УДК 681.513

А.Л. ЛЯХОВ, М.И. ДЕМИДЕНКО

Полтавский национальный технический университет им. Ю. Кондратюка, Украина

НАДЕЖНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ УЧЕБНЫМ ПРОЦЕССОМ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

Исследована задача надежности автоматизированных систем управления учебным процессом в высшем учебном заведении и выделены аспекты, оказывающие наибольшее влияние на программное обеспечение этого типа.

программное обеспечение, функциональная надежность, система управления.

Введение

Развитие системы образования в рамках Болонского процесса предусматривает переход к личностной модели обучения. Организация качественного учебного процесса на основе такой модели требует детального и глубокого анализа информации о каждом студенте, что связано со значительным увеличением потока обрабатываемых и хранимых данных.

Таким образом, задача разработки автоматизированных информационно-аналитических систем управления высшим учебным заведением (ИАСУ) является насущной необходимостью при реформации системы образования.

В работе [1] дан анализ свойств существующих ИАСУ. Результаты анализа позволяют сделать вывод об отсутствии единых представлений и подходов к разработке требований, спецификаций и реализации автоматизированных систем управления учебным процессом обучения личности в высшей школе.

В частности, не исследован вопрос о том, что такое надежность ИАСУ, достаточная для обеспечения качественного и непрерывного учебного процесса.

Надежность ИАСУ

В многообразии свойств существующих ИАСУ([3]-[7]) можно указать несколько (табл. 1), которые являются типичными, и анализ реализации которых позволяет дать оценку степени надежности системы в целом.

Легко увидеть, что современные ИАСУ построены преимущественно по двухуровневой (рис. 1) или трехуровневой схеме (рис. 2).

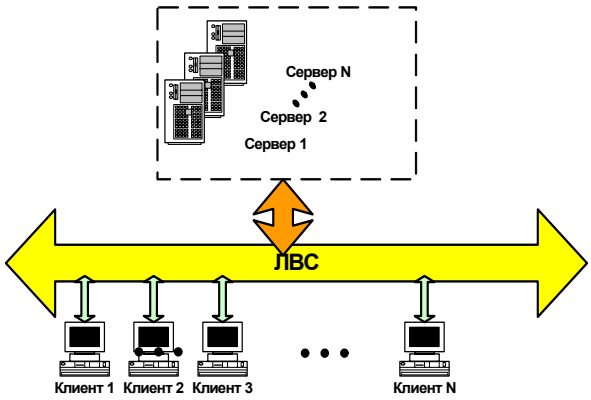

Рис. 1. Архитектура клиент/сервер

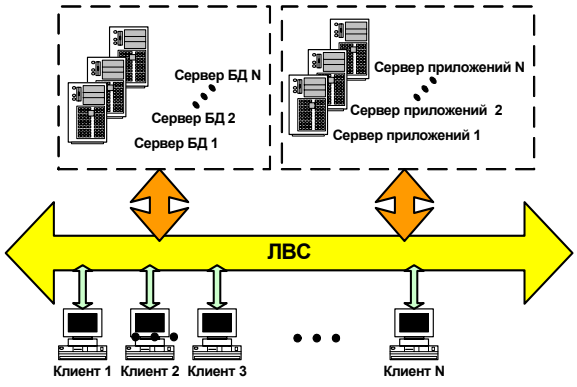

Рис. 2. Архитектура клиент/сервер приложений/сервер баз данных

Таблица 1

Функциональные свойства ИАСУ

Функции\ продукты	Автоматизированная информационная система (типовая) АИСТ ХНДИУ	Интегрированная система управления высшим учебным заведением ХНУВС	«АСУ ВНЗ» Полтавский национальный технический университет	«Университет» REDLABS	«Политех-СОФТ»
Архитектура системы	Клиент-сервер приложений – сервер БД	Клиент-сервер приложений –сервер БД	Клиент-сервер	Клиент-сервер приложений – сервер БД	Клиент-сервер
Поддерживаемые СУБД			Intrbase (Firebird)	Oracle, Informix, Sybase, MS SQL, IBM DB2	Firebird
Разделения прав пользователей	да	да	да	да	Нет
Наличие встроенных функций резервирования и восстановления	нет	нет	нет	Встроенными средствами R/3	Да
Поддержка защищенных сетевых протоколов	нет	нет	нет	да	Нет
Поддержка WEB интерфейса	нет	частично	нет	да	Частично
Минимальная скорость сетевого канала			2Мбит	56 кбит	128 кбит

Характерным является представление ИАСУ в виде отдельных подсистем, соответствующих чаще всего административной структуре ВУЗа, в частности, над общей базой данных. Поэтому можно принять, что надежность системы в целом определяется надежностью каждой подсистемы.

