На правах рукописи

Родина Юлия Владимировна

МОДЕЛИРОВАНИЕ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНОЙ ОРГАНИЗАЦИИ

08.00.13 – Математические и инструментальные методы экономики

Автореферат

диссертации на соискание ученой степени

кандидата экономических наук

Москва

2012

Работа выполнена на кафедре «Банки и банковские технологии» Заочного финансово-экономического института ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации».

Научный руководитель: доктор экономических наук, профессор
Рудакова Ольга Степановна

Официальные оппоненты: доктор экономических наук, профессор
Емельянов Александр Анатольевич,
ФГБОУ ВПО «Национальный исследовательский университет «Московский энергетический институт» (филиал в г. Смоленск), профессор кафедры «Менеджмент и информационные технологии в экономике»

кандидат экономических наук, профессор
Хорошилов Александр Владиевич
Институт ЮНЕСКО по информационным технологиям в образовании, национальный программный специалист, руководитель отдела профессионального и технического образования, развития потенциала педагогических работников и сетевого взаимодействия

Ведущая организация: **ФГУП «Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации»**

Защита состоится «05» декабря 2012 г. в 10-00 часов на заседании диссертационного совета Д 505.001.03 на базе ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации» по адресу: Ленинградский проспект, д.55, ауд. 213, Москва, 125993.

С диссертацией можно ознакомиться в диссертационном зале Библиотечно-информационного комплекса ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации» по адресу: Ленинградский проспект, д.49, комн. 203, Москва, 125993.

Автореферат разослан «30» октября 2012 г. Объявление о защите диссертации и автореферат диссертации «30» октября 2012 г. размещены на официальном сайте Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации по адресу http://vak.ed.gov.ru и на официальном сайте ФГОБУВПО «Финансовый университет при Правительстве Российской Федерации»: http://www.fa.ru .

Ученый секретарь совета Д 505.001.03,
к.э.н., доцент О.Ю. Городецкая

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. Приоритетным направлением развития Российской банковской системы (БС) является внедрение новых информационных технологий. Идет активный перевод совершения банковских операций из традиционных офисов в альтернативные каналы обслуживания: Интернет, устройства самообслуживания, дистанционное банковское обслуживание (ДБО). Число счетов клиентов, имеющих дистанционный доступ возросло за 3 года (с 01.01.2009 г. по 01.01.2012 г.) в 2 раза (с 38 862 тыс. до 79 261,9 тыс.). Все это создает огромные новые возможности для развития банковской системы, но в тоже время формирует и новые риски. Самым быстроразвивающимся видом киберпреступности является мошенничество в системах дистанционного банковского обслуживания. Прогнозируемый доход по итогам 2011 года хакеров из России и стран СНГ составляет 3,7 млрд. долларов. Ожидается, что в 2013-м г. этот показатель будет удвоен.

Эффективная работа банковской системы невозможна без обеспечения высокого уровня информационной безопасности (ИБ) организаций банковской системы. Отдельные сбои в работе организаций могут повлечь развитие системного кризиса платежной системы и нанести существенный ущерб банкам и их клиентам. В стандарте Банка России[1] отмечается, что «обеспечение информационной безопасности является для организаций банковской системы РФ одним из основополагающих аспектов их деятельности». Одним из этапов построения эффективной системы обеспечения информационной безопасности является проведение регулярной оценки риска нарушения информационной безопасности[2].

Особенностью проведения оценки рисков ИБ является недостаточность статистической информации, необходимость использования экспертных оценок, наличие большого количества неопределенностей, вызванных постоянно меняющимися условиями функционирования бизнес-процессов кредитных организаций (КО). Поэтому разработка математической модели, нацеленной на повышение точности оценок потенциальных потерь в результате реализации риска информационной безопасности, позволяющей использовать экспертные оценки, определяет актуальность темы исследования.

---

[1] СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»

[2] В контексте данной работы понятия «риск нарушения ИБ» и «риск ИБ» имеют аналогичные значения

Степень разработанности проблемы.

Рассмотрению проблем информационной безопасности посвящено множество работ, среди которых можно выделить публикации Курушина В.Д., Гайковича В.Ю., Першина А.Ю., Маслова О.Н., Соколова Ю.А., Герасименко В.А., Росса Г.В., Конявского В.А., Завгороднего В.И., Емельянова А.А., Хорошилова А.В. и др.

Основные вопросы управления ИБ и оценки рисков ИБ рассмотрены в отечественных и зарубежных стандартах.

Управление операционным риском рассмотрено в работах Маршалла К., Сазыкина В.Б., Золотарева В.М., Рудаковой О.С., Натуриной М., Громенко О.и др. Также эти вопросы систематизированы Базельским комитетом по банковскому надзору и Банком России.

Исследованию проблемы управления рисками ИБ с помощью нечетких систем посвящены работы таких ученых, как Герасименко В.А., Петренко С.А., Хоффмана Л. и других. Однако, несмотря на это, многие вопросы в данной области остаются недостаточно исследованными.

Современный этап развития теории оценки рисков говорит об актуальности объединения экспертных и математических методов. Такой подход является совершенствованием существующих подходов, позволяя использовать для оценки и прогнозирования рисков адаптированные модели оценки рисков ИБ. Перспективным направлением здесь является использование нечеткой логики (НЛ) для проведения оценки рисков ИБ.

Нечеткая логика широко используется для прогнозирования различных финансовых индикаторов, а также в области оценки риска фондовых инвестиций. Среди работ, посвященных использованию НЛ можно выделить работы Язенина А.В., Недосекина А.О., Штовба С.Д., Масалович А.И., Заде Л., Лукаса В.А., Коско Б.

В последнее время стали появляться работы, связанные с использованием НЛ для оценки рисков ИБ (Гильмуллин Т.М., Сидоров. А.О., Сатыбалдина Д.Ж., Балашов П.А., Кислов Р.И., Безгузиков В.П.).

В то же время отсутствуют работы, которые бы раскрывали особенности использования аппарата НЛ при оценке риска нарушения ИБ в банковской деятельности в условиях дефицита статистических данных и необходимости использования экспертных оценок.

Цель и задачи исследования. Цель работы состоит в разработке модели оценки риска нарушения информационной безопасности кредитной организации, позволяющей повысить точность получаемых значений потенциальных потерь в результате реализации риска информационной безопасности, а также подготовке методических рекомендаций по ее применению.

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

1. Проанализировать современные подходы к управлению информационной безопасностью и рисками информационной безопасности, исследовать связь рисков ИБ с операционными рисками.
2. Провести анализ существующих источников угроз информационной безопасности, уточнить классификацию источников угроз ИБ.
3. Обосновать целесообразность использования нечеткой логики для оценки рисков нарушения ИБ.
4. Модифицировать модель оценки риска нарушения информационной безопасности (ОРНИБ) с использованием нечеткой логики.
5. Выработать механизм повышения точности модели ОРНИБ, построенной с использованием нечеткой логики, за счет решения проблемы сужения диапазона выходных значений и разработки механизма обучения модели ОРНИБ.
6. Разработать инструментарий оценки риска нарушения информационной безопасности по модели нечеткой логики и методические рекомендации по его применению.

Объектом исследования выступает система менеджмента информационной безопасности кредитной организации.

