На правах рукописи

СЕНЦОВА Алина Юрьевна

МОДЕЛИ И МЕТОД ЭКСПЕРТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Специальность 05.13.19 –
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа – 2016

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

Научный руководитель: доктор технических наук, доцент
МАШКИНА Ирина Владимировна

Официальные оппоненты: доктор физико-математических наук, профессор
Белим Сергей Викторович
ФГБОУ ВО «Омский государственный университет им. Ф.М. Достоевского», заведующий кафедрой информационной безопасности

кандидат технических наук, доцент
Абрамов Евгений Сергеевич
Институт компьютерных технологий и информационной безопасности Инженерно-технологической академии ФГАОУ ВО «Южный федеральный университет», заведующий кафедрой безопасности информационных технологий

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет», г. Оренбург

Защита диссертации состоится 20 декабря 2016 г. в 10^{00} часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВО «Уфимский государственный авиационный технический университет» по адресу: 450008, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» _____ 20___ года.

Ученый секретарь
диссертационного совета,
д-р техн. наук, доцент И.Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Сегодня в индустрии информационных сервисов можно наблюдать стремительные темпы развития информационных систем, построенных на основе облачных технологий (ИСОТ). Облачные вычисления позволяют современным компаниям снизить расходы на физическую инфраструктуру, уменьшить затраты времени и ресурсов на администрирование информационных систем, а также снизить финансовые затраты на построение собственной инфраструктуры. Уже сейчас аналитики прогнозируют развитие рынка облачных услуг для бизнеса в России более чем в четыре раза в течение 2016 года (39 млрд. руб.), а к 2020 году объем мирового облачного рынка составит $241 млрд. В связи с тем, что, зачастую, компании-потребители облачных услуг могут обрабатывать в облачных средах критичные для них информационные активы, на сегодняшний день вопрос обеспечения информационной безопасности ИСОТ является наиболее актуальным для потребителя облачных услуг.

Хотя поставщики, обслуживая предприятия с оборотом в миллиарды долларов, делают все возможное для обеспечения максимальной безопасности среды облака, особенности построения облачной инфраструктуры, использование технологии виртуализации и связанная с ней возможность нарушения изоляции виртуальных машин, а также параллельная обработка больших объемов данных разных потребителей облачных услуг на одном физическом сервере позволяют говорить о новых потенциально возможных угрозах информационной безопасности (ИБ), которые будут являться специфичными для облачных сред.

Объективная оценка степени защищенности данных потребителя облачных услуг в облачной инфраструктуре поставщика осуществляется в ходе проведения аудита ИБ. В результате аудита ИБ ИСОТ можно выявить, насколько рационально решены вопросы безопасности информации и контроля доступа в облачной среде, определить, как минимизировать риски при обработке в ИСОТ конфиденциальной информации потребителя облачных услуг, локализовать слабые места в системе обеспечения ИБ и сформулировать рекомендации о путях решения существующих проблем безопасности в системе. Кроме того, потребитель заинтересован в определении поставщиком конкретного механизма для оценки качества предлагаемой облачной услуги.

Степень разработанности темы. На сегодняшней день практически отсутствуют серьезные исследования не только в области аудита информационной безопасности облачных вычислений, но и публикации, посвященные общим вопросам ИБ облачных сред. В работах П.Д. Зегжды, Д.П. Зегжды, Л.К. Бабенко отмечается рост рынка облачных услуг и рассматриваются основные угрозы ИСОТ и, в особенности, угрозы, связные с технологией виртуализации, используемой в облачных вычислениях. В работах С.В. Белима и Н.Ф. Богаченко обосновывается важность обеспечения ИБ в облачных вычислениях и особенно подчеркивается необходимость контроля доступа к предоставляемым поставщику ресурсам. Многие исследования

вопросов безопасности облачных сред, в числе которых работы Маслова В.А., Рахматуллиной А.Р., Варновского Н.П., Захарова В.А., Шокурова А.В., сводятся к проблемам шифрования потока межоблачных данных между поставщиком и потребителем облачных услуг. Однако в них не рассматриваются специфичные для облачных вычислений угрозы и средства защиты. В работах Зубарева И.В., Радина П.К., Демурчева Н.Г., Коваленко О.С., Алимурадова Т.К. рассматриваются основные угрозы ИСОТ, а также отмечается необходимость разделения полномочий облачной среды, но не описываются конкретные механизмы для устранения угроз ИБ и минимизации предоставления избыточных привилегий поставщику ИСОТ. В работах Шаньгина В.Ф., Нестеркиной Е.М., Бердника А.К., Царегородцева А.В., Качко А.К. подчеркивается необходимость стандартизации облачных вычислений в РФ, а также делается вывод: из-за отсутствия стандартов в области ИБ облачных вычислений проведение аудита системы обеспечения ИБ ИСОТ, на сегодняшний день, затруднено. Конкретные же решения в области проведения аудита облачных вычислений также отсутствуют.

Вместе с тем, для обеспечения сохранности конфиденциальной информации, обрабатываемой в облачной среде, существующая система обеспечения ИБ ИСОТ должна периодически подвергаться независимому аудиту, который, в соответствии с требованиями международных стандартов, является одним из обязательных этапов жизненного цикла любой информационной системы.

Объектом исследования является информационная система взаимодействия поставщика и потребителя облачных услуг – система облачных вычислений (СОбВ).

Предметом исследования являются модели и метод экспертного аудита ИБ в системе облачных вычислений.

Целью исследования является повышение оперативности и адекватности оценки уровня опасности инцидентов в системе информационного взаимодействия поставщика и потребителя облачных услуг.

Задачи исследования:

1. Определить *перечень угроз* нарушения информационной безопасности, характерных для облачных вычислений, и *их источники*. Разработать *модель* преднамеренных *угроз* нарушения ИБ с учетом особенностей СОбВ.

