предназначенная для работы с крупными базами данных масштаба предприятия [1].

В виду того, что формы заявок (наименования полей, допустимые значения и т.д.) варьируются в зависимости от целевого патентного офиса, предусмотрена возможность построения динамического пользовательского интерфейса. Для реализации данного подхода созданы специальные вспомогательные таблицы в базе данных, которые хранят описание (метаданные) пользовательского интерфейса для соответствующих полей и таблиц, такие, как тип пользовательского элемента управления и его позиция на экране. Также описание содержит определенные правила заполнения полей, такие, как максимально допустимая длина, минимальное и максимальное значение, тип данных.

Система управления интеллектуальной собственностью построена по принципу «клиент-сервер». Как на стороне сервера, так и на стороне клиента, в качестве платформы программирования используется Microsoft .NET Framework и язык программирования C#, предоставляющий широкие возможности в написании корпоративного программного обеспечения [2].

Не менее важным компонентом программного комплекса является система раскрытия изобретений. В основе данной системы лежит принцип коллаборации – объединения группы лиц для реализации представленного изобретения.

Первый шаг в раскрытии изобретения – отправка заявки, происходящая в два этапа. В целях безопасности и удобства, программное средство помогает пользователю верно заполнить заявку.

Основными данными для первого этапа заполнения заявки является:

- наименование заявки;
- целевая область использования изобретения.

На втором этапе пользователю предлагается предоставить следующие данные:

- файл формы участника;
- файлы-приложения;
- цель изобретения;
- список внутренних участников (сотрудники предприятия);
- список внешних участников (лица, не являющиеся сотрудниками предприятия);
- поверенное лицо;
- руководитель исследования.

После прохождения двух этапов подачи заявки, она отправляется на подтверждение к руководителю исследования. Он тщательно просматривает заявку на предмет ошибок. Далее он имеет права перевести заявку в один из статусов: «Мало информации», «Отклонено», «Подтверждено». При переводе заявки в новый статус необходимо указать причину перевода (комментарий).

Статус «Мало информации» означает, что ответственное лицо в целом принимает заявку, однако для ее подтверждения необходимо больше информации. Заявка с таким статусом отправляется назад к оформителю.

Статус «Отклонено» подразумевает, что ответственное лицо категорически несогласно с поданной заявкой в виду определенных обстоятельств. Примерами таких обстоятельств может являться полное или частичное повторение другого изобретения, а также неактуальность или невозможность реализации.

Заявки в статусе «Подтверждено» отправляются дальше на подтверждение поверенному лицу.

Далее поверенное лицо осуществляет повторную проверку заявки и также имеет право перевести заявку в один из статусов, за исключением того, что статус «Подтверждено» будет означать то, что заявка прошла отбор и готова к разработке.

На каждом этапе действует система уведомлений, позволяющая своевременно обнаружить изменение статуса заявки, а также отслеживать весь ее путь от подачи до реализации.

Подводя итоги, можно сказать, что данная система будет полезна как организациям, разрабатывающим инновационные технологии и желающим защитить права на свою интеллектуальную собственность, так и тем, кому в своей деятельности или производстве необходимо использовать весь потенциал современных инноваций.

Список использованных источников:

1. Кригель, Алекс, SQL. Библия пользователя. Язык запросов SQL – SQL Bible. — 2-е изд./ Алекс Кригель, Борис Трухнов. - М.: Диалектика, 2009. - 752 с.

2. Рихтер, Джеффри. CLR via C#. Программирование на платформе Microsoft .NET Framework 4.5 на языке C#./ Джеффри Рихтер.- Изд-ва: Питер, Русская Редакция, 2012 г. - 656 с.

ИНФОРМАЦИОННО-СТРУКТУРНАЯ ОРГАНИЗАЦИЯ ПРОЦЕССА ОБУЧЕНИЯ

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Петров Н.А.

Скудняков Ю.А.- канд. техн. наук, доцент

В настоящее время подготовка высококвалифицированных специалистов в различных сферах человеческой деятельности может быть осуществлена путем разработки и использования информационно-структурных моделей и электронных средств обучения [1]. Разработке и использованию вышеприведенных моделей и средств организации процесса обучения посвящена данная работа.

Сначала рассмотрим традиционную технологию обучения, которая в настоящее время еще имеет место (рисунок 1).

