Кораблев Антон Вячеславович. Идентификация информационных рисков использования облачных технологий в банковской деятельности: диссертация кандидата Экономических наук : 08.00.13 / Кораблев Антон Вячеславович;[Место защиты: ФГАОУ ВО Самарский национальный исследовательский университет имени академика С.П. Королева], 2017 - 171 с.

**Содержание к диссертации**

Введение

**Глава 1 Информационные риски облачных технологий в банковской деятельности 12**

1.1 Облачные технологии в банковской деятельности: понятие, особенности использования, безопасность 12

1.2 Определение банковских информационных рисков 28

1.3 Особенности современных методик оценки информационных рисков 43

**Глава 2 Оценка информационных рисков 55**

2.1 Нечеткая оценка информационных рисков 55

2.2 Нечеткие измерительные шкалы для оценки элементов модели 69

2.3 Методика получения нечеткой оценки информационных рисков 81

**Глава 3 Идентификация информационных рисков с помощью инструментальных средств 95**

3.1 Программно-технологический комплекс оценки информационных рисков 95

3.2 Применение механизма нечеткого вывода для оценки информационных рисков 117

3.3 Результаты применения программно-технологического комплекса оценки информационных рисков 131

Заключение 145

Список литературы 148

Приложение А Функциональная модель нечеткой оценки информационных рисков 164

Приложение Б Информационные угрозы облачных вычислений 169

* [Облачные технологии в банковской деятельности: понятие, особенности использования, безопасность](http://www.dslib.net/mat-metody/identifikacija-informacionnyh-riskov-ispolzovanija-oblachnyh-tehnologij-v.html#7700481)
* [Нечеткие измерительные шкалы для оценки элементов модели](http://www.dslib.net/mat-metody/identifikacija-informacionnyh-riskov-ispolzovanija-oblachnyh-tehnologij-v.html#7700482)
* [Программно-технологический комплекс оценки информационных рисков](http://www.dslib.net/mat-metody/identifikacija-informacionnyh-riskov-ispolzovanija-oblachnyh-tehnologij-v.html#7700483)
* [Результаты применения программно-технологического комплекса оценки информационных рисков](http://www.dslib.net/mat-metody/identifikacija-informacionnyh-riskov-ispolzovanija-oblachnyh-tehnologij-v.html#7700484)

**Введение к работе**

**Актуальность темы исследования.** Обеспечение своевременного и бесперебойного предоставления банковских услуг является на сегодняшний день основным конкурентным преимуществом для кредитной организации. Решение этих задач основывается на внедрении и эффективном использовании передовых информационных технологий. В основе стратегии перехода от «традиционной» автоматизированной инфраструктуры к облачным сервисам заложена экономическая целесообразность. По оценкам экспертов рынка информационных технологий при такой миграции происходит снижение эксплуатационных издержек в среднем до 40% (по данным консалтинговой компании Markets and Markets). Облачная инфраструктура характеризуется неограниченными вычислительными мощностями, что позволяет своевременно и эффективно реагировать на изменения в конкурентной среде за счет скорости вычислений, масштабируемости виртуальной инфраструктуры, надежности банковских сервисов, доступности финансовых услуг для клиентов.

Предоставление банковских услуг на основе облачных технологий характеризуется возросшим количеством уязвимостей и внешних угроз, что обусловлено сложностью технологических решений и использованием открытых каналов связи. Сбои при предоставлении банковских сервисов, построенных на использовании современных информационных технологий, а также разглашение банковской информации может нанести значительный экономический ущерб банку или его клиентам. Обеспечение контроля над данными является неотъемлемой задачей любой современной информационной системы.

В последнее время развивается научное направление эффективного управления информационными рисками. В международных и российских стандартах процессы управления рисками в основном рассматриваются по отношению к информационным системам. Современный уровень информатизации в организациях позволяет использовать определение уровня риска не только в целях управления информационными технологиями, но и для обеспечения экономической безопасности организации с помощью повышения надежности бизнес-процессов. Следовательно, процесс идентификации рисков с их последующей оценкой необходимо рассматривать в целом не только как технологическую функцию, но и как основу устойчивого функционирования организации.

Управленческие решения по созданию и модернизации информационных технологий должны основываться на регулярной оценке информационных рисков, методическая база которой применительно к реализации технологии облачных вычислений в банковской сфере является в настоящее время практически не разработанной.

**Степень разработанности проблемы исследования.** Методологической базой исследований в области построения защищенных информационных систем являются работы отечественных и зарубежных ученых: А.А. Анисимова, А.И. Берга, Н.А. Гайдамакина, В.А. Герасименко, Д.П. Зегжды, В.А. Конявского, В.П. Мельникова, П.Б. Хорева, В.Ф. Шаньгина, В.И. Ярочкина, М. Витмена, С. Кайраба, Р. Смита, М. Стампа, Н. Фентона, А. Ясона и др. Управление информационными технологиями в банковской деятельности рассмотрено в работах В.В. Андриянова, В.А. Зинкевича, А.В. Золотарюка, О.В. Кабановой, В.Е. Черенкова, Д.В. Чистова и др.

