На правах рукописи

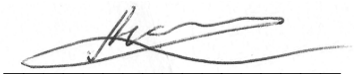
**Атаманов Александр Николаевич**

# ДИНАМИЧЕСКАЯ ИТЕРАТИВНАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Специальность: 05.13.19 − методы и системы защиты информации, информационная безопасность

**АВТОРЕФЕРАТ**

диссертации на соискание ученой степени
кандидата технических наук

Автор: 

Москва − 2012

Работа выполнена на кафедре «Криптология и дискретная математика» Национального исследовательского ядерного университетета «МИФИ» (НИЯУ МИФИ)

**Научный руководитель:** доктор физико-математических наук, доцент Фомичев Владимир Михайлович профессор кафедры «Криптология и дискретная математика» НИЯУ МИФИ

**Официальные оппоненты:** доктор технических наук, профессор Царегородцев Анатолий Валерьевич заведующий кафедры «Комплексная защита объектов информатизации» Всероссийской Государственной налоговой академии Минфина России

кандидат технических наук, доцент Толстой Александр Иванович первый заместитель заведующего кафедры «Информационная безопасность банковских систем» НИЯУ МИФИ

**Ведущая организация:** Федеральное автономное учреждение «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю»

Защита состоится «29» марта 2012 г. в 15 часов 00 минут на заседании диссертационного совета ДМ 212.130.08 при Национальном исследовательском ядерном университете «МИФИ»: 115409, г. Москва, Каширское ш., д. 31. Тел. для справок: +7 (499) 323-95-26.

С диссертацией можно ознакомиться в библиотеке Национального исследовательского ядерного университета «МИФИ».

Отзывы в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, г. Москва, Каширское ш., д. 31, диссертационные советы НИЯУ МИФИ, тел.: +7 (499) 323-95-26.

Автореферат разослан «27» февраля 2012 г.

Ученый секретарь
диссертационного совета  к.т.н., доцент Горбатов В. С.

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** В условиях увеличивающейся сложности информационных систем вопросы обеспечения информационной безопасности приобретают все большее значение для государства и бизнеса. Особое внимание начинает уделяться анализу и оценке рисков информационной безопасности как необходимым составляющим комплексного подхода к обеспечению информационной безопасности.

Автоматизированная система – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. Учитывая разнообразие современных средств автоматизации, особый интерес представляют вопросы анализа рисков в гетерогенных (разнородных) автоматизированных системах.

В соответствии с современным представлением анализ и оценка рисков информационной безопасности выполняются в ходе аудита информационной безопасности автоматизированной системы или на этапе ее проектирования. Основной задачей аудита информационной безопасности является оценка внутренних механизмов контроля информационных технологий и их эффективности, а также архитектуры информационной системы в целом. Аудит информационной безопасности включает в себя многие задачи, в том числе оценку эффективности системы обработки информации, оценку безопасности используемых протоколов и технологий, процесса разработки и управления автоматизированной системой. Стратегической целью аудита информационной безопасности является обеспечение доступности информации в информационной системе, целостности информации и, при необходимости, конфиденциальности информации. Детализация этой цели при аудите конкретных информационных систем приводит к необходимости получения ответов на ряд важных вопросов:

– Доступна ли информация в системе в каждый момент осуществления бизнес процессов?

– Обеспечено ли разграничение доступа к информации в соответствии с установленными полномочиями пользователей?

– Обеспечена ли точность, достоверность и своевременность информации в системе?

Ответы на эти и ряд других важных вопросов при аудите информационной безопасности могут быть получены как результат работы по оценке параметров качества комплексной системы обеспечения информационной безопасности, то есть анализа и оценки рисков информационной безопасности.

Оценка рисков информационной безопасности является неотъемлемой частью аудита информационной безопасности. Это требование зафиксировано в ряде международных и национальных руководящих документов и стандартов, в том числе:

– в Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных» и выпущенных для обеспечения выполнени требований закона

руководящих и методических документах ФСБ России и ФСТЭК России;

- в стандарте СТО БР ИБСС ЦБ РФ;
- в стандарте ГОСТ Р ИСО/МЭК 17799 (ISO/IEC 17799);
- в стандарте ГОСТ Р ИСО/МЭК 27001-2006 (ISO/IEC 27001);
- в стандарте NIST 800-30 (США) и др.

Исследования в области анализа рисков информационной безопасности проводились российскими и зарубежными учеными, среди которых можно выделить Г.А. Остапенко, Д.А. Котенко, И.Л. Алферова, А.Г. Кащенко, М.В. Тимонина, Я.Н. Алгулиева, А.Н. Назарова, Д.О. Карпеева, А.О. Сидорова, А.Г. Лысенко, А.В. Львова, Г.А. Кустова, T.R. Peltier, C. Kairab, C. Alberts, G. Brændeland, A. Papoulis, N.E. Fenton, M. Neil, M. Tailor, F.V. Jensen, и др. Анализ опубликованных работ и существующих подходов показывает, что открытыми остаются ряд вопросов, связанных с автоматизацией процесса получения количественной оценки риска в реальном времени, вопросы оценки вероятности реализации угроз в условиях недостатка статистических данных, вопросы использования противоречивых данных. Кроме того, существующие методики плохо адаптируются к изменениям, вносимым в автоматизированные системы, так как в случае таких изменений требуется повторение всех этапов процедуры аудита системы.

Аудит информационной безопасности, включающий в себя комплексную оценку угроз и рисков, предполагает помимо формальных и объективных проверок многочисленных параметров информационной системы также вынесение обоснованного обобщающего заключения аудитора или группы аудиторов относительно эффективности системы защиты информации и возможных угроз.

В ходе проведения оценки рисков информационной безопасности при построении комплексной системы защиты информации на объекте информатизации возникает задача агрегации экспертных оценок и имеющихся количественных данных. Оценка рисков усложняется также необходимостью учитывать ряд факторов: постоянное появление новых угроз информационной безопасности, ускорение темпов внедрения новых технологий автоматизации деятельности предприятия, возможную потерю актуальности данных, полученных в ходе анализа рисков.

При проведении оценки рисков информационной безопасности между началом исследования системы и выпуском итогового отчета проходит существенный период времени. Это значительно уменьшает ценность некоторых данных и может приводить к снижению уровня решения задач информационной безопасности по обеспечению конфиденциальности, целостности или доступности информации.

Схожие проблемы возникают и при решении других задач аудита информационных технологий. В связи с этим в последние годы активно разрабатывается концепция непрерывного аудита. Непрерывный аудит определяется как среда, позволяющая внутреннему или внешнему аудитору выносить суждения по значимым вопросам, основываясь на серии созданных одновременно или с небольшим промежутком отчетов. Возможность

отслеживать снижение эффективности системы защиты в реальном (или максимально близком к реальному) времени дает возможность заметно повысить уровень решения задач информационной безопасности и позволяет оперативно реагировать на появление новых угроз информационной безопасности.

