

УДК 004.588

Н.А. Маслова, Р.А. Сорокин

Донецкий национальный технический университет, Украина
Украина, 83001, г. Донецк, Артема, 58

Использование облачных технологий как способ повышения защищенности тестовых обучающих систем

N.A. Maslova, R.A. Sorokin

Donetsk national technical university, Ukraine
Ukraine, 83001, Donetsk, Artema, 58

The Using of Cloud Technologies as a Way to Improve the Security of Test Training Systems

Н.О. Маслова, Р.О. Сорокин

Донецький національний технічний університет, Україна
Україна, 83001, Донецьк, Артема, 58

Використання хмарних технологій як засіб підвищення захищеності тестових навчальних систем

В работе рассмотрены особенности использования облачных вычислений в обучении. Выполнена классификация обучающих систем, обзор облачных сервисов. Рассмотрены риски информационной безопасности облачных хранилищ и меры по их снижению. Выделены достоинства и недостатки распространенных облачных сервисов. Приведены требования к построению тестовых обучающих адаптивных систем многоцелевого использования. Показано, что размещение распределенных систем на гибридном облаке и шифрование данных на стороне клиента улучшают показатели безопасности.

Ключевые слова: облачные вычисления, обучающие системы, информационная безопасность, адаптивная система, гибридное облако.

In article the features of use of cloudy calculations in training are considered. The classification of training systems, review of cloudy services is executed. The risks of information security of cloudy storage and measures of their reduction are considered. The advantages and lacks of the widespread cloudy services are selected. The requirements to designing of adaptive training systems of multi-purpose use are given. It is shown, that accommodation of the distributed systems on a hybrid cloud and enciphering of the data on the party of the client is improved by parameters of security.

Key words: cloudy calculations, training systems, information security, adaptive system, hybrid cloud.

У роботі розглянуті особливості використання хмарних обчислень у навчанні. Виконана класифікація навчальних систем, огляд хмарних сервісів. Розглянуті ризики інформаційної безпеки хмарних сховищ і заходи щодо їх зниження. Виділені переваги і недоліки поширених хмарних сервісів. Наведені вимоги до побудови тестових навчальних адаптивних систем багатопільового використання. Показано, що розміщення розподілених систем на гібридній хмарі і шифрування даних на стороні клієнта покращують показники безпеки.

Ключові слова: хмарні обчислення, навчальні системи, інформаційна безпека, адаптивна система, гібридна хмарна структура.

Введение

Современные исследования в области применения компьютеров в обучении развиваются, в основном, в рамках нескольких основных направлений:

- интеллектуальные обучающие системы;
- гипермедийные обучающие системы;
- учебные среды, микромиры и моделирование;
- системы дистанционного обучения.

На сегодняшний день существует множество различных программ учебного назначения, однако они не получили должного уровня использования в учебном процессе. Среди основных причин называют сложность систем, ориентацию на технологические, а не педагогические парадигмы, отсутствие стандартов построения. Последнее приводит к затруднениям в использовании систем непосредственно в учебном процессе, что связано с необходимостью изучения, приобретения и обслуживания целого ряда разнородных систем в одном образовательном заведении. Кроме того, по мере эксплуатации систем постоянно возрастают требования к техническим средствам, что связано с необходимостью наращивания баз знаний, являющихся одной из составных частей обучающей системы. Сами базы знаний требуют квалифицированного сопровождения, пополнения, развития, что сложно осуществлять в случае большого числа пользователей. И, наконец, существует проблема обеспечения безопасности систем обучения, что особенно актуально в современном мире, когда количество угроз ежегодно удваивается.

С развитием технологий облачных вычислений появилась возможность дальнейшего совершенствования тестовых и обучающих систем.

К настоящему моменту известно об использовании облачных технологий в обучающих системах Microsoft, комплексе 1С, университетских обучающих системах для ИТ-образования (Challengers, Visionaries, Niche Players). Указанные системы обладают множеством достоинств. Они эффективны, современны, конкурентноспособны, позволяют образовательным учреждениям и компаниям получать быстрый доступ к улучшенному управлению и безопасности, но имеют один существенный для Украинского рынка недостаток – высокую стоимость [1].

Облачные технологии предполагают удаленную обработку и хранение данных. Пользователю не нужно заботиться о производительности своего персонального компьютера, переживать о свободном пространстве на диске, приобретать программный продукт при необходимости краткосрочного использования. Достаточно иметь выход в Интернет. Пользователь получает ссылку для обращения к системе и работает с ней через браузер.

Разработчику же не нужно устанавливать обучающую систему на компьютере пользователя, обеспечивать ее функционирование, обновление, отслеживать удаление при истечении срока договора и т.п. Использование облачных технологий позволяет снизить нагрузку на сервера обучающих систем, поскольку вся база данных может храниться «на облаке» и обслуживаться администраторами системы одновременно с проведением тестирования или обучения в режиме реального времени. И это лишь некоторые преимущества виртуализации.