Несмотря на то, что в современной научной литературе, в международных и национальных стандартах уделяется большое внимание проблемам анализа, оценки и управления информационными рисками, в них предлагаются наиболее общие рекомендации и не учитываются конкретные специфические особенности ИТ-инфраструктуры банковской организации.

Разработка математических методов и моделей, а также проблемы применения инструментария анализа и оценки информационных рисков нашли свое отражение в научных работах А.М. Астахова, В.Е. Бенинга, В.В. Борисовой, Я.Д. Вишнякова,

В.И. Завгороднего, С.А. Орловского, А.И. Толстого, К. Рэдхеда, Л. Сэведжа, А. Тюнена, Дж. Херберта.

Принимая во внимание труды таких авторов, как А. Аверкина, В.В. Борисовой, А.И. Долженко, Ю.А. Зака, А. Леоненкова, А.О. Недосекина, В. Новака, А. Пегата, С.Д. Штовба, Дж. Бакли, Р. Беллмана, Л. Заде, Б. Коско касающиеся оценки и управления информационными рисками в нечетких условиях, можно сделать вывод, что в научной литературе этот вопрос недостаточно разработан. Так, в передовых отечественных и зарубежных подходах отсутствует проблематика разработки лингвистических шкал для оценки рисков применения современных информационных технологий.

На сегодняшний день практически отсутствуют методы, которые можно использовать для постоянного мониторинга информационных рисков, адекватность которых не зависит от наличия или отсутствия статистических данных в области инцидентов информационной безопасности, экспертные знания в которых сведены к минимуму или основываются на объективных данных об объекте защиты.

Отмеченные проблемы обусловили актуальность выбранного направления исследования и определили постановку цели и задач диссертационной работы.

**Цель исследования** заключается в разработке научно-методического инструментария оперативной идентификации информационных рисков при использовании облачных технологий в банковской деятельности.

Для достижения указанной цели были поставлены и решены следующие **задачи**:

1. Определить компоненты риска с целью выявления специфических информационных рисков использования облачных технологий.
2. Разработать множественную модель представления банковской облачной технологии для последующей оценки сопутствующих информационных рисков.
3. Создать нечеткую модель оценки информационного риска.
4. Сформировать технологию оценки информационных рисков с использованием инструментальных средств, учитывающую механизм нечеткого вывода.
5. Разработать прикладное программное обеспечение для оценки информационных рисков по модели, основанной на теории нечетких множеств и методические рекомендации по его применению.
6. Исследовать эффективность предлагаемой методики и разработанного инструментального средства в условиях работы реальной банковской организации.

**Объектом исследования** являются банковские технологии, использующие облачные вычисления.

**Предметом исследования** являются методы и модели оценки информационных рисков при использовании облачных технологий в банковской деятельности.

**Область исследования** соответствует п. 1.10. «Разработка и развитие математических моделей и методов управления информационными рисками» Паспорта научной специальности 08.00.13 - Математические и инструментальные методы экономики (экономические науки).

**Научная новизна исследования** состоит в разработке методики оперативной оценки информационных рисков при использовании облачных технологий, направленных на повышение эффективности банковской деятельности, а также обосновании направлений совершенствования процессов оценки информационных рисков.

**Положения, выносимые на защиту**. На защиту выносятся следующие результаты исследования, содержащие элементы научной новизны:

1. Предложена расширенная классификация информационных рисков банковских облачных технологий, обусловленная новым видом угроз, которые определяются наличием провайдера облачных услуг и использованием средств виртуализации. Учет выявленных рисков позволяет оптимизировать потенциальный экономический ущерб для банковской организации (C. 37-42).

1. Определен единый подход к идентификации компонентов информационного риска использования облачной технологии в банковской деятельности на основе разработанной множественной модели, которая, в отличие от существующих моделей, позволяет учитывать неограниченное многообразие информационных связей между информационными ресурсами, угрозами и уязвимостями (С. 55-58).
2. Сформирована авторская методика определения итоговой величины потенциального экономического ущерба, стоимости реализации угроз, ценности информационного ресурса, количественной величины риска. Методика основана на разработанной модели нечеткой оценки информационных рисков, которая, в отличие от известных моделей управления рисками, определяет значения элементов по их свойствам, оказывающим непосредственное влияние на уровень информационных рисков применения облачных технологий в банковской деятельности (С. 81-92).
3. Предложен способ повышения точности вычисления информационного риска в банковской организации основанный на развитии механизма нечеткого вывода: увеличение числа входных переменных; детализация продукционных правил вывода; использование специфических нечетких шкал оценки лингвистических переменных характеризующих применение облачных технологий (С. 69-80, 117-131).
4. Обоснована целесообразность применения разработанного инструментального средства нечеткой оценки информационных рисков и методических рекомендаций по его использованию для повышения экономической эффективности банковской деятельности при использовании облачных технологий за счет сокращения сроков клиентского обслуживания, уменьшения операционных издержек, увеличения объема реализации дистанционных услуг (С. 99-116, 131-143).