Оценка параметров информационной системы в ходе непрерывного аудита потребовала адаптации и развития математических методов, в частности, методов многокритериальной оптимизации, применения теории нечетких множеств, аппарата нейорнных сетей, методов количественной оценки рисков и др. Вместе с тем возникает и целый ряд новых задач, в том числе задачи обеспечения адаптации системы анализа и управления рисками информационной безопасности к конкретной автоматизированной системе и новым условиям функционирования этой системы, задачи автоматизации деятельности аудитора, прогнозирования рисков и др.

Таким образом, являются актуальными задачи получения оценок параметров безопасности информационной системы и управления рисками информационной безопасности в автоматизированной системе, с учетом следующих возможностей:

– агрегация разнородных данных;
– обучение в процессе работы и уточнение оценок, полученных на предыдущих этапах анализа;
– использование неточных данных;
– автоматизация большинства процессов принятия решений;
– прогнозирование рисков.

В диссертационной работе решается задача синтеза системы динамического итеративной оценки рисков информационной безопасности, учитывающей указанные выше требования.

**Научными задачами**, решаемыми в работе являются синтез методики, позволяющей находить разбиение значений наблюдаемых параметров автоматизированной системы (входных данных) на классы риска, и оценка апостериорной вероятности реализации угроз информационной безопасности на основании данных наблюдений с учетом выполненного разбиения в условиях функционирования, типичных для современных автоматизированных систем.

**Объектом исследования диссертационной работы** являются гетерогенные автоматизированные системы.

**Предметом исследования диссертационной работы** являются математические модели и методы оценки рисков информационной безопасности в автоматизированных системах.

**Целью диссертационной работы** является совершенствование методики аудита информационной безопасности, направленное на повышение уровня защищенности автоматизированной системы за счет динамической итеративной оценки рисков информационной безопасности.

Для достижения поставленной цели в диссертационной работе решаются **проводятся исследования по следующим направлениям**:

– анализ существующих методов и математических моделей оценки рисков информационной безопасности;

– разработка методики динамической итеративной оценки рисков информационной безопасности в автоматизированной системе;

– разработка математической модели аудита информационной безопасности, используемой для итеративного получения динамической количественной оценки рисков информационной безопасности;

– разработка архитектуры системы динамической итеративной оценки рисков информационной безопасности;

– применение полученных результатов для аудита информационной безопасности конкретных информационных систем на основе внедрения системы динамической итеративной оценки рисков информационной безопасности.

Основными **методами исследований**, используемыми в работе, являются методы математической статистики, структурного и функционального анализа и теории нейронных сетей.

**Научная новизна** работы характеризуется следующими результатами:

– предложен новый подход к проведению автоматизированной итеративной динамической оценки рисков информационной безопасности, отличающийся от существующих возможностями агрегации разнородных данных, обучения в процессе работы и уточнения оценок, полученных на предыдущих этапах анализа, а так же допускающий использование искаженных данных;

– представлена и исследована математическая модель системы оценки рисков информационной безопасности на основе байесовского подхода, применимая для решения задачи итеративной динамической оценки рисков информационной безопасности для широкого класса систем;

– разработаны алгоритмы и оценена вычислительная сложность применения нейронных сетей для решения задачи динамического итеративного анализа рисков информационной безопасности, применимые для реализации подхода динамической итеративной количественной оценки рисков при заданных условиях.

**Практическая значимость** результатов определяется следующим:

– синтезирована система анализа и управления рисками на основе нейронных сетей, обладающая заданными свойствами;

– разработан обучаемый программный комплекс, предназначенный для динамической итеративной оценки рисков информационной безопасности в гетерогенной автоматизированной системе, позволяющий существенно упростить процедуру анализа рисков и повысить точность получаемых оценок за счет использования непрерывности оценки;

– даны практические рекомендации по применению разработанной системы, а также ее программной и аппаратной реализации при создании и поддержке комплексной системы защиты информации на объекте информатизации.

Результаты работы представляют практическую ценность для

обеспечения безопасности информации, обрабатываемой в автоматизированных системах. Результаты дают возможность динамической итеративной оценки рисков , связанных с информационными технологиями, централизованного управления информационной безопасностью и применением политик информационной безопасности.

**Внедрение результатов исследований.** Комплекс внедрен в ряде государственных органов и коммерческих структур. Среди них:

– ОАО «БИТК»;
– ЗАО «Техносерв А/С»;
– ЗАО «ОНЛАНТА»;

**Публикации и апробация работы.** По теме диссертации опубликовано 8 печатных работ (из них 4 статьи в журналах перечня ВАК). Результаты диссертации докладывались на конференциях и семинарах различного уровня:

– Российская научная конференция «Методы и средства обеспечения информационной безопасности», Санкт-Петербург, 2008 г.;
– Научная сессия МИФИ-2008. XIV Всероссийская научная конференция. Проблемы информационной безопасности в системе высшей школы: «Перспективы развития современных систем обнаружения вторжений и предотвращения атак», 2008 г.;
– Межрегиональный семинар «Обеспечение информационной безопасности информационных систем органов исполнительной власти субъектов Российской Федерации», 2010 г;
– XVI всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы», 2009 г.

**Основные положения, выносимые на защиту:**

– методика итеративной динамической оценки рисков информационной безопасности на основе байесовского подхода с помощью нейронных сетей, позволяющая использовать разнородные искаженные данные и основанная на обучении в процессе автоматизированной работы;
– математическая модель системы оценки рисков информационной безопасности, позволяющая непосредственно получать оценки апостериорной вероятности реализации угроз на основе имеющихся наблюдений без необходимости оценки условных вероятностей наблюдаемых значений при реализации угроз;
– технология построения системы динамической итеративной оценки рисков информационной безопасности в гетерогенной автоматизированной системе, позволяющей существенно уменьшить время, необходимое для проведения оценки и обеспечить автоматизированную работу.

**Структура работы**. Работа состоит из введения, четырех глав, заключения, списка литературы, включающего 93 наименования, и 2 приложений. Текст диссертации изложен на 130 страницах, включая 16 рисунков и 11 таблиц.

## СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, выделяются и формулируются цели и задачи исследования, описывается структурно-логическая схема диссертационной работы.

В **первой главе** рассматривается понятие риска информационной безопасности и проводится анализ существующих моделей и методов оценки рисков информационной безопасности, в том числе анализируются их существенные недостатки. Дается оценка применимости различных моделей и методов для решения прикладных задач. Исследуются методы и пути решения поставленной научной задачи.

В главе рассмотрены требования различных нормативных, методических и нормативно-методических документов, в области защиты информации, определяющие процедуру анализа и управления рисками информационной безопасности. Проанализированы Российские требования, стандарты и руководящие документы, стандарты серии ISO/IEC 27000, ISO/IEC 17799, NIST 800-30, SOGP, COBIT, ISM3. Проанализированы средства автоматизации процессов, связанных с анализом рисков.

