ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА Д 212.288.07 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» МИНИСТЕРСТВА ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 20.12.2016 № 27

О присуждении **Сенцовой Алине Юрьевне,** гражданину РФ, ученой степени кандидата технических наук.

Диссертация «Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений» по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность принята к защите 14.10.2016 г., протокол № 24 диссертационным советом Д 212.288.07 на базе Федерального государственного бюджетного образовательного учреждения высшего образования «Уфимский государственный авиационный технический университет» Министерства образования и науки Российской Федерации, 450008, г. Уфа, ул. К. Маркса, 12, созданного приказом Министерства образования и науки Российской Федерации № 192/нк от 09.04.2013 г.

Соискатель Сенцова Алина Юрьевна 1991 года рождения, работает ассистентом кафедры вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет».

В 2013 году соискатель окончила ФГБОУ ВПО «Уфимский государственный авиационный технический университет».

В 2016 году соискатель окончила аспирантуру ФГБОУ ВО «Уфимский государственный авиационный технический университет».

Диссертация выполнена на кафедре вычислительной техники и защиты информации ФГБОУ ВО «Уфимский государственный авиационный технический университет».

Научный руководитель – доктор технических наук, доцент Машкина Ирина Владимировна, Уфимский государственный авиационный технический университет, профессор кафедры вычислительной техники и защиты информации.

Официальные оппоненты:

1. Доктор физико-математических наук, профессор Белим Сергей Викторович, Омский государственный университет им. Ф.М. Достоевского, заведующий кафедрой информационной безопасности.

2. Кандидат технических наук Абрамов Евгений Сергеевич, Южный федеральный университет, заведующий кафедрой безопасности информационных технологий.

дали положительные отзывы на диссертацию.

Ведущая организация ФГБОУ ВО «Оренбургский государственный университет» г. Оренбург в своем положительном заключении, подписанном Соловьевым Николаем Алексеевичем, доктором технических наук, профессором, заведующим кафедрой программного обеспечения вычислительной техники и автоматизированных систем, указала, что диссертация Сенцовой Алины Юрьевны на соискание ученой степени кандидата технических наук является научно-квалификационной работой, в которой содержится решение задач по разработке моделей и метода экспертного аудита информационной безопасности в системе облачных вычислений, имеющей существенное значение для соответствующей отрасли знаний, а именно для проведения аудита ИБ (информационной безопасности). Рассматриваемая работа соответствует требованиям п. 9 Положения о присуждении ученых степеней, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Соискатель имеет 18 опубликованных работ, в том числе по теме диссертации 18 работ, опубликованных в рецензируемых научных изданиях – 8. Общий объем опубликованных работ составляет 93 стр. Теоретические и практические результаты, полученные автором, докладывались и обсуждались на всероссийских и международных конференциях. Кроме того получено свидетельство о государственной регистрации программы для ЭВМ, а также издано одно учебное пособие. Наиболее значимые работы автора:

1. Сенцова, А.Ю. Методология экспертного аудита в системе облачных вычислений // И.В. Машкина, А.Ю. Сенцова. Безопасность информационных технологий. – М.: Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ. 2013. № 4. С. 63−70.

2. Сенцова, А.Ю. Автоматизация экспертного аудита информационной безопасности на основе использования искусственной нейронной сети // А.Ю. Сенцова, И.В. Машкина. Безопасность информационных технологий. – М.: Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ, №2, 2014. С. 118-126.

3. Сенцова, А.Ю. Программное средство для оценки оперативного значения риска нарушения информационной безопасности в системе облачных вычислений // А.Ю. Сенцова, И.В. Машкина. Известия ЮФУ. Технические науки. – Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ. – 2014,№8. С. 6-16.

4. Сенцова, А.Ю. Разработка частной политики информационной безопасности системы облачных вычислений // А.Ю. Сенцова, И.В. Машкина. Вестник УГАТУ. – 2016. – Том 20, № 2 (72). – С. 134-142.

5. Sentsova, A.U. The method of the information security risk assessment in cloud computing systems // A.U. Sentsova, I.V. Mashkina, O.B. Makarevich. Proceedings of the 6th International Conference on Security of Information and Networks (SIN-2013), Aksaray, Turkey. P 446-447.

На диссертацию и автореферат поступили отзывы:

- ведущей организации Оренбургский государственный университет с критическими замечаниями: 1) в разработанной архитектуре системы облачных вычислений отсутствует хранилище файлов потребителя облачных услуг; 2) из описания разработанной модели угроз остается неясным, учитывается ли в ней возможность скрыто нарушать требования частной политики безопасности СОбВ; 3) в модели угроз в качестве объекта атаки не указаны временные данные, создаваемые в процессе миграции виртуальных машин. Кроме того, из текста диссертации неясно какой именно объект соответствует этим данным в разработанной частной политике безопасности; 4) в диссертационной работе заявлено, что исследуется бизнес-модель продажи и использования приложения как услуги (SaaS). Однако остается неясным, может ли использоваться эта услуга потребителем облачных услуг с целью обеспечить защиту своей собственной информационной инфраструктуры с помощью удаленных средств защиты, которые будут располагаться в облаке сообщества; 5) в диссертационной работе не приведены результаты экспериментов с переобучением многослойного персептрона на заданном множестве данных обучающей выборки.