**Теоретическая значимость исследования** заключается в обобщении теоретической и методологической базы исследований для решения задачи идентификации информационных рисков с использованием теории нечетких множеств и нечеткой логики, использовании теоретических положений в решении прикладных задач по формированию инструментов и технологий определения экономического ущерба при реализации информационных рисков.

**Практическая значимость исследования** состоит в разработке прикладного обеспечения для управления информационными рисками предоставления банковских сервисов, ориентированного на широкое использование методов, моделей и инструментальных средств. Достижение приемлемого уровня информационных рисков позволяет обеспечить бесперебойное функционирование информационных систем, что способствует устойчивому экономическому развитию банковской организации. Выявление критических угроз позволяет снизить затраты на создание и поддержание системы работы с банковской информацией. Интерфейс разработанного программного обеспечения позволяет привлекать к оценке рисков специалистов, не обладающих специальными знаниями в области нечетких множеств.

Самостоятельное практическое значение имеют:

1. Модель идентификации информационных рисков с использованием нечеткой логики, позволяющая получать количественные показатели риска при проведении мониторинга безопасного использования банковских информационных систем.
2. Алгоритм реализации модели оценки информационных рисков с использованием математического аппарата теории нечетких множеств и нечеткой логики.
3. Инструментальное средство для решения задачи оценки информационных рисков.
4. Рекомендации по организации практических мероприятий при оценке информационных рисков в банковских организациях.

**Методологической основой исследования** послужили труды отечественных и зарубежных специалистов по проблемам управления рисками, банковского менеджмента, управления информационными технологиями. В работе использовались методы математического анализа, теории нечетких множеств, теории вероятностей и математической статистики.

Информационную базу исследования составили: законодательные и нормативные акты регламентирующие деятельность кредитно-финансовых организаций; статистические данные Центрального банка Российской Федерации и международных консалтинговых компаний; материалы периодических изданий, научно-практических конференций; результаты исследований специалистов в области управления рисками и использования информационных технологий; статистические данные, полученные автором в ходе выполнения исследования.

**Степень достоверности и апробация результатов исследования.** Достоверность результатов и выводов исследования обеспечивается их соответствием методологическим положениям теории управления рисками, применением методов аналитического исследования, использованием теории нечетких множеств. Научные результаты подтверждены практическими расчетами. Основные результаты исследования обсуждались на Всероссийской научно-практической конференции студентов и аспирантов «Перемены в России: прошлое, настоящее, будущее», г.Казань, 27 апреля 2007 г.; 9-й Международной научно-практической конференции «Проблемы развития предприятий: теория и практика», г.Самара, 18-19 ноября 2010 г.; Международной научной конференции «Информационные технологии в финансово-экономической сфере: прошлое, настоящее, будущее», г.Москва, 17 декабря 2013 г.; Международной научно-практической конференции «Наука XXI века: актуальные направления развития», г. Самара, 23 октября 2015 г.; Международной научно-практической конференции «Модернизация экономических систем: взгляд в будущее», г. Прага, Чешская Республика, 6 ноября 2015 г.; Международной научно-практической конференции «Актуальные вопросы и перспективы развития математических и естественных наук», г.Омск, 11 мая 2017 г.

**Внедрение результатов.** На основе разработанных в диссертации моделей и методов оценки информационных рисков создана программа для ЭВМ «Нечеткая оценка информационных рисков», свидетельство о государственной регистрации программ для ЭВМ № 2016616137, дата регистрации 06.06.2016 г.

Результаты исследования отраженны в регламентирующей документации: «Положение по управлению информационными рисками», «Положение по управлению операционными рисками». Созданные документы используется в деятельности отдела информационных технологий филиала Банка ГПБ (АО) в г.Самаре.

Материалы диссертации используются в учебном процессе ФГБОУ ВО «Самарский государственный экономический университет» и отражены в учебно-методических комплексах по дисциплинам «Проектирование экономических информационных систем», «Нечеткие модели принятия решений».

**Публикации.** По теме диссертации опубликовано 13 статей, общим объемом 6,17 п.л. (авторский объем 5,9 п.л.), из них 5 работ общим объемом 3,01 п.л. (авторский объем 2,79 п.л.) опубликованы в изданиях, определенных ВАК Минобрнауки РФ.

