На правах рукописи

Криволапов Вячеслав Григорьевич

КОМПЛЕКСНАЯ МЕТОДИКА МОДЕЛИРОВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОТКРЫТЫХ СИСТЕМ

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Автор: _____

МОСКВА – 2009

Работа выполнена в Московском инженерно-физическом институте
(государственный университет)

НАУЧНЫЙ РУКОВОДИТЕЛЬ: кандидат технических наук,
Горбатов Виктор Сергеевич,
МИФИ (ГУ)

ОФИЦИАЛЬНЫЕ ОППОНЕНТЫ: доктор технических наук,
Королев Вадим Иванович,
ИПИ РАН

кандидат технических наук,
Сычев Артем Михайлович,
ОАО «Россельхозбанк»

ВЕДУЩАЯ ОРГАНИЗАЦИЯ: Российский гуманитарный государственный университет (РГГУ)

Защита состоится «24» июня 2009 г. в 15 час. 00 мин. на заседании диссертационного совета ДМ 212.130.08 в Центре информационных технологий и систем органов внутренней власти (ЦИТиС)
по адресу: 123557, г. Москва, Пресненский Вал 19.

С диссертацией можно ознакомиться в библиотеке МИФИ.

Автореферат разослан: «__»_____200 г.

Просим принять участие в работе совета или прислать отзыв в одном экземпляре, заверенном печатью организации
по адресу: 115409, г. Москва, Каширское шоссе, д.31.

Ученый секретарь диссертационного совета,
кандидат технических наук,
доцент _____В.С. Горбатов

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. Современное общество находится на этапе глобальной информатизации, когда информация представляется как ресурс, имеющий не меньшее значение, чем другие. В связи с этим появляются и развиваются новые подходы к созданию информационных систем, играющих ключевую роль в обеспечении эффективной деятельности любых современных предприятий и организаций. Развитие информационных систем идет под воздействием двух диалектически противоположных факторов.

Первый формируется под влиянием ведущих фирм-производителей компьютерного оборудования, которые, реализуя свою стратегию, стремятся монополистически преобладать в той или иной нише рынка ИТ-технологий.

Второй фактор определяется стремлением к массовому производству и широкому распространению разрабатываемой продукции. Это стремление вызывает необходимость взаимодействия множества организаций, невозможного без четкого определения спецификаций продукта и использования общих стандартов. Подобное взаимодействие приводит к удешевлению товара, улучшению его свойств – благодаря открытости структуры и появлению новых идей. Широкое распространение продукции различных фирм-производителей заставляет решать проблемы совместимости между этими товарами. Так как системы также являются продуктом, возникает необходимость в их унификации.

В настоящее время в сфере ИТ-технологий, благодаря накопленному научному потенциалу и полученным технологическим решениям, следует отметить преобладание влияния второго фактора. Его потенциал аккумулирован в многочисленных документах международного масштаба, которые позволяют преодолеть разрыв между разнородными информационно-техническими продуктами различных фирм и промышленных групп. Эти документы являются результатом коллективной работы большого числа участников процесса стандартизации и представляют научно-методическую основу для изучения различных аспектов развития информационных технологий.

Разработки в этом направлении получили название «открытые системы» (или «открытая среда»), и в связи с интенсивным развитием данной концепции, являются с точки зрения потребителя более предпочтительными, что вызывает необходимость их рассмотрения в различных плоскостях информационных технологий, включая и информационную безопасность этих систем. Говоря об информации как о ресурсе систем управления, можно отметить, что для обеспечения его безопасности необходим комплексный подход, который позволит разносторонне обеспечить целостность, доступность и конфиденциальность.

Многообразие и широкое применение открытых систем в различных сферах человеческой деятельности, а также их зависимость от безопасности информационного ресурса усиливают значимость и актуальность научной проработки исследуемой темы. Фундамент проблемы требует конкретного исследования.

Актуальность вопросов информационной безопасности открытых систем обусловлена проблемами обеспечения целостности, доступности и конфиденциальности параллельно с вопросами обеспечения совместимости, расширяе-

мости и масштабируемости этих систем. В связи с этим для эффективной разработки защиты открытой системы, одним из важных этапов является решение исследовательских задач. Следовательно, анализ безопасности открытых систем является первоочередной задачей для достижения максимального уровня безопасности. В частности, в качестве результата анализа могут выступать оценки рисков информационной безопасности, представляющие не только научный, но и практический интерес, что и определило выбор темы диссертационного исследования.

Степень разработанности проблемы. Исследованием общетеоретических вопросов обеспечения информационной безопасности систем занимались В.Ю. Гайкович, В.Г. Герасименко, А.А. Грушо, А.А. Малюк и другие.

Проблемы защищенности различных систем нашли свое место в работах таких авторов как В.С. Горбатов, В.А. Конявский, О.Б. Макаревич, Ю.Б. Михайлов, В.А. Минаев, А.В. Старовойтов, Д.П. Зегжда и другие. В частности, вопросам анализа и аудита информационных систем свои труды посвятили А.П. Баранов, С.Д. Бешелев, А.П. Курило, В.А. Петров, С.А. Петренко, С.В. Симонов и другие.

Проблемы безопасности открытых систем рассматривались в работах С.В. Запечникова, Н.Г. Милославской, А.И. Толстого, Д.В. Ушакова. В этих трудах отражены решения, применимые на практике, по устранению уязвимых мест при реализации безопасных открытых систем. Однако, недостаточное исследование первоочередных вопросов, связанных с анализом и оценкой защищенности подобных систем также подчеркивает актуальность выбранной темы диссертационной работы.

Целью исследования является повышение уровня защищенности открытых систем.

Достижение поставленной цели диссертационного исследования предполагает решение следующих **задач**:

- уточнить понятие «открытые системы» с точки зрения обеспечения их информационной безопасности;
- провести изучение подходов по моделированию открытых систем, разработать рекомендации по дальнейшему исследованию их защищенности;
- разработать методику оценки рисков для открытых систем на основе процессного подхода;
- провести практическую апробацию методики, например, на основе широко распространенных в образовательной среде систем дистанционного обучения.

Объектом диссертационного исследования являются открытые информационные системы в аспекте обеспечения их информационной безопасности.

Предмет исследования – методика оценки рисков открытых информационных систем.

Методы исследования. Решение сформулированных задач строилось с использованием процессного подхода, применимого к исследованию сложных систем. Для разработки моделей использовалась теория имитационного моделирования. Для оценки угроз применялась теория массового обслуживания, в

рамках которой проводилась имитация модели. Полученные результаты обрабатывались на основе теории вероятностей и математической статистики.

