УДК 004.891.2

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ЭКСПЕРТНОЙ ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ

О. А. Антамошкин, Г. А. Пузанова, В. В. Онтужев

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Россия, Красноярск, просп. им. газ. «Красноярский рабочий», 31.
E-mail: puzanova679@gmail.com

Рассматриваются критические аспекты системы экспертной оценки информационной безопасности в организациях, проводится сравнительный анализ возможных архитектур системы, классификация основных областей информационной безопасности, которые обрабатывает система, описываются основные функции, подсистемы и пользовательские прецеденты рассматриваемой системы экспертной оценки. Выявлено, что архитектура Web-приложения является оптимальной для разрабатываемой системы. Выделены уровни информационной безопасности, оцениваемые в системе: физический, инфокоммуникационный, процедурный административный уровень, анализируемые в контексте важных информационных активов организации. Всего спроектировано 4 основные функции и 6 подсистем экспертной системы.

Ключевые слова: информационная безопасность, архитектура, экспертная система, прецеденты, функции.

DESIGN FEATURES OF THE COMPUTER-AIDED SYSTEM OF ENTERPRISE INFORMATION SECURITY EXPERT ASSESSMENT.

O. A. Antamoshkin, G. A. Puzanova, V. V. Ontuzhev

Siberian State Aerospace University named after academician M. F. Reshetnev
31 “Krasnoyarskiy Rabochiy” prosp., Krasnoyarsk, 660014, Russia.
E-mail: puzanova679@gmail.com

The article considers the critical aspects of design of the computer-aided system of the enterprise information security expert assessment, along with comparative analysis of the possible system architecture, classification of the major areas of information security, which are handled by the system and describes the key features, subsystems and custom use cases of the system. It was revealed that the architecture of Web-based applications is optimal for the system being developed. The levels of information security assessed with the system, such as: physical, ICT, administrative procedural level are analyzed in the context of important information assets of a certain enterprise. The authors designed four main functions and six subsystems of the expert system.

Keywords: information security, architecture, expert system, use cases, functions.

В современной экономической ситуации представляется целесообразным создание системы экспертной оценки информационной безопасности в организациях (СЭОИБО). Данная система предназначена для проведения экспертной оценки защищенности предприятий малого и среднего бизнеса и других организаций аналогичного масштаба. Особенностью эксплуатации данной системы является ее применение в организациях пользователями, не имеющими специальных знаний в области информационной безопасности.

В силу приведенных свойств, на начальном этапе проектирования системы особое внимание уделяется таким вопросам, как: выбор оптимального типа архитектуры, определение уровней анализа и их приоритетности, разработка концепции алгоритма экспертной системы.

Целью данного исследования является пошаговое определение и обоснование приведенных выше критических аспектов проекта экспертной системы оценки информационной безопасности в организациях.

Выбор системной архитектуры. Разработка экспертной системы, как правило, предполагает создание базы знаний. В контексте СЭОИБО необходимо предусмотреть возможность сохранения введенных пользователем данных для будущего использования и статистической обработки.

При проектировании СЭОИБО рассмотрено три варианта системной архитектуры с использованием баз данных: локальное однопользовательское приложение со встраиваемой системой управления базой данных, приложение для использования на локальном сервере конкретной организации, Web-приложение, единое для всех пользователей.

В локальном приложении работа с базой данных скрыта от пользователя, доступ к ней вне приложения невозможен, что обеспечивает необходимый уровень абстракции. Вся работа по вводу данных осуществляется с одной рабочей станции.

Плюсами локальной архитектуры являются:

– отсутствие необходимости передачи данных по сети, следовательно, большая защищенность данных;

– простая установка программы;

– низкая вероятность стороннего доступа к базе знаний;

– возможность работать на компьютере, изолированном от сетей передачи данных;

– абстракция архитектуры – наличие базы данных полностью срыто от пользователя.

В контексте разрабатываемой системы локальная архитектура имеет следующие недостатки:

– невозможность сбора статистики у пользователей для дальнейшего совершенствования алгоритмов экспертной оценки;

– сложность осуществления экспертизы с привлечением нескольких сотрудников организации, имеющих наиболее достоверные сведения в каждой из анализируемых сфер деятельности организации, таких, как управление персоналом и применяемые информационные технологии;

– сложность массового обновления программы при улучшении ее алгоритмов;

– сложность обеспечения кроссплатформенности приложения;

– необходимость предусматривать дополнительные меры контроля количества установленных экземпляров приложений.