**Структура, объём и содержание диссертации.** Диссертационная работа состоит из введения, трех глав, заключения, списка литературы и приложений. Общий объем диссертации составляет 171 страница. Работа содержит 45 таблиц, 57 рисунков, 2 приложения. Список литературы включает 161 наименование.

## Облачные технологии в банковской деятельности: понятие, особенности использования, безопасность

Обеспечение своевременной и бесперебойной обработки информации является одной из главных задач выполнения финансовых операций. Это обусловливает необходимость внедрения и использования в банках передовых информационных технологий [53, 54, 89].

За последнее десятилетие рынок банковских услуг претерпел кардинальные изменения – он приобрел черты динамично развивающегося рынка. При организации работы с клиентами сегодня недостаточно применять традиционные методы предоставления финансовых услуг. Необходимо создавать и правильно использовать новые формы привлечения и обслуживания клиентов на основе внедрения современных информационных технологий. Это, в свою очередь, позволит расширить возможности информационного взаимодействия клиентов и сотрудников банка.

Одной из таких технологий является виртуализация информационного взаимодействия клиентов и банковского персонала, т.е. предоставления банками облачных сервисов.

По оценкам экспертов, к концу 2017 г. половина всех крупных банков как на западе, так и в России будут хранить важную информацию в центрах обработки данных, что позволит им экономить на затратах [143, 144]. По оценкам компании Gartner Group, сегодня более 50% банковских транзакций по всему миру осуществляется посредством облачной инфраструктуры из них 45% – посредством приложений, используемых в рамках модели SaaS, т.е. модели предоставления виртуального взаимодействия [145, 147] (рисунок 1.1.1).

Современные банки представляют собой распределенные организации с развитой телекоммуникационной инфраструктурой. Их ключевым конкурентным преимуществом служит то, что все структурные подразделения банка должны работать в едином информационном пространстве с данными, которые являются актуальными и достоверными для всей организации в целом, что и позволяют сделать облачные сервисы. Хотя эта технология и считается передовой, ее трудно назвать новой. Джон Маккарти, автор термина «искусственный интеллект», в 1960 г. в своих работах уже писал о необходимости совместного использования вычислительных мощностей [67]. Но аппаратные и программные средства тех лет были не способны реализовать такие решения. Некое подобие облачных сервисов было реализовано при использовании майнфреймов, когда пользователи организации могли получить доступ к информационным ресурсам на общем компьютере через терминал. Развитие облаков проходило в четыре этапа (таблица 1.1.1) [133].

Отправной точкой для этой технологии стало появление GRID-систем в 90-х гг. ХХ в. Этот комплекс аппаратных и программных средств дал возможность впервые предоставить компьютерные мощности в виде услуги [108, 111]. GRID-системы послужили импульсом при создании и развитии web-служб, которые явились технологической базой для разработки стандартов интерфейсного взаимодействия между службами [86].

Широкое применение облачные технологии получили в начале XXI в. благодаря тому, что к этому времени была создана разветвленная телекоммуникационная инфраструктура (радиосвязь, кабельные сети передачи данных), которая позволила организовать широкополосный доступ к сети Интернет. Использование общепризнанных международных стандартов при организации предоставления информационных сервисов позволило создавать web-службы, которые способны работать на множестве популярных платформ, что значительно расширило возможности пользователей при подключении к облаку.

На базе облачных технологий реализуются клиентские услуги по отношению к которым и используется определение облачных сервисов. Впервые термин «облачная технология» («computing cloud») использовал Николас Карр [56] в 2004 г. Им было предложено следующее определение: облачная технология – это совместное использование компьютерной инфраструктуры несколькими компаниями.

С широким распространением облачных технологий появилась необходимость в их классификации [104, 105]. Схема классификации таких технологий по уровням их предоставления (рисунок 1.1.2).

В общем виде классификация облачных технологий по видам предоставляемых клиентских сервисов напоминает классификацию классического программного обеспечения в виде прикладных программ, системного программного обеспечения и промежуточного программного обеспечения [65, 72, 89]. Эта особенность свидетельствует о том, что по своей технологической реализации облачные технологии не являются совершенно новым этапом развития сферы информационных технологий. Абсолютная новизна заключается в форме потребления и оплаты облачных сервисов, которая и определяет революционность явления по использованию облачных технологий.