Информационную базу исследования составляют публикации и материалы научно-практических конференций по вопросам, относящимся к теме диссертации, ресурсы Интернет, приведенные в списке литературы.

Научная новизна диссертационной работы состоит в применении комплексного и целостного исследования методов оценки рисков информационной безопасности на основе системного научного подхода. При этом впервые:

- для оценки рисков открытых систем используется процессный подход, как основа для дальнейшего моделирования;
- предложен метод перехода от функциональной модели SADT/IDEF0 к имитационной модели, описанной в терминах математической теории сетей Петри;
- введено понятие «Сеть угроз» на основе определения сетей Петри, и предложены правила перехода от «Сети угроз» к языку имитационного моделирования;
- разработан метод расчета вероятностей реализаций угроз, позволяющий давать практические результаты из формализованных теоретических исследований;
- разработан метод расчета рисков информационной безопасности, на основе вероятностей реализаций угроз и показателей ущерба, оцененных экспертным методом.

Практическая ценность работы определяется вкладом, связанным с решением актуальной научно-практической проблемы – разработки комплексной методики оценки рисков информационной безопасности открытых систем на примере широко используемых систем дистанционного обучения.

Практическая значимость подтверждается внедрением разработанной методики:

- для оценки защищенности информационной системы Оренбургского государственного аграрного университета;
- в учебный процесс, как дополнительный лекционный материал по курсу «Основы информационной безопасности», читаемый для студентов МИФИ, обучающихся по специальности 075500 – «Комплексное обеспечение информационной безопасности автоматизированных систем».
- методика применялась для оценки рисков системы дистанционного обучения Оренбургского государственного института менеджмента на этапе ее проектирования.

Основные положения, выносимые на защиту:

1. Алгоритм методики оценки рисков информационной безопасности открытых систем.

2. Методика перехода от SADT/IDEF0 модели к модели математического аппарата сетей Петри.

3. Определение «Сети угроз» и правила перехода от «Сети угроз» к языку имитационного моделирования.

4. Метод расчета значений рисков информационной безопасности открытых систем.

Апробация работы. Основные положения и наиболее актуальные выводы диссертации докладывались автором на Всероссийских научно-практических конференциях «Проблемы информационной безопасности в системе высшей школы», (2007, 2008 гг.). Материалы диссертации использовались при подготовке лекций и практических занятий по курсу «Основы информационной безопасности» в Московском инженерно-физическом институте и Оренбургском государственном институте менеджмента. Выводы и исследования легли в основу 8 публикаций.

Структура работы. Диссертация состоит из введения, четырех глав, заключения, содержит список использованной литературы из 138 наименований и приложение. В диссертации 140 страница машинописного текста, 15 таблиц, 11 рисунков и приложение.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении раскрыта актуальность темы диссертации, определена цель и охарактеризованы общие направления её реализации.

В первой главе дается научный анализ аспектов безопасности открытых систем. Рассматривается понятие открытости систем и их переход на другой уровень понимания, отличный от представленных ведущими организациями, занимающимися проблемами открытых систем.

Особое внимание уделено определениям понятий открытых систем. Эти понятия отражают техническую сторону, связанную с разработкой и реализацией таких систем. Они выражены через комплекс спецификаций на интерфейсы, сервисы и поддерживаемые форматы данных, достаточный для того, чтобы обеспечить разработанным приложениям возможность переноса с минимальными изменениями на широкий диапазон систем и совместной работы с другими приложениями на локальной и удаленных системах.

Для исследования вопросов безопасности открытых систем использован Приказ № 11462, ФСТЭК России №55, ФСБ России № 86, Мининформсвязи России № 20 от 13 февраля 2008 года «Об утверждении порядка проведения классификации информационных систем персональных данных», на основе которого можно определить место открытых систем в этой классификации. Открытые системы – это фактически системы общего пользования, а персональные данные в них либо выступают для идентификации субъекта, либо являются общедоступными. Следовательно, открытые системы можно отнести к 3 и 4 категориям согласно вышеупомянутому приказу.

Анализ литературы показал, что достаточно адекватным представлением открытых систем может быть структура интранет. Взаимодействие между компонентами внутри интранета осуществляется через стандарты и спецификации открытых систем. Но если рассуждать об открытых системах масштабно, как о системах, которые позволяют взаимодействовать с себе подобными, то понятия «интранет» недостаточно. Говоря о персональных данных, обрабатываемых и хранящихся в интранете, можно заключить, что они могут попасть под любую

категорию вышеназванного приказа. К тому же для этих персональных данных может быть недостаточно обеспечения только конфиденциальности. Значит, такие системы не попадают под понятие типовых информационных систем, а для защиты персональных данных в них используются специализированные средства обеспечения безопасности системы. При таком подходе нельзя говорить об интранете как об открытой системе. Говоря о среде за пределы интранета, необходимо представить понятие «портал». Именно он позволяет представить интранет как возможную открытую систему. Фактически портал отражает собой совокупность технологий и программных средств, позволяющих компаниям «расконсервировать» информацию, которая возникает и накапливается как внутри, так и вне их границ. В подобных системах обмен происходит на протяжении всего времени работы организации, поэтому вопросы обеспечения целостности и доступности имеют тот же приоритет что и вопросы обеспечения конфиденциальности.

В информационной системе возможно присутствие информации ограниченного доступа (государственная тайна, коммерческая тайна и т.д.). Конфиденциальность, представленная через призму таких тайн, предполагает использование специализированных средств защиты, не описанных в существующих стандартах открытых систем. Отметим, что системы, оснащенные такими средствами, не попадают под определение открытых сред. К тому же для таких систем установлены определенные требования в рамках документов уполномоченных органов государственной власти. Таким образом, открытые системы не являются системами, которые хранят государственные и коммерческие тайны, но в них присутствуют персональные данные, что в соответствии с вышеназванным приказом относит их к 3 и 4 категории. А нарушение конфиденциальности таких данных не несет серьезных последствий (экономические, влияние на работоспособность системы) и не имеет высокого приоритета. Вследствие этого конфиденциальность информации в открытых системах ставится на одну черту важности с обеспечением доступности и целостности информации.

Ярким примером портала, а следовательно, и открытых систем, являются системы дистанционного обучения (СДО). На данный момент наиболее широкое распространение получили СДО посредством компьютерных сетей и глобальной сети Интернет. Обычно такие системы централизованны. Обучение и контроль знаний происходит путем подключения к системе дистанционного обучения с использованием специально разработанных программ или web-технологии.

