВНОГО ЗНАЧЕНИЯ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ*

Приводится описание разработки программного средства для оценки оперативного значения риска нарушения информационной безопасности в системе облачных вычислений на основе использования искусственной нейронной сети (ИНС). Под системой облачных вычислений (СОбВ) понимается информационная система взаимодействия поставщика и потребителя облачных услуг. Предложена блок-схема алгоритма, реализующего программное средство, разработаны модуль ввода множества данных обучающей выборки для искусственной нейронной сети, модуль обучения ИНС, модуль получения расчетных значений риска нарушения информационной безопасности. Приведены результаты тестирования программного средства. Предлагаемое программное решение позволяет осуществить анализ реально выявленных угроз и получить численную оценку уровня риска нарушения информационной безопасности СОбВ в реальном масштабе времени с учетом сложных сценариев атак, когда активизируются более одного источника угроз. Численная оценка оперативного значения уровня риска нарушения информационной безопасности, полученная с помощью программного средства, может быть использована в ходе проведения экспертного аудита информационной безопасности СОбВ на основе получения объективных данных с датчиков событий о текущем состоянии защищенности системы облачных вычислений.

Оперативное значение риска; система облачных вычислений; расчет рисков; экспертный аудит; искусственная нейронная сеть; многослойный персептрон; алгоритм обратного распространения ошибки.

A.U. Sentsova, I.V. Mashkina

THE SOFTWARE TOOL FOR THE ESTIMATION OF INFORMATION SECURITY RISK OPERATIONAL VALUE IN THE CLOUD COMPUTING SYSTEM

In this article a description of the software tool for the estimation of information security risk operational value in the cloud computing system on the based of artificial neural network (ANN) is developed. Cloud computing system is the information system of client and vendor interaction. The algorithm block diagram of software tool is proposed, the training sample data set input module for an artificial neural network, the module of training for ANN and the module to obtain an assessment of information risk level are developed. The results of testing software tool are shown. The offered decisions allow to enable the analysis of real identified threats and to obtain an assessment of information security risk level in cloud computing system for the worst case,

* Работа выполнена при поддержке РФФИ (грант № 14-07-00928-а).

when all possible threat sources become active simultaneously. An assessment of the operational information security risk level, obtained on the based of software tools, may be used during the information security expert audit on the based of obtaining objective data from events sensors on the current state of cloud computing system security.

Information security risk operational value; cloud computing system; assessment of information security risk; expert audit; artificial neural network; multilayered perceptron; backpropagation algorithm.

В настоящее время в индустрии информационных технологий можно наблюдать стремительные темпы развития облачных вычислений, но при этом недостаточно широко освещается проблема использования облачных сервисов с точки зрения информационной безопасности. Однако использование средств виртуализации, наряду с другими особенностями облачных вычислений, позволяет говорить о новых потенциально возможных угрозах информационной безопасности, которые будут являться специфическими для облачных сред.

Многими экспертами отмечается, что потребитель облачных услуг имеет тот уровень защищенности в облачной среде, который обеспечивается поставщиком [1, 2], поэтому существующая система обеспечения информационной безопасности «облака» должна периодически подвергаться независимому *экспертному аудиту*, который в соответствии с требованиями международных стандартов является одним из обязательных этапов жизненного цикла любой информационной системы [3].

Экспертный аудит информационной безопасности информационных систем (ИС) представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области безопасности ИС. Считается, что результаты качественно выполненного экспертного аудита информационной безопасности (ИБ) организации позволяют оценить текущую безопасность ИС, прогнозировать и управлять влиянием рисков нарушения ИБ на бизнес-процессы, корректно и обосновано подойти к вопросу обеспечения безопасности информационных активов организации и тем самым повысить эффективность системы защиты информации.

Для осуществления процедуры *анализа исходных данных* аудитор может применить методику, которая позволила бы оценить соответствие используемых в системе обеспечения информационной безопасности механизмов защиты требованиям существующих стандартов ИБ. Другой подход к проведению анализа в ходе аудита основан на *оценке рисков*. В этом случае должны быть идентифицированы все возможные угрозы, выявлены и оценены уязвимости. Эксперт в аудиторском отчете указывает используемый им при анализе метод расчета информационных рисков.

В ходе экспертного аудита важно оценить не только прогнозируемое значение уровня риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз, но и *оперативное* значение риска, когда угроза проявляется по конкретному пути распространения [4].

Прогнозируемые риски связаны с планируемыми к внедрению технологиями для реализации бизнес-процессов, планируемыми средствами и механизмами защиты. Оперативные значения уровня риска нарушения ИБ позволяют принять более рациональное решение с учетом актуальных данных, полученных в процессе мониторинга информационной системы.