Технология реализации облачных услуг в банковской деятельности определяется наличием ряда ограничений. Процессы сбора, обработки и хранения банковских данных подвержены проявлению информационных рисков [61, 82]. Особым требованиям безопасности должны соответствовать помещения, где размещается серверное оборудование, необходимо контролировать доступ к этим помещениям, программное и аппаратное оборудование должно быть сертифицировано ФСБ и ФСТЭК, удаленный доступ к виртуальным серверам должен осуществляться по шифрованным каналам связи с использованием криптографических протоколов. Большинство провайдеров облачных сервисов не могут обеспечить определяемый Центральном банком РФ уровень информационной безопасности. Это обусловливает реализацию облачных вычислений самими банками с использованием собственных ресурсов. При этом реализуется модель облачных вычислений «Приложение как сервис» (SaaS), которая разворачивается с использованием «Частной» модели. Примером могут служить проекты, реализованные в Центральном банке РФ и Сбербанке РФ.

При использовании облачных технологий предполагается установка в центре обработки данных серверов виртуализации, на которых размещаются клиентские приложения. Пользователь независимо от места своего расположения, применяя средства и каналы связи, подключается к банковскому серверу. После прохождения процедуры авторизации и аутентификации пользователь получает доступ ко всем приложениям, которые он использует в своей работе. Схема организации облачных технологий представлена нами на рисунке 1.1.3.

Доступ к банковским серверам, работающим в виртуальном режиме, осуществляется с помощью web-сервисов. Рабочее место сотрудника банка становится виртуальным, что позволяет оптимально использовать имеющиеся материальные, трудовые, административные и информационные ресурсы при организации взаимодействия с клиентами.

Использование виртуализации позволяет сократить стоимость обслуживания технологической инфраструктуры, так как создается единый набор программных и аппаратных средств для всей системы хранения и обработки данных, что определяет снижение затрат на использование специализированного управляющего программного обеспечения и оплату труда сотрудников. Технология позволяет наладить оперативное взаимодействие с территориальными структурными подразделениями, обеспечить защищенность общих информационных ресурсов за счет повышения надежности и отказоустойчивости транзакций.

Палитра банковских услуг, реализуемых с помощью облачных технологий, с каждым годом расширяется. Происходит плавный переход от инфраструктурных предложений IaaS к полноценным SaaS-решениям. По данным компании iKS-Consulting, SaaS сегодня является ведущим сегментом облачного рынка России: в 2015 г. его доля составила 89% всего объема доходов от облачных услуг в стране [143]. Еще 9% приходится на PaaS, в то время как удельный вес инфраструктурных решений постоянно снижается, составляя не более 2% .

Приведем примеры основных облачных технологий, используемых в российских банках. Следует отметить, что на рынке отсутствуют стандартизированные процессы использования банками облачных технологий. Поэтому рассмотрим их на примере отдельной организации.

## Нечеткие измерительные шкалы для оценки элементов модели

Используя теоретические положения, изложенные в п. 2.1, сформируем набор из восьми нечетких измерительных шкал для оценки элементов исследуемой модели: конфиденциальности, целостности, доступности, ценности, воздействия, уязвимости внешних границ, риска, ущерба. Описание соответствующих шкалам нечетких лингвистических переменных указано в таблицах 2.2.1 - 2.2.8. Отдельно для каждой шкалы рассчитаны функции принадлежности для нечетких значений. При построении функций принадлежности использовались несущие множества в соответствии с функцией желательности Харрингтона. Пересечение несущих множеств определено значением 0,08 или ±0,04 от центра общей части. Измерительные шкалы ограничим отрезком [0,1], при этом 0 – это минимальный, а 1 – максимальный уровень для шкалы.

Требуемый уровень информационного риска определяется видом функции принадлежности. Трапециевидная и треугольная функции соответствуют самым жестким требованиям.

Шкала конфиденциальности Sconf представляет собой нечеткую измерительную шкалу обозначающую уровни конфиденциальности информации. С ее помощью можно характеризовать свойство конфиденциальности элементов модели (рисунок. 2.2.1).

Шкала доступности Simplement представляет собой нечеткую измерительную шкалу, обозначающую уровни доступности информационного ресурса. С ее помощью можно характеризовать свойство доступности элементов модели (рисунке 2.2.3).

Доступность зависит от степени мотивации источника угрозы защищаемой информации, обстоятельств формирования уязвимости и эффективности системы защиты информации.

Шкала ценности Svalue представляет собой нечеткую измерительную шкалу обозначающую уровни критичности, позволяет соотнести защищаемую информацию с характеризующей ее качественной категорией (рисунок 2.2.4). Величина возможного ущерба определяется ценностью защищаемой информации: чем выше ценность информации, тем больше величина ущерба.

Разработанная шкала позволяет определить информационные ресурсы, требующие применения специальных средств для обеспечения информационной безопасности. При выборе средств и методов защиты информации, обладающих необходимыми функциональными возможностями, следует определить специфические особенности, характеризующие каждую категорию ценности информации.

1. «Не важная». Не требует защиты.

2. «Важная» и «Очень важная». Организовать защиту такой информации можно с использованием только встроенных средств, которыми обладает программное обеспечение (операционные системы, прикладные программы).

