ОТЗЫВ

официального оппонента, к.т.н., доцента

АБРАМОВА ЕВГЕНИЯ СЕРГЕЕВИЧА

на диссертационную работу Сенцовой Алины Юрьевны «Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений», представленной на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

1. Актуальность темы исследования

В последние годы наблюдается бурный рост числа потребителей облачных услуг. Это связано с тем, что эта новая парадигма в области информационных технологий предлагает технологические преимущества и привлекательные финансовые возможности. Так как потребители облачных услуг зачастую могут обрабатывать в «облаке» критичные информационные активы, на сегодняшний день вопрос обеспечения режима информационной безопасности (ИБ) облачных вычислений (ОВ) становится серьезной актуальной проблемой для поставщика облачных услуг. Аудит ИБ, проводимый в системе облачных вычислений, позволяет оцепить степень защищенности критичных актив потребителя в «облаке». При этом требуется рассмотреть вопросы, связанные с контролем доступа в облачной среде,

минимизацией риска в облачных средах и локализацией слабых мест в «облаке», и сформулировать рекомендации о путях решения проблем ИБ.

В настоящее время научные методики аудита ИБ, позволяющие оценить защищенность такого объекта защиты как система облачных вычислений, а также проработанные отечественные стандарты ИБ в данной области отсутствуют. Это позволяет сделать вывод, что диссертационное исследование, посвященное разработке моделей и метода экспертного аудита информационной безопасности в системе облачных вычислений, является актуальным.

2. Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Обоснованность научных положений, выводов и рекомендаций, сформулированных в диссертационной работе, подтверждена глубоким изучением достаточного числа научных работ отечественных и зарубежных авторов, связанных как с анализом проблем информационной безопасности облачных вычислений, так и с анализом возможностей в сфере аудита безопасности информационных систем. Кроме того, обоснованность результатов диссертационного исследования подтверждается применением известных методов и подходов, результатами апробации предложенного программного модуля для проведения аудита ИБ.

3. Достоверность и новизна полученных результатов

Достоверность полученных результатов диссертационной работы подтверждается логической последовательностью этапов работы, обоснованным выбором используемых методов и подходов, а также результатами апробации предложенного программного модуля для проведения аудита ИБ.

Новизна полученных результатов заключается в модели угроз для ОВ, построенной с помощью нечеткой когнитивной карты, при построении

которой были учтены угрозы, специфичные для облачных сервисов; в методике разработки частной политики безопасности облачных систем, которая позволяет исключить из иерархии ролей суперпользователя облачной системы; в методе экспертного аудита информационной безопасности системы облачных вычислений, реализуемом на основе оценки информационного риска в реальном масштабе времени с помощью искусственной нейронной сети; в программном модуле, с помощью которого можно оценить прогнозируемое и оперативное значения уровня информационного риска.

4. Теоретическая и практическая значимость работы

Теоретическая значимость результатов диссертационного исследования заключается в разработке нового метода экспертного аудита информационной безопасности для системы облачных вычислений на базе методов интеллектуального анализа данных об информационной системе.

Практическая значимость полученных результатов обусловлена тем, что разработанный автором программный модуль позволяет на основе данных с датчиков и сенсоров проводить оперативную оценку информационных рисков с целью дальнейшего принятия решений по выбору варианта реагирования на опасные события.

Практическая значимость результатов диссертационного исследования подтверждена актами об их использовании в ООО «Атлас-Телеком» и в учебном процессе ФГБОУ ВО «Уфимский государственный авиационный технический университет».

5. Оценка содержания диссертации, ее завершенность

Диссертация включает в себя четыре главы. Первая глава посвящена анализу проблем обеспечения информационной безопасности и проведения аудита ИБ в облачных средах. Во второй главе разрабатываются методика формирования частной политики ИБ для системы облачных вычислений и

модель угроз в виде нечетких когнитивных карт. Описываются угрозы нарушения ИБ и их источники, характерные для системы облачных вычислений. Третья глава посвящена разработке метода экспертного аудита ИБ на основе использования искусственной нейронной сети, а также функциональной модели, детализирующей предложенный метод аудита. В четвертой главе приводятся результаты разработки программного модуля, позволяющего автоматизировать процесс аудита ИБ в облачных средах, приведены результаты численного эксперимента.

Содержание диссертации в полной мере отражает суть работы и решение поставленных задач. Диссертация является законченной научно-квалификационной работой, написанной на грамотном научном языке. Автореферат также в полной мере отражает содержание диссертационного исследования.

6. Замечания

1. В диссертационной работе не представлено описание путей распространения угроз на множестве компонентов инфраструктуры системы облачных вычислений, которые отражены в виде модели угроз – нечеткой когнитивной карты.

2. В модели угроз, построенной в виде нечетких когнитивных карт, отсутствует объект атаки «контент сети доставки облака», который присутствует в обобщенной модели угроз.

3. Не приводятся статистические оценки результатов обучения нейронной сети, оценки ее обобщающей способности и результаты проверки на контрольном и тестовом множествах.

4. В диссертационной работе не приводятся размеры тестовой и контрольной выборок, а также способы разбиения генеральной совокупности примеров на три подмножества.

5. Программный модуль реализован с помощью языка программирования Pascal ABC, который в данный момент не поддерживается производителем.

7. Заключение

В целом, несмотря на указанные замечания, которые не снижают общую высокую оценку проведенного исследования, считаю, что диссертация Сенцовой Алины Юрьевны, представленная на соискание ученой степени кандидата технических наук, обладает научной новизной, теоретической и практической значимостью, является научно-квалификационной работой, в которой решена актуальная задача по разработке моделей и метода экспертного аудита информационной безопасности в системе облачных вычислений.

На основании вышеизложенного считаю, что представленная к защите диссертационная работа Сенцовой А.Ю. удовлетворяет требованиям п.9 Положения ВАК о присуждении ученых степеней, предъявляемым к диссертациям на соискания ученой степени кандидата технических наук, а ее автор, Сенцова Алина Юрьевна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
кандидат технических наук, доцент
Абрамов Евгений Сергеевич,
заведующий кафедрой безопасности
информационных технологий ФГАОУ ВО
«Южный федеральный университет»

30.11.2016

Личную подпись
удостоверяю
Ученый секретарь Совета
Южного федерального университета
Мирошниченко О.С.

Кандидатская диссертация защищена
по специальности 05.13.19 – Методы
и системы защиты информации,
информационная безопасность

347922, г. Таганрог,
Ул Чехова, д. 2
Тел. +7(8634) 37-19-05
E-mail: abramoves@sfedu.ru