Предметом исследования являются модели и методы оценки риска нарушения информационной безопасности кредитной организации.

Область исследования. Содержание диссертационного исследования соответствует пунктам 2.5, 2.6 Паспорта специальности 08.00.13 – Математические и инструментальные методы экономики (экономические науки).

Теоретическую и методологическую основу исследования составляют труды отечественных и зарубежных авторов по управлению рисками ИБ, по оценке рисков ИБ, по нечеткой логике и математическому моделированию.

Работа базируется на использовании методов оптимизации и аппроксимации, аппарата нечеткой логики, моделировании систем, экспертных оценок, методов оценки рисков информационной безопасности.

Обработка данных и построение модели осуществлялись с использованием приложений Microsoft Excel и MATLAB, а также при помощи программного продукта, разработанного автором на языке программирования VBA.

Информационную базу исследования составили отечественные и международные стандарты в области обеспечения информационной безопасности; законодательные акты Российской Федерации; нормативные документы Банка России; диссертации, публикации ученых и практиков; доклады отечественных и зарубежных ученых на конференциях и симпозиумах, связанных с темой исследования; результаты аналитических обзоров, исследований и разработок отечественных и зарубежных компаний и организаций, занимающихся вопросами информационной безопасности; материалы периодической печати и сети Интернет.

Научная новизна исследования заключается в построении модели оценки риска нарушения информационной безопасности в условиях дефицита статистических данных.

Наиболее существенные результаты, полученные лично автором и выносимые на защиту:

1. Обоснована необходимость введения нового источника угроз ИБ финансово-кредитных организаций, связанных с возможным нарушением технологии использования их организационно-методического обеспечения. Учет этого источника угроз ИБ позволяет выработать дополнительные меры по защите конфиденциальной информации клиентов.

2. Изложена аргументация по построению модифицированных моделей оценки риска нарушения информационной безопасности с использованием аппарата нечеткой логики, который позволяют расширить границы их применения по сравнению с существующими подходами, в частности методикой оценки рисков CRAMM.

3. Разработаны модифицированные модели и методы оценки риска нарушения информационной безопасности, использующие экспертно-аналитические процедуры, лингвистические переменные и аппарат нечеткого логического вывода. Подтверждена целесообразность использования методики оценки рисков нарушения информа-

ционной безопасности Банка России, которая позволяет получить количественную оценку величины риска для принятия обоснованных решений по управлению им.

4. Предложен способ повышения точности модели оценки риска нарушения информационной безопасности, который базируется на решении проблемы сужения диапазона выходных значений и использовании механизма адаптивного обучения моделей оценки рисков нарушения ИБ.

5. Разработаны эффективные процедуры диалогового взаимодействия работника службы безопасности с компьютерной системой, которые позволяют достаточно просто использовать её для принятия решений по оценке риска нарушения информационной безопасности (получено Свидетельство о государственной регистрации программы для ЭВМ № 2011613248 от 26.04.2011 г.), а также предложены методические приемы сбора, предварительной подготовки исходной информации и получения результатов.

Теоретическая значимость исследования. Теоретическая значимость исследования заключается в адаптации известных математических и инструментальных методов для решения задачи моделирования оценки риска нарушения информационной безопасности в кредитной организации. Полученные результаты исследования позволяют повысить качество принимаемых решений в управлении рисками ИБ.

Практическая значимость исследования. Практическая значимость полученных результатов заключается в том, что разработанная модель ОРНИБ ориентирована на широкое применение в различных подразделениях кредитных организаций и на промышленных предприятиях.

Самостоятельное практическое значение имеют:

- модифицированная модель оценки риска нарушения информационной безопасности с использованием нечёткой логики, которая позволяет получить количественную оценку величины риска для принятия обоснованных решений по управлению им;
- алгоритм реализации модели ОРНИБ в среде VBA на основе нечеткой логики;
- рекомендации по использованию модели ОРНИБ в кредитных организациях и на промышленных предприятиях;
- модификация классов источников угроз ИБ в соответствии с современными тенденциями в данной области, что позволило выработать более конкретные рекомендации для снижения рисков ИБ в кредитных организациях.

Разработанные на основе исследования рекомендации могут быть использованы при реализации программ, связанных с обеспечением информационной безопасности.

Материалы диссертационной работы могут быть использованы при подготовке специалистов в области банковского дела, а также при реализации программ по повышению осведомленности персонала и клиентов организаций в области информационной безопасности.

Отдельные положения и результаты исследования могут быть использованы при изучении дисциплин «Современные банковские технологии» и «Банковский менеджмент».

Апробация и внедрение результатов исследования.

Полученные теоретические, методологические и практические результаты поэтапной разработки проблемы докладывались и обсуждались на: I Международной научно-практической конференции «Информатизация и глобализация экономических процессов в XXI веке: теория и практика» (г. Москва, Всероссийский заочный финансово-экономический институт, 2006 г.); Всероссийской научно-практической конференции «Инновации в современном мире: проблемы и перспективы» (г. Волгоград, Центр прикладных и научных исследований, 30 марта 2009 г.); III международной научно-практической конференции «Управление в XXI веке» (г. Киров, ГОУ ВПО «Вятский государственный гуманитарный университет», 15 апреля 2009 г.); Международной научно-практической конференции «Инновационный путь развития РФ как важнейшее условие преодоления мирового финансового кризиса» (г. Москва, Всероссийский заочный финансово-экономический институт, 21-22 апреля 2009г.); Международной научно-технической конференции «Математические методы и информационные технологии в экономике, социологии и образовании» (г. Пенза, Приволжский Дом знаний, 2009 г.); IV Международной научно-технической конференции «Аналитические и численные методы моделирования естественнонаучных и социальных проблем» (г. Пенза, Приволжский Дом знаний, 19 – 22 октября 2009 г.); IX Международной научно-технической конференции «Проблемы информатики в образовании, управлении, экономике и технике» (г. Пенза, Приволжский Дом знаний, 2009 г.); XXIV Международной научно-технической конференции (зимняя сессия) «Математические методы и информационные технологии в экономике, социологии и образовании» (г. Пенза, Приволжский Дом знаний, 2009 г.); V Всероссийской науч-

но-практической конференции «Резервы экономического роста предприятий и организаций» (г. Пенза, Приволжский Дом знаний, 2010 г.); Международной научно-практической конференции "Экономика, наука, образование: проблемы и пути интеграции", посвященной 80-летнему юбилею ВЗФЭИ (г. Москва, Всероссийский заочный финансово-экономический институт, 26-27 октября 2010 г.); Международной научно-практической конференции «Россия в XXI веке: итоги, вызовы, перспективы» (г. Тюмень, НОУ «Институт экономики и предпринимательства, 2011 г.); V-й Международной научно-практической конференции «Управление в XXI веке» (г. Киров, ГОУ ВПО «Вятский государственный гуманитарный университет», 2011 г.); XXVIII Международной научно-технической конференции (зимняя сессия) «Математические методы и информационные технологии в экономике, социологии и образовании» (г. Пенза, Приволжский Дом знаний, декабрь 2011 г.), II Международной научно-практической конференции «Информационные ресурсы и системы в экономике, науке и образовании» (г. Пенза, Приволжский Дом знаний, апрель 2012 г.).