2. Разработать *методику* формирования частной политики безопасности СОбВ, основываясь на рекомендациях проектов государственных стандартов РФ в сфере облачных вычислений и учитывая специфику информационных систем, построенных на основе технологии облачных вычислений.

3. Разработать *метод проведения аудита информационной безопасности* системы облачных вычислений, основанный на получении численной оценки риска нарушения ИБ с использованием искусственной нейронной сети.

4. Разработать *программный модуль автоматизации процесса экспертного аудита ИБ* СОбВ, реализующий предложенные модели и метод. Исследовать адекватность предложенных моделей и метода на основе вычислительных экспериментов.

Методы исследования. При решении поставленных в диссертационной работе задач использованы методы системного анализа, методы теории защиты информации, теории множеств, теории нечетких когнитивных карт, методология функционального моделирования и моделирования динамических систем, а также теория искусственных нейронных сетей.

Положения, выносимые на защиту

1. Выявлен *перечень угроз* нарушения ИБ от *источников угроз*, характерных для СОбВ, и разработана *модель* преднамеренных целенаправленных *угроз* нарушения ИБ, основанная на построении нечетких когнитивных карт с учетом особенностей инфраструктуры СОбВ.

2. Предложены *модель политики* информационной *безопасности* ИСОТ и *методика разработки частной политики безопасности* СОбВ, основанная на ролевой модели, *позволяющая исключить* из иерархии ролей роль *суперпользователя,* имеющего полномочия напрямую обращаться к результирующим потокам данных, *управлять* всеми конфигурационными файлами СОБВ, и, тем самым, *увеличить* доверие потенциальных потребителей к ИСОТ

3. Разработан *метод аудита ИБ*, основанный на использовании искусственной нейронной сети, отличающийся получением численной оценки оперативного значения риска, когда угроза проявляется по конкретному пути распространения.

4.Разработана *модель программного средства* проведения аудита ИБ системы облачных вычислений и *программный модуль*, автоматизирующий процесс проведения аудита ИБ и *позволяющий посредством информации с датчиков событий* получить численную оценку риска, на основе которой возможен выбор рационального варианта реагирования на инцидент в реальном масштабе времени.

Научная новизна

1. Новизна модели угроз нарушения информационной безопасности в системе облачных вычислений, построенной с помощью нечеткой когнитивной карты, заключается в визуализации путей распространения угроз в облачных средах и в расширении списка источников угроз для СОбВ, что позволяет 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.

2. Новизна *методики разработки частной политики безопасности* для СОбВ, базирующейся на модели ролевого разграничения доступа, *заключается* в назначении 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.

3. Новизна метода проведения *экспертного аудита* информационной безопасности системы облачных вычислений состоит в получении численной 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.

4. Новизна *программного модуля*, реализующего метод аудита ИБ СОбВ, заключается в возможности оценить*:* *прогнозируемое* значение уровня риска нарушения ИБ при проектировании системы защиты информации в СОбВ, *оперативное* значение уровня риска в *реальном масштабе времени* в процессе реализации угрозы по конкретному пути, а также *с учетом сложных сценариев атак*.

Обоснованность и достоверность результатов диссертации основана на использовании известных аналитических методов, а также подтверждается результатами моделирования и результатами апробации программного модуля, реализующего предложенные модели и метод.

Апробация результатов. Основные положения диссертационной работы докладывались и обсуждались на следующих научных конференциях: V, VI, VII, VIII и IX Всероссийских молодежных научных конференциях «Мавлютовские чтения», Уфа, 2011, 2012, 2013, 2014, 2015; XII и XIII Всероссийских конкурсах-конференциях студентов и аспирантов по информационной безопасности «SIBINFO-2012» и «SIBINFO-2013», Томск, 2012, 2013; VIII Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России (ИБРР-2013), Санкт-Петербург, 2013; XII и XIII Международных научно-практических конференциях «Информационная безопасность-2012» и «Информационная безопасность-2012», Таганрог, 2012, 2013; IV Всероссийской молодежной конференции по проблемам информационной безопасности «Перспектива-2014», Таганрог, 2014; XXI Всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Москва, 2014; The 7th International Conference on Security of Information and Networks (SIN 2014), 2014, г. Аксарай, Турция.

Результаты диссертационного исследования внедрены в производственный процесс ООО «Атлас-Телеком» и в учебный процесс кафедры «Вычислительная техника и защиты информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет». На программный модуль, автоматизирующий процесс проведения аудита ИБ, получено свидетельство о государственной регистрации программы для ЭВМ.

Публикации. По материалам диссертации опубликовано 18 научных работ, в том числе 9 статей в рецензируемых научных журналах из перечня

ВАК, 1 статья в зарубежном научном издании, входящем в базу цитирования SCOPUS, получено одно свидетельство о государственной регистрации программы для ЭВМ.

Теоретическая и практическая значимость работы

Теоретическая значимость полученных результатов заключается в расширении списка источников угроз для системы облачных вычислений; в разработанном с использованием методологии функционального моделирования IDEF0 графическом представлении механизма оценивания значений уровня риска нарушения ИБ в реальном масштабе времени с помощью искусственной нейронной сети; в разработанном *методе аудита ИБ в СОбВ*, апробированном на практике при решении задачи определения оперативного значения уровня риска нарушения ИБ; в разработанной *модели частной политики информационной безопасности* СОбВ, соблюдение требований которой позволит увеличить доверие потенциальных потребителей к ИСОТ и модернизированной *методике разработки частной политики безопасности* СОбВ, которая позволяет исключить роль суперпользователя из множества субъектов доступа системы облачных вычислений.