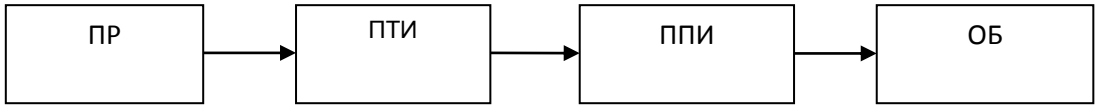

Рисунок 1– Традиционная структура обучения

На рисунке 1 показаны: ПР – преподаватель, являющийся носителем необходимой для обучения информации; ПТИ – процесс трансляции информации от преподавателя обучаемому; ППИ – процесс получения информации обучаемым; ОБ – обучаемый, получающий информацию от ПР.

В настоящее время осуществление процесса обучения по приведенной на рисунке 1 структуре является неактуальным.

Иллюстрация современного подхода организации процесса обучения представлена на рисунке 2.

Рисунок 2 – Современная общая структура обучения

Показанные на рисунке 2 модули имеют следующее назначение соответственно: ФПР – функции преподавателя, заключающиеся в организации деятельности обучаемого в инновационной обучающей среде; НКО – новое качество обучения, отражающее хороший уровень компетентности обучаемого в изучаемой области и высокую степень его мотивации к обучению; ФОБ – функции обучаемого для получения необходимых знаний, умений и навыков.

Современное инновационное обучающе-информационное пространство учебного занятия можно представить в виде схемы, показанной на рисунке 3.

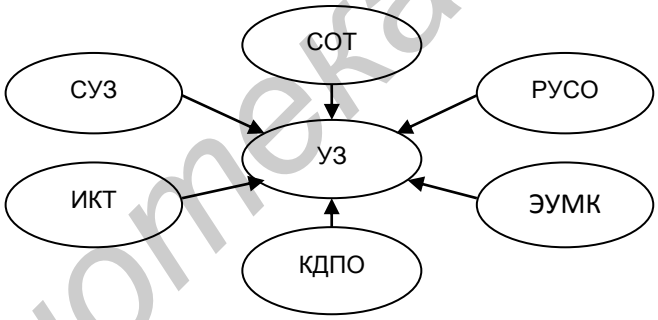

Рисунок 3 – Современное инновационное обучающе-информационное пространство учебного занятия

Названия, отражающие функции модулей структуры на рисунке 3, следующие: УЗ – учебное занятие; ИКТ – информационно-коммуникационные технологии, реализуемые в том числе с помощью современных компьютерных сетей и позволяющие обеспечивать необходимыми информационными ресурсами ИР = {$ир_j$,j = 1,2,…,n} участников учебного процесса; СУЗ – сотрудничество участников учебного занятия (преподавателя и обучаемых), позволяющее осуществлять взаимный информационный обмен между ними с целью получения новых знаний, умений и навыков; СОТ – современные образовательные технологии (модульная технология, технологии проектного, проблемного обучения, групповой дифференциации и дидактической игры), использование которых позволяет обеспечить: внедрение основных направлений педагогической стратегии: гуманизации, гуманитаризации образования и личностно-ориентированного подхода; интеллектуальное разви- тие обучаемых, их самостоятельность в процессе обучения; доброжелательность ко всем участникам учебно- го процесса; развитие творческой деятельности; РУСО – разноуровневое содержание обучения; ЭУМК – эле- ктронный учебно-методический комплекс, использование которого позволяет повысить качество подготовки обучаемых; КДПО – компетентностно-деятельностный подход в обучении.

На основе предложенных в работе информационно-структурных моделей разработано электронное средство обучения для дисциплины «Аппаратное обеспечение компьютерных сетей» в виде программного средства на языке C#.

В результате выполнения данной работы:

– для эффективной организации современного процесса обучения предложены информационно-структурные модели, обладающие наглядностью и возможностью формализации описания учебного процесса;

– разработано электронное средство обучения для изучения дисциплины по аппаратным основам современных компьютерных сетей.

Список использованных источников:
1.Хортон, У. Электронное обучение: инструменты и технологии. Пер. с англ. / У. Хортон, К.. Хортон. – М.: КУДИЦ–ОБРАЗ, 2005. 640 с.

ИССЛЕДОВАНИЕ РЕЗУЛЬТАТОВ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-СЕРВЕРА VCENTER SERVER 5.5

Институт информационных технологий БГУИР, г.Минск, Республика Беларусь

Поклонский С.А., Прузан А.Н.