За отдельные положения исследования получена Почетная грамота Всероссийского заочного финансово-экономического института за победу в I туре «Открытого конкурса 2005 года на лучшую научную работу студентов в высших учебных заведениях Российской Федерации».

Предложения по оценке рисков нарушения информационной безопасности с использованием нечеткой логики и повышения осведомленности персонала в области информационной безопасности применяются в практической деятельности Новомосковского отделения № 2697 ОАО «Сбербанк России». Это дает возможность принимать более обоснованные решения по управлению рисками информационной безопасности и помогает снижению рисков реализации инцидентов ИБ.

В рамках инновационной деятельности в Среднерусском банке ОАО «Сбербанк России» предложение, разработанное в ходе диссертационного исследования и связанное с повышением осведомленности сотрудников в области информационной безопасности для снижения рисков реализации инцидентов ИБ и нанесения банку ущерба, отнесено к категории «лучшие практики».

Модель ОРНИБ используется в работе ООО «Проктер энд Гэмбл Новомосковск» и помогает принимать более обоснованные решения по управлению рисками информационной безопасности.

Разработанный в ходе исследования комплекс программных средств для ЭВМ, позволяющий производить количественную и качественную оценку рисков нарушения ИБ, зарегистрирован в Реестре программ для ЭВМ (Родина Ю.В. «Оценка риска нарушения информационной безопасности по модели нечеткой логики с корректировкой параметров её терм-множеств». Свидетельство о государственной регистрации программы для ЭВМ № 2011613248 от 26.04.2011 г.).

Материалы исследования используются кафедрой «Банки и банковские технологии» Заочного финансово-экономического института Финансового университета в преподавании учебной дисциплины «Банковские электронные услуги».

Результаты внедрения подтверждены соответствующими справками.

Публикации. По теме диссертации опубликовано 17 статей, общим объемом 4,55 п.л. (авторский объем – 4,15 п.л.), из них 4 работы опубликованы в изданиях, определенных ВАК Минобрнауки России.

Структура и объем работы. Диссертационная работа состоит из введения, трех глав, заключения, списка литературы и приложений. Общий объем диссертации составляет 193 страницы. Работа содержит 11 таблиц, 56 рисунков, 8 приложений. Список литературы включает 124 наименования.

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИИ

Далее приводятся основные положения работы, изложенные в разрезе поставленных задач.

1. Проанализировать современные подходы к управлению информационной безопасностью и рисками информационной безопасности, исследовать связь рисков ИБ с операционными рисками.

Наиболее эффективные современные системы управления (менеджмента)[3] информационной безопасностью и рисками информационной безопасности основаны на циклическом и риск-ориентированном подходе.

Система менеджмента информационной безопасности (СМИБ) является частью системы менеджмента организации банковской системы Российской Федерации, предназначенной для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности (СОИБ). Второй составляющей СОИБ является система информационной безо-

[3] Понятия система управления ИБ и система менеджмента ИБ, система управления рисками ИБ и система менеджмента риска ИБ имеют аналогичные значения. Использование разных названий связано с их использованием в российских и международных стандартах.

пасности (СИБ), которая включает в себя совокупность защитных мер, реализующих обеспечение ИБ организации и процессов их эксплуатации.

Для реализации и поддержания ИБ в организации БС РФ необходимо выполнение следующих групп циклических процессов, составляющих СМИБ: «планирование», «реализация», «проверка», «совершенствование».

Создание эффективной СМИБ невозможно без организации систематического подхода к управлению (менеджменту) риска ИБ. В таблице 1 показана взаимосвязь процессов менеджмента риска с фазами процесса СМИБ. Фактически, результаты оценки рисков используются на всех стадиях построения системы обеспечения информационной безопасности.

Анализ функционирования системы обеспечения информационной безопасности включает в себя в обязательном порядке оценку рисков в области ИБ организации, включая оценку уровня остаточного и допустимого риска.

Управление рисками ИБ должно осуществляться четко и последовательно во всей организации. Для управления рисками ИБ могут применяться различные подходы к оценке и управлению рисками, различные степени детализации, которые отвечают требованиям организации. Организация должна сама определить, какой подход к оценке рисков будет использоваться.

Таблица 1

Соотношение процессов СМИБ и процессов менеджмента риска ИБ

Процесс СМИБ	**Процесс менеджмента риска ИБ**
Планирование	Установление контекста Оценка риска Планирование обработки риска Принятие риска
Осуществление	Реализация плана обработки риска
Проверка	Проведение непрерывного мониторинга и переоценки рисков
Совершенствование	Поддержка и усовершенствование процесса менеджмента риска ИБ

Риски ИБ тесно связаны с другими банковскими рисками (операционный, репутационный, стратегический и т.д). Нарушение целостности, доступности или конфиденциальности информационных активов может привести к реализации одного или нескольких банковских рисков, которые, в свою очередь могут привести к реализации системного риска. При рассмотрении различных видов риска особенно интересна взаимосвязь рисков ИБ и операционных рисков, которая хорошо видна при анализе источников угроз, формирующих операционные риски и риски ИБ (таблица 2).

Самая общая трактовка операционного риска используется в Базель II. При этом, в качестве источника угрозы не рассматриваются угрозы, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству. Источники угроз операционного риска, используемые в определении Банка России, в целом соответствуют источникам угроз ИБ. Но источники угроз ИБ имеют более развернутую и наглядную классификацию. Реализация любых угроз за счет источников, показанных в таблице 2, может привести как к реализации риска информационной безопасности, так и к реализации операционного риска. Оценка и управление рисками ИБ положительно сказывается на стабильности кредитной организации и помогает снижению операционных рисков.

Таблица 2.

Источники угроз операционного риска и источники угроз ИБ

Источники угроз операционного риска (из определения Basel II[4])	Источники угроз операционного риска (из определения Банка России[5])	Источники угроз ИБ[6]
-	несоответствие характеру и масштабам деятельности кредитной организации и (или) требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок	Класс 7. Источники угроз ИБ, связанные с несоответствием требованиям надзорных и регулирующих органов, действующему законодательству
неадекватные или ошибочные внутренние процессы, действия сотрудников и систем	нарушение внутренних порядков и процедур проведения банковских операций и других сделок служащими кредитной организации и (или) иными лицами (вследствие некомпетентности, непреднамеренных или умышленных действий или бездействия)	Класс 5. Источники угроз ИБ, связанные с деятельностью внутренних нарушителей ИБ
	несоразмерность (недостаточность) функциональных возможностей (характеристик) применяемых кредитной организацией информационных, технологических и других систем и (или) их отказов (нарушений функционирования)	Класс 4. Источники угроз ИБ, связанные со сбоями, отказами, разрушениями/повреждениями программных и технических средств
Внешние события	в результате воздействия внешних событий	Класс 1. Источники угроз ИБ, связанные с неблагоприятными событиями природного, техногенного и социального характера Класс 2. Источники угроз ИБ, связанные с деятельностью террористов и лиц, совершающих преступления и правонарушения Класс 3. Источники угроз ИБ, связанные с деятельностью поставщиков/провайдеров/ партнеров Класс 6. Источники угроз ИБ, связанные с деятельностью внешних нарушителей ИБ

[4] Международная конвергенция измерения капитала и стандартов капитала: новые подходы // Базельский комитет по банковскому надзору – 2004.
[5] О типичных банковских рисках: Письмо Центрального Банка Российской Федерации от 23 июня 2004 г. N 70-Т
[6] Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности. Рекомендации в области стандартизации Банка России РС БР ИББС-2.2.-2009.

