УДК 681.513

А.Л. ЛЯХОВ, С.В. ВЕРЁВКИН

Полтавский национальный технический университет им. Ю. Кондратюка, Украина

НАДЁЖНОСТЬ СИСТЕМ МОНИТОРИНГА ДЕЯТЕЛЬНОСТИ УЧЕБНЫХ ЗАВЕДЕНИЙ

Исследованы вопросы надежности автоматизированных систем мониторинга деятельности учебных заведений.

мониторинг, надежность, безотказность, работоспособность, защищённость, безопасность

Введение

Высококачественное современное образование и специалист с высоким уровнем квалификации являются одними из основных факторов конкурентоспособности, экономической и национальной безопасности государства.

Именно поэтому Украина определила новую стратегию реформирования системы образования как обеспечение государственных гарантий равного доступа всех граждан к качественному образованию на разных этапах обучения и организацию научного аналитического сопровождения всех управленческих решений.

Составной частью комплекса мероприятий, выполняемых Государственной инспекцией учебных заведений МОН Украины в рамках этой стратегии, является создание национальной автоматизированной системы мониторинга деятельности учебных заведений Украины (АСУ «Рейтинг» [1 - 3]).

Программная часть АСУ «Рейтинг» проектируется и разрабатывается в научно-исследовательской лаборатории проблем прикладного программного обеспечения Полтавского национального технического университета имени Юрия Кондратюка. Архитектура, свойства и принципы управления системы описаны в работе [4], а также в руководстве пользователю [5].

Учитывая важность задачи мониторинга системы образования для Украины, естественно возникает вопрос, в каком смысле и в какой степени такая система должна быть надёжной?

Требования к надёжности информационных систем определяется, прежде всего, их функциональным предназначением.

Существующие системы мониторинга деятельности учебных заведений можно разделить на глобальные, национальные, региональные и локальные. Типичными примерами подобных систем являются: UNESCO EFA Global Monitoring Report [6], проект New Zealand National Education Monitoring Project [7], национальная программа США [8], а также Южно-уральский региональный центр мониторинга системы образования [9] и система мониторинга качества обучения, например, Национального педагогического университета имени М.П. Драгоманова [10].

В месте с тем анализ показывает, что вопросы надёжности подобных систем исследованы совершенно не достаточно.

Данная работа посвящена надёжности программных компонент систем мониторинга.

Анализ требований к надёжности систем мониторинга деятельности учебных заведений

Функциональные спецификации системы мониторинга следующие:

– правильный ввод и обработка данных;

– табличное и графическое представление результатов;

– непрерывность мониторинга;

– иерархия администрирование;

– простой и удобный интерфейс пользователя;

– свободный доступ пользователей к данным и элементам управления в соответствии иерархии полномочий;

– хранение и сохранение данных.

Надёжность систем мониторинга рассматривается нами как функциональная надёжность по таким составляющим [11].

1. ***Работоспособность*** – это обеспечение непрерывности сервисов (непрерывность мониторинга). Непрерывность обеспечивается работоспособностью таких подсистем:

– операционная система. Это может быть UNIX-подобные системы (Linux, FreeBSD, SunOS, HP- UX и другие) или Windows системы (Windows 2003 Server, Windows 2000 Server, Windows NT, Windows XP и другие);

– веб-сервер - серверный программный продукт, обеспечивающий непосредственное функционирование веб-приложений, обработку запросов, выдачу графических файлов и HTML-страниц пользователям;

– рабочая среда программных компонент (компилятор языка программирования PHP, библиотеки функций, которые обеспечивают работу приложений и т.п.);

– база данных – хранилище информации и система обработки SQL-запросов.

Все перечисленные подсистемы являются готовыми компонентами, которые разработаны известными фирмами производителями с учётом существующих стандартов, в частности, по надёжности. Они образуют окружение, обеспечивающее непрерывность всех сервисов соответствии с запросами той программной части, которая создаётся разработчиками системы мониторинга (дальше – «ядро»), чем и обеспечивается её работоспособность.

2. ***Безотказность*** – это способность системы предоставлять именно те сервисы, которые определяются её спецификациями.

Учитывая написанное выше, компоненты, из которых состоит окружение ядра, являются и безотказными.

Вместе с тем, этой безотказностью обуславливается адекватная реакция окружения на все запросы к ядру, в том числе и неправильные («какой запрос – такой ответ»), что может привести к отказу системы мониторинга в целом.

Отказы системы могут быть следствием различных причин. Это ошибки реализации ядра системы мониторинга и ошибки ввода данных.