Основное препятствие при применении данной архитектуры – отсутствие многопользовательского режима, препятствующее участию в экспертизе нескольких сотрудников, а единственный пользователь, ответственный за экспертную оценку, как правило, не обладает всеми необходимыми сведениями для ее проведения. Время, затраченное на получение всей необходимой информации, значительно уменьшит скорость работы с системой.

Архитектура локального серверного приложения предполагает установку на один сервер многопользовательского приложения, содержащего в себе систему управления базой данных и систему обработки данных, в которой реализован экспертный анализ. Все функции интерфейсной подсистемы выполняют клиентские приложения, которые будут устанавливаться на произвольное количество рабочих мест организации. Доступ к серверу может осуществляться либо по локальной вычислительной сети, либо через сеть связи общего пользования.

У данной архитектуры было выявлено одно основное преимущество – возможность работы нескольких пользователей с одним набором данных. Это позволит отразить несколько взглядов на защищенность организации в одной экспертизе, что существенно повысит достоверность экспертиз.

Недостатками такой архитектуры являются:

– сложность установки программы для неопытных пользователей;

– основная нагрузка по обеспечению безопасности передачи данных ложиться на организацию – пользователя системы;

– необходимость организации сервера;

– требования к производительности сервера приложения влекут за собой высокая стоимость оборудования;

– как правило, поддержка данной конфигурации требует отдельного специалиста – системного администратора;

– сложность обеспечения непротиворечивости данных у приложения-клиента и сервера;

– пользователь должен иметь канал связи с достаточной пропускной способностью;

– сложность массового обновления программы из-за распределенности приложения;

– необходимость при разработке обеспечить поддержку различных операционных систем у клиента и сервера;

– необходимость дополнительных мер контроля количества установленных экземпляров, как программы-сервера, так и программы-клиента;

– усложнение разработки из-за необходимости учитывать особенности и клиент-серверной и трехуровневой архитектур приложений.

В силу приведенных выше недостатков, данная архитектура не отвечает задачам системы, поэтому не может быть применена при ее создании.

Еще один вариант, это классическую трехуровневую архитектуру Web-приложение.

У архитектуры Web-приложения можно назвать такие достоинства, как:

– наибольшая простота доступа пользователя к ресурсам системы;

– любое усовершенствование системы сразу доступно всем пользователям;

– введенные данные с разрешения пользователя можно анонимно использовать для анализа и дальнейшего совершенствования алгоритма экспертных оценок;

– полностью прозрачная архитектура системы для разработчика, при этом ее особенности скрыты от пользователя;

– возможность доступа к системе с различных устройств и систем;

– максимальное обеспечение целостности и непротиворечивости данных;

– скорость формирования экспертных оценок и других действий не зависит от аппаратного обеспечения пользователя;

– низкие требования к пропускной способности канала связи пользователя, так как передаются только зашифрованные текстовые данные небольшого объема;

– пользователю не нужно принимать меры для обеспечения защищенности своих данных в системе;

– полный контроль за количеством организаций, использующих систему, и частотой экспертиз;

– возможность предоставления пользователю постоянно обновляемой дополнительной информации по обеспечению информационной безопасности бизнеса.

При рассмотрении данной архитектуры, необходимо учитывать следующие недостатки:

– необходимость обеспечить защиту данных при их хранении и передаче;

– обеспечение параллельной работы большого количества пользователей;

В результате проведенного анализа, выявлено, что архитектура Web-приложения является оптимальной для разрабатываемой системы.

В качестве клиента Web-приложении выступает браузер, в качестве сервера баз данных – одна из существующих систем управления базами данных, в качестве сервера приложений система экспертной оценки

Выбор системы управления базой данных и языка логики приложения. База данных должна совмещать в себе функции базы знаний (хранить данные, необходимые для оценки и правила их обработки), хранилища данных, введенных пользователями, а так же конфигурационных и других данных, необходимых для организации работы Web-приложения [1].

Для того чтобы компенсировать недостатки, найденные при анализе данной архитектуры, необходимо применить шифрование данных AES, зашифрованный протокол передачи данных через Web-узел, защиту от внедрения SQL кода (SQL injection) и межсайтового скриптинга (Cross Site Scripting, XSS).

Был проведен анализ возможных средств реализации данной архитектуры, в том числе системы управления базами данных Fifebird.