Известны несколько программных продуктов, позволяющих автоматизировать анализ исходных данных в ходе аудита на *основе оценки рисков*, однако они не лишены *недостатков*. Так, например, общим недостатком Кондор+, АванГард, Cobra, а также программы *RiskAnalyzer [5]* является *невозможность оценить опе-*

ративное значение уровня риска нарушения ИБ; кроме того, в средствах Кондор+, АванГард, Cobra отсутствует возможность учета сведений о технических х*арактеристиках* используемых или планируемых средств защиты [6], а в программной системе RiskAnalyzer пользователю необходимо вручную строить модель угроз в виде нечетких когнитивных карт.

В работах [4, 7, 8] для оценки оперативного значения уровня риска нарушения информационной безопасности, связанного с появлением угрозы в реальном масштабе времени, впервые предложено использовать искусственную нейронную сеть (ИНС).

В продолжение этих исследований проведены эксперименты с различными архитектурами искусственных нейронных сетей для получения численных оценок оперативного значения уровня риска нарушения ИБ.

Результаты обучения и тестирования архитектуры ИНС на основе многослойного персептрона показали возможность использования выбранной архитектуры для разработки модуля численной оценки риска нарушения ИБ в программном комплексе, предназначенном для автоматизации экспертного аудита нарушения ИБ информационной системы. Выбранная для использования в программном средстве архитектура искусственной нейронной сети показана на рис. 1.

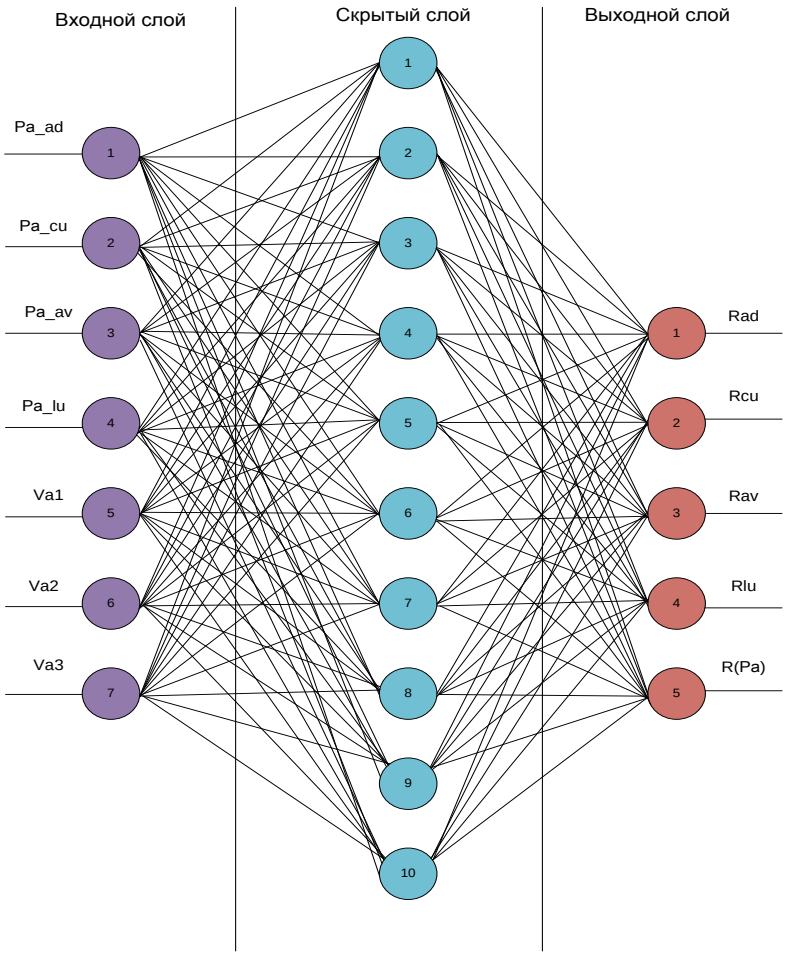


Рис. 1. Архитектура искусственной нейронной сети

В соответствии с предложенным авторами методом оценки оперативного значения уровня риска нарушения информационной безопасности [4, 7, 8] разработано программное средство, реализующее данный метод. Работоспособность программного средства для проведения экспертного аудита ИБ проверена на основе тестовых наборов, сформированных для системы облачных вычислений (СОбВ).

Блок-схема алгоритма реализации модуля численной оценки оперативного значения риска нарушения информационной безопасности приведена на рис. 2.