В результате показано, что тема анализа рисков информационной безопасности, как составной части комплексного подхода к обеспечению информационной безопасности, достаточно широко освещена в целом ряде нормативных и методических документов, а также международных стандартов. При этом основное внимание уделяется организационным вопросам проведения процедуры. Применение результатов описанных процедур затруднительно в задачах управления деятельностью предприятия, так как они имеют качественный характер и не позволяют оценить реальные ожидаемые потери организации в результате инцидентов, связанных с информационной безопасность. Для уточнения полученных в результате процедуры оценок предлагается повторять всю процедуру анализа рисков.

Некоторые отдельные методологии, используемые в практике работы аудиторов и специалистов по безопасности, а также инструментальные средства позволяют проводить количественную оценку рисков. Создан целый ряд программных комплексов, позволяющий автоматизировать отдельные этапы работы специалиста. Однако данные средства не имеют возможностей автоматизации деятельности аудитора при анализе технических рисков, не обладают возможностями к обучению системы при повторном выполнении операций. Результаты их работы плохо подходят для повторного использования в целях обеспечения непрерывного аудита информационной безопасности, так как требуется повторное выполнение всего набора операций, включая организационную составляющую.

Как следствие большого количества стандартов и подходов к анализу рисков информационной безопасности, основные понятия в этой области имеют множество определений. Наиболее подходящим для большинства практических применений определением риска информационной безопасности является приведенное в стандарте ISO 27005. Согласно ему:

«Риск информационной безопасности – это потенциальная возможность использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации».

Проведенный анализ методологий анализа рисков показывает, что во всех из них используется не математическая вероятность наступления события «реализация угрозы», а примерная частота реализации угрозы за заданный промежуток времени. Для оценки вероятностей используют экспертную оценку. В некоторых методологиях и программных средствах поддержки анализа рисков используются статистики по техническим угрозам, и предлагается использовать их для оценки риска в исследуемой организации.

При проведении анализа рисков информационной безопасности в соответствии с описанным подходом не предполагается оценка точности экспертных оценок, не предусматривается возможность уточнения оценок по результатам эксплуатации системы. Кроме того, между началом исследования системы и выпуском итогового отчета как правило проходит существенный период времени. Это значительно уменьшает ценность некоторых данных анализа и может приводить к снижению уровня решения задач информационной безопасности по обеспечению её конфиденциальности, целостности или доступности.

Концепция непрерывного аудита определяет подход к решению этих и других проблем. Совместно с современными моделями управления информационными системами, системами менеджмента информационной безопасности, учета инцидентов информационной безопасности, мониторинга и анализа защищенности, данные методологии позволяют наиболее быстро и эффективно строить и развивать систему защиты информации организации. Система непрерывного динамического аудита и анализа рисков позволяет специалистам проводить итеративную оценку рисков с учетом имеющихся данных по бизнес-ландшафту, актуальной информации по используемым или предполагаемым к внедрению технологиям, имеющимся или возможным уязвимостям и их вероятностям.

Особую роль в непрерывном анализе рисков при этом должна занимать функция прогнозирования рисков, в том числе рисков, связанных с планируемыми к внедрению технологиями и функция уточнения рисков на основе вновь полученных данных. При помощи автоматизации процесса учета угроз, связанных с появлением новых уязвимостей в типовом ПО, инцидентов информационной безопасности, формализации изменений в бизнес-ландшафте и информационной системе, агрегации данных из различных источников можно создать среду, позволяющую специалисту создавать отчеты о состоянии защищенности той или иной информационной системы, основываясь на серии последовательных отчетов, составленных за короткий промежуток времени. Обработка этих данных с использованием методов прогнозирования позволит определить оптимальный набор контрмер с учетом «будущих рисков» и тем самым повысить эффективность внедрения превентивных контрмер и существенно снизить время реакции системы на появление новых уязвимостей.

Во **второй главе** формулируется подход к динамической итеративной оценке рисков информационной безопасности в автоматизированной системе, лишенный указанных выше недостатков.

Из используемых в большинстве стандартов и методологий определений следует, что риск R можно задать следующим выражением:

$$R = P \cdot S,$$

где P – вероятность реализации угрозы, а S – величина последствий. Вероятность реализации угрозы в свою очередь является произведением вероятности реализации уязвимости на вероятность эксплуатации данной уязвимости. Оценка вероятности случайного события – реализации угрозы может рассматриваться как случайная величина. Сложность получения математической вероятности реализации угроз с точки зрения классического определения вероятности приводит к тому, что вероятность P для задач анализа рисков принято оценивать экспертным путем или исходя из статистик по частоте реализации данного класса угроз для данного типа автоматизированных систем на заданном временном интервале.

В рассмотренных в ходе анализа методологиях отсустсвуют прямые указания на используемые методы анализа статистических данных. В некоторых методологиях и работах предлагаются возможные методы учета экспертных оценок.

Аналогичные анализу рисков информационной безопасности задачи возникают в различных областях, среди которых можно выделить анализ рисков в области финансов и управления проектами. Основные математические методы, используемые в данных областях, относятся к традиционной школе статистического вывода и описаны в работах Ньюмена, Пирсона, Фишера и др. В ряде работ предлагаются альтернативные методы анализа. Среди них стоит выделить методы на основе Байесовского подхода.

Как было сказано выше, в задаче анализа рисков априорная вероятностная информация о реализации угроз может быть изменена после получения новых экспертных оценок или в результате наблюдения соответствующих событий, связанных с состояниями и подтверждающих или опровергающих априорную информацию. Многие статистические задачи независимо от методов их решения обладают общим свойством: до того как получен конкретный набор данных, в качестве потенциально приемлемых для изучаемой ситуации должны рассматриваться несколько вероятностых моделей. После того, как получены данные, возникает выраженное в некотором виде знание об относительной приемлимости этих моделей. Одним из способов «пересмотра» относительной приемлимости вероятностных моделей является байесовский подход, основой которого выступает теорема Байеса.

Суть байесовского подхода состоит в том, что рассматриваются степени доверия к возможным вероятностным моделям до получения данных. Степени доверия представляются в виде вероятностей. После получения информации с помощью теоремы Байеса рассчитывается новые значения вероятностей,

отражающие степень доверия к вероятностным моделям на основе вновь полученных данных.

В случае анализа рисков информационной безопасности возможно наблюдать параметры системы информационной безопасности, каждый из которых можно рассматривать как случайную величину Y с плотностью вероятности $P(y|\theta)$ с параметрами $\theta$. На основании этих наблюдений необходимо сделать вывод о случайной величине $\theta$, имеющей распределение вероятности $\pi(\theta)$. Тогда, согласно формуле Байеса:

$$P(\theta|y) = \frac{P(y|\theta) * P(\theta)}{P(y)}.$$

В качестве альтернативы байесовскому подходу можно рассмотреть метод максимума функции правдоподобия, используемый в статистическом оценивании параметров распределения. Байесовский подход для решения поставленных задач при этом имеет преимущества, так как многие свойства оценок, полученных с применением отношения правдоподобия, не выполняются в случае маленького размера выборки.

Применение байесовского подхода помогает также решить вопрос о математических методах оценивания априорных значений, которые могут принимать параметры риска информационной безопасности. Важной особенностью является то, что при наличии большого объема статистических данных ошибочно выбранное априорное распределение вероятностей не повлияет существенно на апостериорное. Однако, что особенно актуально для решения задач анализа рисков информационной безопасности, в условиях отсутствия таких данных целесообразно выбирать распределение, минимально влияющее на апостериорное распределение (т.н. неинформативное распределение).