Практическая значимость разработанных моделей и метода заключается в разработанном *программном модуле*, позволяющем автоматизировать процесс аудита системы защиты информации СОбВ в соответствии с предлагаемым методом аудита ИБ системы облачных вычислений, и в возможности обосновать рекомендации в случае необходимости модернизации сети и установить специфичные для облачных сред средства защиты в целях повышения уровня защищенности всей СОбВ в целом, в возможности принятия решений по выбору рационального варианта реагирования в соответствии с величиной риска в реальном масштабе времени.

Личный вклад. Постановка основных задач принадлежит научному руководителю. Самостоятельно исследованы компоненты архитектуры СОбВ, предложена методика разработки частной политики ИБ: перечень субъектов доступа для СОбВ, иерархическая структура ролей пользователей; осуществлен выбор оптимальной архитектуры ИНС, сформирована обучающая выборка для обучения ИНС, проведены вычислительные эксперименты, разработано алгоритмическое обеспечение для реализации программного модуля.

Материалы диссертационной работы использовались при выполнении гранта РФФИ № 14-07-00928 по теме «Разработка и исследование моделей и методов принятия решений по обеспечению защищенности корпоративных информационных систем и систем облачных вычислений на основе интеллектуальных технологий».

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка используемой литературы и приложений. Содержит 208 с. машинописного текста, 48 рисунков, список использованной литературы из 108 наименований, приложений на 18 с.

СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении обоснована актуальность темы диссертации, сформулированы цель и задачи исследования, определены объект и методы исследования, представлены положения, выносимые на защиту, изложена научная новизна и практическая ценность результатов диссертации, приводятся сведения об апробации работы.

Первая глава посвящена анализу деятельности по обеспечению ИБ в СОбВ, эффективность которой зависит от наличия утвержденной и соблюдаемой политики безопасности и может быть оценена в ходе проведения аудита ИБ.

Приводятся результаты анализа видов облачных услуг и моделей облачного размещения, а также обзор литературных источников, освещающих проблемы облачных вычислений. Анализируется концепция ИБ вычислительного облака. Отмечается, что большинство специалистов считают безопасность барьером для потребителя на пути перехода к облачным вычислениям, что позволяет сделать вывод о необходимости новых технологических решений в области безопасности облачных сред, создания нормативной правовой базы для облачных вычислений в РФ.

Выявляются конкретные проблемы ИБ в облачных средах, среди которых отмечается расширение перечня информационных угроз, появление новых ранее неизвестных уязвимостей и способов реализации атак.

Проанализированы литературные источники, посвященные аудиту ИБ. Подчеркивается, что аудит является основным инструментом оценки эффективности системы обеспечения ИБ и ее соответствия потребностям бизнеса.

Описываются два подхода к проведению аудита ИБ: аудит, базирующийся на анализе рисков нарушения ИБ, и аудит на соответствие стандартам в области ИБ. Отмечается, что для информационных систем, отечественные нормативные документы для которых находятся в стадии разработки, единственным способом оценивания защищенности является аудит, основанный на оценке рисков нарушения ИБ.

Анализируются отечественные нормативные правовые акты в области аудита ИБ. В ходе анализа выясняется, что ни один из предложенных в нормативных актах методов проведения аудита ИБ не удовлетворяет полностью всем факторам, влияющим на выбор метода оценки рисков.

Обосновывается актуальность разработки метода проведения аудита ИБ, который бы исключал выявленные недостатки существующих методов.

На основании сделанных заключений сформулированы основные научно-теоретические задачи, решаемые в диссертационной работе.

Вторая глава посвящена методике формирования частной политики ИБ и разработке модели угроз в системе облачных вычислений на основе построения нечетких когнитивных карт.

В связи с тем, что разработать модель угроз, провести аудит ИБ и оценить уровень защищенности облачной системы в общем виде, без учета

особенностей облачной инфраструктуры потребителя и поставщика облачных услуг, невозможно, на основе проведенного анализа возможных схем клиент-серверного взаимодействия, изучения концепции вычислительного облака для обеспечения услуги SaaS и требований для типовой ИСОТ на примере облачного решения Azure разработана архитектура системы облачных вычислений для облака сообщества (рис. 1).