Многоверсионная архитектура, являющаяся несомненным преимуществом Firebird, обеспечивает параллельную обработку аналитических и оперативных запросов, следовательно, что читающие и пишущие обращения к базе не блокируют друг друга [2].

Для создания логики приложения была осуществлена подборка языка программирования, оптимального для решения задач СЭОИБО [3].

Преимуществами языка Web-разработки PHP является его традиционность; простота; эффективность; безопасность; гибкость.

Таким образом, для реализации системы выбрана система управления базами данных Firebird и скриптового языка программирования общего назначения PHP.

Создание алгоритма экспертной оценки. Информационная безопасность организации – обширная область для анализа, следовательно, для реализации алгоритма экспертной оценки, необходимо ее разбиение на более короткие области.

В базовой модели угроз безопасности персональных данных ФСТЭК России выделяет 5 различных уровней функционирования информационных систем защиты персональных данных: аппаратный уровень, на уровень микрокодов и драйверов устройств, уровень операционной системы, уровень прикладного программного обеспечения, уровень функционирования каналов передачи данных и линий связи [4].

Еще одна распространенная классификация уровней информационной безопасности – выделение законодательного, административного, процедурного программно-технического уровней [5]. Законодательный уровень является важнейшим для обеспечения информационной безопасности. На законодательном уровне особого внимания заслуживают правовые акты и стандарты.

Главная задача мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

К процедурному уровню относятся меры безопасности, реализуемые людьми.

Программно-технический уровень направлен на контроль компьютерных сущностей – оборудования, программ и/или данных, образуют последний и самый важный рубеж информационной безопасности.

В соответствии с нормами ГОСТ выделяются следующие уровни информационной безопасности: управление информационной безопасностью, организационно-административный, безопасность инфокоммуникационной структуры, безопасность услуг, сетевая безопасность, физическая безопасность [6]. Описанные уровни могут быть объединены в три укрупненных уровня: организационный, организационно-технический, технический [7].

В силу специфики разрабатываемой СЭОИБО, ни одна из приведенных классификаций не является оптимальной, так как они не отражают особенностей систем информационной безопасности небольших организаций.

Обобщая существующие сведения, можно выделить следующие уровни информационной безопасности (рис. 1): Физический уровень, Сетевой уровень, Инфокоммуникационный уровень, объединяющий в себе программно-технические методы и средства защиты информации, процедурный уровень административный уровень – действия общего характера, предпринимаемые руководством организации, программу работ в области безопасности (политика безопасности) и обеспечение ее выполнения.

При экспертной оценке информационной безопасности целесообразно начинать с физического уровня, и далее продвигается до наиболее абстрактных уровней. Это необходимо, во-первых, в силу существующей во многих организациях ситуации халатного отношения к аппаратному обеспечению, а, во-вторых, реализация уязвимостей этого уровня может принести наибольший финансовый вред организации.

Последние три уровня (инфокоммуникационный, процедурный, административный) целесообразно рассматривать с точки зрения важных информационных активов организации. Это даст пользователям СЭОИБО уверенность в том, что предложенные экс-

пертной системой рекомендации помогут организации защитить наиболее ценную информацию и поможет учесть при экспертной оценке индивидуальные особенности каждой конкретной организации.

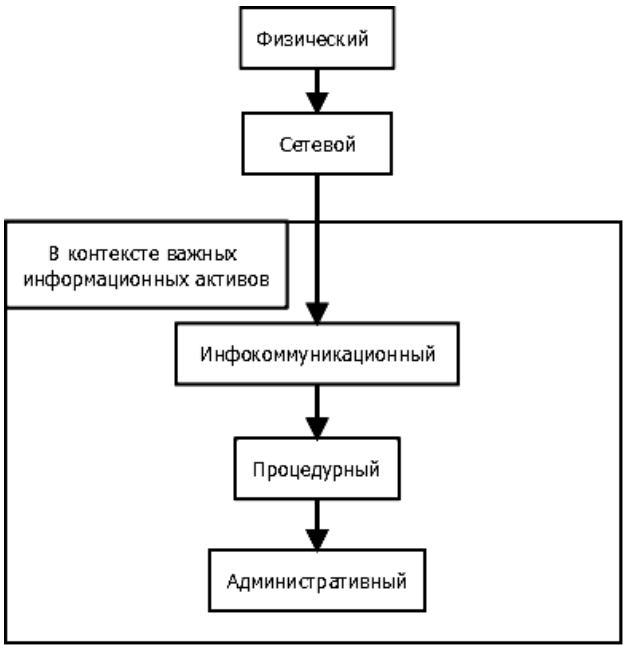

Рис. 1. Последовательность оценки информационной безопасности в системе

Проектирование функций системы СЭОИБО.