К сожалению, на текущий момент позиции Банка России в управлении операционными рисками и рисками ИБ существенно отличаются. Документы, регламентирующие управление операционными рисками носят обязательный характер, а документы, связанные с управлением рисками ИБ – рекомендательный характер. Такое положение существенно снижает желание кредитных организаций внедрять данные документы.

2. Провести анализ существующих источников угроз информационной безопасности, уточнить классификацию источников угроз ИБ.

Проведенный анализ источников угроз свидетельствует о том, что рекомендуемый перечень классов основных источников угроз ИБ в соответствии с РС БР ИББС-2.2-2009 желательно уточнить. Это связано со следующими моментами: 1) по результатам многочисленных исследований и на основании статистических данных самым опасным является мошенничество в системах дистанционного банковского обслуживания; 2) рекомендуемый перечень классов основных источников угроз содержит угрозы, оказывающие непосредственное влияние на организации БС РФ, но, кроме этого, существует ряд угроз, оказывающих опосредованное влияние на организации БС РФ, которые также необходимо учитывать. Поэтому, перечень классов основных источников угроз информационной безопасности нужно дополнить классом 8 (рис. 1, таблица 3).

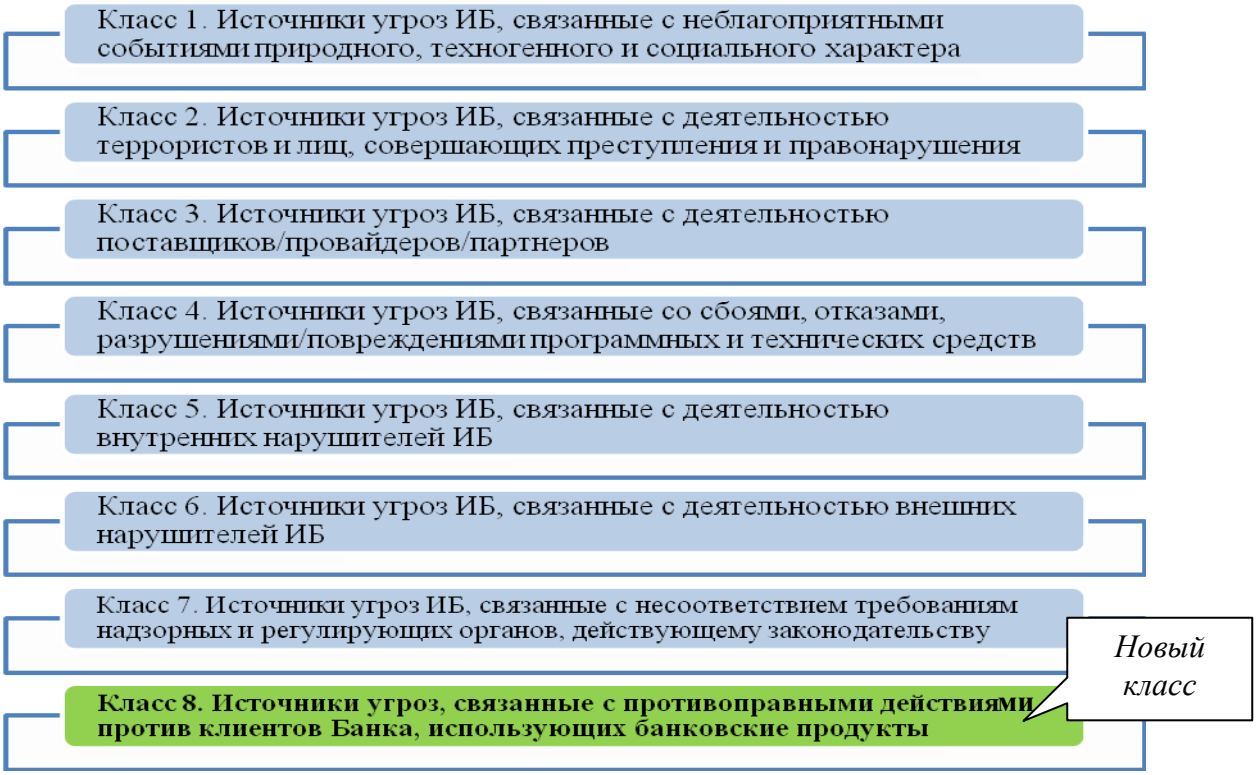

Рис. 1. Модификация классов источников угроз

Проходящие в банках процессы реинжиниринга, современные тенденции развития банковских продуктов приводят к активному переводу банковских операций в альтернативные каналы обслуживания. Стремительный перевод клиентов в альтернативные каналы обслуживания и такой же стремительный рост преступлений, связанных с их использованием вполне может привести к развитию системного кризиса, о котором предупреждает Банк России при самом пессимистичном варианте развития событий, или, как минимум, вызвать существенный отток клиентов из-за недоверия к банковской системе.

С 01 января 2013 года вступают в силу основные положения Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе», обязывающие банки возмещать клиентам ущерб в случае перевода денежных средств без согласия клиента, если банк не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента. Нельзя забывать и про ст. 1095 «Основания возмещения вреда, причиненного вследствие недостатков товара, работы или услуги» Гражданского Кодекса РФ.

Таблица 3

Класс 8. Источники угроз, связанные с противоправными действиями против клиентов Банка, использующих банковские продукты

Источник угроз ИБ	Описание	Возможные причины	Возможные последствия
Мошенничество в системах ДБО юридических лиц	Использование вредоносного ПО; Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение клиентов организации БС РФ.	Недостаточная осведомленность клиентов о требованиях ИБ. Игнорирование клиентами требований ИБ.	Нанесение материального ущерба клиентам. Реализация репутационных рисков для банка.
Мошенничество в системах ДБО физических лиц			
Мошенничество с использованием других банковских продуктов	Умышленные действия сторонних лиц, преследующих мошеннические цели, реализуемые посредством обмана, введения в заблуждение клиентов организации БС РФ.	Недостаточная осведомленность клиентов о банковских продуктах. Игнорирование клиентами элементарных требований безопасности.	

На сегодня можно выделить следующие проблемы: клиенты банков слабо представляют, какие операции могут совершаться в системах ДБО, а какие являются мошенничеством; низкая компьютерная грамотность населения, в результате этого, многие клиенты не представляют, как выглядит лицензионное и антивирусное ПО и т.д.; российский менталитет, считающий «дурным» тоном использование лицензионного ПО (правда, здесь свою роль играет и стоимость лицензионного ПО); излишнее доверие большинства клиентов, позволяющих преступникам широко использовать методы социальной инженерии; требования по обеспечению безопасности рабочего места клиента излагаются таким образом, что большинство клиентов их не по-

нимает в связи с недостаточной подготовкой, или не имеет возможностей для их исполнения (или и то и другое).