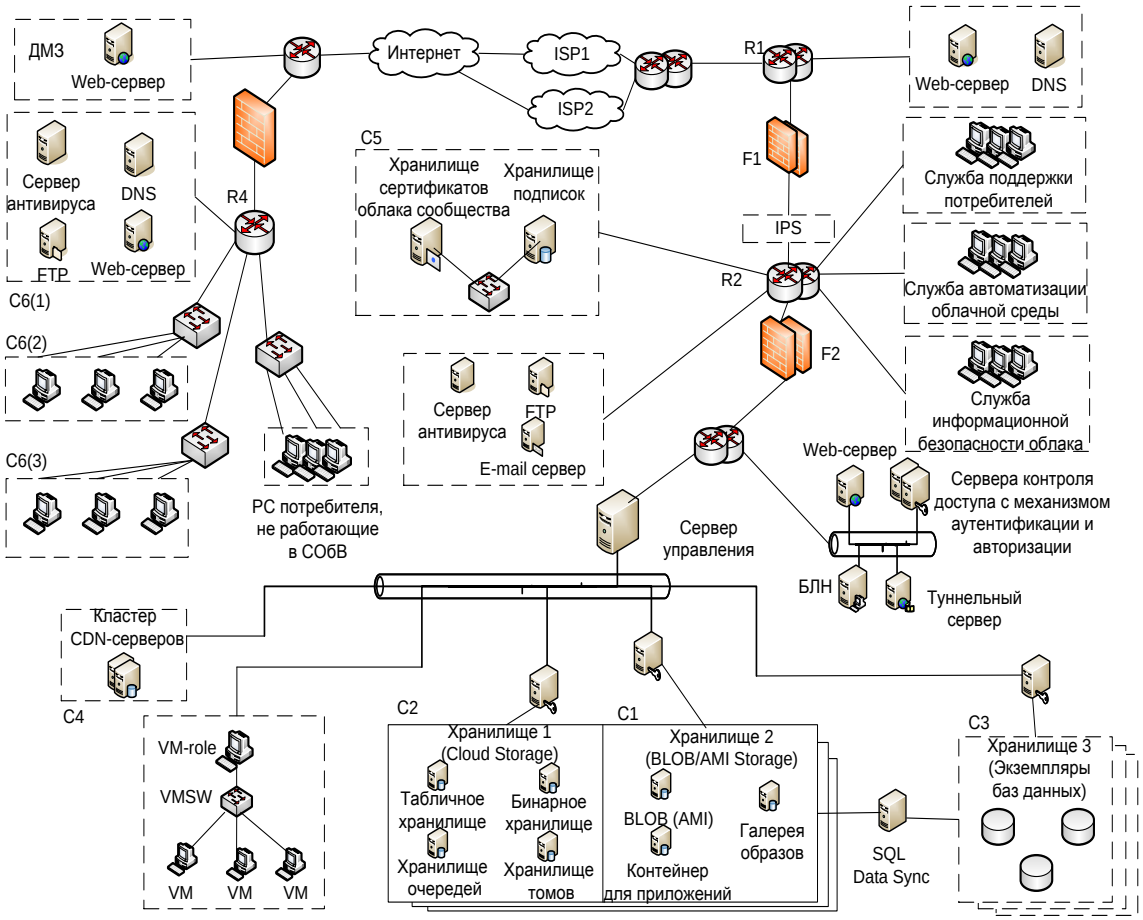

Рис. 1 – Архитектура системы облачных вычислений

На основе проведенных исследований сформирован перечень угроз нарушения ИБ, реализуемых в инфраструктуре системы облачных вычислений.

Для устранения угроз, связанных с неопределённостью при распределении ответственности, поставщику облачных услуг необходимо тщательно прорабатывать политику безопасности. Предлагается модель политики ИБ, включающая в себя совокупность частных политик безопасности и учитывающая особенности услуги SaaS. В диссертационной работе разрабатывается одна из частных политик безопасности СОбВ, а именно политика управления доступом субъектов доступа к информационным объектам. Выявлены сущности, специфичные для системы облачных вычислений, перечень которых представлен в табл. 1.

Табл. 1 (фрагмент) – Выявленные множества сущностей для СОбВ

Обозн.	Наименование
Объекты доступа	
o1	Сайт поставщика облачных услуг
o3 (*i*)	Образы виртуальных машин отдела потребителя облачных услуг, осуществляющего работу по проекту i
o4 (*i*)	Информационные ресурсы по проекту i, хранящиеся в облачном хранилище
o5	Файлы СОбВ, относящиеся к конфигурированию собственных виртуальных машин конкретным потребителем облачных услуг
Субъекты доступа	
LT1	Сотрудник первой линии техподдержки поставщика облачных услуг
LT2	Сотрудник второй линии техподдержки поставщика облачных услуг
P1	Технический директор потребителя облачных услуг
P2, P3	Руководители подразделений потребителя облачных услуг, осуществляющих эксплуатацию СОбВ в соответствии с бизнес-процессами

На основе исследования взаимодействия поставщика облачных услуг с конкретным потребителем – членом облака сообщества, разработана иерархическая структура ролей в СОбВ (рис. 2). Так как система облачных вычислений – это система, в которой взаимодействуют поставщик и потребитель облачных услуг, предложено модифицировать ролевую модель разграничения доступа таким образом, что каждая из представленных сторон (потребитель и поставщик) имеет свою максимальную роль в иерархии, в отличие от известной ролевой модели разграничения доступа, где максимальная роль в иерархии одна. Для поставщика облачных услуг максимальной ролью является роль технического директора поставщика (L1), для потребителя, соответственно, − технического директора потребителя облачных услуг (P1).

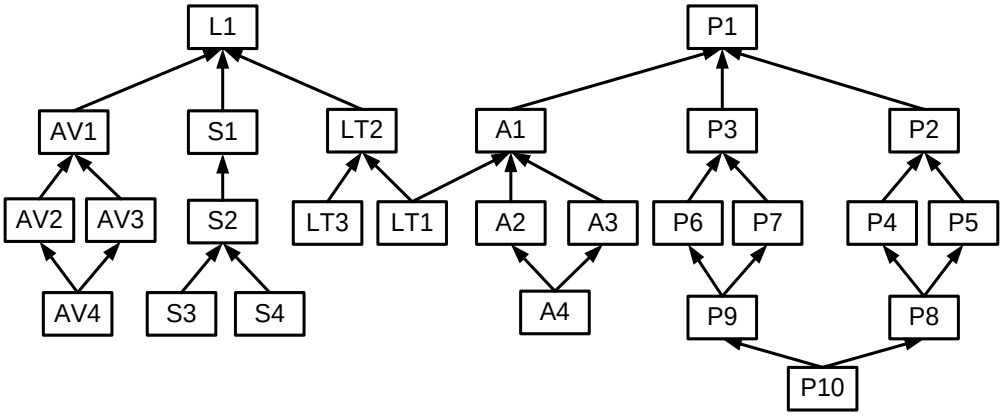

Рис. 2 – Иерархическая структура ролей в СОбВ

На основе выявленного множества сущностей и разработанной иерархической структуры ролей в СОбВ сформирована матрица прав доступа ролей СОбВ.