СДО есть взаимодействие различных систем, удаленных друг от друга территориально, для достижения основной обучающей цели. Это выражение в большей степени описывает такой способ реализации СДО как сетевая технология. Остальные (кейс-технология, ТВ-технология) не рассматриваются из-за интенсивного развития средств цифровой передачи информации.

СДО должна поддерживать следующие взаимодействия:

– с клиентскими системами независимо от того, какую аппаратно-программную среду они используют;
– с подобными системами, используемыми в сфере образования.

Через такие взаимодействия выражаются свойства переносимости данных между системами, способности к взаимодействию с другими системами, способности к масштабируемости СДО, что является свойствами открытых систем.

В СДО, как правило, отсутствует информация, являющаяся государственной или коммерческой тайной. В подобных системах персональные данные не выходят за рамки данных идентифицирующих пользователя в системе, следовательно, принадлежат не выше чем к третьей категории. Очевидно, что в такой системе количество пользователей будет не выше 100 000, следовательно, системы дистанционного обучения принадлежат к четвертой категории, который говорит о том, что информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных. Такую же категорию имеют и открытые системы. Это еще раз показывает возможность исследования систем дистанционного обучения как открытых систем.

Во второй главе проведен анализ существующих оценок защищенности, подходов, методов, и возможности их применения для открытых систем. На основании доказательных выводов о неэффективности их применения по отношению к открытой среде поставлена задача разработки методики оценки рисков – с последующим применением для открытых систем.

Для обеспечения защищенности любых информационных систем осуществляется ряд действий, которые принадлежат этапам жизненного цикла. А начальным этапом эффективного обеспечения информационной безопасности системы является анализ, т.е. практически – определение уровня защищенности системы. Аудит информационной безопасности, получивший широкое распространение при анализе систем, позволяет объективно оценить текущее состояние информационной безопасности компании (системы), а также ее адекватность поставленным целям и задачам бизнеса по увеличению эффективности и рентабельности экономической деятельности компании. Под аудитом информационной безопасности понимается выполнение мероприятий по проверке соответствия используемых механизмов обеспечения информационной безопасности информационной системы или организации, согласно заданным требованиям. Одной из основных задач любого такого аудита является получение результата процесса оценивания рисков безопасности информационной системы.

При отсутствии единой методики оценивания рисков информационной безопасности существуют общие критерии реализации таких методик, которые предполагают использование некой модели или комплекса моделей, что дает возможность охарактеризовать исследуемую систему. Для этого в качестве начальных данных используются знания экспертов или статистические данные появления тех или иных угроз. Значения конечных оценок зависят не только от корректности начальных данных, но от выбранной методики и, соответственно, от применяемой модели.

Требования, предъявляемые к оценке рисков с учетом исследования открытых систем, следующие:

– выбранная в методике стратегия должна быть достаточно гибкой при наращивании системы и иметь возможность достаточно быстрого получения конечных оценок рисков относительно реализованной системы;
– методика должна быть универсальной, чтобы давать оценки для различных по структуре систем, какими являются открытые системы.

При оценке защищенности информационных систем имеется информация о возможных угрозах, возможном (ожидаемом) ущербе от реализации той или иной угрозы. Считается, что риск тем больше, чем больше вероятность происшествия и тяжесть последствий. Формально, в общем виде, получение оценки рисков можно выразить следующим образом:

$$Risk = P_i \times Cl$$

где:

P_i – вероятность наступления события;

Cl – цена потери.

Вместе с тем методы экспертных оценок не лишены известных недостатков. В их числе – субъективность оценок, основанных на интуитивном мнении экспертов; плохая сопоставимость мнений ввиду преимущественно качественного характера оценок; необходимость постоянного привлечения группы высококвалифицированных специалистов, что делает процесс прогнозирования достаточно сложным и трудоемким с организационной точки зрения. Такой процесс очень тяжело поддаётся формализации и последующей автоматизации. Несмотря на эти недостатки, в случаях, когда экспертные оценки являются единственно возможным способом получения информации об исследуемой системе, они выступают как обязательный, а зачастую и основной критерий.

Обобщая проведенный анализ оценки защищенности систем и оценки рисков, можно сделать очевидный вывод, что повышение качества прогнозирования и оценки уровня защищенности возможно при комплексном применении различных методов. В частности, экспертные оценки можно дополнить математическим и имитационным моделированием, синтезируя некую человеко-машинную систему, формализующую знания эксперта (в том числе и интуитивные) в конкретной предметной области путем проведения вычислительного эксперимента с комплексом математических моделей.

В результате предложено разработать методику оценки защищенности на основе комплексного подхода к оценке рисков информационной безопасности. Такая задача наиболее полно осуществима на основе дополнения экспертных оценок методами математической статистики, теории вероятностей и имитационного моделирования.

Третья глава посвящена разработке комплексной методики оценки рисков открытых систем. В этой главе рассматриваются модели исследования открытой системы и модели оценки рисков. Методика позволяет определять:

– степень детализации каждого уровня исследования объекта;
– описание условий работы системы, ее характеристик, сценариев, структур компонентов с использованием метамоделей;
– динамику объекта на основе использования имитационного

моделирования.

Поставленной в работе цели исследования можно достичь комплексным подходом, т.е. дополнением друг друга нескольких методик. Алгоритм предлагаемой методики состоит из нескольких шагов:

1. сбор информации об исследуемой системе;
2. разработка комплекса моделей – от функциональной модели системы к имитационной модели угроз;
3. получение оценок у экспертов;
4. синтез конечных значений оценок рисков открытой системы;
5. синтез погрешностей полученных оценок.

Разрабатываемая методика представлена на рисунке 1 по методологии SADT-моделирования в виде последовательности действий для достижения конечного результата – конечных оценок и величин рисков.