В настоящее время получили распространение более двадцати некоммерческих (общественных) облачных сервисов. Не все они обладают разной надежностью, отказоустойчивостью, предоставляют достаточно места для размещения баз знаний, обеспечивают нужный уровень безопасности [2]. Поэтому вопросы выбора наиболее удобного и защищенного сервиса являются в настоящее время перспективными и актуальными.

Цель статьи – провести анализ облачных сервисов с точки зрения возможности их использования для безопасного размещения тестовых обучающих систем и рассмотреть требования к архитектуре адаптивных обучающих систем многоцелевого использования, размещаемых на «облаке».

Об обучающих системах

Первые исследования возможности использовать компьютер для оптимизации процесса обучения появились в 60-х годах прошлого столетия. Это была книга «The Science of Learning and Art of Teaching» (B.F. Skinner). С этого момента получили развитие сначала простые, а далее – все более емкие и совершенные обучающие системы. Одним из понятий, используемых в обучающих системах, является тест.

Тестирующие системы предназначены в основном для контроля знаний с помощью тестов. Механизм проведения тестирования может включать средства статистической обработки результатов, а следующим этапом является обучение. Примерами тестирующих систем являются TestMaker, TestOfficePro, AnyTest, Teaching Templates, КИОС, МастерТест, Ассистент, Экзаменатор и др.

Обучающая система – это более сложная структура, человеко-машинный комплекс, который работает в диалоговом режиме и предназначен для управления познавательной деятельностью. Она должна включать в себя теоретические материалы, примеры, практические задания и средства контроля приобретенных знаний, умений и навыков, т.е. тестирующий, контролирующий и тренирующий блоки. Примеры обучающих систем: Toolbook, AuthorWare, Director, ComputerMaster, LearnangSpace, Наставник, Адонис, КАДИС и др.

Если система выполняет и контролирующую и обучающую функции, то согласно [3] она называется тестовой обучающей системой.

В настоящее время существует масса специализированных систем обучения, позволяющих проводить обучение и тестирование остаточных знаний в самых разных предметных областях. Типы компьютерных тестовых заданий определяются способами однозначного распознавания ответных действий тестируемого.

Наиболее перспективным направлением развития систем компьютерного обучения является технология искусственного интеллекта (ИИ). Системы, использующие методику ИИ, называют интеллектуальными обучающими системами (ИОС). Методологическая основа проектирования интеллектуальных обучающих систем рассмотрена в исследовательских работах В.П. Беспалько, П.Л. Брусиловского, Ю.И. Лобанова, Л.А. Растригина, А.Я. Савельева, А. В. Соловова и других. Из зарубежных исследователей следует отметить работы A. Bork, D. Callear, D. Sleeman, E. Soloway, G. Weber, B.P. Woolf и др. [4].

Особенностями технологии интеллектуальных обучающих систем являются: моделирование процесса обучения; использование динамически развивающейся базы знаний; автоматический подбор рациональной стратегии обучения для каждого обучаемого; адаптивность; автоматизированный учет информации, поступающей в базу данных.

При этом наиболее прогрессивными можно считать адаптивные модели обучающих систем, которые образуют отдельный подкласс ИОС.

Адаптивная ИОС позволяет не только контролировать знания, но и по результатам тестирования определять, какая часть материала усвоена в недостаточной степени. Затем она предложит обучаемому теоретический материал для повторного изучения, практические примеры и упражнения, даст дополнительные разъяснения по проблемному разделу. Таким образом адаптивная ИОС учитывает особенности знаний каждого конкретного обучаемого.

В работе [5] проведен обзор технологий и их возможностей в адаптивных обучающих системах. В работе показано, что современные обучающие системы возникли не «с нуля», а явились результатом адаптации ИОС с учетом WEB-технологий и подходов к обучению в целом.

Адаптивное представление может улучшить удобство и простоту использования представления материала в курсах. Адаптивная поддержка навигации и адаптивное планирование могут использоваться для всеобъемлющего управления курсом и для помощи обучаемому в выборе наиболее подходящих тестов и задач. Поддержка решения задач и интеллектуальный анализ решений могут значительно усовершенствовать работу с задачами, предоставляя как интерактивный режим работы, так и интеллектуальную обратную связь. Адаптивная поддержка совместной работы открывает новые возможности для общения и сотрудничества.

Преимуществами компьютерного адаптивного тестирования перед традиционным являются:

- возможность адаптации под уровень знаний тестируемого (не придется отвечать на слишком сложные или слишком простые вопросы);
- экономия времени и сил за счет сокращения количества заданий (длина теста может быть уменьшена до 60%) без потери уровня достоверности.

По-сути, речь может идти и об экспертных системах, т.к. по определению это сложные программные комплексы, аккумулирующие знания специалистов в конкретных предметных областях и распространяющие опыт для обучения менее квалифицированных пользователей.