Табл. 2 – Матрица прав доступа ролей пользователей СОбВ

	o1	*o2*	*o3 (1)*	*o3 (2)*	*o4 (1)*	*o4 (2)*	*o5*	*o6 (1)*	*o6 (2)*	*o7*	*o8*	*o9*	*o10 (1)*	*o10 (2)*	*o11 (1)*	*o11 (2)*
L1	rw	w	-	-	-	-	-	rw	rw	rw	rw	rw	-	-	-	-
LT2	rw	w	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
LT1	r	-	-	-	-	-	-	-	-	rw	rw	r	-	-	-	-
LT3	r	-	-	-	-	-	-	w	-	-	-	-	-	-	-	-
S1	rw	-	-	-	-	-	-	rw	-	rw	rw	rw	-	-	-	-
S2	rw	-	-	-	-	-	-	rw	-	r	rw	r	-	-	-	-
S3	r	-	-	-	-	-	-	rw	-	r	-	r	-	-	-	-
S4	r	-	-	-	-	-	-	rw	-	r	r	r	-	-	-	-
AV1	r	w	-	-	-	-	-	r	rw	r	r	r	-	-	-	-
AV2	r	w	-	-	-	-	-	r	rw	-	-	-	-	-	-	-
AV3	r	-	-	-	-	-	-	-	rw	r	r	r	-	-	-	-
AV4	r	-	-	-	-	-	-	-	rw	-	-	-	-	-	-	-
P1	r	rw	rwe	rwe	rw	rw	rw	-	-	rw	rw	r	rw	rw	rw	rw
A1	r	rw	rw	rw	-	-	rw	-	-	rw	rw	-	-	-	rw	rw
A3	r	rw	-	w	-	-	rw	-	-	rw	-	-	-	-	w	w
A2	r	rw	-	w	-	-	-	-	-	r	-	-	-	-	w	w
A4	r	rw	-	-	-	-	-	-	-	r	-	-	-	-	-	-
P2	r	rw	re	-	rw	-	-	-	-	r	-	r	rw	-	rw	-
P4,5	r	r	re	-	rw	-	-	-	-	-	-	-	rw	-	rw	-
P8	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
P3	r	rw	-	re	-	rw	-	-	-	r	-	r	-	rw	-	rw
P6,7	r	r	-	re	-	rw	-	-	-	-	-	-	-	rw	-	rw
P9	r	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

В диссертационной работе во внимание принимаются угрозы несанкционированного доступа, источниками которых являются субъекты, нарушающие политику разграничения доступа: потребитель облачных услуг или запущенный им процесс, сотрудник поставщика облачных услуг, *другой потребитель облачных услуг* (наличие данного источника обусловлено динамической масштабируемостью и консолидацией вычислительных ресурсов, а также возможностью самообслуживания потребителей), злоумышленник − субъект, не являющийся потребителем услуг облака сообщества.

С учетом всех возможных источников угроз, объектов атак и уязвимостей компонентов инфраструктуры СОбВ, а также с учетом частной политики ИБ для облака сообщества SaaS, разработана модель угроз в виде двух нечетких когнитивных карт (НКК). В качестве примера на рис. 3 представлена НКК − модель угроз несанкционированного доступа, реализуемых злоумышленником, с целью проникновения с удаленного компьютера внутрь защищаемой системы облачных вычислений и реализуемых сотрудником-нарушителем другого потребителя облачных услуг связанных с попыткой повышения полномочий другим потребителем не в соответствии с ролью, предоставленной ему для выполнения функциональных обязанностей.

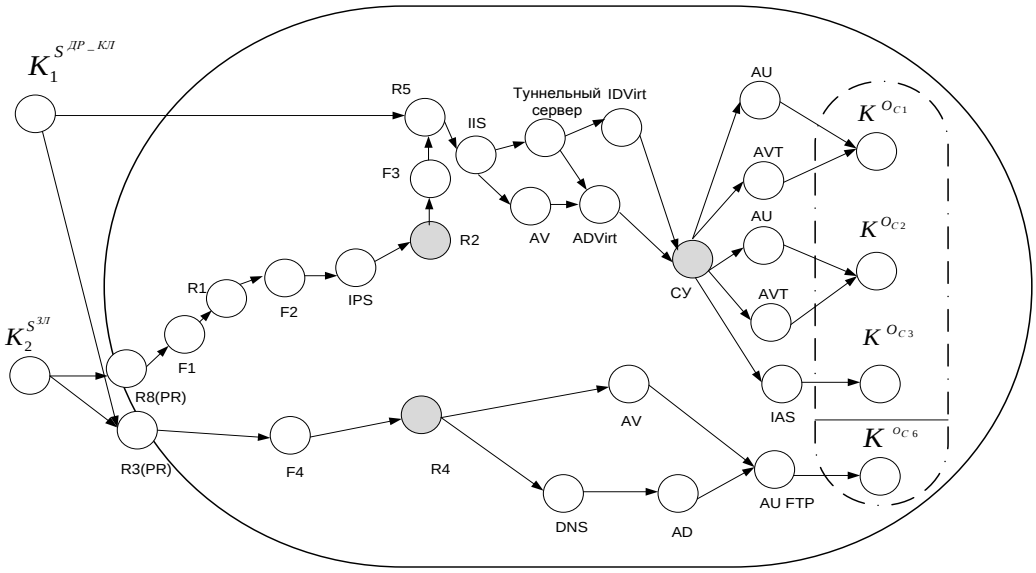

Рис. 3 − НКК1 – модель угроз несанкционированного доступа, реализуемых злоумышленником и другим потребителем облачных услуг

Вторая НКК, приведенная в диссертационной работе, представляет собой модель внутренних угроз несанкционированного доступа, реализуемых сотрудником службы поставщика облачных услуг и сотрудником-нарушителем компании потребителя облачных услуг, которые пытаются превысить свои полномочия не в соответствии с ролью, предоставленной им для выполнения функциональных обязанностей.

Разработка модели угроз и оценка величин угроз является необходимым этапом разработанного метода экспертного аудита.

Третья глава посвящена разработке метода проведения экспертного аудита ИБ системы облачных вычислений, основанного на получении численной оценки риска нарушения ИБ с использованием искусственной нейронной сети.