1. Формирование гибкого списка критериев оценки в соответствии с особенностями предприятия.

2. Формирование экспертных оценок информационной безопасности организаций. Формирование экспертных оценок производится при помощи сочетания четкой и нечеткой логики, за основу алгоритма взяты методики оценки соответствия СТО БР ИББС-1.2-2010 [8], комбинированный подход [9], NIST [10].

3. Ведение базы состояния информационной безопасности. По желанию пользователей может производиться сохранение введенных параметров оценки для ведения статистики и мониторинга изменений в будущем.

4. Формирование рекомендаций по улучшению информационной безопасности Основа для подбора рекомендаций – стоимостная оценка реализации угроз ценным информационным активам организации. Данный показатель будет рассчитываться с использованием экспертных знаний и сведений об информационных активах, полученных от пользователей СЭОИБО.

Для оптимальной реализации описанных функций, система разделяется на 6 подсистем: доступа к базе данных, управления правами доступа, пользовательского интерфейса, управления критериями, генерации оценок, генерации рекомендаций.

Выделены основные варианты использования (use case) системы с точки зрения пользователя (рис. 2).

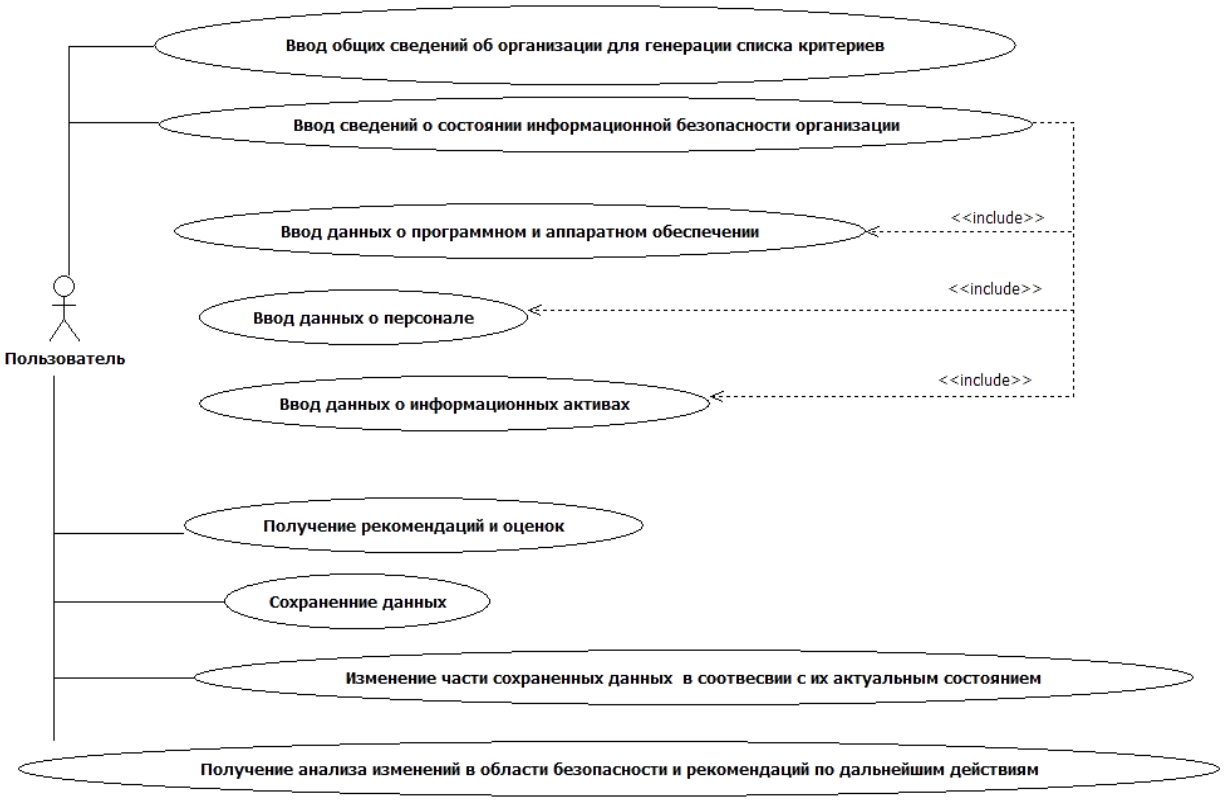

Рис. 2. Варианты использования экспертной системы

Прецеденты, включенные (include) прецедент «Ввод сведений о состоянии информационной безопасности организации» разделены по тематике вводимой информации. При применении системы в организациях за выполнение каждого прецедента должны отвечать различные сотрудники, так как каждый вариант использования требует специфической компетенции в определенных областях, знания реального положения дел организации в этой сфере.

Вариант использования «Ввод данных о программном и аппаратном обеспечении» объединяет в себе все технические аспекты защищенности информации. Это одна из важнейших сфер обеспечения информационной безопасности в организациях. Так в списке уязвимостей ГОСТ 13335–3 14 из них касаются аппаратного обеспечения, а 22 – программного [9].

В ходе проведенного исследования было выявлено, что архитектура Web-приложения, реализованная средами системы управления базами данных Firebird и языка программирования PHP, является оптимальной для разрабатываемой системы.

Были выделены следующие уровни информационной безопасности, оцениваемые в системе: физический, инфокоммуникационный, процедурный административный уровень, анализируемые в контексте важных информационных активов организации. Также были спроектированы 4 основные функции СЭОИБО, 6 подсистем и варианты ее использования с пользовательской точки зрения.

Библиографические ссылки