Надежность подсистем ИАСУ рассматриваем как комплекс качеств: работоспособность, безотказность, безопасность, защищенность [2], каждый из которых имеет следующую составляющую: аппаратную, программную и человеческий фактор (рис3).

1. ***Работоспособность*** – свойство системы выполнять свои функции в любое время эксплуатации.

Программная составляющая рассматриваемых систем является либо коммерческим продуктом, либо введена в эксплуатацию в соответствии с существующими требованиями к надежности. Таким образом, можно считать, что программная часть ИАСУ является работоспособной.

Аппаратную составляющую систем также можно считать работоспособной, так как все оборудование, как правило, изготовлено в соответствии с существующими требованиями и стандартами. Благодаря модульной структуре компьютерного оборудования время диагностики и устранения неисправностей невелико по сравнению с периодом жизни ИАСУ. Таким образом, можно считать, что и аппаратная часть ИАСУ также является работоспособной.

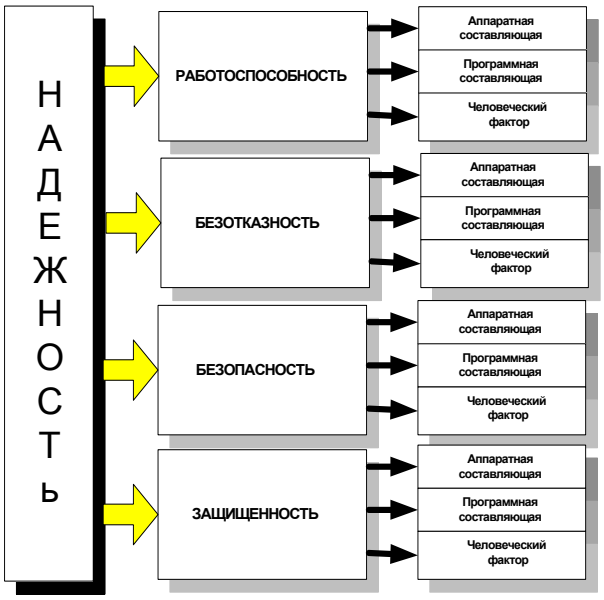

Рис. 3. Составляющие надежности подсистемы ИАСУ

Работоспособность (*человеческий фактор*) во многом определяется актуальностью задачи автоматизации управления для каждого конкретного ВУЗа. В данной работе принимаем, что все необходимые условия труда и мотивации персонала созданы и работоспособность обеспечена.

Безотказность – это способность системы предоставлять сервисы в соответствии с требованиями заказчика.

Безотказность подсистемы имеет такую структуру (рис. 4):

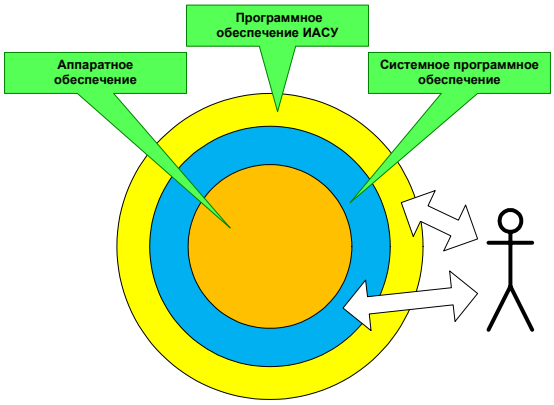

Рис. 4. Структура безотказности подсистемы

1. Безотказность аппаратной составляющей (рис.1-2):
   - безотказность клиентских терминалов;
   - безотказность ЛВС;
   - безотказность серверов.
2. Безотказность программного обеспечения:
   - безотказность системного ПО;
   - безотказность ПО ИАСУ.
3. Безотказность человеческого фактора.

В Украине при разработке ИАСУ используются однотипные клиентские системы, изготовленные в соответствии с существующими требованиями и стандартами. Поэтому будем считать их отказоустойчивыми.