Архитектура экспертной системы включает в себя два основных компонента: базу знаний (хранилище единиц знаний) и программный инструмент доступа и обработки знаний, состоящий из механизмов вывода заключений (решения), приобретения знаний, объяснения получаемых результатов и интеллектуального интерфейса. Причем, центральным компонентом экспертной системы является база знаний, которая выступает по отношению к другим компонентам как содержательная подсистема, составляющая основную ценность.

К обучающим системам предъявляются высокие требования, такие как:

- защита от копирования, списывания и несанкционированного доступа к вопросам;
- большая тестовая база (в более общем случае – база знаний);
- простота программного интерфейса;
- удобство администрирования теста;
- полная автоматизация процесса тестирования;
- минимизация времени посылки запроса/ получения отклика системы.

В то же время недостатком многих существующих ИОС называют ориентацию на специальные знания в рамках определенного предмета, так что в них не предусмотрена возможность простой адаптации к другой предметной области. Более общий подход состоит в развитии интеллектуального окружения (оболочки), из которого затем можно получить много ИОС путем наполнения различным содержанием баз знаний. По сути последняя структура является еще более широким понятием, чем обучающая система и носит название «учебный курс» [6].

Об облачных вычислениях

В соответствии с определением Национального института стандартов и технологий (США) [7] облачные вычисления – это модель предоставления повсеместного и удобного сетевого доступа к общему пулу конфигурируемых вычислительных ресурсов (сетей, серверов, систем хранения данных, приложений и сервисов), которые могут быть быстро предоставлены и освобождены с минимальными усилиями и без обращения к сервер-провайдеру.

Облачная модель имеет пять характерных особенностей:

- принцип самообслуживания;
- стандартный сетевой доступ;
- модель множественной аренды (multi-tenant model);
- гибкое и быстрое выделение требуемых объемов вычислительных ресурсов;
- контроль объемов потребляемых услуг.

Тремя основными моделями облачных сервисов являются SaaS, которая организуется так, что клиент получает доступ к приложениям, размещенным в облачной инфраструктуре; PaaS, в которой платформы и средства развертывания приложений предлагаются как услуга; IaaS, в которой в качестве услуги предлагается инфраструктура.

И, наконец, существуют следующие модели внедрения (развертывания) облачных технологий: частное облако; общее облако (модель совместного использования); публичное (общедоступное) облако; гибридное облако.

К достоинствам облачных (иной термин – виртуальных) технологий относят сокращение операционных и отсутствие капитальных затрат, отказоустойчивость, динамическую масштабируемость.

А в числе слабых сторон называют проблему обеспечения информационной безопасности. При этом риски информационной безопасности, возникающие в модели частного облака, отличаются от рисков, возникающих при использовании публичного, общего или гибридного облака.

В случае использования частного облака решением всех проблем безопасности занимается лицо, которому принадлежит облако или фирма, которую наняли для обслуживания. В публичном облаке решение всех проблем информационной безопасности – задача организации, создавшей этот сервис, а доступ к ресурсу имеет любой желающий. В гибридной модели используется совокупность нескольких виртуальных хранилищ с различными моделями внедрения, объединенных единой технологией. В этом случае части системы могут располагаться, например, на общем или публичном облаке, а наиболее важные данные – на частном.

Для рассматриваемой модели системы обучения использование частного облака не предполагается, поэтому и риски, связанные с этим направлением, не рассматриваются.

Итак, для облачных вычислений, в основе которых лежат общая, публичная или гибридная модели развертывания, можно выделить следующие риски информационной безопасности [8].

Общие (классические, традиционные) риски информационной безопасности. К ним относятся риски, связанные с уязвимостями сетевых протоколов, серверов приложений и операционных систем (ОС). К этой группе относятся риски, связанные с разграничением доступа, использованием небезопасных программных интерфейсов (API), утечка и утрата данных и т.п.

Следующая группа – риски, связанные с применением виртуальной среды, т.е. непосредственно с технологией облачных вычислений. Это отсутствие стандартов в организации услуг облачных сервисов; дефицит информации о расположении компонент облачной ИТ-структуры («размытие периметра»); аутсорсинг (например, привлечение оператора связи, недостаточно уделяющего внимание вопросам безопасности передачи информации).

Группа рисков, которую можно назвать «привязка к провайдеру» и отнести в нее следующие риски: ликвидация сервиса, связанная с уходом с рынка провайдера услуг; проблемы с оборудованием провайдера (сбои, форс-мажор); отсутствие связи; незаконные действия персонала провайдера; финансовые и юридические проблемы (банкротство, арест или конфискация оборудования).

Следующая группа рисков связана с разделяемыми ресурсами. Это проведение DDos-атак на провайдера или его клиентов; проблемы с оборудованием в цепочке задействованных для размещения облачных сервисов компьютеров; программные или иные сбои в цепи взаимосвязанных провайдеров; получение несанкционированного доступа к данным или компонентам виртуальной инфраструктуры со стороны других клиентов провайдера облачных услуг.