3. «Конфиденциальная». Требует использования специальных средств и методов защиты информации (аппаратные и программные средства информационной безопасности). 4. «Строго конфиденциальная». Необходимо привлечение не только специальных средств и методов защиты информации, но и проведение инженерно-технических мероприятий информационной безопасности (физическая защита зданий, помещений).

Наиболее ценная информация нуждается в самых эффективных мероприятиях по своей защите, так как может представлять повышенный интерес со стороны злоумышленников.

Шкала воздействия Seffect представляющая собой нечеткую измерительную шкалу, обозначающую уровни воздействия элементов модели друг на друга (рисунок 2.2.5), характеризует нечеткую зависимость от реализации угрозы.

Шкала оценки уязвимости внешних границ Svulner представляет собой нечеткую измерительную шкалу, обозначающую уровни реализации уязвимости (рисунок 2.2.6). Наличие данной шкалы обусловлено спецификой исследуемой предметной области – особенностями облачной технологии. Используя разработанную шкалу и собранные данные, необходимо оценить границы облачных вычислений по отношению к внешним угрозам. Первоначально оцениваются облака, из которых исключены средства и мероприятия обеспечения защиты информации, а после доработки анкет рассматриваются облака, в которых используются средства и методы защиты.

Шкала риска Srisk представляет собой нечеткую измерительную шкалу при помощи которой оценивается информационный риск (рисунок 2.2.8). Полученное нечеткое значение подлежит дефазифицированию на шкале Srisk = [0,1].

Для определения границ уровней информационного риска разработаем шкалу, в которой уровень риска связан с соответствующими контрмерами (таблице 2.2.7).

Шкала ущерба Sloss представляет собой нечеткую измерительную шкалу, обозначающую уровни ущерба (рисунок 2.2.8). Шкала предназначена для оценки величины ущерба и характеризует нечеткое отношение элементов модели друг на друга. Полученное нечеткое значение подлежит дефазифицированию на шкале SIoss =№M

Данный набор шкал следует считать минимальным для исследуемой модели облачной технологии. Для расширения модели возможно введение дополнительных шкал эффективности защиты информации или возможности реализации угроз.

## Программно-технологический комплекс оценки информационных рисков

Исследование модели облачной технологии и описание ее элементов проводятся на всех иерархических уровнях управления для определения информационных ресурсов, подлежащих защите. Реализовать эту задачу можно только с помощью специальных методов и инструментальных средств. Их совокупность образует технологию оценки информационных рисков (рисунок 3.1.1).

Наличие технологии и ее внутреннее содержание устанавливаются в «Политике безопасности», которая является основным документом, регламентирующим правила, процедуры, принципы управления информационной безопасностью в организации. В разработке документа принимают участие все структурные подразделения организации, которые определяют: ценность информации, сопровождающей бизнес-процессы, реестры открытой и закрытой информации; технологии работы с электронной/бумажной информацией. На основе анализа представленной информации формируют набор программно-аппаратный средств защиты и соответствующий им комплекс организационных мероприятий. Подписывает «Политику» первое лицо компании (в банке – председатель правления), поэтому ее выполнение обязательно для всех сотрудников организации. С использованием данных «Политики безопасности» и иных регламентирующих документов (таблица 3.1.1) составляются перечни необходимых программно-аппаратных средств защиты информации (криптографические методы, защита от несанкционированного доступа, средства идентификации и др.) и организационных мероприятий обеспечения безопасности защищаемых информационных ресурсов. Исследуются процедуры защиты центра обработки данных (архивирование баз данных, резервирование данных, разработанные процедуры по восстановлению данных и др.), инженерно-технические методы и средства защиты помещений, в которых находится конфиденциальная информация (серверные комнаты, сейфы, контрольно-пропускные системы и др.), а также разрабатываются мероприятия обеспечения безопасности информационных ресурсов при чрезвычайных ситуациях (природно-климатические явления, техногенные происшествия).

Данные, собранные при описании модели облачной технологии, необходимы на этапе разработки анкет, которые используются для проведения процедуры сбора экспертных оценок. При разработке анкет учитываются особенности организации в виде ее специализации (сфера деятельности), масштаба деятельности, стратегических и оперативных задач развития. В общем, анкеты должны отражать текущий уровень зависимости бизнес-процессов от используемой облачной технологии. Определим приемы, которые применим при сборе и фиксации информации.

Анкетирование. Разрабатывается документ, который содержит набор заранее определенных вопросов. Структура и содержание вопросов должны отвечать требованию однозначного толкования, они должны быть просты для понимания. После подготовки базы анкет они размещаются в информационном контенте, доступ, к которому предоставляется заранее определенной группе экспертов.

Собеседование. Представляет собой интервьюирование эксперта. С целью сокращения затрат на этапе описания информационной системы собеседование необходимо проводить с применением современных коммуникационных технологий – IP-телефонии и видеоконференций.