Для дальнейшего успешного развития ДБО и снижения рисков его использования (помимо широко внедряющихся технических средств) необходимо проведение постоянных широкомасштабных мероприятий по повышению осведомленности клиентов в области ИБ. Существующие на сегодняшний день варианты обучения было бы целесообразно дополнить проводимыми на постоянной основе бесплатными семинарами для физических и юридических лиц. Такие мероприятия могут дать следующий положительный эффект: ненавязчивая реклама банковских продуктов помогает расширению их использования; повышение грамотности клиентов банка способствует снижению риска совершения мошенничества в их отношении, и, как следствие, снижению репутационных рисков банка; подготовка к проведению семинаров и их проведение повышает квалификационный уровень сотрудников банка; выявление неясных для клиентов моментов при совершении банковских операций, их пожеланий и потребностей может помочь развитию банковских операций; формирование положительного имиджа банка, так как свидетельствуют о заботе банка о своих клиентах.

Безопасное использование ДБО тесно связано с соблюдением организационных требований обеспечения ИБ со стороны клиентов. Банки должны осознать свою заинтересованность в решении данного вопроса и начать принимать превентивные меры для предотвращения в дальнейшем негативных последствий.

3. Обосновать целесообразность использования нечеткой логики для оценки рисков нарушения ИБ.

Можно представить следующую последовательность развития методов оценки рисков: методы, использующие статистические данные → экспертные методы → математические методы и модели оценки. Современный этап развития теории оценки рисков говорит об актуальности объединения экспертных и математических методов. Такой подход является совершенствованием существующих подходов, позволяя использовать для оценки и прогнозирования рисков адаптированные модели оценки рисков ИБ. Метод экспертных оценок используется для оценки рисков ИБ в связи с тем, что часто для этих рисков затруднительно определить стоимостное выражение, а также из-за отсутствия полноценных исторических и статистических данных о реализованных рисках.

Экспертная оценка риска ИБ дает возможность определить уровень рисков ИБ на уровне подразделений, бизнес-линий, отдельных операций или групп операций, а также обеспечить категорирование операций по уровню приемлемого риска.

Проведение экспертной оценки рисков ИБ позволяет: определить операции и процессы подразделения (или банка), которые наиболее подвержены рискам ИБ; выявить слабые места в отдельных составляющих бизнес-процессов; оценить величину возможного ущерба и вероятность его возникновения по конкретным видам рисков; оценить допустимый уровень риска; оценить качество и достаточность принимаемых мер по обработке риска; обосновать принимаемые решения по обработке рисков ИБ.

В общем случае риск определяется как произведение вероятности наступления события на возможный ущерб. Однако, наиболее часто в качестве исходных данных используются качественные величины. В связи с этим операция умножения для них не определена и в явном виде формула не может быть использована. Поэтому в последнее время для оценки рисков ИБ рассматривается необходимость применения альтернативных методов. Наиболее актуальным из которых является использование математического аппарата нечеткой логики. Нечеткая логика обладает следующими свойствами: учитывает особенности человеческого восприятия, нечеткие утверждения и оценки; дает возможность формализовать качественную информацию, полученную от экспертов, и описать ее в виде системы правил ЕСЛИ-ТО, позволяющих анализировать результаты работы; взаимосвязь входных и выходных переменных модели НЛ представляется в виде трехмерной поверхности, удобной для качественного анализа и оценки адекватности модели; возможность формулирования достоверных заключений исходя из неполных или приблизительных входных данных; устойчивость к неточным оценкам отдельных свойств элементов.

Большинство методик ОРНИБ основано на табличных методах и использовании качественных оценок, что является идеальным для применения аппарата НЛ для оценки рисков ИБ. Существующие качественные методики оценки рисков ИБ не обладают достаточной точностью получаемых результатов, а количественные методики сводятся к вероятностным оценкам, что в отсутствии статистики инцидентов не дает достоверных результатов. Модели на основе НЛ лишены вышеперечисленных недостатков и могут работать с нечеткими оценками экспертов. Поэтому, для математического описания и моделирования оценки риска нарушения ИБ, в большей степени, чем классическая математика и логика, подходит именно нечеткая логика.

4. Модифицировать модель ОРНИБ с использованием нечеткой логики

Для выбора оптимальной модели ОРНИБ были разработаны модифицированные модели и методы оценки риска нарушения информационной безопасности, использующие экспертно-аналитические процедуры, лингвистические переменные и аппарат нечеткого логического вывода. Для того чтобы понять как влияет число используемых градаций значений входных и выходных переменных на построение моделей НЛ, были модифицированы две модели ОРНИБ с различным числом уровней входных и выходных параметров: модель на основе методики оценки рисков CRAMM и модель на основе рекомендаций Банка России. Первая модель использует в качестве входных параметров вероятность наступления ущерба и стоимость ущерба, имеющие по пять уровней. Выходной параметр «Риск» имеет девятиуровневую шкалу значений. Вторая модель на входе имеет переменные «Степень возможности реализации угроз ИБ» и «Степень тяжести последствий от потери свойств ИБ» (имеющие по 4 возможных значения) и на выходе переменную «Риск», значение которой может принимать одно из двух значений («допустимый» и «недопустимый»).

По результатам моделирования можно сделать следующие выводы:

- Обе исследуемые модели соответствуют условиям прозрачности модели НЛ.
- При обучении моделей сохраняются свойства прозрачности.
- Для обучения моделей ОРНИБ целесообразно использовать изменение параметров функций принадлежностей (ФП) - увеличение «ширины» ФП входных переменных (дисперсия для кривых Гаусса) с одновременным уменьшением дисперсии по выходной переменной.
- Использование различного числа уровней фактически не влияет на адекватность модели.
- Меньшее число уровней облегчает программную реализацию.
- Меньшее число градаций входных и выходных параметров упрощает проведение оценки рисков на локальном уровне, так как меньшая дифференциация облегчает присвоение согласованных оценок в масштабе организации, что актуально для организаций, имеющих большое количество филиалов. Целесообразно проводить оценку рисков ИБ и на уровне подразделений, так как региональные особенности могут вносить существенную погрешность в консолидированную оценку риска.

Таким образом, методика оценки рисков нарушения ИБ, рекомендованная Банком России, при меньшем числе уровней позволяет наилучшим образом использо-

вать возможности аппарата нечеткой логики, что позволяет расширить границы ее применения по сравнению с существующими подходами (в частности, методикой оценки рисков CRAMM). Существенным плюсом данной методики является возможность количественной оценки величины риска, что очень важно для принятия обоснованных решений по управлению риском.

5. Выработать механизм повышения точности модели ОРНИБ, построенной с использованием нечеткой логики, за счет решения проблемы сужения диапазона выходных значений и разработки механизма обучения модели ОРНИБ.

Для повышения точности необходимо произвести обучение модели ОРНИБ. При этом итерационно изменяют параметры модели ОРНИБ для того, чтобы минимизировать отклонение выходных данных логического вывода от экспериментальных данных. Для этого применяют изменение весовых коэффициентов и изменение параметров ФП. Необходимо отметить, что при обучении моделей часто делают упор на достижение максимальной точности. При этом теряется прозрачность модели НЛ, что отрицательно сказывается на возможности содержательной интерпретации данной модели. Для модели ОРНИБ при обучении обязательным условием является сохранение прозрачности модели.