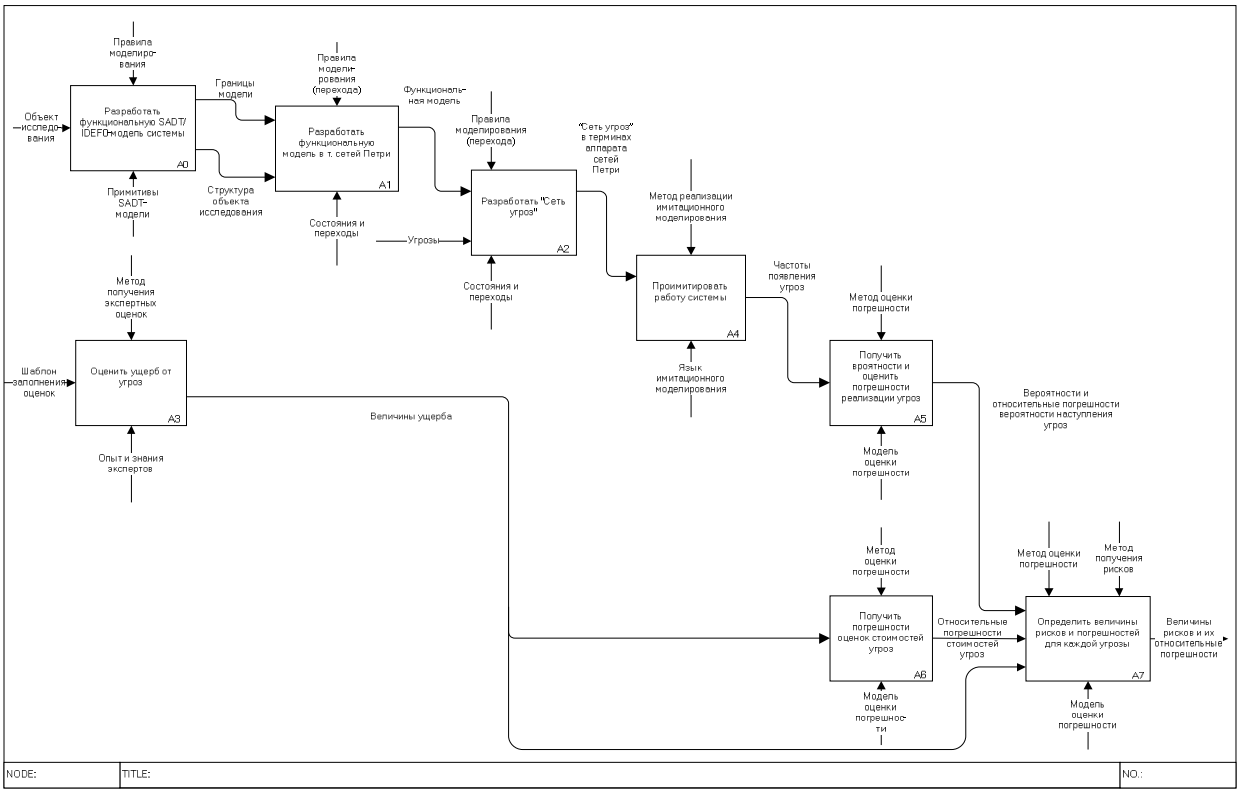

Рисунок 1. Последовательность действий в методике оценки рисков открытых систем

Для построения моделей анализа функциональной составляющей объекта исследования предлагается применить методологию SADT/IDEF0.

Для дальнейшего изложения материала по анализу рисков открытых систем в работе предлагается использовать аппарат сетей Петри, так как он не диктует какого-либо специфического метода моделирования систем, а предоставляет гибкий инструмент для моделирования, который можно интерпретировать по-разному.

Функционирование сети Петри описывается формально с помощью множества последовательностей срабатываний и множества достижимых в сети разметок. Эти понятия определяются через правила срабатывания переходов сети.

На сегодняшний день нет единого методологического базиса, который позволил бы перейти от функциональной модели исследуемой системы к модели, применимой для исследования информационной безопасности системы. В связи с этим возникает необходимость разработки возможных правил такого перехода, т.е. преодоления разрыва между функциональной базовой моделью и имитационной моделью.

Модель, описанная на основе SADT/IDEF0-моделирования, имеет ряд преимуществ: за счет использования понятий «Цель» и «Точка зрения» она позволяет очертить предметную область, графически представить модель, за счет декомпозиции более детально рассмотреть функционирование необходимых компонентов. Тем не менее, данная модель не позволяет рассмотреть изменение состояния системы при воздействии на нее угроз. В рамках диссертационной работы предлагается компенсировать этот разрыв построением модели системы на основе аппарата сетей Петри, полученной из модели системы на основе SADT/IDEF0-моделирования, так как они имеют ряд общих признаков:

– включают не только наглядное, но и математическое представление;
– универсальны, т.е. применяются в довольно широком кругу описываемых систем;
– позволяют описывать динамику и имитировать работу системы;
– имеют небольшое количество «примитивов».

Так как оба вида моделирования имеют «примитивы» и графическое представление модели, то задачу по преобразованию из одного типа моделирования в другой предлагается свести к преобразованию значений их «примитивов». Для SADT-моделирования основными «примитивами» будут являться интерфейсные дуги и функциональные блоки. Для сетей Петри – это состояния и переходы.

Согласно теории построения моделей с использованием аппарата сетей Петри, переход сработает, если будут выполнены все предусловия для срабатывания перехода. После срабатывания перехода появляются постусловия.

В моделировании посредством SADT/IDEF0 функциональный блок выполнит свое назначение, если будет предоставлена вся заявленная информация для этого блока, т.е. входная информация, управление, механизмы. После выполнение завершения работы функционального блока появляется выходная информация. Таким образом, будет получено преобразование SADT/IDEF0-модели в термины сети Петри (Таблица 1).

Таблица 1

Таблица преобразований «примитивов» SADT/IDEF0-моделирования в термины сетей Петри

SADT/IDEF0	Сеть Петри
Вход, Управление, Механизм	Предусловия (состояния)
Функциональный блок	Переход
Выход	Постусловия (состояния)

Следует отметить, что при преобразовании из SADT-модели в сеть Петри не всегда удается точно найти переходы и состояния в сети Петри, соответствующие коду ICOM и функциональному блоку в SADT-модели. Некоторые функциональные блоки и ICOM-коды удается описать с использованием нескольких состояний и переходов. Эта проблема приводит к повышению сложности понимания преобразованной модели. В этом случае предлагается компенсировать несоответствие уровня декомпозиции между моделями, используя вложенные сети Петри. Вложенные сети Петри позволят в рамках предложенной методики работы исследовать более подробно нужные аспекты в области информационной безопасности, т.е. описать более подробно те действия или события в системе, которые относятся к вопросам информационной безопасности, полагаясь на вложенность структуры (получение и детальное рассмотрение модели в сетях Петри одного процесса или действия). Необходимо заметить, что такой подход уменьшит разногласия по преобразованию моделей.

В дальнейшем целесообразным является использование модели, ориентированной именно на систему информационной безопасности объекта в условиях функционирования системы. Поэтому необходимо перейти от общей, функциональной модели, реализованной с использованием сетей Петри, к функциональной модели, отражающей действия злоумышленника при переходе из одного состояния в другое, которую предлагается назвать «Сеть угроз».