Введены понятия прогнозируемого значения уровня риска нарушения ИБ и оперативного значения уровня риска. Оценка *прогнозируемого* значения риска связана со *стратегией* безопасности, которая разрабатывается для СОбВ заблаговременно. В ходе мониторинга безопасности системы обеспечивается получение информации о состоянии сетевых устройств в облаке, о событиях, нарушающих безопасность, в *реальном масштабе времени*. На основе численного *оперативного* значения уровня риска возможно принятие решений о том, какие именно тактические действия необходимо применять в данный конкретный момент времени.

Метод экспертного аудита, предложенный в работе, включает в себя:

- построение модели угроз в виде нечеткой когнитивной карты;
- аналитические расчеты прогнозируемых значений уровня риска нарушения ИБ в системе облачных вычислений, которые выполняются на основе построенной модели угроз;
- формирование на основе результатов аналитических расчетов прогнозируемых значений уровня риска множества данных обучающей выборки, настройка и обучение ИНС;

● определение оперативного значения уровня риска в реальном масштабе времени на основе данных с датчиков событий;

● формирование аудитором отчета на основе полученных прогнозируемых значений уровня риска;

● принятие решений о выборе адекватного варианта реагирования на опасные события на основе оперативного значения уровня риска.

Для успешного использования нейронных сетей специалисту по ИБ необходимо сформировать множество данных обучающей выборки, исходя из текущих сведений о рассматриваемой системе. Производится выбор оптимальной структуры нейронной сети и выбор эффективного по своим параметрам алгоритма обучения ИНС, в которых будет учитываться специфика обучающей выборки.

В качестве числовых входных данных для формирования репрезентативного множества данных для обучения искусственной нейронной сети предлагается использовать *результаты расчета прогнозируемого значения риска* нарушения ИБ СОбВ. В таблице 3 приведен фрагмент множества данных для обучения ИНС.

Табл. 3 – Фрагмент множества данных обучающей выборки

ЗЛ	ДР_ПОТ	ПОС	ПОТ	С1	С2	С3	С4	R
0	0	0	1	0	0	0,3	0,7	0,008
0	0	0	1	0	0,1	0,3	0,6	0,0288
0	0	0	1	0,1	0,1	0,3	0,5	0,041
0	0	0	1	0,2	0,1	0,3	0,4	0,054
0	0	0	1	0,3	0,1	0,3	0,3	0,066
0	0	0	1	0,4	0,1	0,3	0,2	0,079
0	0	0	1	0,5	0,1	0,3	0,1	0,091
0	0	0	1	0,6	0,1	0,3	0	0,1
0	0	1	0	0	0	0,3	0,7	0,15
0	0	1	0	0	0,1	0,3	0,6	0,13
0	0	1	0	0,1	0,1	0,3	0,5	0,11
0	0	1	0	0,2	0,1	0,3	0,4	0,088
0	0	1	0	0,3	0,1	0,3	0,3	0,066
0	0	1	0	0,4	0,1	0,3	0,2	0,044
0	0	1	0	0,5	0,1	0,3	0,1	0,022

Проведен численный эксперимент, в ходе которого выявлено, что сформированное в работе репрезентативное множество данных обучающей выборки вырабатывает у выходных сигналов нечувствительность к вариациям входных величин при условии, что эти вариации находятся в допустимых границах [0,1]. Также выходы ИНС не зависят от шага дискретизации, который будет использован для натренированной нейронной сети. Кроме того, аналогичные входные сигналы вызывают аналогичные реакции даже в случае, если они не входили в состав обучающего множества.

Для проведения аудита ИБ на основе оценки риска был выбран персептрон с одним скрытым слоем, представленный на рис. 4.

На основе предложенного метода экспертного аудита ИБ разработаны IDEF0 модели. В соответствии с методом, контекстный функциональный блок представлен тремя подпроцессами: «Рассчитывать прогнозируемый риск нарушения ИБ», «Настраивать и обучать нейронную сеть», «Рассчитывать оперативное значение уровня риска нарушения ИБ».

Четвертая глава посвящена рассмотрению практических аспектов использования предложенного метода аудита ИБ СОбВ.

Приводятся результаты численного эксперимента, в ходе которого исследовалась эффективность алгоритма обратного распространения ошибки для обучения искусственной нейронной сети на сформированном множестве данных обучающей выборки.

Результаты обучения и тестирования нейронной сети показали возможность использования выбранной архитектуры и алгоритма обучения ИНС для разработки модуля численной оценки риска нарушения ИБ в программном комплексе, предназначенном для автоматизации аудита ИБ СОбВ.

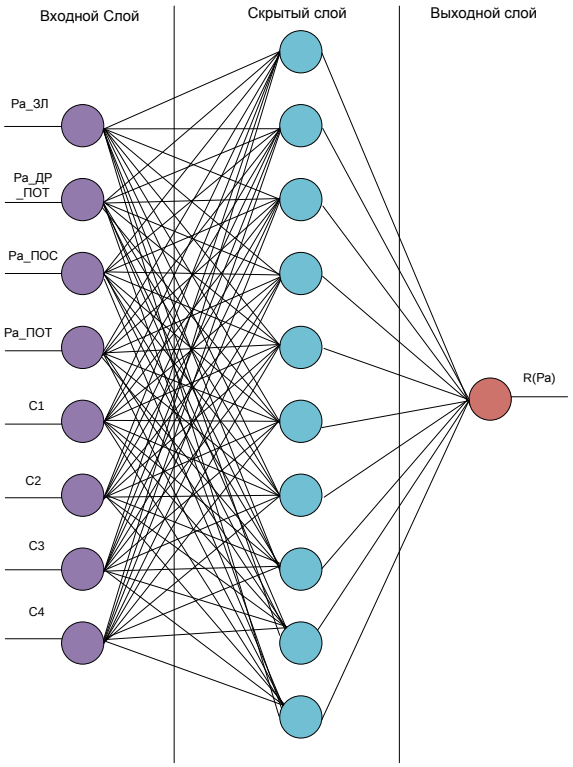

Рис. 4 – Нейронная сеть, используемая для проведения аудита ИБ

Разработаны модель программного средства, блок-схема алгоритма, UML-диаграмма программного модуля.