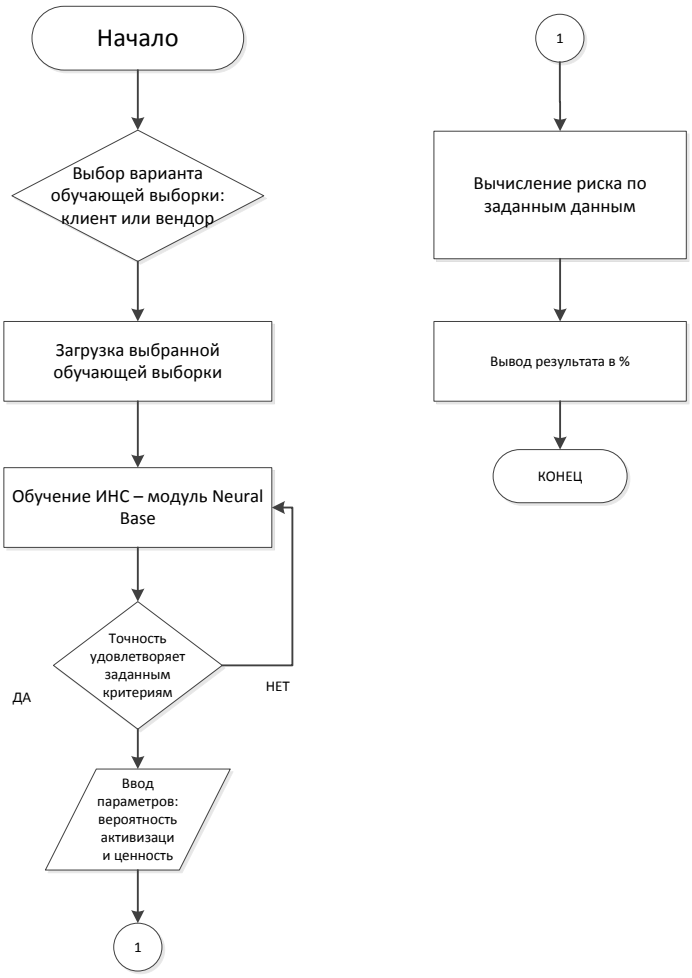


Рис. 2. Блок-схема алгоритма реализации модуля оценки оперативного значения уровня риска нарушения ИБ

Программное средство реализовано на языке высокого уровня Pascal ABC с использованием среды программирования Borland Delphi 7.0 и библиотеки компонентов NeuralBase.

Преимуществом разработанного программного средства является то, что в нем реализована модель, позволяющая осуществлять анализ реально выявленных угроз и проводить оценку рисков нарушения информационной безопасности с учетом сложных сценариев атак, когда активизируются более одного источника угроз.

В ходе работы с программным средством пользователь может отдельно рассчитать долю оперативного значения уровня риска нарушения ИБ на стороне потребителя СОбВ и на стороне поставщика облачных услуг, в этом случае необходимо определить перечень защищаемых информационных активов, обрабатываемых в исследуемый период времени в информационных системах потребителя и поставщика соответственно.

Затем в модуль ввода исходных данных загружается обучающая выборка для обучения искусственной нейронной сети. Экранные формы, иллюстрирующие работу модуля, приведены на рис. 3.

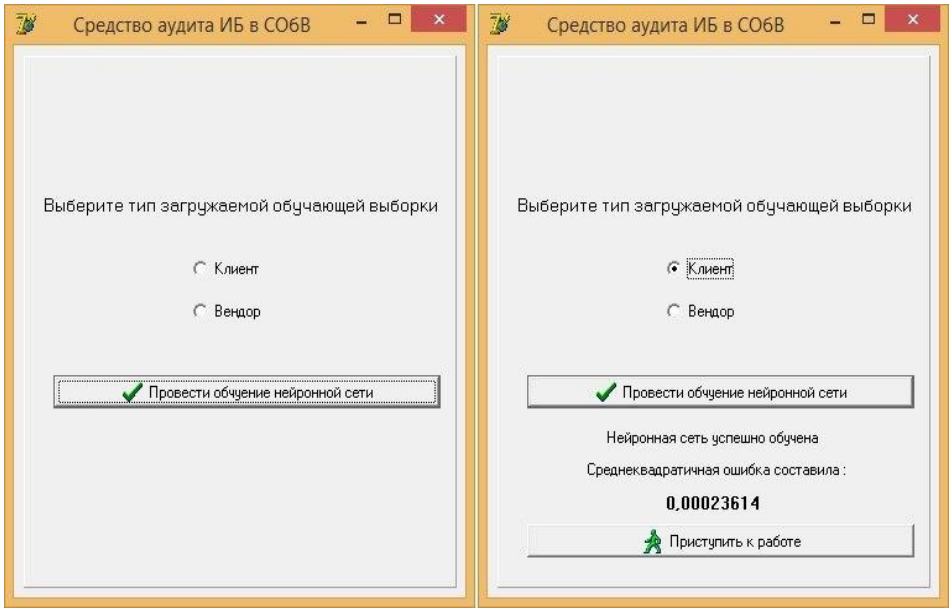


Рис. 3. Экранные формы для задания процедуры обучения ИНС с выведенным значением среднеквадратичной ошибки