Таким образом, «Сеть угроз» – это дополненная действиями злоумышленника функциональная модель системы, описанная с использованием аппарата сетей Петри. При этом, основываясь на определении сети Петри, в работе дано следующее определение «Сети угроз»:

«Сеть угроз», N_u – это упорядоченный набор состояний и мест, зависимых между собой функцией инцидентности.

$$N_u = (S, T, M_0, F),$$

где:

$S = (U, E)$ – множество всех мест;

$U = \{u_1 ... u_n\}$ – множество угроз, представленных в данной модели;

$E = \{e_1 ... e_n\}$ – множество разрешенных действий модели, причем $U \cap E = \varnothing$;

T – множество переходов, т. е. различные действия над моделью.

Отмечено, что срабатывание переходов, предоставляющих движение в множество переходов, задается вероятностью срабатывания.

$ver : T \to [0,1)$ – функция, отображающая множество T в интервал $[0,1)$, где $ver(t_i)$ – вероятность срабатывания перехода t_i при условии наличия возможности его срабатывания;

F – функция инцидентности;

M_0 – начальная разметка сети.

Следующий этап в предложенной методике моделирования и оценки рисков для создания и улучшения системы информационной безопасности заключается в переходе от «Сети угроз» к имитационной модели, в которой задаются вероятности возникновения угроз.

Вследствие того, что довольно затруднительно рассчитать аналитически вероятности возникновения угроз в системе с использованием графа достижимости, основанного на сетях Петри (затруднительно представить формально изменение состояния системы при возникновении вероятностных характеристик возникновения угроз), в качестве альтернативы целесообразно воспользоваться имитационным моделированием, реализованном на ЭВМ.

В главе представлены правила перехода от «Сети угроз» к имитационной модели, описанной посредством языка имитационного моделирования GPSS.

Можно применить модель злоумышленника с приоритетами, которая предполагает, что злоумышленник при наличии нескольких уязвимостей перебирает их в заранее известной последовательности, пока одна из них не реализуется. Задавшись вероятностями выполнения действий злоумышленника в «Сети угроз» через экспертные оценки и проводя имитационное моделирование, можно определить частоту реализации каждой угрозы на основе выбранной модели злоумышленника. Этот этап позволит связать воедино мнения экспертов (экспертные оценки) и структуру исследуемой системы. Он является конечной точкой получения необходимых промежуточных значений для получения результата, конечных оценок. После преобразования «Сети угроз» в имитационную модель, в которой переходам сопоставлены вероятности срабатывания, полученные по методу экспертных оценок, и моделирования, местам оказываются сопоставлены случайные величины.

В работе принято, что эти величины имеют распределение Бернулли. Это позволило, применяя Центральную предельную теорему, показать, что искомая вероятность реализации угрозы может быть найдена по формуле

$$p_i = \frac{k_i}{n},$$

где k_i - абсолютная частота реализации угрозы, а n – число запусков модели. Задавшись доверительной вероятностью P_d, можно определить абсолютную и относительную погрешности δp_i величины p_i по следующим формулам:

$$\Delta p_i = t_{p\sigma_i} = t_p \cdot \sigma_i ;$$

$$\delta p_i = \frac{t_{p\sigma_i}}{p_i},$$

где:

$$\Phi(t_p) = \frac{1 + P_d}{2};$$

$\Phi(z)$ – интегральная функция стандартного нормального распределения:

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-\frac{t^2}{2}} dt ;$$

$$\sigma_i^2 = \frac{k_i}{n^2}(1 - \frac{k_i}{n}).$$

Так как оценки экспертов тяготеют к истинному значению ущерба, а значения оценок, существенно отличающиеся от истинных, имеют малую вероятность появления, предположено, что каждая экспертная оценка принадлежит нормальному распределению с математическим ожиданием, равным истинному значению стоимости угрозы, и дисперсией, различной для каждого эксперта.

Известно, что множество экспертных оценок стоимости s_{ij} i- ой угрозы имеет распределение Лапласа. При небольшом количестве экспертов выборочное среднее $\hat{s}_i$ оценок стоимости i-ой угрозы имеет распределение, близкое к распределению Лапласа, однако с точностью, достаточной для практических нужд, можно считать его нормальным. В работе показано, что в этом случае

$$P_d = 2\Phi(\frac{t_{p\sigma_i}\sqrt{n}}{\sigma_{S_i}})\text{-}1,$$

где:

$t_{p\sigma_i}$ - половина ширины доверительного интервала;

n – количество экспертных оценок (экспертов);

$$\sigma_{S_i} \approx \sqrt{\frac{1}{n-1}\sum_{j=1}^{n}(s_{ij} - m_{S_i})^2};$$

$$m_{S_i} \approx \frac{1}{n}\cdot\sum_{j=1}^{n} s_{ij}.$$

Исходя из полученных формул и задавшись доверительной вероятностью P_d, можно определить половину ширины доверительного интервала $t_{p\sigma_i}$. Тогда относительная погрешность конечной оценки ущерба от i-ой угрозы δs_i может быть найдена по формуле:

$$\delta s_i = \frac{t_{p\sigma_i}}{s_i},$$

причем s_i будем считать равной $\hat{s}_i$.

Для определения количества экспертов, достаточного для получения заданной погрешности можно воспользоваться следующей формулой:

$$n \geq \frac{M^2 + C^2}{C^2}, \qquad (1)$$

где:

$$C = \frac{\delta s}{\Phi^{-1}(\frac{P_d + 1}{2})},$$

M – максимальное относительное отклонение оценок экспертов,

δs – требуемая относительная погрешность.

Очевидно, что минимальным количеством будут являться два эксперта; в случае наличия одного эксперта о какой-либо оценке погрешностей говорить невозможно, так как отсутствует разброс оценок.

При разработке имитационной модели и описания в ней выбранных угроз может возникнуть такая ситуация, при которой при учете всех угроз модель получается громоздкой и неудобной для последующего анализа. В этом случае

предложено исследуемые угрозы классифицировать согласно нарушениям основных свойств информационной безопасности и оперировать ими вместо отдельных угроз. За счет этого имитационная модель будет содержать только три исхода, представляющих нарушения соответствующих свойств ИБ. При этом для получения оценок вероятностей реализации отдельных угроз появляется необходимость в дополнительных оценках условных вероятностей реализации угроз при реализации нарушений основных свойств информационной безопасности. Эти оценки могут дать эксперты. В работе получены формулы расчёта искомых вероятностей и их погрешностей в этом случае.