Надежность ЛВС зависит от надежности структурированной кабельной системы (СКС) и надежности активного оборудования. Надежность СКС у каждого ИАСУ своя. Это зависит от соответствия СКС стандартам (согласно ISO 11801 гарантируется минимум 10 лет работы СКС). По этому, исходя из вышесказанного, СКС также можно считать отказоустойчивыми.

Безотказность активной составляющей зависит от правильности подбора оборудования и его конфигурирования, что относится к человеческому фактору.

Общеизвестно, что серверное оборудование отличается повышенной надежностью по сравнению с обычным оборудованием для ПК.

Таким образом, в целом аппаратную составляющую подсистем ИАСУ можно считать безотказной.

Безотказность программной составляющей ИАСУ состоит из безотказности системного ПО и безотказности ПО ИАСУ.

Основу системного ПО составляет операционная система. ОС делятся на серверные (server) и клиентские (workstation). Серверные ОС имеют более высокий уровень отказоустойчивости по сравнению с клиентскими ОС. Кроме того ОС постоянно совершенствуются, регулярно выпускаются обновления. Поэтому отказоустойчивость ОС достаточна.

Большая часть ПО ИАСУ, используемых в Украине, является либо коммерческим продуктом изготовленным и введеным в эксплуатацию в соответствии с существующими требованиями к надежности (таблица, [1]).

Исключение составляют системы, разрабатываемы собственными силами ВУЗов [1]. Сопоставление мер, предпринимаемых для обеспечения надежности подобных ИАСУ с требованиями, предъявляемыми существующими стандартами (ISO 15408: Common Criteria for Information Technology Security Evaluation, ISO 17799: Code of Practice for Information Security Management), то можно сделать вывод про недостаточность решения этой проблемы.

Таким образом, можно считать, что программная часть ИАСУ является достаточно отказоустойчивой.

Безотказность человеческого фактора обусловлена взаимодействием персонала с программным обеспечением и зависит от таких факторов:

- психологического состояния;
- физического состояния;
- уровня квалификации;

– опыта работы;

– эргономических характеристик пользовательского интерфейса.

В процессе длительной работы с ИАСУ в течение рабочего дня психологическое и физическое состояние человека изменяется в сторону ухудшения. Количество ошибок данных увеличивается к концу рабочего дня. Так же количество ошибок зависит объема обрабатываемых данных. В частности, скорость обработки очень быстро падает с увеличением объема вводимой информации. На рис. 5, взятом из работы [1], видно, что эта зависимость имеет экспоненциальный характер, количество вводимых данных резко уменьшается, что фактически можно считать отказом системы.

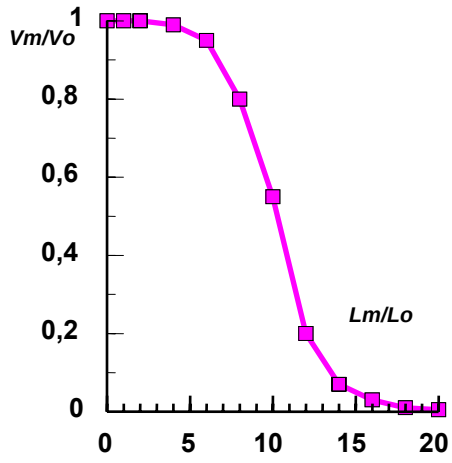

Рис. 5. Уменьшение скорости визуальной обработки информации человеком при увеличении ее объема

Кроме этого, причинами сбоев в программном обеспечении из-за человеческий фактора могут быть:

✓ Нарушения правил эксплуатации системного ПО.

– изменение конфигурации системного ПО без предварительной проверки, его влияния на ПО ИАСУ;

– внесение изменений в системное ПО, которое приводит к сбою (некорректное обновление компонентов ОС).

✓ Нарушение правил эксплуатации ПО ИАСУ

– ошибки при (пере)конфигурировании системы;

– не соблюдение системных требований к аппаратному обеспечению или программному обеспечению;

– выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

✓ Ввода некорректных данных в систему:

– неэргономичность интерфейса;

– большое количество одновременно-вводимых данных;

– психофизическое состояние;

– мотивация;

Первые две проблемы решаемы организационными мерами (повышение квалификации персонала, мотивационными воздействиями обращением к службе технической поддержки и.т.п.,)

Решение третей проблемы лежит в плоскости внесения изменений в ПО, а именно в разработка эргономичных интерфейсов, которые бы брали часть интеллектуальных функций человека на себя.