Для снижения перечисленных выше рисков информационной безопасности, предлагается реализовать описанные ниже контрмеры:

- тщательный выбор и проверка провайдера услуг;
- наличие у поставщика услуг сертификатов безопасности;
- законодательное закрепление соглашений о сотрудничестве;
- привлечение нескольких провайдеров (резервирование);
- использование открытых стандартов;
- учет месторасположения центров обработки данных провайдера (страна и ее законодательство);
- наличие требований по надежности и защищенности каналов связи.

Кроме перечисленных, можно указать риски, связанные с выделением и освобождением памяти, очисткой ресурса после его освобождения. Эти риски можно минимизировать, если контролировать очистку ресурса после его освобождения, либо самостоятельно удалять данные из хранилища.

С целью снижения риска падения сервера, многие поставщики «облачных» услуг создают резервные копии и распределяют их по различным региональным серверам, поэтому риск потери данных снижается до 1%.

К вопросам защиты данных фирмы, предоставляющие услуги облачных сервисов, относятся по-разному. Одни из них предусматривают шифрование данных как на серверах, так и на стороне клиента (Wuala, CloudSafe, MozyHome, SpilderOak, TeamDrive), другие, которых явное большинство, предпочитают заботиться лишь о защите данных на стороне сервера, забывая или не придавая значения безопасности приема/передачи данных и защите на стороне клиента.

Самые известные «облачные» хранилища – Dropbox, Box, SugarSync, Amazon Cloud Drive, SkyDrive, «Google Диск», «Яндекс.Диск». У «облачных» хранилищ нет ограничения в скорости скачивания и сроке хранения данных, они подключаются в виде диска, который отображается в операционной системе и опознается файловыми менеджерами, данные, размещенные на «облачных» дисках, доступны постоянно.

Так как нашей задачей является размещение на облачных ресурсах обучающей системы, наряду с безопасностью сервиса нас волнуют вопросы быстродействия; максимально возможного объема выделяемой дисковой памяти (для размещения базы знаний); возможность параллельной работы с файлами (для администрирования или пополнения базы знаний в on-line режиме; предоставление доступа к файлам; работа с любыми расширениями файлов как через веб-интерфейс, так и клиентское приложение; автоматическая синхронизация; интеграция в Windows; возможность запуска исполняемого модуля с облачного сервиса и локальное хранение баз данных.

По оценкам журнала Chip по скорости загрузки данных наиболее «быстрым» хранилищем является Cloudme (3303Кбайт/с), а наиболее медленным – облачный сервис Box (97Кбайт/с). Скорость же скачивания данных наиболее высока на Drive onWEB (3793Кбайт/с).

Для пересылки информации часто используют туннель SSL. Он достаточно быстр и защищен от перехвата. Если упомянуть об используемых алгоритмах шифрования, то чаще всего это алгоритм AES (Advanced Encryption Standard) с ключами большой длины (до 256 бит).

С точки зрения безопасности необходимо отметить, что лишь пять виртуальных сервисов (Wuala, CloudSafe, MozyHome, SpiderOak, TeamDrive) используют три вида шифрования – на стороне сервера, при передаче данных и на стороне клиента. Большинство ограничиваются шифрованием при передаче, а CloudMe и ADrive и вовсе не используют шифрование.

Большинство хранилищ хранят коды шифрования на собственных серверах, что снижает качество защиты из-за возможности получения доступа к информации сотрудниками фирмы-организатора сервиса. Шифрование на стороне сервера с использованием личного ключа, хранящегося локально, предлагает сервис iDrive. И все же остаточный риск сохраняется: хакеры или сотрудники сервиса могут вклиниться между туннелем SSL и шифрованием на стороне сервера. Защититься от этого можно только с помощью кодирования AES на стороне клиента. Это происходит автоматически у сервиса Wuala, но он сложен в управлении, работает с перебоями, предполагает установку дополнительного программного обеспечения на компьютере клиента (в частности, Java).

Постановка задачи

Целью работы является не только анализ облачных сервисов, но и возможность их использования для безопасного размещения тестовых обучающих систем.

В работах [9-11] рассматривались различные аспекты безопасности информационных систем. Так, в [9] выполнен анализ методов защиты, проведена классификация алгоритмов шифрования, предложены примеры программной реализации некоторых алгоритмов. Вопрос сравнительного анализа алгоритмов шифрования рассмотрен в работе [10]. Приведены аналитические выражения для оценок сложности ряда алгоритмов, предложена модификация алгоритма RSA, удобная при работе с реляционными базами данных и позволяющая существенно уменьшить количество вычислительных операций, что может привести к более эффективному выполнению процесса. Работа [11] посвящена вопросам обеспечения информационной безопасности систем управления базами данных и их серверных компонентов. Предлагается механизм использования имеющихся ресурсов СУБД для построения удобной пользователю защищенной системы.