- официального оппонента, д.ф.-м.н., профессора Белима С. В. (Омский государственный университет им. Ф.М. Достоевского) с критическими замечаниями: 1) архитектура предложенной системы предполагает использование достаточно большого количества виртуальных машин. Однако хорошо известно, что виртуализация снижает скорость предоставления данных потребителю услуг. В связи с чем необходимо дополнительное тестирование скорости отклика на запрос, так как этот параметр определяет такую составляющую информационной безопасности как доступность; 2) из формального описания математической модели, представленной в разделе 2.3 остаётся непонятным, что с алгебраической точки зрения представляют собой такие сущности как система защиты информации Q и угроза безопасности информации U. В тексте диссертации написано, что они представлены некоторым набором множеств. Но остаётся неясным имеется в виду декартово произведение множеств или некоторое хитрое

множество из разнородных элементов; 3) в тексте диссертации нейронная сеть, используемая для проведения аудита информационной безопасности, в выходном слое имеет пять нейронов, тогда как аналогичная нейронная сеть, приведенная в автореферате, в выходном слое имеет один нейрон. Какая именно сеть использовалась в работе?

- официального оппонента, к.т.н., доцента Абрамова Е.С. (Южный федеральный университет) с критическими замечаниями: 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) в диссертационной работе 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.

- получено 6 положительных отзывов на автореферат. 1. РУНЦ «Информационная Безопасность – Юг России» ФГАОУ ВО «Южный федеральный университет» с критическим замечанием: из текста автореферата неясно, какие функции выполняют первая, вторая и третья линия техподдержки поставщика облачных услуг и чем эта служба отличается от службы автоматизации ИСОТ. 2. Оренбургский государственный университет с критическим замечанием: из текста автореферата остается неясным, учтен ли при составлении модели угроз в виде нечетких когнитивных карт уровень оркестровки облачных сред. 3. Кубанский государственный университет, замечание которого связано с ограниченностью объема автореферата. 4. Башкирский государственный

университет, замечание которого связано с ограниченностью объема автореферата. 5. Томский государственный университет систем управления и радиоэлектроники с критическим замечанием: не совсем понятно, что автор подразумевает под «датчиками опасных событий» в контексте систем облачных вычислений. 6. Институт информационных технологий и телекоммуникаций Северо-Кавказского федерального университета (ИИТТ СКФУ) с критическим замечанием, которое связано с ограниченностью объема автореферата.

Выбор официальных оппонентов и ведущей организации обосновывается их широкой известностью своими достижениями в данной отрасли науки, наличием публикаций в соответствующей сфере исследования и способностью определить научную и практическую ценность диссертации.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработаны *модель угроз* нарушения информационной безопасности в системе облачных вычислений (СОбВ), построенная с помощью нечеткой когнитивной карты, отличающаяся возможностью визуализации путей распространения угроз в облачных средах и расширения списка источников угроз для СОбВ, позволяющая учесть угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, а также учесть такой источник угроз как другой потребитель облачных услуг, реализующий собственные бизнес-задачи; *метод проведения экспертного аудита* информационной безопасности системы облачных вычислений, отличающийся получением количественной оценки оперативного значения уровня риска нарушения информационной безопасности с использованием искусственной нейронной сети при обработке ею информации с сенсоров и датчиков опасных событий, обучение которой осуществляется на множестве данных обучающей выборки, сформированной на основе аналитических расчетов прогнозируемого значения уровня риска с использованием когнитивной карты в качестве модели угроз, что позволяет поставщику облачных услуг обосновать свои возможности по обеспечению

защищенности критичной информации потребителя и обеспечить адекватное реагирование на возможные инциденты в реальном масштабе времени; *модель программного средства* проведения аудита информационной безопасности (ИБ) системы облачных вычислений и *программный модуль*, автоматизирующий процесс проведения аудита ИБ и позволяющий посредством использования информации с датчиков событий получить количественную оценку риска, на основе которой возможен выбор рационального варианта реагирования на инцидент в реальном масштабе времени.

предложена *методика разработки частной политики безопасности* для СОбВ, базирующаяся на модели ролевого разграничения доступа, отличающаяся назначением нескольких максимальных ролей, которые имеют одновременно и максимально необходимую роль в собственном подразделении облака сообщества, и необходимую роль для поддержки бизнес-процессов СОбВ, что позволяет исключить пользователя, получающего по иерархии ролей права суперпользователя поставщика и исключить возможность для него напрямую обращаться к потокам данных потребителя облачных услуг и управлять всеми конфигурационными файлами системы облачных вычислений.

