Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК004.056.5

Гуринович
Андрей Вячеславович

Модели и алгоритмы оценки безопасности облачных услуг

АВТОРЕФЕРАТ
на соискание академической степени
магистра технических наук

по специальности и 1-40 80 05 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Научный руководитель
Глухова Л. А.
к.т.н, доцент

Минск 2014

КРАТКОЕ ВВЕДЕНИЕ

Облачные услуги характеризуются доступностью из любой точки земли и возможностью получить необходимые услуги из кластера вычислительных ресурсов по-требованию. Использование облачных услуг является экономически эффективным и позволяет масштабировать ресурсы следуя за возрастающей нагрузкой. При всех преимуществах облачных услуг, миграция к поставщикам облачных услуг ставит новые вызовы к механизмам обеспечения безопасности.

Существуют стандарты обеспечения безопасности ИС:ориентированные на обеспечение безопасности любых информационных системили только для облачных. Однако, эти стандарты являются массивными, требуют привлечения внешних организаций-аудиторов, требуют создания моделей рисков, не имеют способа получения численной оценки безопасности и не достаточно детализированы для использования этих стандартов для автоматизированной оценки безопасности.

Для преодоления этих недостатков, в данной работе создаются алгоритмы и модели оценки и обеспечения безопасности. Предлагаются новые технические меры контроля и способы получения численной интегральной оценки безопасности облачных услуг.

Для демонстрации возможности автоматизации оценки безопасности облачных услуг, спроектировано ПС выполнения оценки безопасности. Описаны преимущества созданных моделей и алгоритмов оценки безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования.

Целью диссертационной работы является разработка моделей и алгоритмов оценки безопасности облачных услуг для обеспечения их безопасности. Разработанные модели должны быть применимы для организаций любых размеров, любой области деятельности.

Для достижения цели необходимо решить следующие задачи

1. Проанализировать существующие подходы к обеспечению безопасности ИС
2. Определить недостатки существующих моделей и алгоритмов оценки и обеспечения безопасности
3. Синтезировать модели и алгоритмы оценки безопасности, лишенные найденных недостатков

4. Показать применимость разработанных моделей и алгоритмов

Объектом исследования безопасность облачных услуг.

Предметом исследования являются методы и алгоритмы, использующиеся для оценки и обеспечения безопасности облачных услуг.

Основной *гипотезой*, положенной в основу диссертационной работы, является предположение о различии подходов к обеспечению безопасности традиционных и облачных ИС а так же возможность создания численной модели оценки безопасности для организаций любых размеров.

Связь работы с приоритетныминаправлениями научных исследований и запросами реального сектора экономики

Работа выполнялась в соответствии научно-техническими заданиями и планами работ кафедры «Программное обеспечение информационных технологий»:

1. «Разработать модели, методы, алгоритмы для оценки параметров, повышения надежности и качества функционирования аппаратно-программных средств систем и сетей сложной конфигурации и внедрить в современные обучающие комплексы » (ГБ № 11-2004, № ГР 20111065, научный руководитель НИР –В. В. Бахтизин).

Личный вклад соискателя

Диссертация представляет собой самостоятельное исследование, выполненное лично автором. Результаты, приведенные в диссертации, получены соискателем лично.

Вклад научного руководителя Л.А. Глуховой, заключается в формулировке целей и задач исследования.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались и обсуждались на 49 научной конференции аспирантов, магистрантов и студентов «Компьютерные системы и сети» (Минск, Беларусь, 2013); VIII международной научно-методической конференции “Дистанционное обучение – образовательная среда XXI века” (Минск, Беларусь, 2013); VII международной научно-методической конференции “Высшее техническое образование:проблемы и пути развития” (Минск, Беларусь, 2014).

Опубликованность результатов диссертации

По теме диссертации опубликовано 2 печатные работы, из них 2 работы в сборниках трудов и материалов международных конференций.

Структура и объем диссертации

Диссертация состоит из введения, трех глав, заключения, списка использованных источников и приложений. В первой главе представлен анализ предметной области, проанализированы и изучены существующие стандарты в области оценки безопасности облачных услуг, по существующим стандартам, созданы алгоритмы и модели, по которым в стандартах происходит оценка и обеспечивается безопасность. Выявлены существующие проблемы, показаны направления их решения.

Вторая глава посвящена разработке моделей и алгоритмовоценки безопасности облачных услуг. Предложены новые модели безопасности, модели и формулы оценки безопасности, алгоритм обеспечения безопасности.