В работе рассмотрена следующая модель нарушителя информационной безопасности. В случае реализации угрозы безопасности сети злоумышленник разрабатывает сценарий атаки, использующий одну уязвимость. При этом нарушение безопасности происходит путем эксплуатации наибольшей уязвимости. В случае если несколько уязвимостей равноценны, из них выбирается одна произвольная.

Рассмотрим следующую байесовскую сеть. Ее интерпретация в терминах анализа рисков может быть следующей. Обозначим возможную угрозу информационной безопасности системы как T, а вероятность успешной реализации угрозы – $p(T)$, имеющиеся уязвимости – $U_1, \dots, U_n$, и вероятности успешной эксплуатации уязвимостей – $p(U_1), \dots, p(U_n)$ соответственно. Условную величину «потенциал атаки» обозначим через A. Переменная $A \in [0,1]$ и является случайной величиной с распределением $f(A)$.

Величины $u_1, \dots, u_n \in [0,1]$. Будем говорить, что угроза $U_i$ не реализуется, если $A \leq p(U_i)$, и реализуется, если $A > p(U_i)$. Для простоты записи будем обозначать как $U_i$ факт эксплуатации уязвимости, а $\neg U_i$ – отсутствие факта эксплуатации уязвимости. В рамках анализа рисков важно рассмотреть вероятность реализации угроз через эксплуатацию

соответствующих уязвимостей. Ребра графа, изображенного на рисунке 1, представляют собой условную зависимость событий.

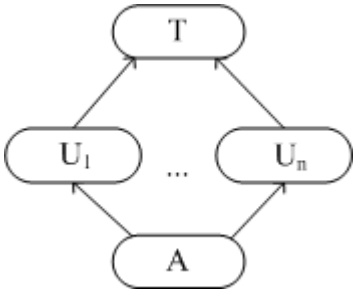



Рисунок 1 – Байесовская сеть реализации угроз информационной безопасности

Вероятность на общем пространстве в условиях модели независимых угроз определяется выражением:

$$P(T,(U_1,\dots,U_n),A) = P(T\,|(U_1,\dots,U_n))P(A)\prod_{i=1}^{n} P(U_i \mid A).$$

Выполняя маргинализацию до $P(T)$ получаем:

$$P(T) = \int P\big(A|(U_1,\dots,U_n)\big)\,x$$

$$x[\int \prod_{i=1}^{n} P(U_i \mid A)\, f(A)dA)]d(U_1,\dots,U_n).$$

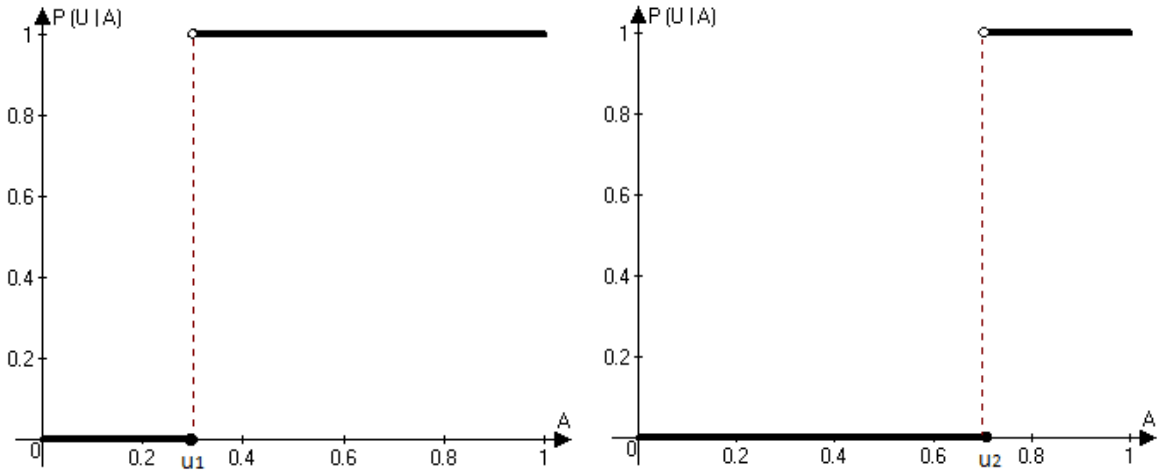
Из дихотомического характера переменных и условий

$$A \le p(U_i) \Rightarrow p(U_i) = 0 \text{ и } A > p(U_i)\text{я} \Rightarrow p(U_i) = 1$$

следует, что

$$P(U_i|A) = 0 \text{ если } A \le p(U_i) \text{ и } P(U_i|A) = 1 \text{ если } A > p(U_i).$$

Данный вывод можно изобразить графически для некоторых значений $p(U_j)$ и $p(U_k)$ следующим образом.



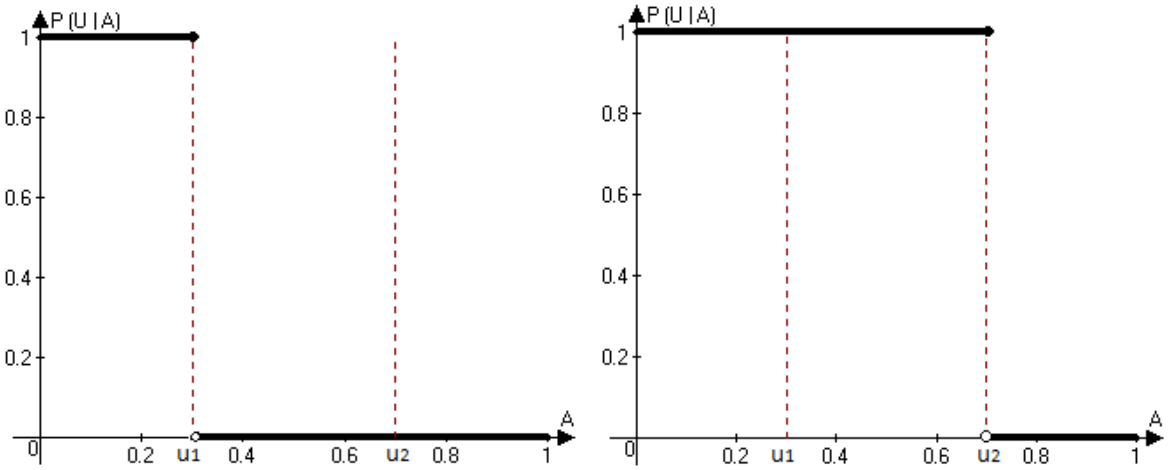



Рисунок 2 – Значение $p(U_j)$ и $p(U_k)$ при условии A

В соответствии с данным подходом получаем:

$$\int \prod_{i=1}^{n} P(U_i \mid A)\, f(A) dA = \min(1 - U_1, \ldots, 1 - U_n),$$

$$\int P\left(\neg U_j \middle| A\right) \prod_{i \neq j} P(U_i \mid A)\, f(A) dA = \max\left(0, U_j - \sum_{i \neq j} U_i\right).$$

В общем случае данные выводы сложно применить на практике. В большинстве задач получить апостериорные вероятности p(θ|y) затруднительно.