В информационной безопасности существует понятие информационного риска, который определяется как функция трёх переменных:

- вероятности существования угрозы;
- вероятности существования незащищенности;
- потенциального воздействия.

Если любая из этих переменных приближается к нулю, полный *риск* приближается к нулю, т.е.

$$R = \sum_{k=1}^K P_{1k} + \sum_{k=1}^K P_{2k} + \sum_{k=1}^K P_{3k},$$

$$R \rightarrow 0, \text{ если } P_1 \vee P_2 \vee P_3 \rightarrow 0.$$

В применении к обучающим системам задача выбора облачного сервиса с минимизацией рисков в общем виде может быть сформулирована следующим образом.

Итак, пусть U – множество параметров, по которым оценивается качество облачного сервиса ($U = \{u_i \mid i=1..N\}$, где u_i – i -й параметр, используемый при оценке качества сервиса). Этими параметрами являются, например, максимальный размер файла, который может быть загружен на сервис; объем дискового пространства, первоначально выделяемого пользователю и т.п.

Лучшим будем считать сервис, на котором достигается:

$$\max \sum_{i=1}^N u_i,$$

при условии, что суммарный риск информационной безопасности:

$$R - > 0.$$

Анализ показал, что для размещения обучающих систем, достаточно удобным по всем перечисленным параметрам является сервис Dropbox. Он не имеет ограничений на объем загружаемого файла, при установке интегрируется в Проводник Windows в раздел «Избранное», синхронизируется со всеми устройствами, на которых установлено клиентское приложение, позволяет строить гибридные структуры, работает по адресу и по прямой ссылке, проводит синхронизацию для двух и более аккаунтов. Однако, наряду со всеми перечисленными достоинствами имеет существенный с точки зрения безопасности недостаток – отсутствие шифрования на стороне клиента.

Таким образом, для повышения защищенности данных при использовании сервисов без шифрования на стороне клиента, таких, как, например, Dropbox, SkyDrive или Google Drive, необходимо принять меры по защите информации дополнительными программами. Это могут быть программные продукты Vohscryptor, Cloudfogger или Truecrypt или иные, в том числе и собственной разработки.

В результате рассмотрения всех аспектов, можно сделать следующие выводы.

Во-первых, рынок виртуальных хранилищ и сервисов к настоящему моменту может предоставить около 30 «облачных» ресурсов, имеющих различные характеристики по управляемости, функциональности, быстродействию, предлагаемой памяти и безопасности.

Во-вторых. Несмотря на то, что применение виртуальной среды приводит к появлению новых рисков безопасности, эти риски можно минимизировать применением достаточно простых контрмер, в основном управленческого и организаторского плана, перечисленных выше.

В-третьих. Использование публичного облака может повысить показатели безопасности системы благодаря тому, что в этом случае инфраструктура принадлежит организации, которая это облако создала, обслуживает и принимает максимально возможные меры по обеспечению безопасности работы со своими сервисами. В этом случае затраты клиента также могут снизиться не только в случае использования бесплатных хранилищ, но и при аренде приложений, т.к. он не заботится о поддержке инфраструктуры и разработке приложений.

В-четвертых. Снизить риски безопасности можно использованием гибридного облака как модели развертывания облачных вычислений, так как при этом провайдеру услуг можно передать только часть функций системы, а часть данных разместить на собственных, надежно защищенных ресурсах.

И, наконец, в-пятых, важным моментом является обеспечение информационной безопасности на стороне клиента, применение таких стандартных механизмов обеспечения информационной безопасности, как криптография, аутентификация, шифрование, блокировка перехватов, исключение возможности подмены информации при ее передаче по каналам связи, борьба с несанкционированным доступом к системе и т.п.

Требования к обучающей системе, размещаемой на «облаке»

Перед формированием модели обучающей системы, размещаемой на «облаке», нужно четко очертить набор функций и требований к ней. Перечислим основные функции, требования, выдвигаемые к блоку тестирования:

- основная функция – обеспечение эффективного тестирования знаний;
- точная и способная к адаптации оценка результатов тестирования;
- удобство и легкость создания и модификации тестов;
- отсутствие твердой привязки к какому-нибудь предмету, области знаний;
- возможность одновременного тестирования неограниченного количества пользователей;
- отсутствие жесткой привязки к конкретному аппаратному и программному обеспечению;
- легкая наращиваемость, масштабируемость системы;
- высокая безопасность, защищенность;
- неограниченное количество тестов, тем, вопросов и вариантов ответов;
- контроль времени тестирования;
- поддержка режима модульного контроля, в процессе которого существует ряд вопросов и время, в течение которого на них необходимо ответить.

Задания должны быть краткими, ясными и корректными, не допускать двусмысленности. Все ответы, в случае необходимости их выбора, должны быть правдоподобными и равно привлекательными.