Целью применения вышеописанных методик является получение величины риска**,** обусловленного i-ой угрозой. Обозначим эту величину W_i**.**
Тогда:

$$W_i = p_i \cdot s_i$$

Относительная погрешность величины риска определяется по следующей формуле:

$$\delta W_i = \delta p_i + \delta s_i$$

Для автоматизации расчетов по предложенной методике, можно использовать существующие программные продукты. Например, для расчета имитирования работы исследуемой системы применим программный продукт GPSS. Для автоматизации расчета нахождения величины риска информационной безопасности и относительной погрешности, можно применять следующие программные продукты: wxMaxima, Microsoft Office: Excel, Open Office: Calc.

Четвертая глава посвящена экспериментально-практической части применения предложенной методики. Представлено получение оценок рисков информационной СДО.

Для исследования системы дистанционного обучения получена диаграмма АО (рис. 2).

SADT/IDEF0-модель СДО А0 преобразована в модель на основе терминов сетей Петри. Классифицированы виды угроз, используемые в работе.

В качестве методики опроса экспертов применялся метод Дельфы. В опросе участвуют 17 экспертов. Далее, на основе этого списка и заранее подготовленной «Сети угроз», предлагается оценить вероятность появления того или иного события в «Сети угроз» и оценить ущерб, понесенный от реализации той или иной угрозы. После получения оценок имитируется работа системы на основе имитационной модели и выявляются частоты реализации угроз или классов угроз.

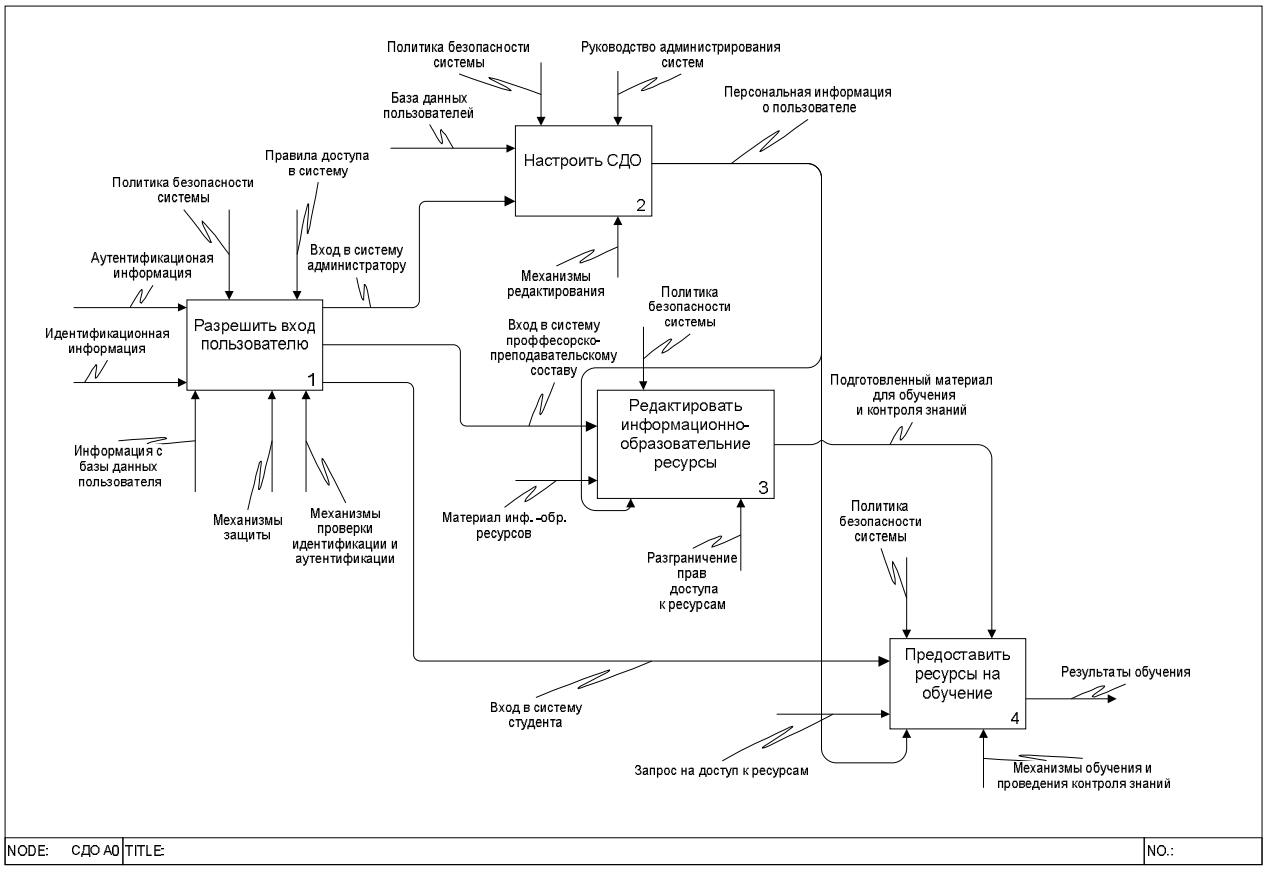

Рисунок 2. Диаграмма АО системы дистанционного обучения

Из модели СДО, представленной в терминах аппарата сетей Петри, получена «Сеть угроз». В ней моделируются нарушения конфиденциальности (РА), целостности (РВ) и доступности (РС).

В соответствии с правилами преобразования «Сети угроз» в имитационную модель на языке GPSS получена модель. Результаты имитации модели приведены в таблице 2.

Таблица 2

Результаты запуска «Сети угроз»

Параметр	Значение
Количество подключений	75068
Количество реализаций нарушения целостности информации (А)	4068
Количество реализаций нарушения конфиденциальности (В)	1826
Количество реализаций нарушения доступности информации (С)	4106

Получены значения вероятностей реализаций угроз:

$P(A) \approx 4068/75068 \approx 0{,}0542$

$P(B) \approx 1826/75068 \approx 0{,}0243$

$P(C) \approx 4106/75068 \approx 0{,}1$

Для оценки погрешностей задана доверительная вероятность $P_d = 0{,}95$. Тогда:

$$\Phi(t_p) = \frac{1 + P_d}{2} = 0{,}975$$

Из таблицы значений функции Ф можно получить величину t_p:

$t_p \approx 1{,}959$

Вычисление величин σ_A, σ_B и σ_C:

$$\sigma_A \approx \sqrt{\frac{P(A)(1-P(A))}{n}} \approx \sqrt{\frac{0{,}05126}{75068}} \approx 0{,}0005623$$

$\sigma_B \approx 0{,}0008263$

$\sigma_c \approx 0{,}0008299$

Вычисление абсолютных погрешностей $\Delta P(A)$, $\Delta P(B)$ и $\Delta P(C)$:

$$\Delta P(A) = t_{p\sigma_A} = t_p \sigma_A \approx 0{,}0011;\ \Delta P(B) = t_{p\sigma_B} \approx 0{,}0016;\ \Delta P(C) = t_{p\sigma_C} \approx 0{,}0016$$

Относительные погрешности составят:

$\delta P(A) \approx 0{,}0011 / 0{,}0542 \approx 0.02$

$\delta P(B) \approx 0{,}0016 / 0{,}0243 \approx 0.066$

$\delta P(C) \approx 0{,}0016 / 0{,}1 \approx 0{,}016$

Таким образом, искомые вероятности:

P(A)=(5,4±0,1)%;

P(B)=(2,4±0,6)%;

P(C)=(10±0,6)%.