введены термин «система облачных вычислений», подразумевающий систему информационного взаимодействия потребителя и поставщика облачных услуг, и термин «оперативное значение уровня риска нарушения информационной безопасности», подразумевающий численное значение уровня риска в реальном масштабе времени, когда угроза распространяется по одному из спрогнозированных путей.

Теоретическая значимость исследования обоснована тем, что:

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) **использованы** теория нечетких когнитивных карт, модель ролевого разграничения доступа, методы системного анализа, методология функционального моделирования и моделирования динамических систем, теория искусственных нейронных сетей,

изложены *этапы проведения аудита* информационной безопасности на основе

оценивания защищенности системы облачных вычислений, *этапы создания частной политики безопасности* для системы облачных вычислений,

изучены *применимость* научно-теоретических результатов при проведении экспертного аудита информационной безопасности в системе облачных вычислений, *множество* возможных преднамеренных угроз информационной безопасности в информационной системе, построенной на основе облачных технологий.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены: *в организации ООО «Атлас-Телеком», являющейся потребителем облачных услуг,* метод проведения экспертного аудита информационной безопасности в системе облачных вычислений, а также *в учебном процессе на кафедре вычислительной техники и защиты информации ФГБОУ ВО «УГАТУ»* - метод построения моделей угроз информационной безопасности в виде нечетких когнитивных карт, методика разработки частной политики информационной безопасности в системе облачных вычислений,

предложен метод проведения аудита информационной безопасности, который является насущным и актуальным в связи с тем, что нормативная база РФ в области защиты облачных сред слабо проработана, а практически применимые методы анализа информационного риска отсутствуют не только в нормативных документах РФ, но и в международных стандартах и актах,

созданы модель автоматизированного средства, блок-схема алгоритма работы программного модуля и программный модуль, позволяющие аудитору автоматизировать процесс проведения аудита информационной безопасности и обеспечивающие по результатам экспериментов повышение оперативности обработки опасных событий в системе облачных вычислений более чем в 10 раз.

Оценка достоверности результатов исследования выявила:

теория построена на использовании апробированных методов исследования, корректном применении математического аппарата и согласуется с известными теоретическими положениями,

для экспериментальных работ результаты исследования подтверждаются актом внедрения в организацию ООО «Атлас-Телеком», которая является потребителем облачных услуг, а также подтверждаются результатами проведенных расчетов и имитационного моделирования;

использованы статистические данные и международные базы данных уязвимостей программного и аппаратного обеспечения информационных систем и сервисов безопасности.

Личный вклад соискателя состоит в:

получении соискателем всех основных результатов, выносимых на защиту, подготовке публикаций, в том числе в рецензируемых изданиях из перечня ВАК, и выступлениях на всероссийских и международных конференциях.

Диссертационный совет пришел к выводу, о том, что в диссертации:

-соблюдены установленные Положением о присуждении ученых степеней критерии, которым должна отвечать диссертация на соискание ученой степени;

- отсутствуют недостоверные сведения об опубликованных соискателем ученых степеней работах, в которых изложены основные научные результаты диссертации;

- соискатель ссылается на авторов и источники заимствования;

- оригинальность диссертационной работы составляет 91,42%.

Диссертационная работа Сенцовой А.Ю. «Модели и метод экспертного аудита информационной безопасности в системе облачных вычислений» соответствует п. 9 Положения о присуждении ученых степеней (утвержденного Постановлением Правительства Российской Федерации от 24 сентября 2013 года № 842, в редакции с изменениями, утв. Постановлением Правительства РФ от 21 апреля 2016 года № 335), предъявляемых к кандидатским диссертациям.

Тема работы и содержание исследований соответствуют паспорту научной специальности ВАК 05.13.19 – Методы и системы защиты информации, информационная безопасность по пунктам п.7 «Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения»; п. 14 «Модели,

методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности».

Диссертация Сенцовой А.Ю. является законченной научно-квалификационной работой, в которой решена задача проведения аудита информационной безопасности системы облачных вычислений, имеющей существенное значение для развития соответствующей отрасли знаний, а именно для проведения аудита ИБ.

.На заседании 20.12.2016 г. диссертационный совет принял решение присудить Сенцовой А.Ю. ученую степень кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

При проведении тайного голосования диссертационный совет в количестве 17 человек, из них 6 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 22 человек, входящих в состав совета, проголосовали: за – 17, против – 0, недействительных бюллетеней – 0.

Председатель
диссертационного совета Султанов Альберт Ханович

Ученый секретарь
диссертационного совета Виноградова Ирина Леонидовна

20 декабря 2016 года