Получена оценка точности настройки весовых коэффициентов нейронной сети. Расчет риска нарушения информационной безопасности проводился с помощью модуля и вручную. Результаты показали работоспособность программного модуля, устойчивость к некорректным входным данным и воспроизводимость полученных результатов. Точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле, можно оценить с помощью диаграммы (рис. 5).

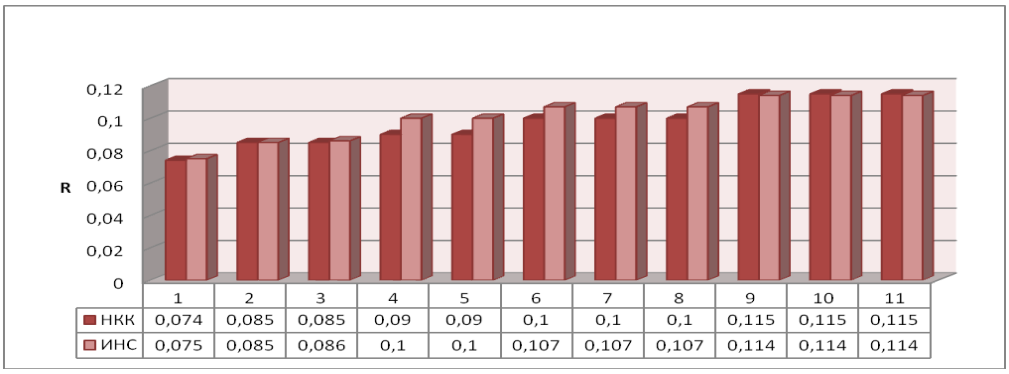

Рис. 5 – Диаграмма точности настройки ИНС

С помощью программного модуля проведен эксперимент, результаты которого позволяют оценить долю ущерба от угроз, реализуемых злоумышленником, другим потребителем, сотрудником поставщика и сотрудником потребителя, от суммарного потенциально возможного ущерба (рис. 6).

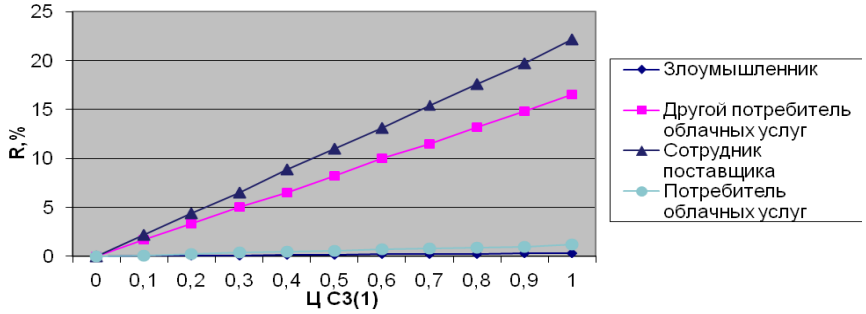

Рис. 6 – График оценивания доли ущерба от угроз от суммарного потенциально возможного ущерба

Таким образом, расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью внутренних источников угроз в СОбВ, являются с точки зрения ИБ наиболее опасными.

Практическая реализация предложенного метода аудита возможна на основе автоматизированной системы, состав модулей и структура которой представлены на рис. 7.

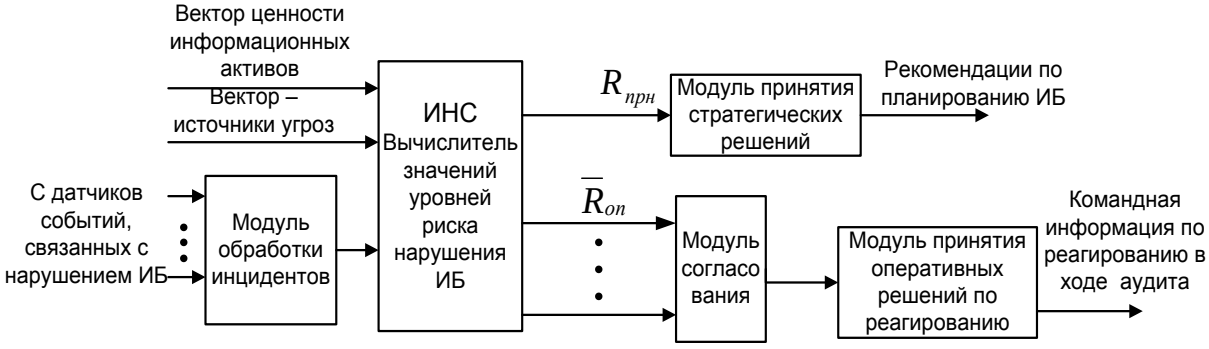

Рис. 7 – Структура автоматизированной системы проведения экспертного аудита: $R_{прн}$ – прогнозируемое значение риска; $R_{оп}$ –оперативное значение риска

На основе экспериментов можно сделаны выводы об эффективности и целесообразности разработанного метода экспертного аудита информационной

безопасности в системе облачных вычислений и разработанного на его основе программного модуля.

В **заключении** приведены основные результаты диссертационного исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ И ВЫВОДЫ

1. Предложена *методика разработки частной политики безопасности* СОбВ, *отличающаяся назначением* нескольких максимальных ролей, которые имеют одновременно и *максимально необходимую роль* в собственном подразделении облака сообщества СОбВ, что позволяет *исключить* из иерархии ролей роль *суперпользователя*, имеющего полномочия напрямую обращаться к результирующим потокам данных, управлять всеми конфигурационными файлами СОБВ, и *увеличить* доверие потенциальных потребителей к ИСОТ.