Параметры ФП можно определить опытным путем. Функция Гаусса (1) (где a – математическое ожидание, σ^2 – дисперсия),

$$y = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-a)^2}{2\sigma^2}} \quad (1),$$

перед использованием в качестве ФП модифицирована (2) так, что «высота» вершины (её ордината) всегда остается равной 1.

$$c = e^{-k\cdot(g+a)^2} \quad (2)^7.$$

Для коррекции формы ФП будем изменять два параметра функции Гаусса – дисперсию и математическое ожидание. Как показало моделирование в пакете Fuzzy Logic увеличение «ширины» ФП входных переменных (дисперсия для кривых Гаус-

[7] Два введённых для этого коэффициента (k и a) графически представляют собой «ширину» ФП (коэффициент k) – аналог параметра «дисперсия» и координату вершины ФП на оси абсцисс (коэффициент a) – аналог параметра «математическое ожидание». Данная модификация функции Гаусса вызвана удобством программирования и специальным ограничением на постоянство ординаты вершин ФП. В модифицированной функции Гаусса координаты оси абсцисс задаются переменной g, а координаты оси ординат – переменной c.

са) с одновременным уменьшением дисперсии по выходной переменной дает наиболее плоскую (более гладкую) равномерную поверхность.

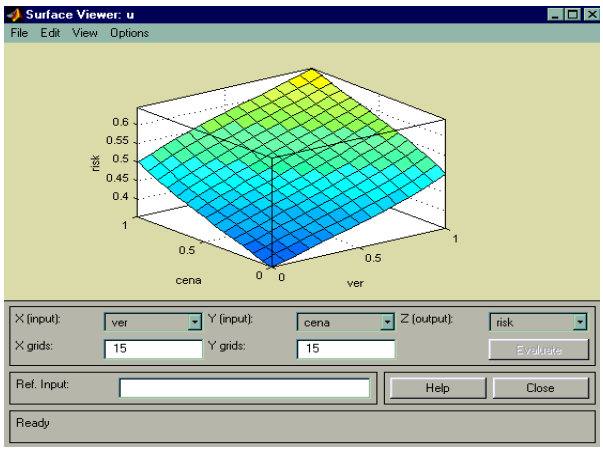

Рис. 2. Поверхность системы нечеткого вывода

Графический интерфейс Fuzzy Logic позволяет получить трехмерное изображение «поверхности системы нечеткого вывода» (рис.2) и график зависимости выходной величины от любой из входных переменных. Таким образом, он позволяет контролировать качество работы механизма вывода. Гладкий и монотонный график зависимости логического вывода свидетельствует о достаточности и непротиворечивости используемых правил вывода.

Использование метода «центра тяжести» при проведении дефазификации приводит к сужению диапазона выходных значений. То есть, уровень риска ни при каких условиях не будет принимать максимальные или минимальные значения. Для ОРНИБ с использованием НЛ, чтобы устранить эффект сужения диапазона, целесообразно ввести поправочный коэффициент. В этом случае модель объекта будет выглядеть следующим образом (рис. 3)[8]. Данная функция поправки растягивает выходную переменную до нормированного значения переменной “risk” 0÷1 относительно среднего значения 0,5.

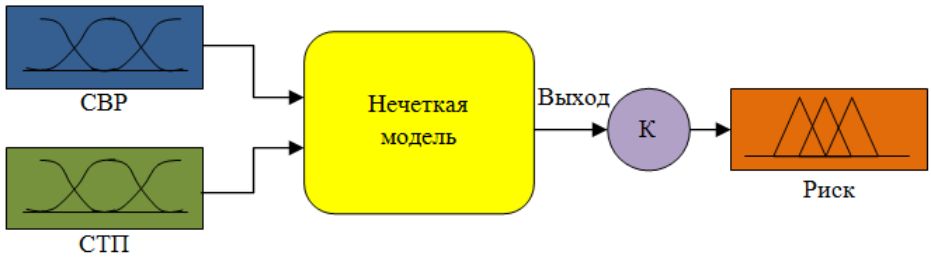

Рис. 3. Модель объекта с использованием поправочного коэффициента

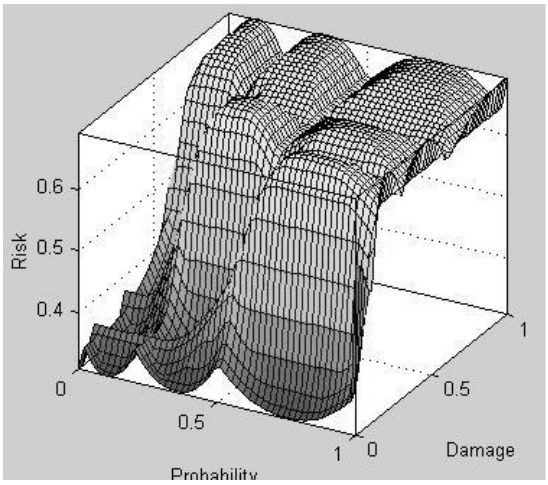

Рис. 4. Вид поверхности модели НЛ

Получение параметров ФП при использовании аппарата НЛ для ОРНИБ сводится к решению задачи оптимизации, где крите-

[8] СТП - степень тяжести последствий нарушения ИБ; СВР - степень вероятности реализации угроз ИБ.

рием оптимизации является минимум площади, ограниченной между целевой и полученной функцией, а параметрами оптимизации – дисперсия и математическое ожидание ФП, выраженные кривыми нормального распределения ошибок (Гаусса). Как видно из рисунка 4, поверхность исходной модели не является монотонной и гладкой функцией. Множество локальных минимумов и максимумов ухудшают адекватность модели и точность вычисления величины риска. Решаемая в исследовании задача оптимизации позволяет получить значение коэффициентов модели, которые приводят ее к монотонному виду. Для решения задачи многомерной оптимизации целесообразно воспользоваться методом Гаусса-Зейделя (наискорейшего спуска).

6. Разработать инструментарий оценки риска нарушения ИБ по модели нечеткой логики и методические рекомендации по его применению.

По результатам исследования разработана программа «Оценка риска нарушения информационной безопасности по модели нечёткой логики с корректировкой параметров её терм-множеств» (свидетельство о государственной регистрации программы для ЭВМ № 2011613248) с использованием стандартных встроенных средств программирования (VBA), что позволяет обеспечить совместимость с аппаратным и программным обеспечением, используемым практически в любой организации, снизить стоимость программного обеспечения.

Программа предназначена для моделирования и вычисления величины риска нарушения ИБ в качественной и количественной (денежной) форме на основании рекомендаций в области стандартизации Банка России РС БР ИББС-2.2-2009 с использованием аппарата НЛ. Инструментарий содержит эффективные процедуры диалогового взаимодействия работника службы безопасности с компьютерной системой, которые позволяют достаточно просто использовать её для принятия решений по оценке риска нарушения информационной безопасности. Также предложены методические приемы сбора, предварительной подготовки исходной информации и получения результатов. Кроме этого, программный модуль обеспечивает решение проблемы сужения диапазона выходных значений и содержит механизм адаптивного обучения модели оценки риска нарушения ИБ.