Анализ рисков информационной безопасности на основе имеющихся данных непрерывного аудита можно рассмотреть как задачу классификации входных данных. При этом классы могут быть заданы, например, как «опасная активность», ведущая к реализации угроз, и «неопасная активность».

В ряде работ показано, что искусственные нейронные сети могут быть использованы для решения данной задачи. Наиболее часто встречающийся подход заключается в обучении нейронной сети таким образом, чтобы она реализовывала нелинейную функцию дискриминации, обеспечивающую прямое разделение входных векторов на классы. Более общий и перспективный подход заключается в обучении нейронной сети таким образом, чтобы выходными значениеми системы являлись апостериорные вероятности принадлежности входных данных заданным классам. Также показано, что можно построить нейронную сеть, которая после своего обучения позволит непосредственно получать оценки условной вероятности p(y|θ). Можно определить также способы обучения таких сетей и способы оценки получаемых результатов. Данный вывод является очень важным для задач анализа рисков информационной безопасности и может быть весьма полезен для решения задачи итеративной динамической оценки рисков информационной безопасности.

Применение искусственных нейронных сетей для решения поставленной задачи позволяет также обеспечить ряд важных свойств

системы, в том числе возможность обучения системы в процессе функционирования и адаптацию к различным условиям функционирования. При их применении не возникает необходимости в предварительном детальном моделировании автоматизированной системы.

В **третьей главе** подробно описана архитектура системы итеративной динамической оценки рисков с применением байесовского подхода на основе нейронных сетей, обосновывается выбор структуры сети, типов нейронов и алгоритмов обучения.

В работе предложено определение понятия непрерывного аудита как среды, позволяющей специалисту оценивать риски информационной безопасности основываясь на созданных одновременно или с небольшим промежутком отчетов о функционировании автоматизированной систем, средств защиты информации и инцидентов информационной безопасности, связанных с реализацией угроз.

Для реализации непрерывной оценки рисков необходимо создать систему динамического итеративного анализа рисков информационной безопасности. В работе предложена архитектура такой системы. На рисунке 3 изображена диаграмма потоков данных системы.

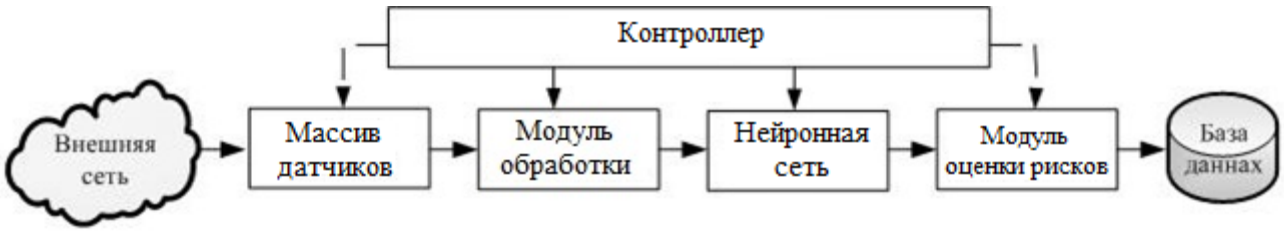



Рисунок 3 – Схема потоков данных

Входом системы являются данные датчиков (например, системы обнаружения вторжений, антивирусных программ, межсетевых экранов) о потенциально опасной активности, общем уровне сетевой активности, нагрузке на тот или иной участок автоматизированной системы, и т.д., а также экспертные оценки количественных показателей функционирования системы информационной безопасности. Эти данные преобразуются в канонический вид – для этого выполняется их нормализация и выравнивание.

В качестве архитектуры программного комплекса была выбрана классическая клиент-серверная архитектура. При этом, учитывая специфику задачи, был применен агентский подход к сбору данных.

Агенты безопасности устанавливаются на все СВТ или ключевые точки обмена информацией. Основной функционал агентов безопасности, применяемый для решения рассматриваемой задачи, заключается в сборе и передаче необходимых данных серверам управления безопасностью. В целях обеспечения масштабируемости архитектуры, сервера безопасности должны предусматривать возможность создания иерархии. При этом вся иерархия серверов безопасности реализует функционал модуля оценки рисков и функции нейронной сети. Распределенная архитектура позволяет одной

нейронной сети в случае необходимости физически реализовываться несколькими серверами безопасности.

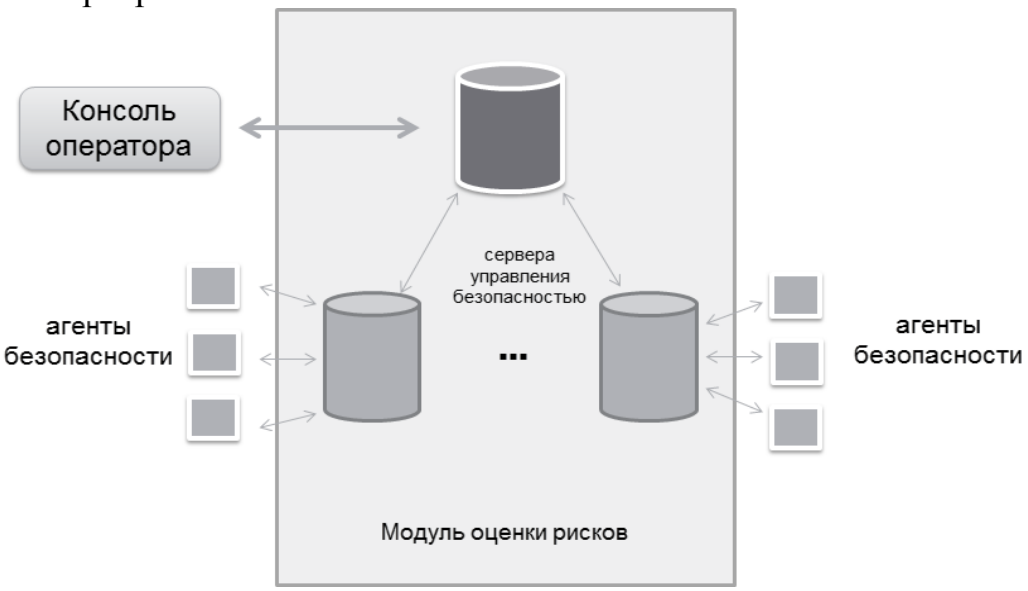



Рисунок 4 – Схема взаимодействия модулей комплекса

Модуль нейронной сети при этом функционирует в составе распределенного модуля оценки рисков и, по сути, решает задачу классификации входных векторов. В работе рассмотрены различные архитектуры нейронных сетей, применимые в качестве ядра системы динамической итеративной оценки рисков информационной безопасности, и оценена возможность их применения для решения поставленных задач. В частности, рассмотрены сети с алгоритмами обучения с учителем и без, в том числе многослойные персепртроны с прямым распространением сигнала, сети встречного распространения на основе нейронов Кохонена и Гроссберга, самоорганизующиеся сети Кохонена, сети с обратной связью Хопфилда и Хэмминга, сети динамической ассоциативной памяти, сети и алгоритмы на основе адаптивной резонансной теории, когнитроны и неокогнитроны. Показано, что большинство типов искусственных нейронных сетей может быть использовано для задачи количественной оценки рисков информационной безопасности.

