ОБЕСПЕЧЕНИЕ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ И НАДЕЖНОСТИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

К. Г. Колодий (Иркутск, ИрГУПС)

CORPORATE INFORMATION SYSTEMS FUNCTIONING QUALITY SUPPORT AND RELIABILITY

K.G. Kolodiy (Irkutsk, ISURE)

This article contains possible problems of corporate information systems functioning quality support and reliability. Solution methods used in Unified information system ISURE are shown. Corporate information systems quality improvement recommendations are offered.

В современном информационном обществе невозможно представить крупную организацию не использующую в своей деятельности последние достижения науки в информационных технологиях. Крупные организации в своей структуре имеют различные подразделения и филиалы. Каждое подразделение решает задачи только своей компетенции, но при этом не может функционировать изолированно. Поэтому для повышения эффективности своей работы организации используют крупные корпоративные информационные системы (КИС). Можно выделить два направления автоматизации деятельности крупной организации:

- приобретение и внедрение коммерческих программных продуктов;
- разработка своей собственной КИС.

Приобретение и внедрение таких коммерческих программных продуктов как SAP R/3, MILLENNIUM ERP, ASoft CRM и др. требует не только больших финансовых затрат, но также и квалифицированной поддержки. Поэтому многие организации принимают решение о разработке своей собственной КИС.

Разработка собственной КИС это непрерывный процесс, который прекращается только в случае принятия решения об отказе от использования этой КИС. Это связано с необходимостью периодически адаптировать функциональность КИС к изменяющимся бизнес-процессам организации.

В процессе эксплуатации собственной КИС возникает необходимость в высоком качестве функционирования, надежности и защищенности информационной системы. Для эффективного решения этих задач, необходимо в процессе разработки КИС выполнять следующее:

- документировать все требования;
- придерживаться принятых стандартов разработки программного обеспечения;
- документировать код;

- инспектировать код;
- проводить тестирование.

Рассмотрим как решаются эти задачи, на примере Единой информационной системы (ЕИС) Иркутского государственного университета путей сообщения (ИрГУПС). ЕИС ИрГУПС представляет собой веб-систему с единой базой данных и различными интерфейсами для подразделений (рисунок 1). ЕИС взаимодействует с другими специализированными программными средствами, например: программное обеспечение 1С, используемое в бухгалтерии, система формирования нагрузки и расписания, система дистанционного обучения и др. ЕИС в своей архитектуре использует SOAP-сервер, который работает с единой базой данных. Подсистемы ЕИС обращаются к SOAP-серверу для чтения и сохранения данных. Взаимодействие со сторонними программными система также происходит посредством вызова SOAP-функций [1].

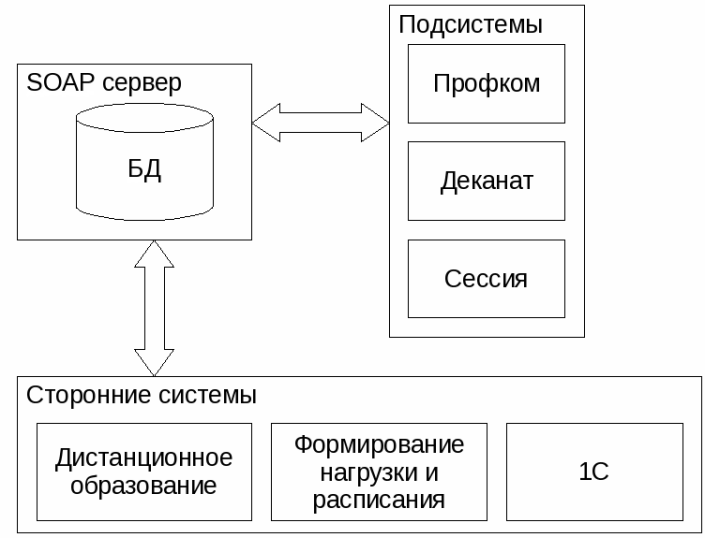

Рисунок 1. Упрощенная схема ЕИС

Первое что необходимо для повышения качества любой разрабатываемой программной системы — это документирование процесса разработки. Требования собираются посредством анкетирования подразделений или на основании рапортов и заявок по расширению функциональности, а также проводятся совещания с сотрудниками подразделений. Все требования к ЕИС формализуются и записываются с использованием унифицированного языка моделирования UML. Это позволяет проводить проверку после реализации новой функциональности на соответствие первоначальным требованиям.

Также в отделе, который занимается разработкой ЕИС, приняты правила по оформлению исходного кода:

- использование комментариев с указанием авторства и назначения модуля;

- использование комментариев для пояснения логики алгоритмов;
- использование названий переменных, упрощающих понимание алгоритма;
- использование отступов для упрощения восприятия блоков кода;
- и др.

Имеется документ, регламентирующий то, как обрабатывать данные поступающие от пользователя, прежде чем их использовать в алгоритме, как формировать динамические запросы, как обрабатывать результаты запросов, как обрабатывать ошибки, возникающие при выполнении алгоритма и др. Так как ЕИС это веб-система, то имеются определенные требования к коду, который исполняется на стороне клиента (в браузере). HTML, JavaScript и другой код по возможности должен выполняться одинаково в различных браузерах без использования дополнительно устанавливаемых плагинов. Выполнение данных требований позволяет изначально писать достаточно качественный программный код, который выполняет требуемую функциональность, при этом защищен от большинства уязвимостей характерных для веб-систем (например: SQL Injection [2]) и легко сопровождаем.