В третьей главе проанализировано и спроектировано программное средство для автоматизации процесса оценки безопасности облачных услуг и проведено сравнение разработанных моделей и алгоритмов со существующими стандартами.

Общий объем работы составляет 95 страниц, из которых основного текста– 75 страниц, 16 рисунков на 9 страницах, 8 таблиц на 5 страницах, список использованных источников из 33 наименований на 3 страницах и 3 приложения на 9 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ

Во введении определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В первой главеизучены характеристики, отличающие облачные услуги от услуг хостинга и описаны преимущества и вызовы, возникающие при переходе информационных систем в облако. Были описаны предпосылки и возможные причины необходимости управления ИБ. Кратко описаны существующие методы обеспечения безопасности. Указана связь между оценкой безопасности и обеспечением безопасности. Описаны особенности обеспечения безопасности в сфере облачных услуг. Перечислены основные игроки на поле обеспечение безопасности облачных услуг.

Рассмотрены существующие стандарты оценки и обеспечения безопасности ISO/IEC 27001:2013 и FedRAMP, описаны основные этапы развития стандартов. Описаны основные руководящие документы этих стандартов и их назначение. При рассмотрении стандартов проводилась их оценка с выявлением достоинств и недостатков. Сформулированы различные подходы к созданию СУ ИБ. Были перечислены технические меры контроля в стандартах ISO/IEC 27001:2013 и FedRAMP и угрозы безопасности, которые

устраняются техническими мерами этих стандартов. Для стандарта FedRAMP описано взаимодействие различных организаций при сертификации и стандартизации в сфере облачных услуг. Критически оценена возможность использования этих стандартов в частных компаниях и возможные препятствия при реализации. Описаны алгоритмы проведения оценки безопасности. Проанализирован циклический процесс обеспечения безопасности в стандарте ISO/IEC 27001:2013 и соответствующая ему схема Plan-Do-Check-Act и приведены основные методы оценки рисков. Текстовое описание процесса сертификации по стандарту ISO/IEC 27001:2013 представлено в виде алгоритма(блок-схема).

Сформулированы основные недостатки стандартов ISO/IEC 27001:2013 и FedRAMP для оценки и обеспечения безопасности: отсутствие облачной специфики(в стандарте ISO), привязанность к гос. органу FedRAMP(в FedRAMP), необходимость во внешних аудиторах, сложность процесса оценки рисков, недостаточность информации в стандартах для численной оценки безопасности. Поставлена задача по созданию модели и алгоритмов, лишенных данных недостатков.

Во второй главе создана модель безопасности облачных услуг. Она приведена на рисунке 1.

Модель является иерархической и содержит 3 уровня: характеристика – группы – меры. Показана аналогия между характеристикой “защищенность” стандарта SQUARE и характеристикой “безопасность” разрабатываемой модели. В подглавах описаны, как выбранные меры решают конкретные проблемы безопасности и указано соответствие между созданными мерами и мерами стандартов для групп мер “инвентаризация”, “контроль доступа”, “контроль доступности”, “сеть”, “журналирование и мониторинг” и “автоматизация”.