Поэтому стоит упомянуть требования к тестовым заданиям:

- содержание тестового задания должно требовать от испытуемого однозначного ответа;
- содержание тестового задания должно быть ориентировано на получение ответа только по одной задаче из конкретной области знаний;
- следует избегать тестовых заданий, требующих развернутых ответов;
- основные термины тестового задания должны быть явно и ясно определены;
- тестовые задания должны быть прагматически корректными и рассчитаны на испытуемых с заданным (исходным) уровнем подготовки по конкретной предметной области;
- тестовое задание должно формулироваться в утвердительном или повелительном предложениях;
- количество слов в тестовом задании не должно превышать 10.

Перейдем к рассмотрению перечисленных выше требований применительно к поставленной задаче.

Объектом управления обучающей системы является тестируемый. Субъекты управления – преподаватель и обучающая система, которая дополняет, но не заменяет преподавателя. Цели обучения:

- тестирование (проверка) знаний, умений и навыков с учетом уровня подготовленности обучаемого (адаптация);
- выявление проблемных направлений и предложение к изучению теоретического материала в соответствии с выявленными пробелами;
- оценка вновь приобретенных знаний.

Достаточно подробно структура системы описана в [12].

Уточним ту часть требований, которые относятся к построению тестовой обучающей адаптивной системы, размещаемой на виртуальных ресурсах.

1. Построение распределенной системы – применяется для невозможности одновременного получения правильных ответов обучаемым или посторонним. Это может повлечь распространение ответов среди студентов и дальнейшее неадекватное тестирование. Данная проблема решается путем разделения программы на клиентскую и серверную части. Таким образом, студент не знает, где и как именно хранится информация о вопросах и ответах тестовой системы.

2. Организация базы знаний как отдельного блока и возможность ее размещения на ином (не том, что сама обучающая система) ресурсе.

3. Система разграничения прав доступа, аутентификация пользователей, парольная защита входа.

4. Большая тестовая база – предназначена для разнообразия теста и как можно меньшей повторяемости вопросов. Чем меньше вероятность повторения вопросов, тем объективнее можно оценивать результат тестирования. В разрабатываемой системе предполагается наличие специального окна, при помощи которого в базу могут быть добавлены вопросы и варианты ответов.

5. Простота интерфейса программы. Требования к интерфейсу описываемой системы – минимум окон, таймер, индикатор прогресса «пройденных» вопросов, доступное меню с системой подсказок.

6. Простота администрирования теста – это требование немаловажно, т.к. каждый преподаватель может создать свой тест и добавить его в базу. Простота администрирования решается введением в программу отдельного окна, в котором можно ввести новый вопрос, варианты ответа и сохранить информацию. Такое администрирование позволит до минимума сократить обслуживание программы сторонними специалистами.

7. Полная автоматизация процесса тестирования. Тестирование проводится без контроля преподавательского состава за ходом тестирования. Поэтому весь процесс – от задания вопросов теста преподавателем, проведения тестирования, до оценки полученного результата, – должен проходить по единому сценарию, без возможности студента повлиять на ход его выполнения. Результат тестирования – ведомость по группам и справка о тестировании каждого студента.

8. Быстрота загрузки. Этот критерий следует обозначить как немаловажный, ведь облачные сервисы имеют различную производительность.

9. Система должна быть универсальной. Для того, чтобы преподаватель мог эффективно использовать программу, необходимо, чтобы была возможность вносить изменения в тесты в самой тестирующей программе, применение тестирующей программы не должно требовать опыта работы с другими приложениями.

10. Система должна обеспечивать повсеместную и удобную работу с прикладными решениями на различных клиентских устройствах с различными операционными системами. При этом клиенты могут использовать устройства с малой вычислительной мощностью, мобильные устройства. Клиенты могут вообще не устанавливать на свои устройства программное обеспечение обучающей системы или ограничиться «легким» клиентским приложением, не требующим большого количества ресурсов.

11. Все основные вычисления, прикладная логика должны реализовываться в серверном блоке системы. Этот блок обеспечит масштабируемость, устойчивость к отказам, динамическое перераспределение нагрузки и взаимодействие с базой знаний.

12. База знаний может располагаться как на сервере клиента, так и на одном из «облачных» дисков. В этом случае требования шифрования данных на стороне клиента и работа по ссылкам являются обязательными.

Прочие требования к построению системы сформулированы в [13].

По окончании теста студенту выставляется соответствующая отметка или дается оценка уровню знаний в процентном или бальном соотношении (критерий оценки также задается преподавателем). При этом по недостаточно хорошо освоенному вопросу ему будет предложено повторно изучить темы из данного курса, в которых он допустил ошибки. Для этого в программу вводятся ссылки на файлы, содержащие электронные

учебные пособия, которые также могут быть размещены отдельными элементами на облачных дисках. При этом использование гибридной модели допускает выбор наилучшего по параметру скорости считывания информации и максимально допустимому размеру файла хранилища. Материалы учебных пособий могут быть размещены как на локальном компьютере, так и находиться в сети Интернет, что зависит от технических возможностей и схемы проведения процедуры тестирования.