Анализ документации. Собрать информацию о методах обеспечения и контроля информационной безопасности можно при анализе нормативной и регламентирующей документации, которая утверждена в организации. При описании элементов можно использовать только один из приемов сбора и фиксации данных, но самую качественную информацию (выполнение требований ее актуальности, достоверности, полноты) можно получить, используя сразу комплекс приемов: например, и анкетирование, и собеседование, и анализ документации.

Качественные данные позволят установить границы модели на основании описания используемых внешних и внутренних ресурсов, а также взаимосвязи необходимых ресурсов.

Для облаков важным элементом становятся внешние границы, которые определяют уязвимости, соответствующие внешним угрозам защищаемой информации (удаленные сетевые атаки). Уязвимости, определяемые внешними границами, для облачных вычислений можно выявить на основании следующих факторов: количества и видов точек выхода в сеть Интернет (радиоточка, выделенный канал); особенностей технологии взаимодействия с удаленными пользователями (серверы виртуализации); характеристик сетевого оборудования; способов создания и использования общего информационного пространства организации; приемов внешнего администрирования программно-аппаратных средств.

Для определения оценки потенциала нарушителя необходимо заранее оценить вероятность события реализации каждого из процессов разработанной модели нарушителя. Низкая вероятность реализации любого из процессов модели нарушителя уменьшает его общий потенциал. Это необходимо учитывать при определении совокупной оценки потенциала нарушителя.

Как было отмечено выше, источник формирует угрозу защищаемой информации только при наличии соответствующей уязвимости в объекте защиты. Поэтому необходимо составить реестр всех возможных уязвимостей информационной технологии.

Уязвимость нарушает политику информационной безопасности при возникновении ошибки во время осуществления мероприятий по обеспечению информационной безопасности, при проектировании системы безопасности, при мониторинге системы безопасности.

Идентификация уязвимостей может быть осуществлена двумя способами.

1. С помощью стандартных списков уязвимостей. Необходимо осуществить выборку уязвимостей из их стандартных списков в зависимости от применяемых в организации методов и информационных средств защиты. Наличие стандартных уязвимостей в конкретной системе безопасности проверяется средствами ее тестирования.

2. С помощью методов сбора и фиксации информации. Разработку вопросов для интервьюирования и анкет, которые будут предоставлены экспертам, необходимо осуществить на основе анализа документации: технических документов к аппаратным и программным средствам, с использованием которых реализуется облако; результатов предыдущих процедур аудита информационной безопасности.

Выявленные уязвимости информационной технологии служат основой для определения текущего уровня ее безопасности. Контрольный список, определяющий соответствие текущего состояния безопасности, должен содержать основные правила по защите информационных ресурсов, которые будут применяться для идентификации уязвимостей.

Полученный перечень идентифицированных уязвимостей позволяет провести оценку потенциала информационного риска, который основан на соответствующем источнике угрозы для защищаемой информации с учетом выявленной уязвимости.

Главной задачей при идентификации информационных рисков является определение коэффициентов изменений элементов защиты вследствие реализации конкретного информационного риска. Для этого можно использовать экспертные оценки или статистические данные, собираемые при мониторинге защищенности информации.

При подготовке, проведении экспертизы и обработке полученной экспертной информации целесообразно использовать уже ранее созданные и зарекомендовавшие себя методы. Исходя из этого, можно воспользоваться методом Дельфи, который является самым используемым на практике для обработки экспертных оценок, с последующим прогнозированием значений показателей (рисунок 3.1.2).

Порядок проведения экспертизы по методу Дельфи следующий:

1. Постановка целей и задач проведения экспертизы.

2. Определение состава экспертов, проверка их компетентности.

3. Разработка процедуры проведения экспертизы, программы, выбор необходимых информационных технологий.

4. Проведение экспертизы, сбор данных.

5. Обработка собранных данных, анализ результатов.

## Результаты применения программно-технологического комплекса оценки информационных рисков

Технологический процесс получения оценки информационных рисков должен обеспечить автоматизацию основных этапов обработки информации по сбору исходных данных, регистрации и первичной обработке собранных данных (соответствие требованиям их актуальности, достоверности, полноты) по вводу данных в модель, ее реализации и исследованию полученных результатов. Для достижения поставленных целей разработанная технология оценки информационных рисков (см. рисунок 3.1.1) оформлена в виде регламентной процедуры (см.рисунок 3.3.1-3.3.2), которая входит в состав документов: «Положение по управлению информационными рисками», «Положение по управлению операционными рисками», «Методическая инструкция оператора программы «Нечеткая оценка информационных рисков». Наличие такого набора документов гарантирует прозрачность процессов оценки информационных рисков, что повышает безопасность использования комплекса информационных систем в кредитной организации.