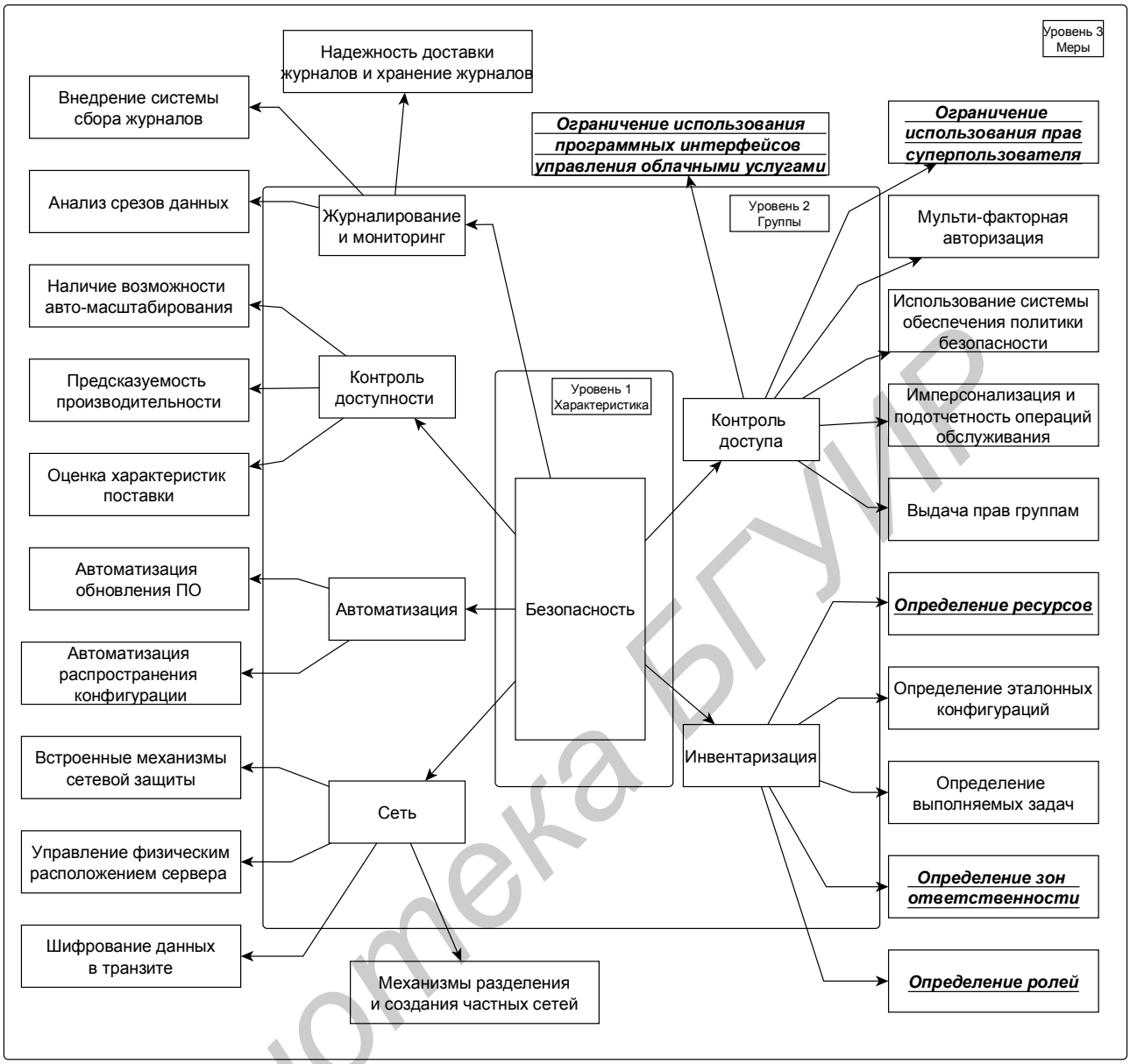

Рисунок 1 – Модель безопасности облачных услуг

Создана модель оценки безопасности облачных услуг, введено понятие обязательных и необязательных мер.Для получения численной оценки использована методика средневзвешенных значений, аналогичная методике оценки качества ПС, определенной в стандарте ГОСТ 28195-89. Приведены формулы для вычисления показателей мер, интегральных показателей групп контроля и общей оценки безопасности системы. Создана модель оценки безопасности облачных услуг(диаграмма IDEF0), где описаны шаги, предпринимаемые для получения оценки безопасности.Алгоритм оценки безопасности приведен на рисунке 2. Модель оценки приведена на рисунке 3.