Выводы

Внедрение современных информационных технологий в обучение позволяет достичь запланированных результатов только при условии надежной, безопасной и производительной работы всей ИТ-инфраструктуры. К ней предъявляются все возрастающие требования повышения производительности и надежности при постоянном увеличении объемов обрабатываемой информации.

По мере развития технологий виртуализации появилась возможность дальнейшего совершенствования тестовых и обучающих систем. Но «облачных» хранилищ существует достаточно много. Они имеют различные характеристики и степени обеспечения безопасности. С переходом на технологию виртуализации организационные и управленческие моменты несколько усложняются. Необходимо взвешенно и продуманно подойти к решению вопросов обеспечения безопасности, учесть новые риски, преобразовать или спроектировать систему таким образом, чтобы ее архитектура органично вписалась в облачные сервисы.

Литература

1. Яблонский С.А. Модернизация рынка информационных технологий на основе облачных вычислений / С.А. Яблонский // *Материалы конференции : «Устойчивое развитие российских регионов: инновации, институты и технологические заимствования»*. – Екатеринбург, 2010.
2. Лучшие бесплатные он-лайн хранилища. Обзор // *Chip*. – 2012. – № 10. – С. 76-79.
3. Мельников А.В. Принципы построения обучающих систем и их классификация / А.В. Мельников, П.Л. Цытович // *Электронный журнал «Педагогические и информационные технологии»*. – 2001. – № 4.
4. Журкин А.А. Информационно-коммуникационные технологии адапционного обучения с элементами искусственного интеллекта / А.А. Журкин // *Ученые записки: электронный научный журнал Курского государственного университета*. – 2012. – № 4 (24), Т. 2. – С. 204-212.
5. Брусиловский П.Л. Адаптивные обучающие системы в World Wide Web: обзор имеющихся в распоряжении технологий / П.Л. Брусиловский [Электронный ресурс] // *International Forum of Educationl Technology & Society*. – Режим доступа : <http://ifets.ieee.org/russian/depository/WWWITS.html>.
6. Дуплик С.В. Модели педагогического тестирования / С.В. Дуплик // «Вестник Казанского Государственного Технического университета им. А.Н.Туполева». – 2003 г. – № 2. – С. 74-79.
7. Основы Облачных вычислений [Электронный ресурс] // *Рекомендации NIST*. – Режим доступа : <http://cloud.sorlik.ru/definition.html>.
8. Веселов Е.А. Риски информационной безопасности облачных вычислений и меры по их снижению / Е.А. Веселов // *Материалы Всероссийского профессионального форума : «Эффективный документооборот в органах власти и местного самоуправления» (ИНФОДОКУМ-2012)*.
9. Маслова Н.А. Анализ и выбор методов защиты экономических данных / [Н.А. Маслова, К.Н. Ефименко, Д.С. Демченко]. – Депон. рукопись ДРНТИ Украины, Донецкий государственный технический университет. – Донецк. – 2000. – 14 с.
10. Маслова Н.О. Використання стратегії розподілу для оптимізації обчислення НЗД у алгоритмах шифрування / Н.О. Маслова // *Управляющие системы и машины*. – Киев. – 2002. – № 2. – С. 74-84.

11. Маслова Н.А. Информационная безопасность систем управления базами данных / Н.А. Маслова // Комп'ютерна математика. Оптимізація обчислень : зб.наук. праць НАН України, інститут кібернетики ім. В.М.Глушкова. – Київ. – 2001. – Т. 1. – С. 271-280.
12. Шупік Д.Є. Підсистема тестування та закріплення знань з фахових дисциплін за допомогою комп'ютера / Д.Є. Шупік, Н.О. Маслова // Матеріали першої міжнародної науково-технічної конференції : «Інформатика й комп'ютерні технології». – Донецьк. – 2005, ДонНТУ. – С. 121-122.
13. Маслова Н.О. Методичні вказівки до виконання курсового проектування з дисципліни «Основи візуального програмування» / Н.О. Маслова, Р.О. Сорокін. – Донецьк. – 2013. – 33 с.