Ошибки реализации ядра системы мониторинга:

– Некорректная методика расчёта рейтинга учебных заведений;

– Ошибки алгоритма мониторинга;

– Ошибки программной реализации системы мониторинга.

Подобные ошибки в полном объёме очень трудно выявить на этапе проектирования и реализации системы, а также в процессе эксплуатации, т.к. работоспособность может сохраняться.

Локализация и устранение ошибок алгоритма и программной реализации может быть осуществлена известными методами [11, 12].

Ошибки, связанные с некорректностью методики мониторинга в целом, имеют системный характер. Их устранение требует проведение комплекса мероприятий с привлечением специалистов в различных областях: педагогов, работников аппарата управления системой образования (МОН, Государственная инспекция учебных заведений, област-

ные, районные и городские отделы управления), а также научно исследовательских организаций. Их задача – планирование и проведение эксперимента, моделирующего деятельность системы мониторинга, а также интерпретацию результатов мониторинга.

В рамках программы создания системы мониторинга деятельности учебных заведений Украины (АСУ «Рейтинг») [1-5] в настоящее время планируется проведение подобного эксперимента с участием МОН Украины, Национального педагогического университета имени М.П. Драгоманова (Киев), Переяслав-Хмельницкого государственного педагогического университета имени Григория Сковороди, школ и органов управления системы образования Киевской, Полтавской и Ровенской областей, а также разработчиков программного обеспечения (ЛППО кафедры КИТиС Полтавского национального технического университета имени Юрия Кондратюка).

Ошибки ввода данных:

– ошибки ввода запросов пользователем в процессе просмотра результатов мониторинга;

– ошибки ввода в процессе заполнения базы данных;

– ошибочный или злонамеренный ввод запроса в адресною строку браузера [4].

Устойчивость системы по отношению к таким ошибкам фактически означает её защищённость.

3. ***Защищённость*** – свойство программной системы противостоять случайным или намеренным искажением входных данных.

Исходные данные для системы мониторинга обычно вводятся пользователем с помощью специальных программных средств. Ошибки ввода при этом имеют случайный характер, и их полное устранение не представляется возможным. Усилия разработчиков должны быть направлены на разработку средств уменьшающих их количества (дружественный интерфейс, средства синтаксического контроля и т.п.). Программа с помощью которых, осуществляется ввод исходных данных, обычно физически не связана с основной серверной частью. Поэтому эти вопросы здесь не рассматриваются. Они требуют отдельных серьёзных исследований.

Основные типы уязвимостей программных систем с архитектурой клиент-сервер по отношению к злонамеренному вторжению, достаточно хорошо исследованы [13-15].

Серьёзную опасность для Web-приложений представляет так называемый - ***Cross-Site Scripting***. Эта атака основана на внедрении злоумышленном в Web-страницу своих HTML-директив. Благодаря этому часто удается «украсть» конфиденциальные данные пользователя, в том числе пароли, и таким образом получить доступ к информации, изменение которой приведёт к отказу системы.

В частности хакер получает возможность внедрить свой код, ведущий к отказу системой управления Web-страницами.

Не менее опасною для системы мониторинга является атака, известная как ***PHP Source Injection*** или просто ***PHP-инъекция.*** Язык программирования PHP позволяет разработчикам программ внедрять любой PHP-код на серверной стороне системы. В качестве значения аргумента функции include указывается путь к файлу, содержащему полноценный код PHP-программы, Файл может быть размещён на сервере или же на любом удалённом компьютере, в частности, хакера. Таким образом, это конструктивное свойство может быть источником отказов системы.

Еще одним фактором опасности является атака, известная как ***SQL-инъекция.*** Злоумышленники могут изменить параметры, передаваемые серверу, таким образом, что изменится SQL-запрос, и они получают неавторизированный доступ к базе данных. В результате содержимое БД может быть не санкционировано, изменено или даже уничтожено.

Более того, с помощью специальным образом написанного запроса, можно даже получить доступ к окружению ядра.

Все перечисленные причины отказа обусловлены отсутствием контекстной проверки входных данных у интерпретаторов языков высокого уровня.

Возможным подходом к созданию защиты системы от подобных вторжений является разработка на основе спецификаций системы мониторинга массива шаблонов правильных запросов и дополнительного программного модуля, который будет распознавать ошибочные или злонамеренные запросы в потоке входных данных.

4. ***Безопасность.*** Если потеря работоспособности или отказ системы не наносит существенного урона людям или окружающей среде, то её называют *безопасной*.