1. Оптимизация настроек систем управления базами данных / С. Н. Ежеманская, И. В. Ковалев, А. В. Прокопенко, Р. Ю. Царев, Е. В. Гражданцев // Программные продукты и системы. 2008. № 2 (82). С. 54–56.

2. Царев, Р. Ю. Среда исполнения мультиверсионного программного обеспечения // Программные продукты и системы. 2007. № 2 (78). С. 29–30.

3. Русаков М. А., Царев Р. Ю. Методы повышения надежности программного обеспечения // В мире научных открытий. 2011. № 8 (20). С. 32–41.

4. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) / Федеральная служба по техническому и экспортному контролю, 2008 [Электронный ресурс]. URL: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god. (дата обращения 14.05.2013).

5. Галатенко В. А. Информационная безопасность грани практического подхода [Электронный ресурс] // Корпоративные информационные системы : конф. М., 1999. URL: http://www.citforum.ru/seminars/cis99/galat2.shtml. (дата обращения 14.05.2013).

6. ГОСТ Р 52448–2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения». М. : Издат. стандартов, 2005.

7. ГОСТ Р 53110–2008 «Система обеспечения информационной безопасности сети связи общего пользования». М. : Издат. стандартов, 2008.

8. Стандарт Банка России СТО БР ИББС-1.2–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» // Вестник Банка России. 2010. № 36–37 (1205–1206).

9. ГОСТ Р ИСО/МЭК 13335-3–2007 «Методы и средства обеспечения безопасности»: Методы менеджмента безопасности информационных технологий. М. : Издат. стандартов, 2007.

10. Руководство по управлению рисками для систем информационных технологий: рекомендации Национального института стандартов и технологий [Электронный ресурс] // Центр компетенции по электронному правительству при Американской торговой палате в России. М., 2003. 1999. URL: http://egov-center.ru/sites/default/files/000077.pdf. (дата обращения 14.05.2013).

References

1. Ezhemanskaya S. N., Kovalev I. V., Prokopenko A. V., Tsarev R. Yu., Grazhdantsev E. V. *Programmnye produkty i sistemy*. 2008, no. 2 (82), p. 54–56.

2. Tsarev R. Yu. *Programmnye produkty i sistemy*. 2007, no. 2 (78), p. 29–30.

3. Rusakov, M. A. *V mire nauchnykh otkrytiy*. 2011, no. 8 (20), p. 32–41.

4. *Bazovaya model' ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh (vypiska)* (The base model of security threats personal data during their processing within the information systems of personal data (extract)). Federal'naya sluzhba po tekhnicheskomu i eksportnomu kontrolyu, 2008, available at: http://fstec.ru/normativnye-i-metodicheskie-dokumenty-tzi/114-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-i-metodicheskie-dokumenty/spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god.