В качестве ядра системы в данной работе используются сети с обучением с учителем на основе многослойного персептрона с прямым распространением сигнала. В работе рассмотрены также возможности применения других, более современных архитектур сети.

Как было сказано выше, возможно построить нейронную сеть для решения задачи классификации входных n-мерных векторов на два класса – «опасная активность» и «неопасная активность». Данная классификация может быть проведена отдельно для каждой угрозы. Таким образом, для решения задач анализа рисков информационной безопасности при идентификации N актуальных рисков можно построить N трехслойных нейронных сети с прямым распространением сигналов, которые обеспечат в результате обучения оценку апостериорной вероятности реализации угрозы.

При этом данные m представляют собой отчеты о каком-либо параметре функционирования системы за фиксированный промежуток времени.

Важным вопросом является обучение нейронных сетей. Применение изложенного подхода позволяет использовать несколько важных свойств. Во-первых, на качество оценки вероятности с помощью нейронных сетей существенное влияние оказывает выбор данных для обучения. Для обеспечения корректной реакции системы возможно искусственно изменить пропорции событий, которые могут привести к реализации угроз информационной безопасности. При этом получаемое апостериорное распределение вероятности будет смещено в сторону увеличения вероятности реализации угроз на основе реальных данных. Однако для коррекции результирующего распределения можно использовать априорные оценки вероятности появления событий. Для получения результирующих оценок апостериорных вероятностей достаточно умножить результат оценки на отношение априорных вероятностей. Сеть при этом оказывается корректно обученной, а при изменении априорных вероятностей отсутствует необходимость в переобучении.

Можно также рассматривать сети с двумя выходами, каждый из которых будет отвечать за оценку вероятности принадлежности входных данных заданному классу. Альтернативный подход, используемый в работе, состоит в наличии одного выхода. Тогда для двух классов $C_1$ и $C_2$ и данных $m$ вероятность $p(C_2|m)$ вычисляется на основе выхода $p(C_1|m)$ как

$$p(C_2 \mid m) = 1 - p(C_1 \mid m).$$

Можно показать, что в случае гладкой функции с добавленным Гаусовским шумом нейронная сеть со схемой кодирования «1 из с», обученная минимизировать среднеквадратическое отклонение, будет апроксимировать апостериорную вероятность. Однако для решения задач классификации в целях оценки рисков информационной безопасности более актуальным является анализ решения задачи кодирования «1 из 2» с распределения Бернули. В этом случае для активации нейрона необходимо применить сигмоидальную функцию активации вида

$$g(a) = \frac{1}{1+e^{-a}}.$$

Тогда, учитывая что все значения вероятностей по определению лежат в диапазоне [0,1] функция ошибки обучения зависит от данных обучения, и имеет вид:

$$\gamma = -\sum\sum_{k=1}^{c}\left\{d_n^k \ln\left(\frac{y_k^n}{d_k^n}\right) + (1-d_n^k)\ln\left(\frac{1-y_k^n}{1-d_k^n}\right)\right\},$$

где $y_k^n$ – соответсвтующие выходные значения, а $d_k^n$ – целевые значения обучения.

Для обучения такого многослойного персептрона может применяться известный метод обратного распространения ошибки. Данный метод обучения

многослойного перцептрона впервые был описан в 1974 г. А.И. Галушкиным, а также независимо и одновременно П. Дж. Вербосом. Далее существенно развит в 1986 г. Д. И. Румельхартом, Дж. Е. Хинтоном и Р. Дж. Вильямсом и, независимо и одновременно, С. И. Барцевым и В. А. Охониным (Красноярская группа). Это итеративный градиентный алгоритм, который используется с целью минимизации ошибки работы многослойного персептрона и получения желаемого выхода.

Идея этого метода состоит в распространении сигналов ошибки от выходов сети к её входам, в направлении, обратном прямому распространению сигналов в обычном режиме работы. Барцев и Охонин предложили сразу общий метод («принцип двойственности»), применимый к более широкому классу систем, включая системы с запаздыванием, распределенные системы, и т.п. Для данного метода существует доказательство сходимости, однако оно содержит предположение о бесконечно малом шаге подстройки весов нейронов. В реальных условиях метод сходится не всегда и обладает рядом недостатков. П. Д. Вассерман описал адаптивный алгоритм выбора шага, автоматически корректирующий размер шага в процессе обучения. Суть метода состоит в объединении идеи машины Коши с идеей градиентного спуска обратного распространения, что позволяет построить систему, которая находит глобальный минимум, сохраняя высокую скорость обратного распространения. Данный метод был использован в работе для обучения всех сетей прямого распространения сигнала.

В работе показано, что система с предложенной архитектурой может быть использована для оценки апостериорных вероятностей реализации угроз информационной безопасности на основе наблюдения информации от датчиков, одновременно предоставляющих отчеты о функционировании системы за определенный промежуток времени. Для данной системы заданы функции активации нейронов, и описан алгоритм обучения нейронных сетей.

В главе также рассмотрена точность оценки апостериорной вероятности с помощью многослойного персептрона. Получено выражение Q для ошибки оценки:

$$Q = \int_{x\in X} \sum_{i=1}^{m} [F_i^2(x) - (2F_i(x) - 1)P(w_i|x)]f(x)dx =$$

$$= \int_{x\in X} \sum_{i=1}^{m} \left[\left(F_i(x) - P(w_i|x)\right)^2 + P(w_i|x)\left(1 - P(w_i|x)\right)\right] f(x)dx,$$

где F(x) – целевое отображение (апостериорная вероятность), w – вектор принадлежности классам, x – входные вектора, f(x) – функция плотности вероятности.

Можно обозначить:

$$\sigma_A^2 = \int_{x\in X} \sum_{i=1}^{m} P(w_i|x)\left(1 - P(w_i|x)\right)f(x)dx,$$

$$\sigma_\varepsilon^2 = \int_{x \in X} \sum_{i=1}^{m} \left(F_i(x) - P(w_i|x)\right)^2 f(x)dx.$$

Тогда $Q = \sigma_A^2 + \sigma_\varepsilon^2$, $\sigma_A$ – можно интерпретировать как ошибку аппроксимации, а $\sigma_\varepsilon$ - как ошибку оценки.

Определена вычислительная сложность оценки рисков с помощью искусственной нейронной сети с прямым распространением сигналов, обученная по методу обратного распространения ошибки.