Охрименко А. А. – канд. техн. наук, доцент

Рассматриваются вопросы достаточности работ по тестированию информационной безопасности программного обеспечения веб-сервера vCenter Server 5.5. Показывается, что качество и объём таких работ недостаточны для полного устранения дефектов программного обеспечения сервера.

Под угрозой информационной безопасности информационного объекта принято понимать возможные воздействия на него, приводящие к ущербу. Некоторое свойство объекта, делающее возможным возникновение и реализацию угрозы, называется уязвимостью. В докладе на примере веб-сервера vCenter Server делается попытка исследования результатов тестирования информационной безопасности таких сложных информационных объектов, как веб-сервера.

Под веб-сервером обычно понимают сервер, принимающий HTTP-запросы от клиентов (обычно веб-браузеров) и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными. Веб-сервером называют как ПО, выполняющее функции веб-сервера, так и непосредственно компьютер, на котором установлено это ПО.

В последнее время, когда в ИТ-индустрии стали широко использоваться облачные технологии [1, 2], для реализации последних очень популярной стала серверная виртуализация. Одним из главных компонентов серверной виртуализации, предложенной американской компанией VMware, является VMware vSphere – платформа для виртуализации ИТ-инфраструктуры предприятия. Платформа vSphere подразумевает одновременное использование ESXi хостов (x86) и vCenter Server для их централизованного управления.

vCenter Server – главный инструмент управления для администраторов vSphere. Он предоставляет единую точку контроля за всеми компонентами в виртуальном датацентре и выполняет некоторые важные функции. vCenter позволяет конфигурировать новые ESXi хосты, хранилище (в т. ч. облачное [1, 2]), сеть и характеристики виртуального оборудования различных инфраструктурных компонентов, создавать и импортировать новые виртуальные машины, производить мониторинг и отчёты о производительности гостевой ОС, виртуальных машин и ESXi хостов. vCenter управляет правами, разрешениями, ролями на различных уровнях виртуальной инфраструктуры, унифицирует ресурсы различных хостов ESXi и позволяет обеспечивать общий доступ к ним для любых виртуальных машин в датацентре. Это достигается назначением ресурсов кластера хостов ESXi виртуальным машинам с учётом назначенных администратором политик.

При разработке программного обеспечения веб-серверов и веб-приложений широко используется такой вид нефункционального тестирования как тестирование безопасности. При этом применяются такие вспомогательные очень сложные программные средства, как Wapiti 2.1.0, Netsparker Community Edition, N-Stalker Free Version, Websecurify, Skipfish, OWASP WebScarab Project и другие.

Тем не менее, проведенное тестирование не всегда помогает полностью выявить уязвимости веб-сервера. Пример: 29 декабря 2016 года американским институтом NIST была выявлена и внесена в базу уязвимостей новая уязвимость CVE-2016-7460 сервера vCenter Server 5.5. Уязвимость была обнаружена в одной из функций ПО сервера – функции Single Sign-On. Уязвимость позволяла удаленным злоумышленникам читать произвольные файлы или вызывать отказ в обслуживании через XML-документ содержащий объявление внешней сущности, связанной с ссылкой на сущность, относящуюся к XML External Entity (XXE) уязвимости. На стадии тестирования безопасности сервера уязвимость не удалось обнаружить, и только к 01.03.2017 компании VMware удалось устранить присутствующие в ПО сервера дефекты. Компания при этом понесла как материальные (известно, что цена устранения дефекта тем меньше, чем раньше он обнаружен), так и моральные (потеря репутации у потребителей) убытки.

Вывод: Тестированию безопасности на стадии разработки ПО серверов уделяется недостаточно внимания. Объём работ по тестированию безопасности надо увеличить, а их качество – повысить.

Список использованных источников:
1. Прузан А.Н. Мониторинг инцидентов информационной безопасности в облачных вычислениях на малом предприятии/ Прузан А.Н., Николаенко В. Л., Сечко Г. В. // Доклады БГУИР. – 2015 – № 7 (93). – С. 126–128.
2. Николаенко, В.Л. Опыт мониторинга инцидентов информационной безопасности в облачных вычислениях/ В.Л. Николаенко, А.Н. Прузан, Г.В.Сечко, Т.Г. Таболич // Сб. статей III межд. заоч. НПК «Информационные системы и технологии: управление и безопасность» (декабрь 2014). – Тольятти- 2014. – 345 с. – С. 209–215