Алгоритм программы представлен на рис. 6. Алгоритм включает в себя создание модели ОРНИБ с использованием НЛ с исходными значениями переменных этой модели, автоматическую оптимизацию исходной модели с получением новых значе-

ний переменных модели, для анализа и проверки данной модели на адекватность и графическое отображение модели в виде трехмерной поверхности.

Вид модели ОРНИБ с использованием нечеткой логики представлен на рис. 5.

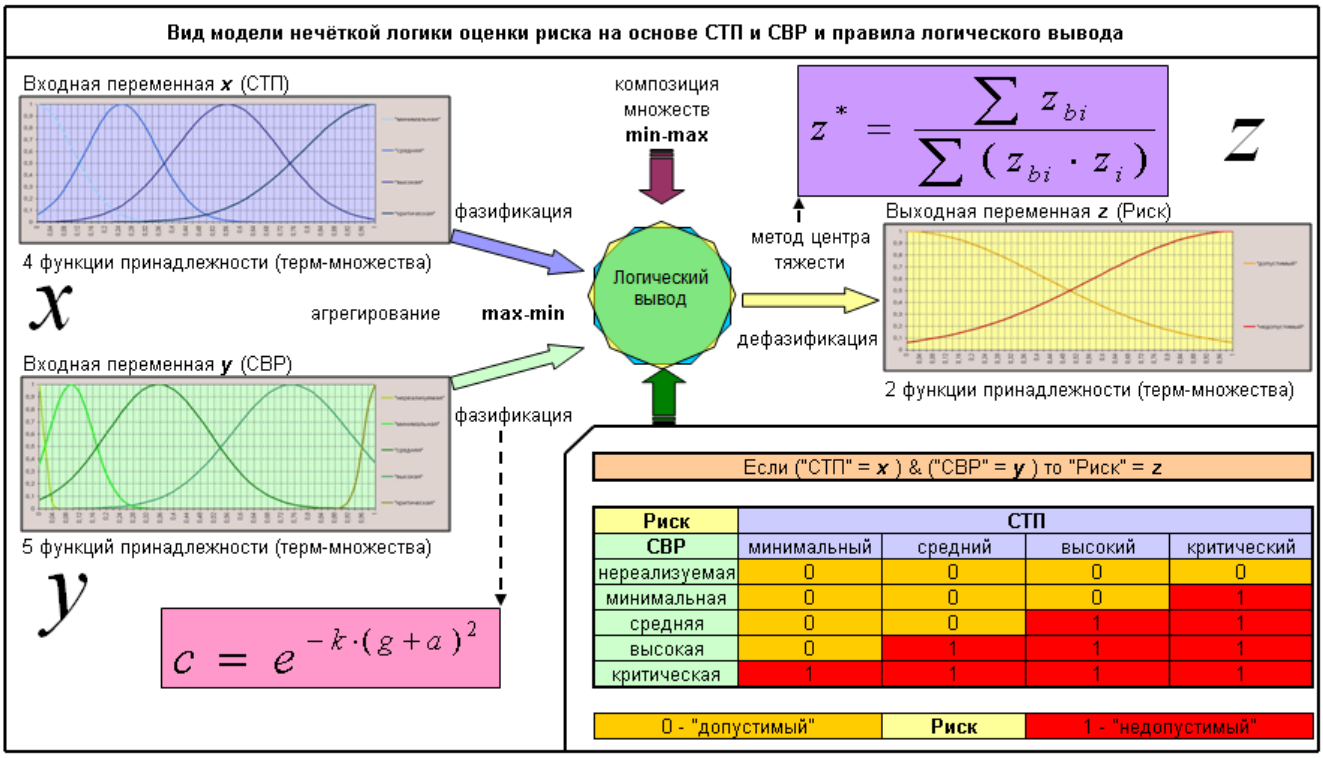

Рис. 5. Вид модели ОРНИБ с использованием НЛ на основе СТП и СВР и правила логического вывода

Программа может быть использована в кредитных организациях и на промышленных предприятиях при определении параметров обработки риска нарушения ИБ. Результаты оценки риска нарушения ИБ могут быть представлены в наглядной форме в виде трехмерного графика, который позволяет визуально оценить текущее значение риска и его общее положение на карте риска. Такая зрительная оценка дает возможность при принятии решений делать более обоснованные заключения.

В заключении диссертационной работы обобщены итоги проведенного исследования, сформированы основные выводы, полученные в результате исследования.