Обучение ИНС проводится с помощью алгоритма обратного распространения ошибки (back propagation), который впервые был описан А.И. Галушкиным, а также независимо и одновременно с ним Полом Дж. Вербосом и считается в настоящее время одним из наиболее эффективных алгоритмов обучения искусственной нейронной сети [9]. Данный алгоритм определяет стратегию подбора весов многослойной сети с применением градиентных методов оптимизации. В процессе обучения рассчитывается целевая функция в виде квадратичной суммы разностей между фактическим и ожидаемым значениями выходных сигналов.

Существенным отличием разработанного программного средства «Средство аудита в СОбВ» от существующего продукта Matlab 6.0, в котором также можно осуществить обучение нейронной сети с помощью алгоритма обратного распространения ошибки, является *возможность задания количества эпох* для обучения многослойного персептрона**,** что *позволило повысить в 3 раза* точность настройки ИНС по сравнению с данными, полученными при тестировании работы многослойного персептрона в среде Matlab.

Блок-схема алгоритма обучения многослойного персептрона применительно к вопросу проведения аудита информационной безопасности системы облачных вычислений, приведена на рис. 4.

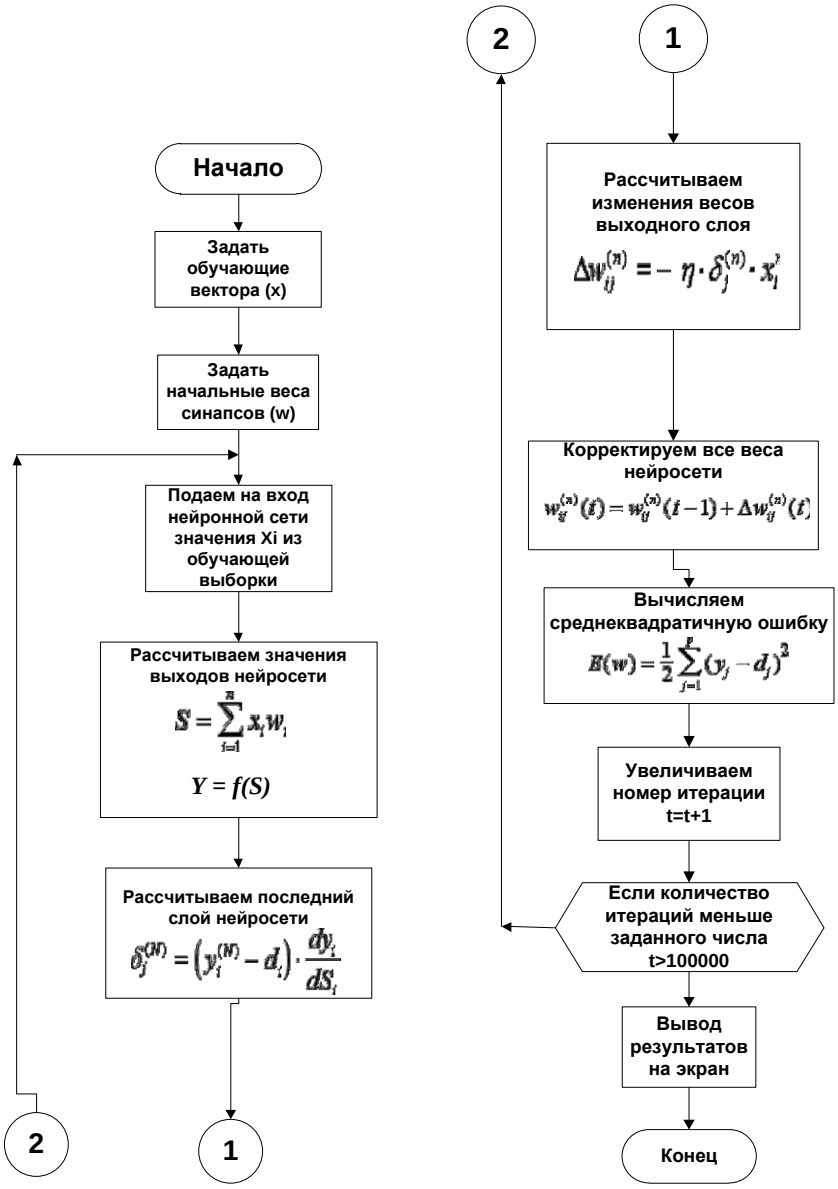


Рис. 4. Алгоритм обратного распространения ошибки

После успешного обучения нейронной сети и достижения необходимого уровня среднеквадратичной ошибки, пользователю предлагается ввести числовое значение параметра «ценность» информационных активов и вероятность активизации угрозы.