2. Разработана модель преднамеренных (целенаправленных) угроз нарушения информационной безопасности в системе облачных вычислений, основанная на построении нечетких когнитивных карт, в которой учитываются специфичные угрозы и уязвимости, связанные с динамической масштабируемостью, консолидацией вычислительных ресурсов, возможностью самообслуживания потребителя облачных услуг, с деятельностью такого источника угроз как другой потребитель облачных услуг, который, является клиентом облака сообщества и должен обслуживаться поставщиком изолированно.

3. Предложено два подхода к аудиту ИБ СОбВ: расчет *прогнозируемого* значения риска нарушения информационной безопасности с учетом всего перечня потенциально возможных угроз и расчет *оперативного* значения риска нарушения ИБ, когда угроза проявляется по конкретному пути распространения в реальном масштабе времени.

4. Предложен *метод* проведения *экспертного аудита* информационной безопасности, который позволяет получить численную оценку *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 расчетных значений прогнозируемого уровня риска нарушения информационной безопасности, что позволит поставщику облачных услуг *обеспечить* адекватное реагирование на возможные инциденты в реальном масштабе времени и *обосновать* свои возможности по обеспечению защищенности критичной информации потребителя.

5. Создан программный модуль, автоматизирующий процесс проведения аудита информационной безопасности, с помощью которого оценено оперативное значения уровня риска нарушения информационной безопасности системы облачных вычислений. В примере, приведенном в диссертационной работе, суммарный риск нарушения информационной

безопасности в реальном масштабе времени составил 2,82%. Оценена точность настройки весовых коэффициентов нейронной сети, реализованной в программном модуле, точность составила 0,1% при прохождении ИНС десяти эпох обучения.

6. Оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью внутренних источников угроз СОбВ (администратора поставщика облачных услуг и другого потребителя облачных услуг), являются с точки зрения ИБ наиболее критичными для системы облачных вычислений.

Перспективы дальнейшей разработки темы. Дальнейшим развитие диссертационной работы может быть исследование возможности выбора рационального варианта оперативного реагирования на возможные инциденты, связанные с увеличением уровня риска в реальном масштабе времени.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых журналах из списка ВАК

1. Сенцова, А.Ю. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем // И.В. Машкина, А.Ю. Сенцова, Р. М. Гузаиров, В. Е. Кладов Известия ЮФУ Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ. – 2012. №1. С. 25-35.

2. Сенцова, А.Ю. Разработка нечетких когнитивных карт и искусственной нейронной сети для оперативной оценки информационных рисков в системе облачных вычислений // И.В. Машкина, А.Ю. Сенцова, Е.С. Степанова. Журнал «Нейрокомпьютеры разработка и применение». – М.: Изд-во «Радиотехника», 2013. С. 26-30.

3. Сенцова, А. Ю. Анализ информационных рисков в среде облачных вычислений на основе интеллектуальных технологий // А.Ю. Сенцова, И.В. Машкина. Безопасность информационных технологий. – М.: Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ, №1, 2013. С. 120-121.

4. 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.

5. Сенцова, А.Ю. Анализ проблемы обеспечения информационной безопасности в облачных средах // А.Ю. Сенцова, И.В. Машкина. Безопасность информационных технологий. – М.: Национальный исследовательский ядерный университет «МИФИ» ВНИИПВТИ. – 2014. – №1, С 72-74.

6. 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.

7. 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.

8. 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.

Объекты интеллектуальной собственности

9. Свидетельство о государственной регистрации программы для ЭВМ № 2014616279. Средство проведения экспертного аудита информационной безопасности / Сенцова А.Ю., Машкина И.В., Чайка В.Ю. Зарег. 19.06.14. – М.: Роспатент, 2014.

Публикации SCOPUS

10. 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.

В других изданиях

11. Сенцова, А.Ю. Метод получения численной оценки уровня риска в системе облачных вычислений на основе данных об опасных событиях в реальном масштабе времени // Сенцова А.Ю., Машкина И.В., Материалы XIII Международной научно-практической конференции «Информационная безопасность-2013» Ч. 2. Материалы III Всероссийской молодежной конференции «Перспектива-2013». – Таганрог: Изд-во ЮФУ, 2013. 252с. – С. 209-215.

12. Сенцова, А.Ю. Использование искусственной нейронной сети для оценки риска нарушения информационной безопасности в системе облачных вычислений // Сенцова А.Ю., Машкина И.В. Информационная безопасность регионов России (ИБРР-2013) VIII Санкт-петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г.: Материалы конференции / СПОИСУ. – СПб., 2013. – С. 66-67.

13. Сенцова, А. Ю. Программное средство экспертного аудита информационной безопасности на основе искусственной нейронной сети // Сенцова А.Ю., Машкина И.В. Информационное противодействие угрозам терроризма. Научно-практический журнал, Ростов-на-Дону. – 2014, № 23. − С. 29-36.

14. Sentsova, A.U. Geoinformation system in the projection on the network topology as object of protection // A.U. Sentsova, I.V. Mashkina, R.M. Guzairov. Proceedings of the 13th International Workshop on Computer Science and Information Technologies CSIT`2011. Volume 1, Ufa State Aviation Technical University, 2011 P. 172-176.

Диссертант  Сенцова А.Ю.

СЕНЦОВА Алина Юрьевна

МОДЕЛИ И МЕТОД ЭКСПЕРТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Специальность 05.13.19 –
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 17.10.2016. Формат 60×84 1/16
Бумага офсетная. Печать плоская. Гарнитура Times New Roman.
Усл. печ. л. 1,0. Уч.-изд. л. 0,9.
Тираж 100 экз. Заказ № ____.

ФГБОУ ВО «Уфимский государственный авиационный
технический университет»
Центр оперативной полиграфии
450008, Уфа-центр, ул. К. Маркса, 12