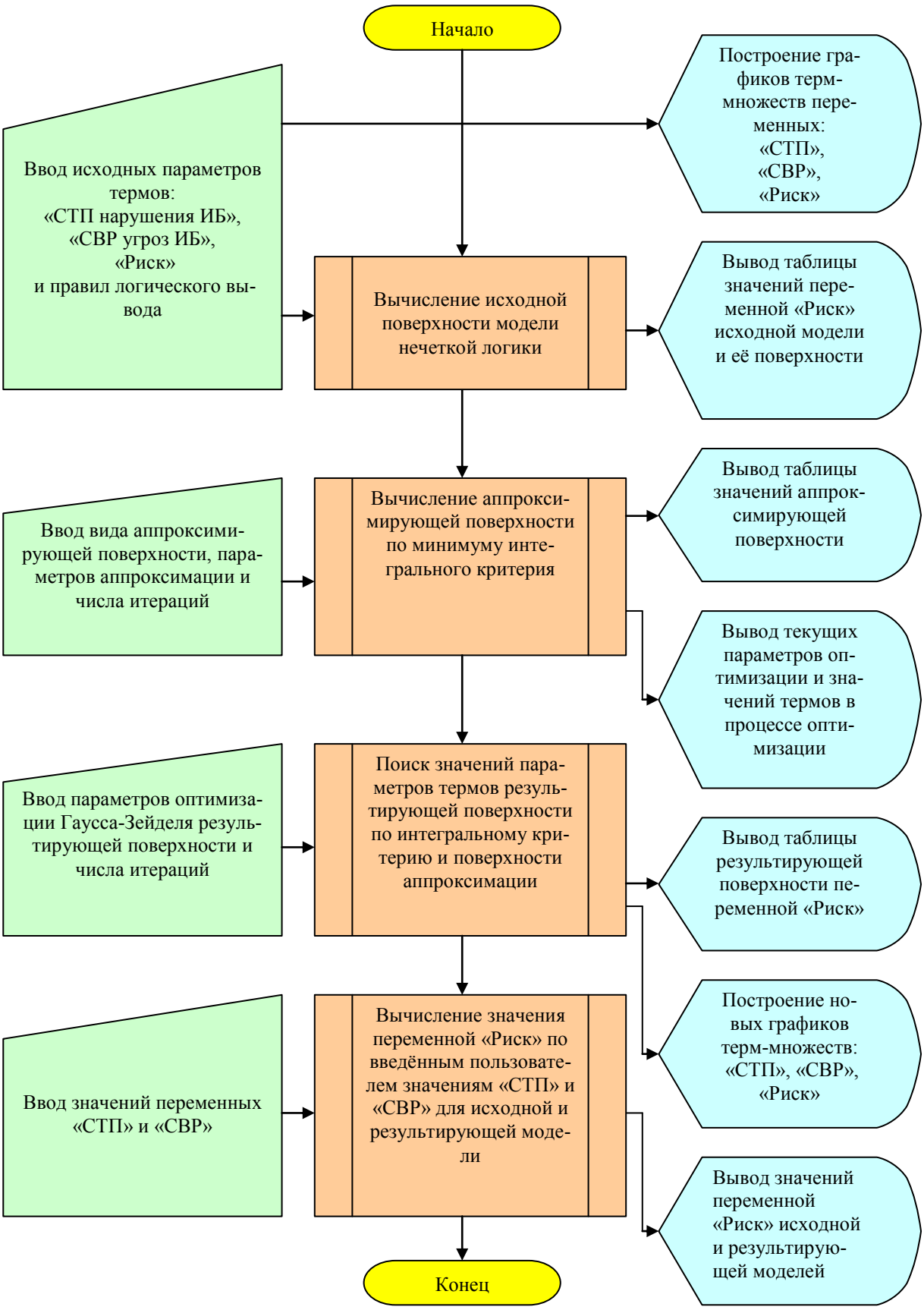

Рис. 6. Алгоритм ОРНИБ с использованием НЛ

Основные положения и результаты диссертации изложены в следующих публикациях.

Статьи, опубликованные в журналах, определенных ВАК Минобрнауки России:

1. Родина Ю.В. Анализ угроз информационной безопасности кредитных организаций [текст]/ Ю.В. Родина, О.С. Рудакова //Национальные интересы: приоритеты и безопасность. Научно-практический и теоретический журнал. - 2009. - № 23(56). С. 61-67. (0,8/0,6 п.л.)
2. Родина Ю.В. Оценка риска нарушения информационной безопасности по модели нечёткой логики с корректировкой параметров её терм-множеств [элект. ресурс] / Ю.В. Родина // Управление экономическими системами: электронный научный журнал. – 2011. - № 6. URL: http://www.uecs.ru. № гос.рег.статьи: 0421100034/0186. Дата обращения: 24.05.2012 (0,6 п.л.)
3. Родина Ю.В. Использование многомерной оптимизации для коррекции поверхности нечеткой модели оценки риска нарушения информационной безопасности [текст]/ Ю.В. Родина // Интеграл. – 2011. - № 4(60). С. 38. (0,125 п.л.)
4. Родина Ю.В. Дистанционное банковское обслуживание. Источники угроз [текст]/ Ю.В. Родина // Интеграл. – 2012. - № 1(60). С. 40. (0,125 п.л.)

Статьи, опубликованные в других научных изданиях и журналах:

5. Родина Ю.В. Анализ рисков информационной безопасности коммерческого банка на основе применения аппарата нечеткой логики [текст]/ Ю.В. Родина, О.С. Рудакова // Информатизация и глобализация экономических процессов в XXI веке: теория и практика. Сборник статей по материалам Международной научно-практической конференции Москва (Россия) ВЗФЭИ, 23 мая 2006 г. т.2. – М.: ВЗФЭИ, 2006. С. 40-50. (0,6/0,4 п.л.)
6. Родина Ю.В. Некоторые особенности применения аппарата нечёткой логики при анализе рисков информационной безопасности [текст]/ Ю.В. Родина // Управление в XXI веке [Текст]: материалы III международной научно-практической конференции. 15 апреля 2009 г., г. Киров / под. ред. В.Т. Юнгблюда, Е.А. Юшиной. – Киров: Изд-во ВятГГУ, 2009. С. 458-461. (0,23 п.л.)
7. Родина Ю.В. Использование нечеткой логики при анализе рисков информационной безопасности [текст]/ Ю.В. Родина // Инновационный путь развития РФ как важнейшее условие преодоления мирового финансового кризиса: Материалы международной научно-практической конференции 21-22 апреля 2009 г. Заседания секций. Том 1. – М.: ВЗФЭИ, 2009. С. 371-372. (0,15 п.л.)

8. Родина Ю.В. Расчет параметров функций принадлежности [текст]/ Ю.В. Родина // Математические методы и информационные технологии в экономике, социологии и образовании: сборник статей XXII Международной научно-технической конференции. – Пенза: Приволжский Дом знаний, 2009. С. 85-87. (0,125 п.л.)
9. Родина Ю.В. Некоторые особенности построения моделей с использованием нечетной логики [текст]/ Ю.В. Родина // Аналитические и численные методы моделирования естественнонаучных и социальных проблем. Сборник статей IV Международной научно-технической конференции. - Пенза: Приволжский Дом знаний, 2009. С. 195-197. (0,16 п.л.)
10. Родина Ю.В. Безопасность банковских карт [текст]/ Ю.В. Родина // Проблемы информатики в образовании, управлении, экономике и технике: сборник статей по материалам IX Международной научно-технической конференции. – Пенза: Приволжский дом знаний, 2009. с. 141-144. (0,2 п.л.)
11. Родина Ю.В. Оценка рисков информационной безопасности [текст]/ Ю.В. Родина // Математические методы и информационные технологии в экономике, социологии и образовании: сборник статей XXIV Международной научно-технической конференции. - Пенза: Приволжский дом знаний, 2009. С. 290-292. (0,14 п.л.)
12. Родина Ю.В. Повышение осведомленности персонала в области информационной безопасности [текст]/ Ю.В. Родина // Резервы экономического роста предприятий и организаций: сборник статей V Всероссийской научно-практической конференции. – Пенза: Приволжский дом знаний, 2010. С.47-49. (0,14 п.л.)
13. Родина Ю.В. Рекомендации банка России в области оценки рисков информационной безопасности[текст]/ Ю.В. Родина // Экономика, наука, образование: проблемы и пути интеграции: сборник статей Международной научно-практической конференции, посвященная 80-летнему юбилею ВЗФЭИ, 26-27 октября 2010 г. Заседание секций. Т.1секции 1-8. - М.: ВЗФЭИ, 2011. С. 217-218. (0,15 п.л.)
14. Родина Ю.В. Особенности реализации оценки рисков информационной безопасности на основе нечеткой логики[текст]/ Ю.В. Родина // Россия в XXI веке: итоги, вызовы, перспективы. Материалы международной научно-практической конференции. – М.: НОУ «Институт экономики и предпринимательства»; Тюмень: ООО «Ист Консалтинг», 2011. С. 157-162. (0,4 п.л.)
15. Родина Ю.В. Использование электронных подписей [текст]/ Ю.В. Родина // Управление в XXI веке, Сборник статей V-й международной научно-практической конференции, 6 мая 2011 г., г. Киров / под ред. Е. А. Юшиной. – Киров: Изд-во ВятГГУ, 2011. С. 187-190. (0,2 п.л.)

16. Родина Ю.В. Определение исходной поверхности нечеткой модели оценки рисков информационной безопасности [текст]/ Ю.В. Родина // Математические методы и информационные технологии в экономике, социологии и образовании: Сборник статей XXVIII Международной научно-технической конференции. – Пенза: Приволжский дом знаний, 2011. С. 146-149. (0,2 п.л.)
17. Родина Ю.В. Риски информационной безопасности и операционные риски банка [текст]/ Ю.В. Родина // Информационные ресурсы и системы в экономике, науке и образовании: сборник статей II Международной научно-практической конференции. – Пенза: Приволжский Дом знаний, 2012. С. 113-116. (0,2 п.л.).