Поэтому можно сделать вывод, что надежность определяется надежностью системы ввода данных. Но обеспечить путем совершенствования средств интерактивных средств нельзя (рис. 5). Поэтому необходима автоматизация, интеллектуальных функций[1] т.е. интеллектуализация.

3. *Безопасность* - свойство системы, гарантирующее, что она безопасна для людей и окружающей среды, чем, фактически определяется степень ее надежности.

Аппаратное обеспечение разработано и произведено, согласно, современных требований экологической безопасности. В составе устройств миними-

зировано количество вредных для природы и человека материалов и веществ.

Отказы ПО ИАСУ не могут нанести быть непосредственной причиной существенного вреда человеку или окружающей среде.

Вместе с тем, деятельность ВУЗа охватывает широкий спектр задач (например: учебный процесс, научные разработки, финансово-хозяйственная деятельность, и т .д.). ВУЗ также является организацией (юридическим лицом) предоставляющей научно-образовательные услуги, а именно:

– подготовка специалистов;

– проведение фундаментальных и прикладных научных исследований.

Рассмотрим некоторые типичные функции ВУЗа.

1. Учебный процесс. Нарушение работы ИАСУ учебным процессом может привести к нарушению учебного процесса. Нарушение работы такой подсистемы могут быть вызваны систематическими ошибками ввода данных. При длительной эксплуатации ПО такие ошибки накапливаются и могут внести искажение в работу системы. Потеря накопленной информации, может привести к финансовым потерям

2. Научные исследования. Научная работа ВУЗа построена на договорной основе (госбюджетное финансирование, зарубежные гранды, хозяйственные договора и т.п.). В случае отказов программного или аппаратного обеспечения может произойти изменение сроков выполнения исследований, искажение результатов следований, потеря результатов исследований.

Искажение результатов исследований в свою очередь может привести, в зависимости от тематики исследований, к разного рода угрозам человеку или окружающей среде. Кроме того любой сбой приводит к финансовым потерям.

3. Финансово-хозяйственная деятельность. В зависимости от формы собственности ВУЗы подчиняются в своей финансовой деятельности большому количеству законодательных актов, в которых большинство действий регламентируются некоторыми сроками их выполнения. Поэтому сбои ИАСУ могут привести к нарушению своевременного выполнения обязательных действий, что в свою очередь тянет за собой финансовые потери.

В процессе длительной эксплуатации ИАСУ в ней могут накапливаться ошибки данных, которые со временем искажают работу системы. Если система разрабатывается силами Вуза, возможно накопление дефектов программного обеспечения. Совокупность ошибок программного обеспечения, ошибок данных, износа аппаратного обеспечения приводит к уменьшению надежности ИАСУ. А любой сбой такой системы будет приводить к потерям, которые влияют на работу ВУЗа. Поэтому ИАСУ, в процессе длительной эксплуатации, *приближается к уровню критической для бизнеса*

4. *Защищенность* - свойство системы противостоять случайным или намеренным вторжениям в нее, приводящим к отказу.

Для обеспечения защищенности аппаратной составляющей достаточно провести стандартные технические мероприятия по обеспечению условий эксплуатации и ограничить к доступ к оборудованию[10].

Таким образом, для ИАСУ защищенность означает, прежде всего, защищенность программного обеспечения от вторжений.

Существует три типа повреждений системы, которые могут быть вызваны внешними воздействиями [2]:

1. *Отказ в предоставлении системных сервисов.* Система может быть переведена в такое

состояние, когда нормальный доступ к системным сервисам становится невозможным.

2. *Разрушение программ и данных.* Компоненты программного обеспечения системы могут быть несанкционированно изменены. Это может повлиять на поведение системы, а, следовательно, на надежность и безопасность. Если повреждение серьезно, система может стать не пригодной к эксплуатации.

3. *Раскрытие конфиденциальной информации.* Информация, находящаяся под управлением системы, может быть конфиденциальной, внешнее проникновение в систему может сделать ее публично доступной. В зависимости от типа данных, это может повлиять на безопасность системы и вызвать дальнейшие изменения в системе, которые скажутся на ее работоспособности и безотказности.