Literatura

1. Jablonskij S.A. Modernizacija rynka informacionnyh tehnologij na osnove oblačnyh vychislenij : Materialy konferencii «Ustojchivoe razvitie rossijskikh regionov: innovacii, instituty i tehnologicheskie zaimstvovanija». – Ekaterinburg, 2010.
2. Luchshie besplatnye on-lajn hranilishha. Obzor. // Chip. –2012. – № 10. – S. 76-79.
3. Mel'nikov A.V. Principy postroenija obuchajushhih sistem i ih klassifikacija / A.V. Mel'nikov, P.L. Cytovich // Jelektronnyj zhurnal «Pedagogicheskie i informacionnye tehnologii». – 2001. – № 4.
4. Zhurkin A.A. Informacionno-kommunikacionnye tehnologii adapcionnogo obuchenija s jelementami iskusstvennogo intellekta. // Uchenye zapiski: jelektronnyj nauchnyj zhurnal Kurskogo gosudarstvennogo universiteta. – 2012. – № 4 (24), T. 2. – S. 204-212.
5. Brusilovskij P.L. Adaptivnye obuchajushhie sistemy v World Wide Web: obzor imejushihhsja v rasporjazhenii tehnologij // International Forum of Educationzl Technology & Society. – <http://ifets.ieee.org/russian/depository/WWWITS.html>.
6. Duplik S.V. Modeli pedagogicheskogo testirovanija // «Vestnik Kazanskogo Gosudarstvennogo Tehnicheskogo universiteta im. A.N. Tupoleva». – № 2. – 2003 g. – s. 74-79.
7. Osnovy Oblachnyh vychislenij // Rekomendacii NIST. – Rezhim dostupa : <http://cloud.sorlik.ru/definition.html>.
8. Veselov E.A. Riski informacionnoj bezopasnosti oblačnyh vychislenij i mery po ih snizheniju. // Materialy Vserossijskogo professional'nogo foruma «Jeffektivnyj dokumentooborot v organah vlasti i mestnogo samoupravlenija» (INFODOKUM-2012).
9. Maslova N.A. Analiz i vybor metodov zashhity jekonomicheskikh dannyh /N. Maslova, K.N. Efimenko, D.S. Demchenko – Depon.rukopis' DRNTI Ukrainy, Donec.gos.tehn.un-t. – Doneck. – 2000. – 14 s.
10. Maslova N.O. Viktoristannja strategii rozpodilu dlja optimizacii obchislennja NZD u algoritmah shifruvannja // Upravljajushhie sistemy i mashiny. – Kiev. – 2002. –№ 2. – S. 74-84.
11. Maslova N.A. Informacionnaja bezopasnost' sistem upravlenija bazami dannyh // Komp'juterna matematika. Optimizacija obchislen': Zb.nauk. prac' NAN Ukraïni, institut kibernetiki im.. V.M.Glushkova. – Kiiiv. – 2001. – t.1. – S. 271-280.
12. Shupik D.Є. Pidsistema testuvannja ta zakriplennja znan' z fahovih disciplin za dopomogoju komp'jutera / D.Є. Shupik, N.O. Maslova // Materiali pershoї mizhnarodnoї naukovo-tehničnoї konferencii «Informatika j komp'juterni tehnologii». – Donec'k. – 2005, DonNTU. – s. 121-122.
13. Maslova N.O. Metodichni vkazivki do vikonannja kursovogo proektuvannja z disciplini «Osnovi vizual'nogo programuvannja» / N.O. Maslova, R.O. Sorokin. – Donec'k. – 2013. – 33 s.

RESUME

N.A. Maslova, R.A. Sorokin

The Using of Cloud Technologies as a Way to Improve the Security of Test Training Systems

In given article the analysis of training systems is carried out and their classification is executed. The requirements to designing and architecture are formulated. There are three necessary regimens for modern system: the testing, the control and training. The training systems should adapt for a level of knowledge of the users, to be intellectual, to have the distributed structure. The knowledge base of training system should be filled with the data from various areas, and to be multifunctional.

The important problem of training systems is their security. The data and elements of system should be inaccessible to copying and change. Risks of information safety and measures of their reduction therefore are considered. The advantages and lacks of the most widespread cloudy storehouses are selected.

Use of a public cloud can raise parameters of security of system. The organization, which has created cloud, serves and accepts the greatest possible measures on maintenance of safe job with him. In this case protection of the information placed on cloudy services is care of the professionals. But payment of the work of the professionals requires significant expenses. And we have characteristic risks are deficiency of the information about an accommodation a component of virtual structure, outflow and loss of the data.

Use of free-of-charge storages considerably reduces cost of support of system. The free-of-charge storages have a different level of protection. For the maximal security the data should be ciphered at reception and transfer, on the party of a server and on the party of the client.

Hybrid cloud it's one of models of cloudy storages. Thus provider of services it is possible to pass of functions of system, and the data given to place on the own reliably protected resources. Protect them with additional programs. To carry out enciphering on the party of the client. To store the keys on local computers of the developer of system.

Transition to virtual technology it's necessary stage of development of training systems. The expenses for operation of systems are reducing, the service becomes simpler. The risk of loss of the data is reduced up to 1 %. But with transition to virtual technology the organizational and administrative moments become complicated. It is necessary is weighed and is balanced to approach to the decision of questions of a safety, to take into account new risks, to transform or to design system so that her architecture was entered in cloudy services.

Статья поступила в редакцию 08.04.2013.