Следует заметить, что значение параметра «ценность» информационного актива не может быть получено путем какого-либо объективного измерения. Ценность информации может быть задана собственником и определяется степенью полезности или важности для него какого-либо актива. Возможные виды последствий и их значимость определяются собственником информации, который может опираться в своих суждениях на рекомендации, приведенные в [10].

Программное средство выполняет процедуры контроля корректности вводимых пользователем данных и вывода соответствующих предупреждений об ошибках в случаях, если:

- суммарное значение параметра «ценность» для защищаемых информационных активов на стороне потребителя СОбВ и на стороне поставщика облачных услуг не равно единице;
- задана равной нулю ценность активов на клиентской части СОбВ;
- параметр «ценность» для конфигурационных файлов и для гипервизора не принадлежит интервалу [0,2;0,7].

Процедура контроля корректности вводимых данных представлена на рис. 5.

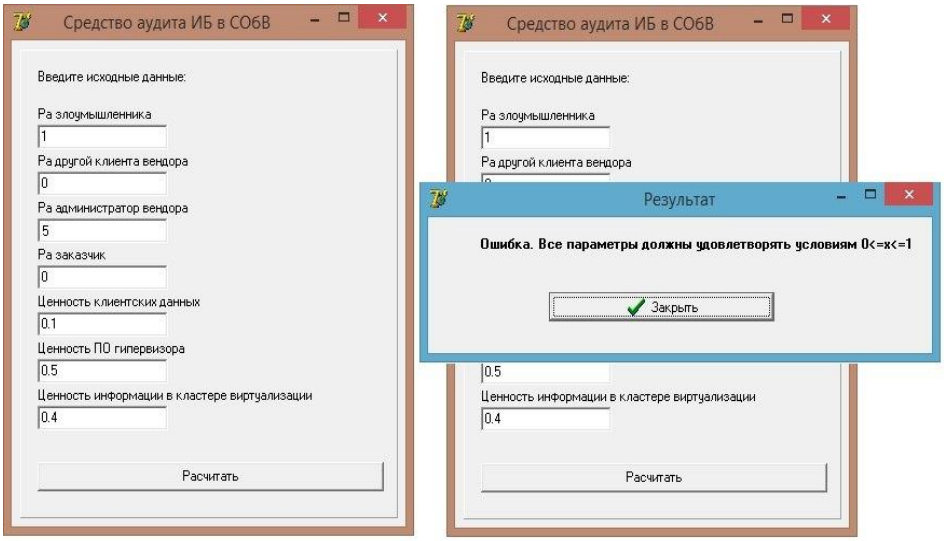


Рис. 5. Процедура контроля корректности вводимых данных и экранная форма предупреждения об ошибке

На основе полученной информации о ценности активов, обрабатываемых на стороне поставщика облачных услуг и на стороне потребителя СОбВ, а также о вероятности активизации угрозы, реализуемой на том или ином пути, программная система рассчитывает уровень оперативного значения уровня риска нарушения информационной безопасности для СОбВ. Результаты расчета риска нарушения ИБ в реальном масштабе времени представлены на рис. 6.

С помощью программного средства был произведен вычислительный эксперимент, в ходе которого менялись значения вероятности активизации угрозы и ценности информационных активов в диапазоне [0,1]. Для этого был сформирован тестовый набор, состоящий из значений входов нейронной сети, не входящих в исходную обучающую выборку для искусственной нейронной сети. Результаты эксперимента сравнивались с эталонными значениями, полученными при расчете риска нарушения информационной безопасности по методу, предложенному в [8]. В качестве иллюстрации сравнения эталонного значения уровня риска нарушения ИБ и значения, полученного с помощью программного модуля, была построена диаграмма, приведенная на рис. 7. Результаты эксперимента показали, что выход искусственной нейронной сети с требуемой точностью совпадает с ожидаемыми значениями.