Как показывает анализ, в вузах защита ИАСУ организована, как правило, по двухуровневой схеме. Первый уровень защиты предназначен для предотвращения вторжений к клиентским терминалам или серверам. (получение локального или удаленного доступа к ОС, разрушение программного обеспечения, блокирования служб или сервисов) реализован системным программным обеспечением:

- операционные системы серверов (ограничение доступа, реализация защищенных сетевых протоколов);
- операционные системы клиентов (ограничение доступа с общим ресурсам и сервисам);
- антивирусные ПО;
- сетевые экраны.

Серверные ОС, сетевые экраны, антивирусное ПО серверов, выполняют задачу защиты от внешних угроз. При правильно реализованной сетевой архитектуре ВУЗа, основными угрозами для ИАСУ являются разного рода DoS атаки, «зомбрование клиентов». Проблема целостности данных и ПО реализуется регулярным автоматическим резервным копированием на внешние накопители.

Клиентские ОС, антивирусное ПО клиентов выполняют задачу защиты ограничения доступа к общим ресурсам и сервисам, защиту клиентского ПО.

Второй уровень защиты предназначен для предотвращения вторжения путем интерактивного ввода данных пользователем ИАСУ в систему доступа к конфиденциальной информации.

На защищенность ИАСУ оказывает влияние и человеческий фактор. Как показывает практика, в 90% правонарушения связанных, с информационными системами совершаются с участием сотрудников, которые имеют доступ к системе. В большинстве случаев это несанкционированный доступ к информации.

Это значит, что ИАСУ должны иметь хорошо организованную иерархическую систему администрирования.

Для повышения защищенности ИАСУ следует регулярно проводить обновление системного ПО, которое влияет на безопасность системы. Проводить необходимые технические, программные и организационные мероприятия обеспечения информационной безопасности [10].

Выводы

1. ИАСУ управления учебным процессом должны обладать высокой надежностью. Уровень надежности должен быть тем выше, чем продолжительнее время эксплуатации системы. При длительной эксплуатации уровень надежности ИАСУ должен приближаться *к уровню надежности систем, критических для бизнеса.*

2. ВУЗы при разработке ИАСУ уделяют вопросам надежности недостаточно внимания, что может приводит к потерям, размеры которых можно оценить только в процессе длительной эксплуатации.

3. Надежность ИАСУ определяется, в первую очередь, такой компонентой как защищенностью программного обеспечения.

4. Основным фактором, влияющим на эту компоненту надежности, является «человеческий фактор». При этом основными источниками отказов ИАСУ могут быть дефекты разработки ПО, ошибки администрирования и ошибки ввода данных.

5. Комплекс мер по повышению надежности ИАСУ состоит, прежде всего, формировании и анализе требований к надежности ИАСУ на этапе проектирования с помощью существующих методик (например, [11]) и разработка программной части с учетом этих требований.

6. Поскольку ошибки ввода данных трудно поддаются формализации, защищенность ИАСУ от «человеческого фактора» может быть обеспечена только путем интеллектуализации пользовательского интерфейса.

Литература

1. Ляхов А.Л., Демиденко М.И. Основные свойства автоматизированных систем моделирования и управления учебным процессом в вузе. – Сб. трудов Второй научно-практической конференции «Математическое и имитационное моделирование систем», МОДС 2007. – К.:2007. – С. 75-80.

2. Соммервилл И. Инженерия программного обеспечения, 6-е издание.: Пер. с англ. – М.: Издательский дом "Вильяме", 2002. – 624 с.

3. [Электронный ресурс]. – Режим доступа: http://www.khadi.kharkov.ua/default.asp?id=73&mnu=73.

4. [Электронный ресурс]. – Режим доступа: http://www.univd.edu.ua/index.php?id=164&lan=ukr

5. [Электронный ресурс]. – Режим доступа: http://www1.pntu.edu.ua/cit/index.php?option=com_content&task=blogsection&id=8&Itemid=40.

6. [Электронный ресурс]. – Режим доступа: www.redlabs.ru.

7. [Электронный ресурс]. – Режим доступа: www.politek-soft.kiev.ua.

8. Липаев В.В, «Надежность программных средств». – М.: СИНТЕГ, 1998.

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

10. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М., 2004. – 240 с.

11. [Электронный ресурс]. – Режим доступа: http://shop.globaltrust.ru/osnov.php?idstat=49&idcatstat=1&PHPSESSID=22ac9190e268d89cfbad237f6b2e1b5b.

Поступила в редакцию 13.02.2008

Рецензент: д-р техн. наук, проф. И.А. Жуков, Национальный авиационный университет, Киев.