Расчет количества экспертов в группе, необходимых для достижения заданной погрешности, проводится следующим образом: необходимо определить количество экспертов при 10% погрешности, доверительной вероятности 95% и максимальном относительном отклонении оценок экспертов – 20%. Тогда из (1) получается $n \geq 17$. Таким образом, для достижения поставленных условий нужно не менее 17 экспертов.

Конечные значения расчета стоимостных оценок и их относительных погрешностей отражены в таблице 3. Строками (с 1 по 17) представлены оценки ущерба для угроз, оглашенные каждым экспертом, а столбцами (с 1 по 16) – оценки ущерба для каждой угрозы. Для каждой угрозы приведены значения ущерба (s_i) и относительные погрешности полученных оценок δ_{S_i}.

Таблица 3

Получение стоимостных оценок и их относительных погрешностей через экспертные оценки

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	14900	17800	10000	16200	12000	1900	0	11100	20500	3900	4700	12500	1400	27800	14800	3800
2	14300	7000	7500	16600	12600	2600	0	8800	16600	5000	4300	7300	1600	17100	13700	3900
3	11200	13400	5700	14200	9400	2500	0	9100	23800	3700	3400	9800	1600	19800	12600	4700
4	12400	13100	5600	16600	14700	2900	0	8200	20800	3200	3800	11600	1100	12800	13900	4600
5	12200	15800	8800	12300	12900	3300	0	12500	18500	4200	5400	9600	1100	20400	13800	6200
6	13300	7900	10000	15000	14100	2400	0	11000	22300	4900	5000	8800	1400	22200	11600	4100
7	13500	11600	8300	12000	14800	2500	0	9000	22000	3400	4800	9900	1400	24800	15100	3700
8	11400	12500	9600	13700	9200	2700	0	8700	22400	4500	3500	10800	1400	22700	16500	4400
9	14200	12300	9600	10100	8600	2800	0	12400	17500	4600	4400	12200	1000	19200	18600	3400
10	12200	12100	9300	15300	11200	2000	0	7800	19400	4100	3700	9000	2000	19500	12500	3300
11	10000	12800	9500	13100	12100	2700	0	11600	22400	4800	4400	11400	1300	26300	17100	4000
12	11200	12500	9100	14000	8500	2600	0	7400	18500	5300	5100	7400	1700	25400	12900	4500
13	13400	14000	9000	18200	8000	1900	0	8000	17600	3600	5000	8900	1500	15000	11600	6100
14	7200	13700	7000	10400	12100	2600	0	11000	25500	3500	4000	8900	1600	24300	9400	4900
15	15400	11500	6900	17800	11200	2400	0	8000	16400	4100	4100	12600	1100	30100	15200	2900
16	14300	17800	8200	11900	8400	1800	0	11300	17000	2500	4000	14300	1000	21400	15800	4400
17	12900	16000	8300	9900	10600	2700	0	11800	27800	3800	4300	13300	1200	30500	15900	4000
s_i	12590 ± 960	13050 ± 1370	8380 ± 660	13960 ± 1250	11200 ± 1070	2490 ± 190	-	9870 ± 840	20530 ± 1560	4070 ± 350	4350 ± 280	10490 ± 9780	1380 ± 130	22310 ± 2360	14180 ± 1090	4290 ± 420
δ_{s_i}	0,07	0,1	0,08	0,09	0,09	0,08	-	0,09	0,08	0,09	0,06	0,09	0,09	0,1	0,08	0,1

Оценки условных вероятностей угроз рассчитываются по той же методике, что и оценки ущерба от угроз. В таблице 4 приведены конечные значения условных вероятностей угроз при реализации в каждом из свойств ИБ.

Таблица 4

Получение условных вероятностей угроз в процентах

Угрозы	Усл.вер.A	Усл.вер.B	Усл.вер.C
1	61,294	0	0
2	5,235	10	2,941
3	5,176	9,706	3,059
4	2,824	9,353	0
5	0	19,765	10,882
6	9,588	0	0
7	0	0	14,294
8	0	0	18,235
9	0	0	20,118
10	5,0588	0	0
11	7,765	0	9,647
12	0	0	4,706
13	0	15,235	5,176

Таблица 4

Получение условных вероятностей угроз в процентах (Продолжение)

Угрозы	Усл.вер.A	Усл.вер.B	Усл.вер.C
14	2,176	0	0
15	0	0	5,235
16	0	0	2,118

Таблица 5 показывает результаты расчета относительных погрешностей условных вероятностей угроз при реализации в каждом из свойств ИБ.

Таблица 5

Получение относительных погрешностей условных вероятностей угроз при реализации в каждом из свойств ИБ

Угрозы	Отн.погр.усл.вер. A	Отн.погр.усл.вер. B	Отн.погр.усл.вер. C
1	0,085	0	0
2	0,094	0,086	0,106
3	0,109	0,101	0,086
4	0,107	0,118	0
5	0	0,104	0,086
6	0,134	0	0
7	0	0	0,085
8	0	0	0,072
9	0	0	0,096
10	0,085	0	0
11	0,088	0	0,1
12	0	0	0,117
13	0	0,078	0,087
14	0,086	0	0
15	0	0	0,122
16	0	0	0,075

На основе условных вероятностей и вероятностей нарушения свойств рассчитаны вероятности реализации угроз и их погрешности. Результаты представлены в таблице 6.