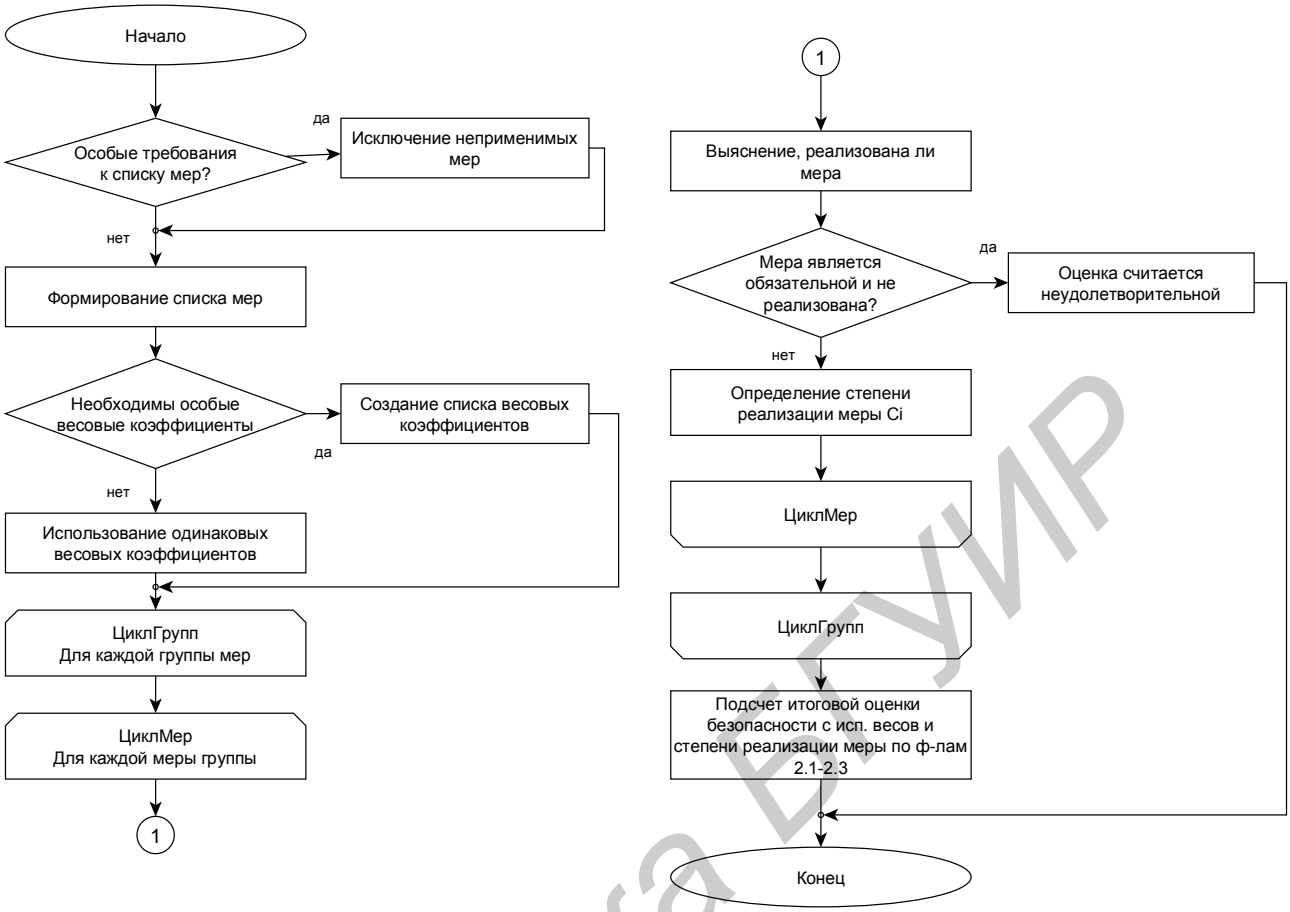

Рисунок 2 – Алгоритм оценки безопасности облачных услуг

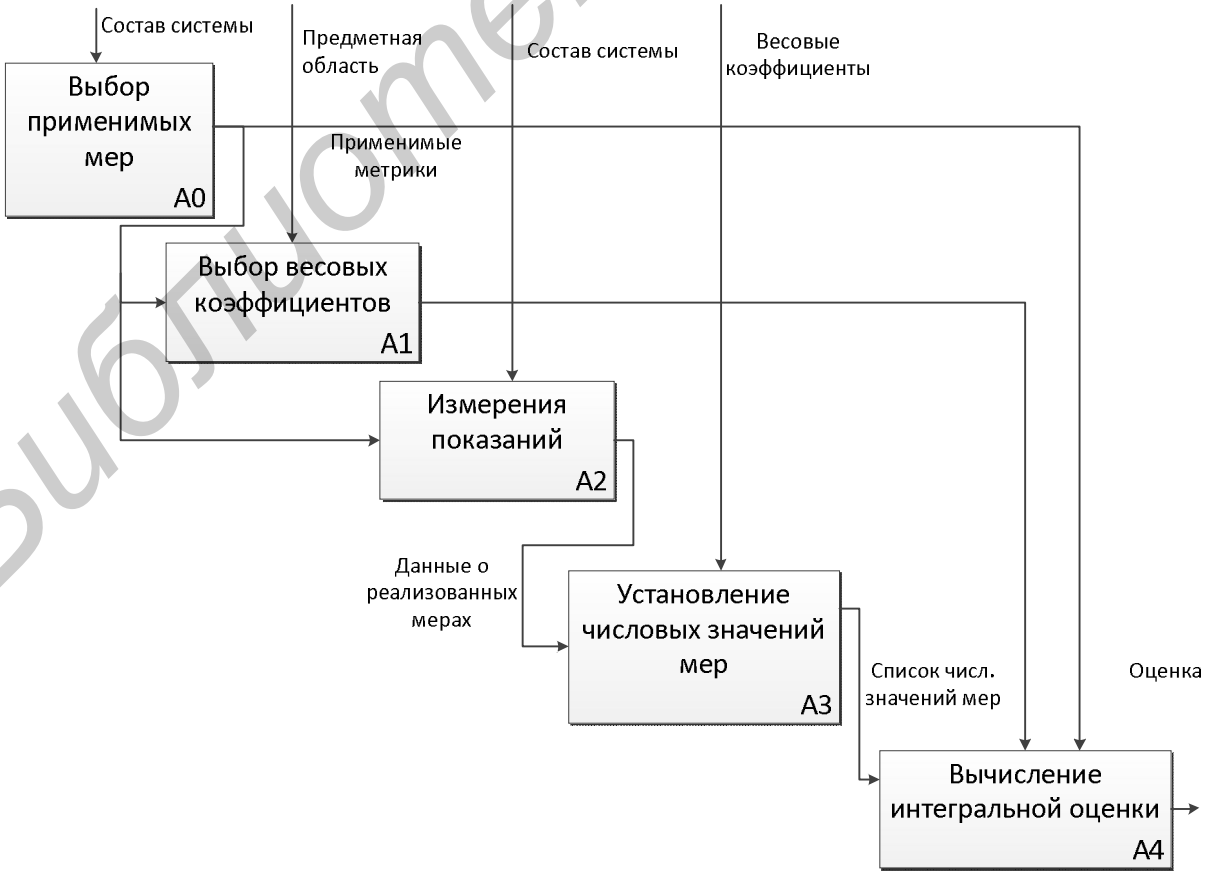

Рисунок 3 – Модель оценки безопасности облачных услуг

Итоговая оценка системы(S) вычисляется исходя из весовых коэффициентов мер(W), весовых коэффициентов групп(X), численных значений контролей(Ci), отражающих степень реализации каждого контроляс учетом наличия нереализованных обязательных мер контроляCo. Итоговая оценка безопасности является числом в диапазоне [0;1], где большему значению соответствует большая безопасность системы.

$$A_i = \frac{C_i W_i}{\sum_n W_n} \quad (1)$$

$$B_j = \frac{X_j \sum_i A_i}{\sum_n X_n} \quad (2)$$

$$S = \begin{cases} 0, \text{при } \sum C_o > 0 \\ \sum_j B_j, \text{при } \sum C_o = 0 \end{cases} \quad (3)$$

Разработан алгоритм обеспечения безопасности облачных услуг. В алгоритме используется предопределенный процесс оценки безопасности, описанный в модели оценки, детализируются мероприятия, происходящие до и после оценки безопасности. Алгоритм является итеративным и не имеет условия окончания.Алгоритм представлен на рисунке 4.