Детализируем процедуру по входящим в нее действиям с указанием ответственных лиц и сроков выполнения. Данные операции помещаются в раздел обязанностей должностных инструкций руководителя отдела ИТ и ответственного сотрудника ИТ.

При реализации технологии оценки информационных рисков наряду с разработанной АИС «НОИР» и инструментальным средством математического моделирования «MATLAB» могут использоваться и иные программные продукты. Предложим следующий набор программных средств для оценки информационных рисков, доступный большинству организаций (рисунок 3.3.3).

Программный продукт для оценки рисков должен охватывать все их компоненты и взаимосвязь между компонентами риска, включать в свой состав модули сбора/анализа данных и вывода результатов, отражать политику и подход организации к оценке рисков, формировать понятные и точные отчеты, сохранять историю сбора и анализа данных, содержать полную и понятную документацию, быть совместимым с программным и аппаратным обеспечением, используемым в организации, а также сопровождаться обучением и поддержкой пользователей.

Выбранный программный продукт должен отражать общий подход организации к оценке информационных рисков.

Существует достаточное количество хорошо себя зарекомендовавших и широко используемых методов оценки и управления информационными рисками.

Преимуществами использования программного обеспечения данного класса являются: стандартизация технологии оценки информационных рисков; интеграция с информационными системами организации (единая информационная база); формирование отчетности, а также в интеграция этого инструмента с внешними средствами контроля.

К числу наиболее распространенных недостатков относят: несовместимость с международными стандартами; неполный охват информационных ресурсов (большинство продуктов сосредоточиваются только на управлении операционными рисками в сфере информационных технологий, игнорируя остальные виды бизнес-процессов); сложность использования (многие продукты слишком сложны в использовании); затруднение процесса осознания рисков, так как расчет рисков выполняется автоматически и скрыт от пользователя.

На российском рынке предлагается большое количество систем для оценки и управления информационными рисками (таблица 3.3.2).

Внедрение выбранного инструментального средства защиты как компонента единой системы информационной безопасности должно быть экономически обосновано.

Рассмотрим процесс управления информационными рисками как мероприятия по разработке, внедрению и сопровождению специальных инструментальных средств обеспечения информационной безопасности. Для этого необходимо оценить экономическую эффективность от реализации проекта внедрения таких средств защиты. Рассчитаем также и показатель совокупной стоимости владения комплексной системой информационной безопасности.

Основным показателем экономической эффективности такого инвестиционного проекта как затраты при оценке информационных рисков является чистая приведенная стоимость [53]

Экономическая эффективность при реализации проекта оценки информационных рисков состоит в минимизации информационных и финансовых потерь при предоставлении облачных вычислений. Эффективность также зависит от совместной максимизации доходов при предоставлении облачных клиентских слуг и высокой вероятности завершения проекта с учетом математического ожидания потерь от прекращения проекта.

Внедрение методики оценки информационных рисков может состоять из мероприятий: выбора на рынке готового программного продукта или расширение, уже функционирующей системы, за счет покупки дополнительных моделей и интеграции их в корпоративной информационной системе.

Приведем статистические данные по выявленным угрозам защищаемой информации в облачной инфраструктуре до и после внедрения методики получения оценки информационных рисков (таблица 3.3.5). После внедрения рекомендованных контрмер, направленных на снижение уровня информационных рисков, произошло резкое увеличение выявленных инцидентов по угрозам «Несанкционированный доступ со стороны персонала, обслуживающего облачную инфраструктуру», «Попытки анализа сетевого трафика», «Попытки доступа через открытые порты» раньше не выявлялись. Общее увеличение выявленных угроз позволяет банку определить слабые места, которые более подвержены информационным рискам. Внедрение специальных средств повлияло на качество работы персонала с информационными системами банка, об этом свидетельствует снижение количества выявленных инцидентов по показателю «Ошибки при техническом обслуживании облачной инфраструктуры» С целью определения косвенного экономического эффекта от внедрения предложенной методики по оценке информационных рисков был проведен анализ финансово-экономического состояния филиала Банка ГПБ (АО) в г.Самаре. Результаты исследования представлены в таблице 3.3.6

Основные финансово-экономические показатели деятельности банка изменились. В целом можно констатировать, что изменения имеют положительную динамику.

1. Увеличился объем реализации услуг в натуральном выражении на 28,4%, в стоимостном - на 18,9%.

2. Возросла прибыль в целом по банку на 14%, на 1 нормо-ч. - на 17,8%.

3. Повысилась рентабельность услуг на 6,1%.

4. Сократились сроки выполнения процедур при анализе взаимоотношений с клиентами в среднем на 48,5%.

5. Несмотря на увеличение затрат на информационную безопасность, за отчетный период уменьшились операционные издержки на 270,6 тыс.руб.