5. Galatenko V. A. *Informatsionnaya bezopasnost' grani prakticheskogo podkhoda* (Information Security faces a practical approach). *Konferentsiya "Korporativnye informatsionnye sistemy"* (Conference on "Corporate Information Systems"), Moscow, 1999, available at: http://www.citforum.ru/seminars/cis99/galat2.shtml.

6. *GOST R 52448–2005 "Zashchita informatsii. Obespechenie bezopasnosti setey elektrosvyazi. Obshchie polozheniya"* (GOST R 52448–2005 "Information Security. Ensuring security of telecommunication networks. General provisions"). Moscow, IPK, 2005, 23 p.

7. GOST R 53110–2008 "Sistema obespecheniya informatsionnoy bezopasnosti seti svyazi obshchego pol'zovaniya" (GOST R 53110–2008 "Information security system of of public communication network"). Moscow, IPK, 2008, 19 p.

8. *Vestnik Banka Rossii*. 2010, no. 36–37 (1205–1206).

9. *GOST R ISO/MEK 13335-3–2007 "Metody i sredstva obespecheniya bezopasnosti": Metody menedzhmenta bezopasnosti informatsionnykh tekhnologiy* (GOST R ISO / IEC 13335-3–2007 "Methods and tools to ensure security": Methods for Management of Information Technology Security). Moscow, IPK, 2007, 49 p.

10. *Rukovodstvo po upravleniyu riskami dlya sistem informatsionnykh tekhnologiy: Rekomendatsii Natsional'nogo instituta standartov i tekhnologiy* (Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology). Moscow, 2003, available at: http://egov-center.ru/sites/default/files/000077.pdf. (14.05.2013)

УДК 621.31:681.5

СТРУКТУРА WEB-СЕРВИСА ДЛЯ МОДЕЛИРОВАНИЯ ЭЛЕКТРИЧЕСКИХ СХЕМ С СУЩЕСТВЕННЫМИ НЕЛИНЕЙНОСТЯМИ

К. В. Богданов, А. Н. Ловчиков

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Россия, Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: 2519869@gmail.com, ivt_anlovch@sibsau.ru

Цель работы заключается в создании программного обеспечения, позволяющего проводить анализ и моделирование в системах с несколькими блоками, обладающими существенной нелинейностью, такими как электронные ключи, например. Сложность создания такой системы заключается в том, что существующие подходы к моделированию предполагают решение системы дифференциальных уравнений, при составлений которой вносятся искусственные ограничения, влияющие на поведение системы непосредственно в моменты переключений. Предлагаемый подход опирается на представление модели не как единой, описываемой одним набором ДУ, а как набора взаимодействующих между собой простых систем. Так как такое моделирование накладывает специфичные требования на оборудование, было выдвинуто предложение разработать данное ПО как систему, работающую в облаке.

Ключевые слова: нелинейные системы, моделировнаие, функциональные языки программирования, облачные сервисы.

STRUCTURE OF SIGNIFICANT NONLINEARITY ELECTRIC CIRCUITS OF THE WEB-SERVICE MODELING

K. V. Bogdanov, A. N. Lovchikov

Siberian State Aerospace University named after Academician M. F. Reshetnev
31 "Krasnoyarskiy Rabochiy" prosp., Krasnoyarsk, 660014, Russia
E-mail: 2519869@gmail.com, ivt_anlovch@sibsau.ru

The objective of the work is the creation of such a software system which will help to analyze and model the systems with multiple blocks bearing the significant nonlinearity (as transistor keys, for example). The complicity of this work is in need of creation of the main system of differential equations for the system as a whole. Such systems of differential equation has some important restrictions that may affect the results of modeling, especially in bifurcation points. We offer a method that represents the system as a number of connected simple subsystems. Each of them has its own math model. This approach impose specific requirements on hardware, so we offer to use the cloud computing to solve this inconvenience.

Keywords: nonlinear systems, modeling, functional programming, cloud computing

Моделирование и анализ работы электронного оборудования – весьма сложная задача, для решения которой активно используется специализированное программное обеспечение – EDA-системы. Развитие таких систем идёт, по большей части, экстенсивным путём, начиная от систем, созданных в 70-ых годах прошлого столетия. Как правило, улучшаются пользовательские интерфейсы, расширяются базы данных электронных компонент и т. п., в то время как основные вычислительные алгоритмы остаются прежними.