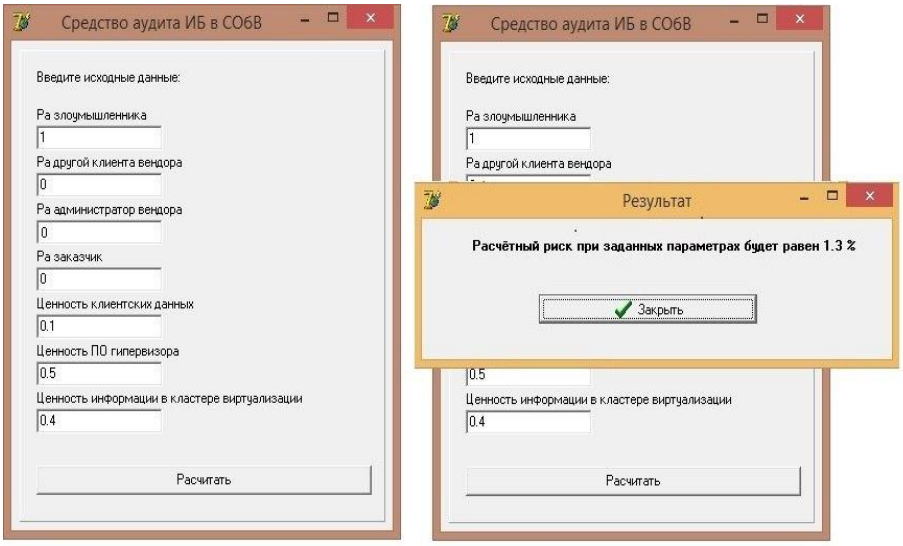
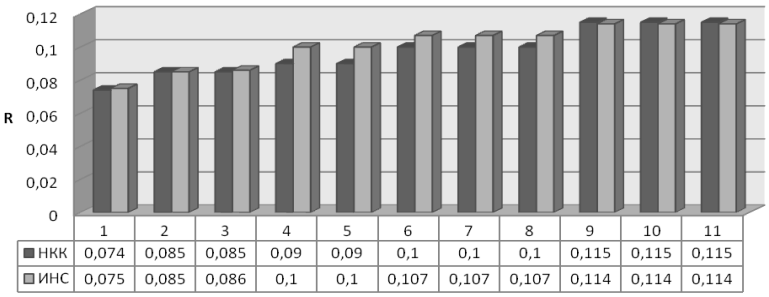


Рис. 6. Экранная форма с результатами работы программного средства



	1	2	3	4	5	6	7	8	9	10	11
НКК	0,074	0,085	0,085	0,09	0,09	0,1	0,1	0,1	0,115	0,115	0,115
ИНС	0,075	0,085	0,086	0,1	0,1	0,107	0,107	0,107	0,114	0,114	0,114

Рис. 7. Диаграмма значений уровней рисков, рассчитанных с помощью метода численной оценки риска нарушения ИБ и с помощью программного средства на основе ИНС в зависимости от номеров наборов исходных данных

Корректность работы программного средства была проверена на контрольном примере. На основе результатов проверки корректности работы программного средства был построен график зависимости ценности информации и оперативного значения уровня риска, представленный на рис. 8.

Таким образом, оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью администратора поставщика облачных услуг, являются наиболее опасными.

На основе приведенных в работе исследований можно сделать вывод о *возможности использования искусственной нейронной сети,* обученной с помощью множества данных обучающей выборки, полученной в результате расчетов прогнозируемых значений рисков с использованием нечетких когнитивных карт, *для численного оценивания оперативного значения риска нарушения ИБ в СОбВ*.

Достоинством реализованного в программной системе метода является возможность оценить уровень риска нарушения информационной безопасности в *реальном масштабе времени* в процессе реализации угрозы по конкретному пути.

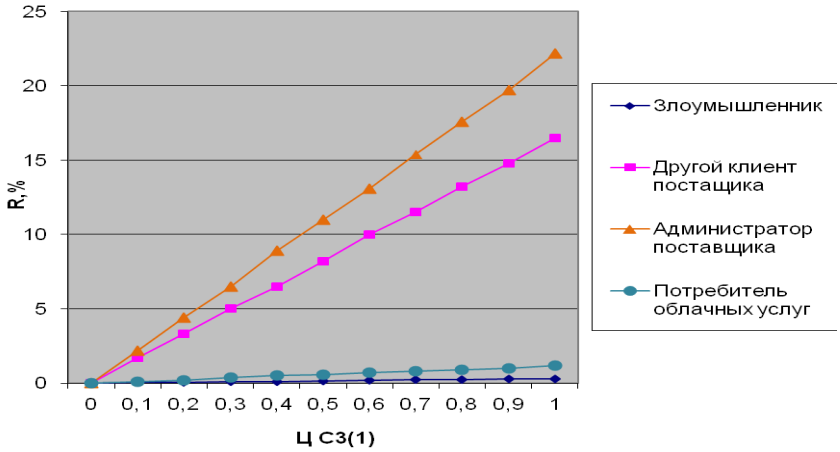


Рис. 8. График зависимости значения уровня риска от ценности информации, обрабатываемой в кластере виртуализации

Анализ результатов работы программного средства показал, что *метод,* реализованный в нем, *позволяет получить количественные оценки выходных данных,* что является одним из важнейших требований ГОСТ [11] для выбора метода оценки риска.