Таблица 6

Вероятности реализации угроз и их погрешности

Угрозы	Вероятность реализации угроз	Погрешности
1	0,019	0,002
2	0,008	0,001
3	0,008	0,001
4	0,006	0,001
5	0,017	0,002
6	0,002	0,0004
7	0,008	0,001
8	0,01	0,001
9	0,011	0,001
10	0,001	0,0002
11	0,007	0,001
12	0,003	0,0004

Таблица 6

Вероятности реализации угроз и их погрешности (Продолжение)

Угрозы	Вероятность реализации угроз	Погрешности
13	0,011	0,001
14	0,001	0,0001
15	0,003	0,0004
16	0,001	0,0001

Для каждой угрозы рассчитана величина риска, а результаты представлены в таблице 7.

Таблица 7

Конечные стоимостные оценки и их относительные погрешности

№ узрозы	Величина риска (W_i)	Относительная погрешность (δ_{w_i})
1	187,69	0,21
2	108,31	0,23
3	68,62	0,21
4	80,34	0,24
5	186,63	0,22
6	5,80	0,25
7	0	0,11
8	98,39	0,19
9	225,90	0,20
10	5,00	0,22
11	31,15	0,19
12	26,97	0,24
13	15,26	0,20
14	11,81	0,24
15	40,60	0,23
16	4,97	0,20

Для наглядности и дальнейшего анализа следует рассмотреть результаты полученных величин в виде диаграммы (рис. 3).

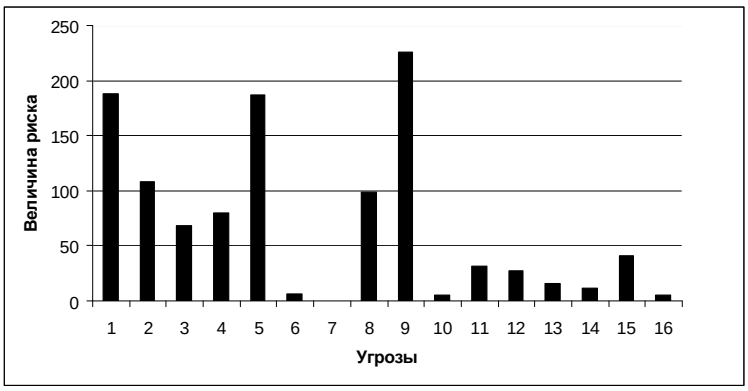

Рисунок 3. Диаграмма величины риска для каждой угрозы

После оценки рисков, т.е. выявления потенциально опасных угроз для системы, выполняется анализ рисков и выбор контрмер по уменьшению их влияния.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ И ВЫВОДЫ

1. Несмотря на многообразие стандартов открытых систем, среди них отсутствуют положения, посвященные вопросам безопасности. В связи с этим для классификации открытых систем был использован Приказ № 11462, ФСТЭК №55, ФСБ № 86, Мининформсвязи № 20 от 13 февраля 2008 года «Об утверждении порядка проведения классификации информационных систем персональных данных», который позволил показать что открытые системы попадают под третью и четвертую категории обрабатываемых в информационной системе персональных данных.

2. На основе проведенного анализа различных подходов к оценке защищенности систем делается вывод неэффективности их применения к открытым системам, так как исследуемые методики представляют собой различную интерпретацию результатов экспертных оценок. Предложено разработать комплексную формализованную методику оценки защищенности открытых систем, и в качестве конечного результата, использовать значения рисков информационной безопасности. Такая оценка позволит обоснованно распределить ресурсы и ранжировать угрозы по уровню возможного получения потенциального ущерба.

3. В рамках разработанной методики были получены следующие результаты:

- обоснован выбор SADT/IDEF0 моделирования и аппарата сетей Петри для моделирования ИБ открытых систем, т.к. при этом выборе систему можно изучить в динамике, что позволит получить больше информации об объекте исследования.
- представлен метод, позволяющий преобразовать SADT/IDEF0 модель в модель, описанную в терминах сетей Петри, который дает возможность исследовать систему с точки зрения информационной безопасности;
- разработан метод перехода от имитационной модели, представляющей функциональную сторону открытой системы, к «Сети угроз», направленный на изучение аспектов информационной безопасности исследуемой системы. Разработаны правила имитации «Сети угроз» на языке GPSS.

Эти правила позволят проимитировать работу системы и получить результаты для следующего этапа моделирования;

– предложен метод определения величин рисков для открытых информационных систем. Метод достижения результата основан на обработке данных, извлеченных из имитации модели исследуемой системы, и результатов, полученных от экспертов, т.е. количественных оценок ущерба от реализованных угроз. Для определения достоверности результатов моделирования предложено использовать значения относительных погрешностей искомых оценок рисков информационной безопасности.

4. На основе разработанной методики представлена экспериментально-практическая реализация оценки рисков системы дистанционного обучения, как одного из наиболее ярких примеров открытых систем.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Криволапов, В.Г. Использование SADT – моделирования в системах защиты информации: материалы международной научно – практической конференции «Философия. Культура. Гуманизм: история и современность» / В.Г. Криволапов. – Оренбург: ИПК ГОУ ОГУ. – 2006. – С. 296-298.
2. Криволапов, В.Г. Возможность моделирования систем информационной безопасности на основе сетей Петри / В.Г. Криволапов // Безопасность информационных технологий. –2007. – № 3. – С. 50-51.
3. Криволапов, В.Г. Аспекты безопасности GRID – технологии: сборник научных трудов XIV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы» / В.Г. Криволапов. – М.: МИФИ. – 2007. – С. 80-81.
4. Криволапов, В.Г. Реализация модели системы реагирования на DOS-атаки сетями Петри / В.Г. Криволапов // Безопасность информационных технологий. – 2008. – № 2. – С. 53-56.
5. Криволапов, В.Г. Состояние развития информационных технологий для бизнеса и коммерческого использования / В.Г. Криволапов, М.М. Бикмухаметов // Известия ОГАУ. – 2008. – № 2 (18). – С. 159-163.
6. Криволапов, В.Г. Методика моделирования систем информационной безопасности на основе SADT – моделирования и аппарата сетей Петри / В.Г. Криволапов // Известия ОГАУ. – 2008. – № 3 (19). – С. 175-177.

7. Криволапов, В.Г. Проблемы информационной безопасности дистанционного обучения: сборник научных трудов XV Всероссийской научной конференции «Проблемы информационной безопасности в системе высшей школы» / В.Г. Криволапов. – М.: МИФИ. – 2008. – С. 79-80.
8. Криволапов, В.Г. Обзор защиты информации при «виртуализации основных направлений деятельности человека»: сборник статей XI Международной научно-практической конференции «Проблемы образования в современной России на постсоветском пространстве» / В.Г. Криволапов. – Пенза: ПГТА. – 2008. – С. 221-223.