Систему мониторинга, как было показано выше, можно считать работоспособной, следовательно, основным аспектом обеспечения безопасности является обеспечение отказоустойчивости. Комплекс мер по обеспечению безотказности предложен выше.

Вместе с тем представляет интерес ответ на вопрос, в какой степени система мониторинга образования должна соответствовать требованиям безопасности?

Закономерности развития системы образования могут быть выявлены только в результате длительного мониторинга. Отказы системы мониторинга могут приводить к неэффективным или неправильным управленческим решениям на протяжении длительного периода эксплуатации, последствия которых могут быть очень серьёзными с экономической точки зрения или даже катастрофическими (например, для отдельных учебных заведений и его сотрудников - решение о закрытии и т.п.).

С такой точки зрения, система мониторинга образования действительно является безопасной, но лишь при непродолжительной эксплуатации.

Отказы системы мониторинга образования в процессе долгосрочной эксплуатации могут привести к значительным экономическим потерям и поэтому уровень безопасности системы в целом должен быть достаточно высоким.

Выводы

В данной работе исследованы вопросы надежности автоматизированных систем мониторинга деятельности учебных заведений.

Разработка программного окружения ядра системы мониторинга обеспечивает работоспособность системы в целом.

Надёжность системы мониторинга определяется в основном ее отказоустойчивостью, что можно обеспечить двумя комплексами мер:

– проведение масштабного эксперимента решение, о котором должно приниматься на уровне МОН Украины.

– защищённость ввода данных. Решение этой задачи возможно путём разработки дополнительного программного модуля, с уровнем искусственного интеллекта достаточным для распознавания ошибочных или злонамеренных запросов в потоке входных данных.

Безопасность системы мониторинга обеспечивается степенью ее надежности, т.е., как показано в данной работе – степенью отказоустойчивости.

В процессе долгосрочной эксплуатации отказы системы мониторинга могут приводить к значительным и даже к катастрофическим экономическим последствиям. Следовательно, по степени надежности системы мониторинга образования приближаются к критическим системам.

Литература

1. Указ Президента України від 04.07.05 № 1013/2005 „Про невідкладні заходи щодо забезпечення функціонування та розвитку освіти в Україні”.

2. Доручення Прем'єр-міністра України від 25.07.05 № 34531/2/2-05.

3. Накази Міністерства освіти і науки України від 29.07.05 № 454 та 12.08.05 № 473.

4. Бурлаков О.М., Ляхов О.Л., Вірьовкін С.В., Захаров С.О. «Автоматизована система моніторингу діяльності навчальних закладів України» // Друга науково-практична конференція з міжнародною участю «Математичне та імітаційне моделювання. МОДС'2007». Тези доповідей. 25-29 червня 2007 р. – К., – 2007. – С. 71-75.

5. АСУ «Рейтинг». Інформаційно-методичний посібник із використання автоматизованої системи «РЕЙТИНГ» / Під заг. ред. О.М. Бурлакова. –1-ше видання. – Полтава: ПолтНТУ, 2007. – 52 с.

6. UNESCO EFA Global Monitoring Report [Электронный ресурс]. – Режим доступа: http://portal.unesco.org/education .

7. New Zealand National Education Monitoring Project [Электронный ресурс]. – Режим доступа: http://nemp.otago.ac.nz .

8. Национальная программа США [Электронный ресурс]. – Режим доступа: http://www.child-education-usa.com .

9. Южно-уральский региональный центр мониторинга системы образования [Электронный ресурс]. – Режим доступа: http://cmso.edu.ru .

10. Система мониторинга качества обучения Национального педагогического университета имени М.П. Драгоманова.

11. Соммервилл И. Инженерия программного обеспечения, 6-е издание. : Пер. с анг. – М. : Издательский дом «Вильямс», 2002. – 624 с.

12. Харченко В.С., Скляр В.В. и др. Оценка и обеспечение качества программных средств космических систем / Под ред. В.С. Харченко, Б.М. Конорева – Национальное космическое агентство Украины, Государственный центр регулирования качества, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2007. – 244 с.

13. Сайт Web Site Security [Электронный ресурс]. – Режим доступа: http://www.cgisecurity.com.

14. Сайт Websecurity Веб безпека [Электронный ресурс]. – Режим доступа: http://websecurity.com.ua.

15. Сайт Security Lab [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/.

Поступила в редакцию 20.02.2008

Рецензент: д-р техн. наук, проф. И.Б. Сироджа, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.