Инспектирование документации и исходного кода существенно влияет на качество программы. При разработке ЕИС инспектирование проводиться одним сотрудником отдела разработки по личной просьбе другого. Первые версии некоторых подсистем разрабатывают студенты университета в рамках прохождения производственной практики. Эти подсистемы проходят обязательное инспектирование сотрудниками отдела разработки. Обнаруженные ошибки могут быть занесены в систему командной работы Tutos.

Внесение изменений в веб-систему сразу отражается на ее работе, поэтому проводить отладку и тестирование на эксплуатируемой системе нельзя. Для разработки ЕИС были созданы тестовые версии подсистем в окружении приближенном к окружению эксплуатируемой ЕИС. Обновление эксплуатируемой системы происходит только после того как в тестовой версии проведены соответствующие испытания. Для быстрой разработки и отладки у каждого разработчика локально установлены тестовые версии подсистем, которые он разрабатывает и сопровождает. Эксплуатируемая и тестовая системы имеют свои базы данных. К базе данных эксплуатируемой системы доступ для внесения изменений в структуру имеет только один человек. К тестовой базе данных доступ имеется у каждого разработчика. Периодически структура тестовой базы данных заменяется структурой базы данных эксплуатируемой системы. Это позволяет избежать различий между базами данных эксплуатируемой и тестовой ЕИС. Такой подход организации разработки и тестирования позволяет обеспечивать надежность функционирования ЕИС.

Так как в основе системы лежит SOAP-сервер с функциями, то правильности функционирования этих функций уделено особое внимание. При написании функции

разработчики проводят отладку и тестирование. Затем с определенной периодичностью все существующие функции проходят тестирование в автоматическом режиме. Для этого была создана система тестирования функций [3]. Тестирование проводится по принципу черного ящика, когда задаются входные воздействия, а ожидаемый результат сравнивается с получаемым. Обнаруженные ошибки автоматически фиксируются в системе командной работы Tutos. Автоматическое тестирование SOAP-функций позволяет оперативно выявлять ошибки, которые могут возникать из-за изменений в других частях системы.

Разработка и отладка веб-интерфейса пользователя проводиться на локальных компьютерах программистов. Окончательное тестирование проводится вручную силами всех свободных разработчиков на момент внедрения подсистемы. Проверяется корректность отображения HTML кода в различных браузерах, правильность выполнения JavaScript и работоспособность всех гиперссылок подсистем.

В ЕИС пользователи оперируют с конфиденциальными данными, поэтому проблеме обеспечения безопасности уделено особое внимание. Для решения этой задачи используются различные методы и средства защиты информации.

Во-первых, адреса баз данных и SOAP-серверов известны только разработчикам и доступны только из локальной сети университета. Сканирование и перехват данных (пароли, личные сведения и др.) в коммутируемых сетях, какой является сеть университета, практически невозможно.

Во-вторых, периодически производиться сохранение копий баз данных и скриптов ЕИС. Это позволяет в случае сбоев (аварийное отключение электропитания, некорректные действия пользователей и разработчиков, действия злоумышленника и др.) восстанавливать актуальное состояние баз данных и подсистем.

В-третьих, в ЕИС реализована политика безопасности избирательного управления доступом на основе ролей. Каждый пользователь имеет доступ только к определенным ресурсам, которые необходимы ему для выполнения своих служебных обязанностей. При этом все действия пользователя журналируются.

Использование принятых стандартов кодирования в отделе по разработке ЕИС, позволяют гарантировать некоторый уровень защищенности. Однако программирование наиболее подвержено человеческому фактору, а это значит, что программист может написать код не производящий необходимые проверки входных данных или код, использующий большие вычислительные мощности, и тем самым подверженный DoS атакам и др. Проведение тестирование подсистем на наличие таких ошибок зачастую не проводится, а если проводится, то в ручную и не гарантирует необходимый уровень покрытия тестами.

В работе «Анализ защищенности web-сервисов» [4] автором была проведена оценка

рисков угроз SOAP-сервера ИрГУПС и рассчитана эффективность контрмер. Результаты показали важность SOAP-сервера для ЕИС и хорошую эффективность используемых мер защиты.

Приведем рекомендации, которые позволят повысить, численно оценивать и контролировать уровень качества ЕИС:

- внедрить обязательную процедуру инспектирования новых и измененных модулей;
- внедрить средство для автоматической проверки работоспособности гиперссылок;
- внедрить средство для автоматической проверки данных получаемых от пользователя на подверженность атакам злоумышленника;
- внедрить средство для автоматизации тестирования нагрузки;
- внедрить обязательную фиксацию всех ошибок в системе командной работы Tutos;
- внедрить процедуру замера метрик и расчета качества кода;
- внедрить процедуру оценки рисков и эффективности контрмеры.

ЛИТЕРАТУРА

1. Арбатский Е.В. Использование SOA при создании корпоративной информационной системы на примере единой информационной системы Иркутского Государственного Университета Путей Сообщения // Труды XII Байкальской Всероссийской конференции «Информационные и математические технологии в науке и управлении». Иркутск. 2007. часть II. с. 65-72.

2. Threat Classification. Официальный сайт Web Application Security Consortium [Электронный ресурс] — http://www.webappsec.org/projects/threat/

3. Система тестирования функций: Св. об офиц. рег. прогр. для ЭВМ №2008611205, Россия // ГОУВПО ИрГУПС (ИрИИТ); Колодий К.Г., заявл. 26.11.2007, зарег. 07.03.2008.

4. Колодий К.Г. Анализ защищенности web-сервисов. // Современные технологии. Системный анализ. Моделирование. ИрГУПС. - 2009. - № 1. С.141-145.