Программное средство зарегистрировано в Федеральной службе по интеллектуальной собственности [12].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. – М.: ДМК Пресс, 2012. – 592 с.
2. *Демурчев Н.Г., Ищенко С.О.* Проблемы обеспечения информационной безопасности при переходе на облачные вычисления // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – 265 с.
3. ГОСТ Р ИСО/МЭК 12207-10. Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств. – М.: Стандартинформ, 2010.
4. *Машкина И.В., Сенцова А.Ю.* Методология экспертного аудита в системе облачных вычислений // Безопасность информационных технологий. – 2013. – № 4. – С. 63-70.
5. *Степанова Е.С., Хабибуллин Р.М., Машкина И.В*. Программная система оценки рисков нарушения информационной безопасности на основе построения нечетких когнитивных карт // Материалы XII Международной научно-практической конференции «Информационная безопасность». Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 185-191.
6. *Гузаиров М.Б., Машкина И.В., Степанова Е.С.* Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности // Безопасность информационных технологий. – 2011. – № 2. – С. 37-49.
7. *Машкина И.В., Сенцова А.Ю.* Автоматизация экспертного аудита информационной безопасности на основе использования искусственной нейронной сети // Безопасность информационных технологий. – 2014. – № 2. – С. 65-70.
8. *Машкина И.В., Сенцова А.Ю., Степанова Е.С.* Разработка нечетких когнитивных карт и искусственной нейронной сети для оперативной оценки информационных рисков в системе облачных вычислений // Нейрокомпьютеры разработка и применение. – 2013. – С 26-30.
9. *Осовский С.* Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. – М.: Финансы и статистика, 2002. – 344 с.

10. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (дата обращения 06.08.2014).
11. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска. – М.: Стандартинформ, 2012.
12. *Сенцова А.Ю., Машкина И.В., Чайка В.Ю.* Средство проведения экспертного аудита информационной безопасности // Свидетельство о государственной регистрации программы для ЭВМ № 2014616279. 2014.

REFERENCES

1. *Shan'gin V.F.* Zashchita informatsii v komp'yuternykh sistemakh i setyakh [Protection of information in computer systems and networks]. Moscow: DMK Press, 2012, 592 p.
2. *Demurchev N.G., Ishchenko S.O.* Problemy obespecheniya informatsionnoy bezopasnosti pri perekhode na oblachnye vychisleniya [Problems of information security in the transition to cloud computing], Materialy XI Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'» [Proceedings of the XI International scientific-practical conference "Information security"]. Part. 1. Taganrog: Izd-vo TTI YuFU, 2010, 265 p.
3. *GOST R ISO/MEK 12207-10.* Informatsionnaya tekhnologiya. Sistemnaya i programmnaya inzheneriya. Protsessy zhiznennogo tsikla programmnykh sredstv [State Standard *R ISO/MEK 12207-10.* Information technology. System and software engineering. The life cycle processes softwareъ. Moscow: Standartinform, 2010.
4. *Mashkina I.V., Sentsova A.Yu.* Metodologiya ekspertnogo audita v sisteme oblachnykh vychisleniy [The methodology of the expert audit in the system of cloud computing], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security], 2013, No. 4, pp. 63-70.
5. *Stepanova E.S., Khabibullin R.M., Mashkina I.V.* Programmnaya sistema otsenki riskov narusheniya informatsionnoy bezopasnosti na osnove postroeniya nechetkikh kognitivnykh kart [A software system for the evaluation of risks to information security based on the construction of fuzzy cognitive maps], *Materialy XII Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Informatsionnaya bezopasnost'»* [Proceedings of the XII International scientific-practical conference "Information security"]. Part 2. – Taganrog: Izd-vo TTI YuFU, 2012, pp. 185-191.
6. *Guzairov M.B., Mashkina I.V., Stepanova E.S.* Postroenie modeli ugroz s pomoshch'yu nechetkikh kognitivnykh kart na osnove setevoy politiki bezopasnosti [Building a threat model using fuzzy cognitive maps based on the network security policy], *Bezopasnost' informatsionnykh tekhnologiy* [Information Technology Security]. 2011, No. 2, pp. 37-49.
7. *Mashkina I.V., Sentsova A.Yu.* Avtomatizatsiya ekspertnogo audita informatsionnoy bezopasnosti na osnove ispol'zovaniya iskusstvennoy neyronnoy seti [Automation expert information security audit based on the use of artificial neural networks], Bezopasnost' informatsionnykh tekhnologiy [Information Technology Security]. 2014, No. 2, pp. 65-70.
8. *Mashkina I.V., Sentsova A.Yu., Stepanova E.S.* Razrabotka nechetkikh kognitivnykh kart i iskusstvennoy neyronnoy seti dlya operativnoy otsenki informatsionnykh riskov v sis-teme oblachnykh vychisleniy [Development of fuzzy cognitive maps and artificial neural network for rapid assessment of information risks in the cloud computing system], *Neyrokomp'yutery razrabotka i primenenie* [Neurocomputers development and application], 2013, pp. 26-30.
9. *Osovski S.* Sieci neuronowe dla przetwarzania informacji. Oficyna wydawnicza Politechnili Warszawskiej. Warszawa, 2000 [Russ. ed.: Osovskiy S. Neyronnye seti dlya obrabotki informatsii. Moscow: Finansy i statistika Publ, 2002, 344 p.
10. *GOST R ISO/MEK 27005-2010*. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoy bezopasnosti [State Standard *R ISO/MEK 27005-2010.* Information technology. Methods and means of security. The risk management information security]. Available at: http://docs.cntd.ru/document/gost-r-iso-mek-27005-2010 (accessed 6 August 2014).
11. *GOST R ISO/MEK 31010-2011*. Menedzhment riska. Metody otsenki riska [State Standard *R ISO/MEK 31010-2011*. The management of risk. Risk assessment methods]. Moscow: Standartinform, 2012.