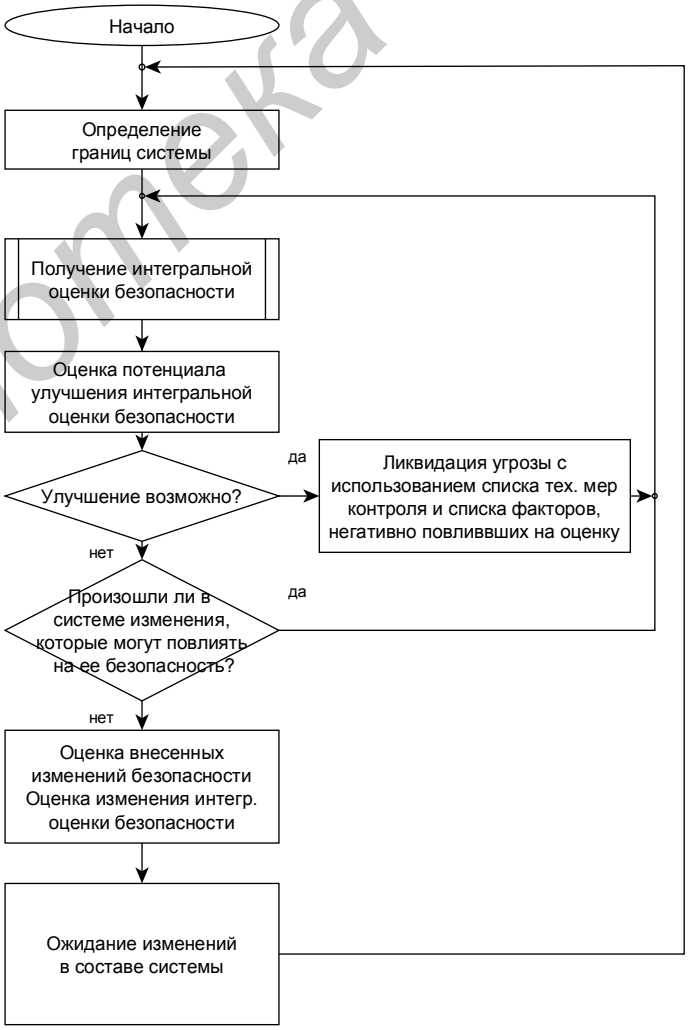

Рисунок 4 – Алгоритм обеспечения безопасности облачных услуг

В третьей главе производится моделирование предметной области оценки безопасности облачных услуг и формируются требования к ПС оценки облачных услуг. На основе сформированных требований и модели предметной области, сформирована структурная модель ПС, представленная в виде диаграммы классов.

Произведена сравнительная оценки существующих и разработанных моделей и алгоритмов, в таблице сведены наиболее важные различия моделей и алгоритмов оценки безопасности по стандартам и по моделям и алгоритмам, разработанным в данной работе.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложена модель безопасности облачных услуг, представляющая собой иерархическую структуру трех уровней вложенности (характеристика–группы–меры). Разработанные новые технические меры контроля и использованы существующие меры описанные в стандартах ISO 27001:2013 и FedRAMP. Предложенная модель специфична для облачных услуг.
2. Разработана модель процесса оценки безопасности облачных услуг, состоящая из шагов выбора применимых мер, выбора весовых коэффициентов, измерения показаний системы, определены числовых значений этих показаний и вычисления итоговой(интегральной) оценки.
3. Разработаны алгоритмы оценки и обеспечения безопасности облачных услуг, использующие разработанную модель процесса оценки безопасности облачных услуг для отслеживания прогресса задачи обеспечения безопасности.
4. Смоделирована предметная область оценки безопасности облачных услуг. С использованием модели оценки безопасности облачных услуг спроектировано ПС для выполнения оценки. ПС оценки безопасности облачных услуг разработано и представлено в приложении.
5. Произведено сравнение моделей определенных в существующих стандартах безопасности и разработанной модели, показано, что созданная модель решает поставленные задачи.

Рекомендации по практическому использованию результатов

1. Разработанные алгоритмы и модели могут использоваться для оценки безопасности используемых облачных услуг(как части обеспечения безопасности) организациями любых форм собственности и размеров.

2. Модели и алгоритмы разработаны таким образом, чтобы оценка могла быть осуществлена техническим специалистом. Из модели сознательно исключены нетехнические аспекты безопасности(такие, как определение контрактных обязательств). При необходимости создания всеобъемлющей системы управления информационной безопасностью(СУ ИБ), новые меры разработанной модели можно комбинировать с стандартами в области СУ ИБ.

3. Реализованное ПС оценки безопасности облачных услуг позволяет систематизировать процесс оценки безопасности. В ПС присутствуют механизмы продолжения работы над ранее произведенной оценкой, что позволяет работать над оценкой итеративно, что может быть удобно при использовании алгоритма обеспечения безопасности облачных услуг.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Гуринович, А.В. Обеспечение безопасности обучающих систем при использовании облачных технологий / А.В. Гуринович, Л.А. Глухова // Материалы VII международной научно-методической конференции “Высшее техническое образование:проблемы и пути развития” . – 2014. – с. 142.

2-А. Гуринович, А.В. Обеспечение безопасности дистанционного обучения при использовании СДО moodle / А.В. Гуринович, Л.А. Глухова // Материалы VIII международной научно-методической конференции “ДИСТАНЦИОННОЕ ОБУЧЕНИЕ – ОБРАЗОВАТЕЛЬНАЯ СРЕДА XXI ВЕКА”. – 2013. – с. 173-174.