Показано, что обучение сети зависит только от объема обучающих векторов и сходимости алгоритма за конечное время. То есть в случае сходимости алгоритма обучения сложность получения оценки и сложность обучения линейно зависят от объема входных данных. Вычислительная сложность T имеет вид

$$T = O(n).$$

В **<u>четвертой главе</u>** рассматриваются вопросы реализации предложенной архитектуры, ее настройки и эксплуатации. Приводятся результаты работы по реализации системы, описываются проведенные эксперименты. Рассмотрены примеры практического применения полученных автором результатов при решении конкретных прикладных задач в трёх проектах.

В соответствии с приведенными выводами, применение нейронных сетей для решения задачи динамической итеративной оценки рисков позволяет обеспечить оценку апостериорной вероятности реализации угроз информационной безопасности.

Для рассмотрения примера была взята нейронная сеть с прямым распространением сигналов и обратным распространением ошибки. При моделировании системы была создана сеть, которая состоит из трех слоев, один из которых скрытый, имеет три входа и один выход. На вход подаются данные датчиков $D = \{d_1, d_2\}$, такие, что $d_i \in \{0,1, \dots ,50\}$. Для обучения сети использовался набор данных, который был получен при помощи рандомизации с заданным распределением вероятности. Была определена одна угроза U. Количество датчиков было определено равным двум для простоты визуализации отображений.

Обозначим:

– $P(U)$ – априорная вероятность реализации угрозы U, полученная с помощью экспертной оценки или на основании статистики по автоматизированной системе с аналогичными характеристиками;

– $P(d_i|U)$ – вероятности наблюдать данные $d_i$ в случае реализации угрозы;

– $P(d_i)$ – вероятности появления данных $d_i$.

Были созданы случайные тестовые, проверочные и контрольные выборки значений величины $d_i$. На основе значений датчиков и оценки выхода нейронной сети Y оценена возможность использования нейронной сети с предложенной архитектурой по оценкам апостериорных вероятностей $P(U|d_i)$. Для этого задаются значения датчиков в таблице 1.

Таблица 1 – Возможные показатели датчиков

| Наименование | Значения | Мощность |
|---|---|---|
| Обнаруженные IDS попытки атак ($d_1$) | 0:1:50 | 51 |
| Сообщения о попытках нарушения правил разграничения доступа ($d_2$) | 0:1:50 | 51 |

Для создания обучающих выборок и тестовых векторов было взято некое случайное отображение $f\{d_1, d_2\} \to p$. Отображение было получено с помощью функции peaks на языке MATLAB со следующими параметрами:

```
Z=rot90((peaks(50)+10)/25).
```

Функция peaks строит некоторое отображение в интервале $[-10; +10]$. Данные были нормализованы с помощью тривиальных преобразований. График, изображенный на рисунке 1, иллюстрирует полученное тестовое отображение.

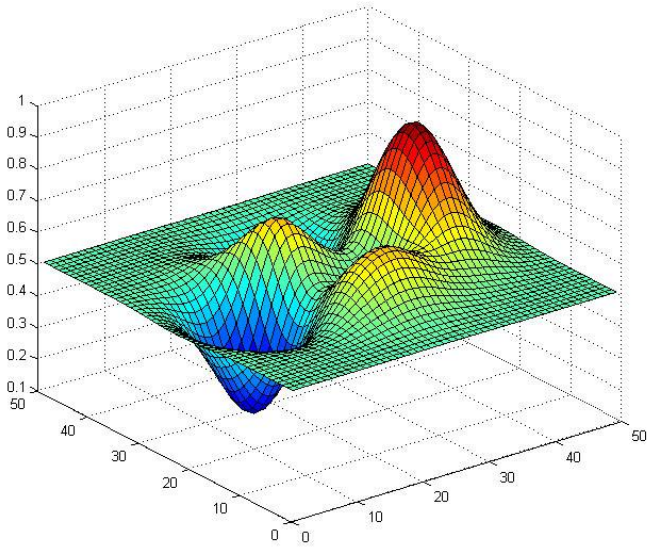



Рисунок 5 − Сетчатый график тестового отображения для двух параметров

Затем, с помощью пакета Neural Network Toolbox for MATLAB была спроектирована простая трехслойная нейронная сеть с прямым распространением сигнала. Множество точек было разбито на выборки в пропорциональном отношении, указанном в таблице 2.

Таблица 2 – Пропорции разбиения множества тестовых точек

| | | |
|---|---|---|
| Обучающая выборка | 60% | 1500 образцов |
| Валидационная выборка | 15% | 375 образцов |
| Тестовая выборка | 25% | 625 образцов |

Результаты оценки качества аппроксимации представлены в таблице 3. Для каждой сети проведено 10 экспериментов. В таблице представлены

средние значения.

Таблица 3 – Результаты обучения сети

| Количество нейронов | Количество итераций | Среднее значение среднеквадратического отклонения на 10 экспериментах |
|---|---|---|
| 1 | 14 | 0,006044 |
| 2 | 25 | 0,005150 |
| 3 | 36 | 0,004508 |
| 4 | 37 | 0,004164 |
| 5 | 59 | 0,003408 |
| 8 | 65 | 0,001737 |
| 11 | 68 | 0,001008 |
| 14 | 168 | 0,000426 |
| 17 | 115 | 0,000257 |
| 20 | 144 | 0,000119 |
| 23 | 186 | 0,000060 |
| 26 | 163 | 0,000055 |
| 29 | 192 | 0,000022 |
| 32 | 131 | 0,000016 |
| 35 | 244 | 0,000008 |

Получены графики сетчатых поверхностей выходных значений нейронных сетей для всех возможных входных значений. Некоторые графики изображены на рисунках 6-7.

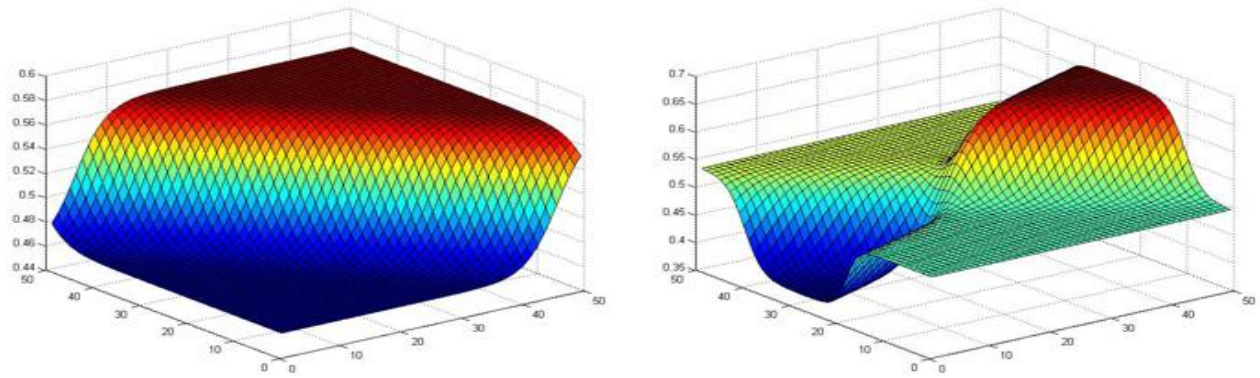


Рисунок 6 – Сетчатые графики поверхностей выходных значений с окраской по высоте для нейронной сети с 1 и 2 нейронами соответственно