12. *Sentsova A.Yu., Mashkina I.V., Chayka V.Yu.* Sredstvo provedeniya ekspertnogo audita informatsionnoy bezopasnosti [Tool expert information security audit], *Svidetel'stvo o gosudarstvennoy registratsii programmy dlya EVM № 2014616279. 2014* [The certificate of state registration of the computer program No. 2014616279. 2014].

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Машкина Ирина Владимировна – Уфимский государственный авиационный технический университет; e-mail: mashkina_vtzi@gmail.com; 450000, Республика Башкортостан, г. Уфа, ул. К. Маркса, 12; тел.: +79279277089; кафедра вычислительной техники и защиты информации; д.т.н.; профессор.

Сенцова Алина Юрьевна – e-mail: sentsova.alina@yandex.ru; тел.: +79174568307; аспирантка.

Mashkina Irina Vladimirovna – The Ufa State Aviation Technical University; e-mail: mashkina_vtzi@gmail.com; 12, K. Marx's street, Ufa, 450000, Russia; phone: +79279277089; chair of computer facilities and information protection; dr. of eng. sc.; professor.

Sentsova Alina Uryevna – e-mail: sentsova.alina@yandex.ru; phone: +79174568307; postgraduate student.

УДК 004.9

К.В. Курносов, В.В. Селифанов

ТРЕБОВАНИЯ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ

Ввиду отсутствия требований для оценки систем защиты информации для технологий, реализующих виртуальные инфраструктуры, была поставлена цель по их разработке. В соответствии с руководящими и методическими документами в области технической защиты информации была разработана модель инфраструктуры, построенной с применением технологии виртуализации, в которой содержится информация ограниченного доступа, не содержащая сведений составляющих государственную тайну. Были определены виды потенциальных нарушителей безопасности, выделены актуальные угрозы, и выработан набор требований для оценки безопасности таких инфраструктур. При решении этих задач проводился анализ отечественной литературы по данному вопросу, нормативной и методической документации в области защиты информации, моделирование информационной инфраструктуры, угроз и нарушителя безопасности с учетом специфики технологий виртуализации. Объектом исследования в данной статье выступает виртуальная инфраструктура, включая ее компоненты. Предметом исследования являются требования и методика для оценки безопасности системы защиты информации для виртуальных инфраструктур.

Виртуализация; виртуальная инфраструктура; виртуальная машина; гипервизор; информационная безопасность; требования информационной безопасности.

K.V. Kurnosov, V.V. Selifanov

INFORMATION PROTECTION SYSTEM REQUIREMENTS FOR VIRTUAL INFRASTRUCTURE

Due to the lack of requirements for the evaluation of information security systems technology for implementing virtual infrastructure, the goal was set for their development. In accordance with the guiding and methodological documents in the field of technical protection of information, a model was developed infrastructure, built with the use of virtualization technologies, which contains information of restricted access, not containing information constituting state secrets. Were defined the types of potential offenders security, the urgent threats, and develop a set of requirements for safety assessment of such infrastructure. In solving these problems were analyzed na-