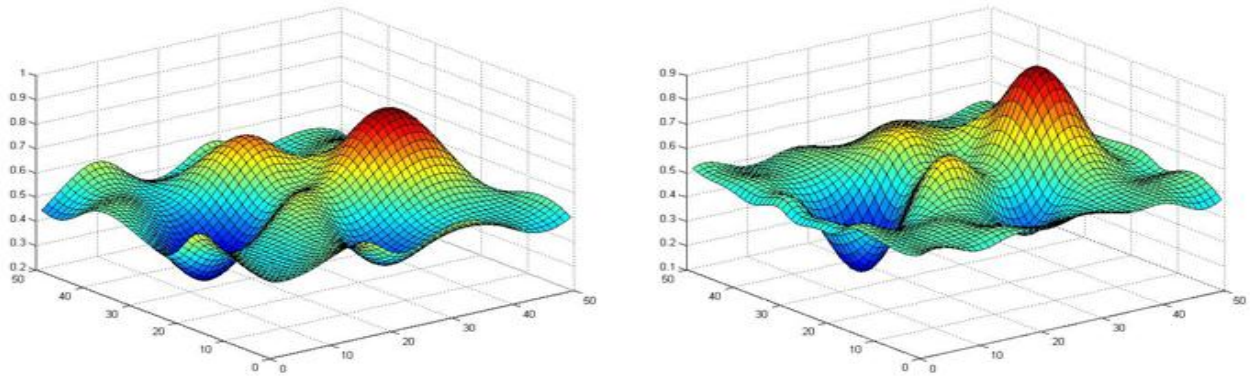


Рисунок 7– Сетчатые графики поверхностей выходных значений с окраской по высоте для нейронной сети с 8 и 17 нейронами соответственно

Из полученных результатов следует, что исходная зависимость может быть достаточно точно аппроксимирована нейронной сетью. Очевидно, что увеличение количества нейронов ведет к увеличению сложности и степени нелинейности выходного отображения за счет добавления большего количества нелинейных функций.

Полученный результат может быть использован для оценки рисков информационной безопасности. В частности, можно учитывать уровень доверия аналитика к имеющимся тренировочным данным и к репрезентативности выборки для получения разного типа зависимостей. Так, если имеется большое количество данных и экспертным путем эти данные признаны достаточно точно отображающими зависимости вероятности реализации угрозы от тех или иных условий, то количество нейронов в сети для данной угрозы может быть увеличено. В случае недостатка данных или сомнения в их достоверности, можно искусственно уменьшить количество нейронов, чтобы избежать переобучения сети.

В главе также подробна описана созданная программная реализация на языке C/C++ и способы обеспечения качества программного кода, используемые в работе.

В первом реализованном проекте разработанный комплекс динамической итеративной оценки рисков информационной безопасности был использован в составе системы обеспечения информационной безопасности для оценки рисков информационной безопасности в автоматизированной системе ОАО «Безопасность информационных технологий и компонентов».

Во втором проекте разработанный комплекс динамической итеративной оценки рисков информационной безопасности был использован в составе системы обеспечения информационной безопасности облачного сервиса «ONLANTA Cloud Secuirty» ЗАО «Онланта».

В третьем проекте разработанный комплекс динамической итеративной оценки рисков информационной безопасности был использован в составе системы обеспечения информационной безопасности тестового стенда компании ЗАО «ТЕХНОСЕРВЪ А/С».

Указанные внедрения подтверждены соответствующими актами.

В **заключении** приведены основные результаты диссертационной работы и подведены итоги.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В ходе выполнения работы были получены следующие научные и практические результаты:

1. На основе анализа существующих методов оценки рисков информационной безопасности предложен новый подход к проведению итеративной динамической оценки рисков информационной безопасности.
2. С использованием математической модели, реализующей байесовский подход, разработаны алгоритмы применения нейронных сетей для решения задачи динамической итеративной оценки рисков информационной безопасности, и на их основе синтезирована система оценки рисков информационной безопасности, обладающая заданными свойствами.
3. Разработан и применен для решения практических задач обучаемый программный комплекс, предназначенный для итеративной динамической оценки рисков информационной безопасности в гетерогенной автоматизированной системе, позволяющий существенно упростить процедуру анализа рисков на основе использования непрерывности оценки.

## ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Основные положения диссертационной работы опубликованы в 8 печатных трудах, в том числе в 4 статьях в журналах, включенных ВАК РФ в перечень ведущих рецензируемых научных журналов и изданий:

1. **Атаманов А.Н. Применение искусственных нейронных сетей для динамической итеративной оценки рисков информационной безопасности в автоматизированных системах // Образование. Наука. Научные кадры. 2012 − №3, − с. 37-41**
2. **Атаманов А.Н. Методика динамической итеративной оценки рисков информационной безопасности в автоматизированных системах // Глобальный научный потенциал. 2012 − №3, − с. 28-33**
3. **Атаманов А.Н. Модуль нечеткого вывода на основе нейронных сетей для динамического итеративного анализа рисков информационной безопасности // Безопасность информационных технологий. 2011, №1, – с. 34-37**
4. **Атаманов А.Н. Динамическая оценка эффективности системы защиты информации // В сб. материалов XVI всероссийской научно-практической конференции «Проблемы информационной безопасности в системе высшей школы», Безопасность Информационных Технологий. Мск., 2009. – с. 95-96**
5. Атаманов А.Н. Вопросы оценки рисков информационной безопасности в автоматизированных системах // Современная наука: актуальные проблемы теории и практики. 2012 − №3, − с. 17-20

6. Атаманов А.Н. Вопросы анализа рисков информационной безопасности при построении системы защиты конфиденциальной информации // Информационная безопасность. 2012 − №3, − с. 25-29

7. Атаманов А.Н. Технология защиты в гетерогенных сетях «Diamond ACS» // В сб. материалов межрегионального семинара «Обеспечение информационной безопасности информационных систем органов исполнительной власти субъектов Российской Федерации». Мск., 2010. – с. 43-45

8. Атаманов А. Н., Минаева Е. В. Мониторинг информационных рисков как средство повышения защищенности информационных систем // В сб. материалов российской научной конференции «Методы и средства обеспечения информационной безопасности». СПб., 2008. – с. 97

**Личный вклад автора** в работах, написанных в соавторстве, состоит в следующем: [8] – анализ методов реализации динамической итеративной оценки рисков информационной безопасности в составе системы непрерывного мониторинга и аудита.

*Атаманов Александр Николаевич*

# ДИНАМИЧЕСКАЯ ИТЕРАТИВНАЯ ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Подписано в печать 31.01.12. Формат 60x84 $^{1}/_{16}$.
Усл. печ. л. 1,0. Уч.-изд. л. 1,0. Тираж 100 экз. Заказ № 37

Национальный исследовательский ядерный университет «МИФИ» (НИЯУ МИФИ)

115409, Москва, Каширское шоссе, 31