РАЗРАБОТКА ЗАЩИЩЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ТРУДОУСТРОЙСТВА ВЫПУСКНИКОВ ВУЗОВ

А.А. Шайдуров
Алтайский государственный университет, г. Барнаул

Вопрос о трудоустройстве после обучения в ВУЗе является предметом размышления у всех студентов. В каких дисциплинах нужно получить наиболее глубокие знания - одна из основных проблем, стоящих перед абитуриентами. Любая должность имеет свои собственные требования, которые должны быть удовлетворены. Студент, в свою очередь, должен обладать определенными профессиональными навыками, умениями, соответствовать требованиям, которые выдвигает работодатель.

Наиболее распространенные автоматизированные системы трудоустройства выпускников позволяют следующее.

1. Работодателям - осуществлять поиск соискателей на замещение вакантных должностей среди студентов и выпускников учреждений профессионального образования всех субъектов Российской Федерации;
2. Студентам - расширять параметры поиска работы во всех субъектах Российской Федерации соответственно полученным знаниям, устремлениям и карьерным амбициям;
3. Органам исполнительной власти, имеющим в своем ведении образовательные учреждения и осуществляющим управление в сфере образования - оперативно принимать управленческие решения по различным направлениям деятельности сферы образования, в том числе связанным с приведением объемов и профилей подготовки квалифицированных кадров в соответствии с потребностями рынка труда субъектов Российской Федерации [1, 2].

Но такие системы не могут дать студентам исчерпывающую информацию о тех дисциплинах, которые ему необходимо глубоко изучать, для того, чтобы занимать желаемую должность. С учетом вышесказанного возникает необходимость создания системы, предоставляющей помощь студенту при выборе будущей должности (профессии). Такая система позволит студенту исходя из должности, которую в будущем он хочет занимать, определить те дисциплины, на которые стоит обратить наибольшее внимание, для того чтобы соответствовать компетенциям, необходимым при исполнении обязанностей. Данная информационная система может применяться в ВУЗах заведующим кафедрой, в целях помощи студентам в определении их дальнейшей учебной и трудовой деятельности.

Принцип работы такой системы заключается в том, что на этапе наполнения информационной системы, на вход программы поступают данные в виде списка дисциплин, причем каждой дисциплине соответствует тематический план занятий, а так же список соответствующих компетенций. Каждая компетенция имеет описание. Так же на вход системы подаются должности, с соответствующими им требованиями, которые сохраняются в информационную базу 1с. Назначение разрабатываемой системы заключается в формировании соответствий между изучаемыми дисциплинами и должностями. Соответствия формируются на основе выявления совпадений между требованиями к должностям, компетенциями дисциплин и тематическим планом дисциплин.

В соответствии с обеспечением информационной безопасности, информационная система трудоустройства выпускников была построена на базе 1С:Предприятие 8. Система 1С:Предприятие 8 предлагает современный механизм аутентификации, как один из инструментов администрирования. Он позволяет определить, кто именно из пользователей, перечисленных в списке пользователей

системы, подключается к Программе в данный момент, и предотвратить несанкционированный доступ в Программу.

В 1С:Предприятие 8 поддерживается три вида аутентификации, которые могут использоваться в зависимости от конкретных задач, стоящих перед администратором информационной базы:

- аутентификация 1С:Предприятия - аутентификация по созданному в Программе пользователю и паролю;
- аутентификация операционной системы - в Программе для пользователя выбирается один из пользователей операционной системы. Программа анализирует, от имени какого пользователя операционной системы выполняется подключение к Программе, и на основании этого определяет соответствующего пользователя Программы;
- OpenID-аутентификация - аутентификацию пользователя выполняет внешний OpenID-провайдер, хранящий список пользователей.

Базовый принцип защиты данных в клиент-серверном варианте заключается в том, что пользователи не имеют прямого доступа к файлам информационной базы. «Посредником» между клиентами 1С:Предприятия 8 и сервером СУБД является рабочий процесс rphost, который обращается с запросом к СУБД от имени своей учетной записи. Затем полученный результат возвращает клиенту. Однако, использование клиент-серверного варианта не означает автоматически стопроцентную защиту информации.

Для обеспечения комплексной безопасности системы необходима настройка защищенности информационной системы на различных участках. Можно выделить три основных участка защиты данных:

- клиент - кластер 1С:Предприятия;
- кластер 1С:Предприятия – СУБД;
- пользователь системы.

Обеспечение защиты данных «клиент – кластер 1С:Предприятие 8» осуществляется следующим образом. При подключении к информационной базе пользователь указывает свой логин и пароль. Если в системе существует учетная запись с соответствующими параметрами, то доступ разрешается. Учетная запись создается для каждой информационной базы, используемой пользователем. При этом выполняется запрос к рабочему процессу кластера, расположенному на сервере 1С:Предприятия. Информация, передаваемая по сети на данном участке может быть зашифрована полностью или частично. Безопасность работы кластера обеспечивается исполнением приложения от имени учетной записи 1С:Предприятия в Windows. Контроль доступа к общим настройкам кластера осуществляется от имени учетной записи администраторов кластера 1С:Предприятие 8.

Обеспечение защиты данных «клиент – кластер 1С:Предприятие 8». Защита данных, передаваемых между кластером серверов 1С:Предприятия и сервером СУБД, осуществляется средствами СУБД. MS SQL Server позволяет организовать шифрование передаваемых данных с помощью сертификатов.

Участок защиты данных «пользователь системы». Даже самая совершенная защита не может гарантировать безопасность системы, если к ней имеет доступ недобросовестный или неаккуратный пользователь. Таблицу 1 можно использовать при проведении аудита безопасности системы.

При построении информационной системы аудит безопасности проводился следующим образом:

1. При проверке доступа пользователей к административным действиям конфигуратора был составлен список всех ролей, имеющих права на выполнение административных функций. Затем был составлен список пользователей, которые

приписаны к этим ролям. Далее была осуществлена проверка, что для каждого пользователя из списка верно следующее:

- Сотруднику действительно необходимы административные права для выполнения его служебных обязанностей.
- Сотрудник имеет достаточную квалификацию для того, чтобы не причинить непреднамеренный вред системе.
- Сотрудник пользуется доверием.

Таблица 1. Аудит безопасности системы

Вероятная угроза безопасности	Участок	Вероятность	Последствия	Вероятный злоумышленник
1. Доступ пользователей к административным действиям конфигуратора	Клиент	Высокое	Копирование всей информации	Программист, продвинутый пользователь
2. Отсутствие разграничений доступа в режиме 1С:Предприятие"	Клиент	Среднее	Копирование ключевой информации	Программист, продвинутый пользователь
3. Несанкционированный доступ к данным сервера СУБД	СУБД	Средняя	Порча информации, копирование информации	Администратор
4. Использование старых логинов	Клиент, Кластер, СУБД	Низкая	Последствия зависят от прав учетной записи	Уволенный сотрудник
5. Несанкционированный доступ к файлам кластера серверов	Кластер	Низкая	Порча информации, возможность создания новых баз	Администратор, программист
6. Наличие уязвимостей операционной системы, СУБД	Клиент, Кластер, СУБД	Низкая	Повышение прав с помощью «ломалок», опубликованных в интернете, возможно полное копирование информации	Администратор, Продвинутый пользователь
7. Вирусы, трояны, логгеры	Клиент, Кластер, СУБД	Низкая	Порча информации, получение данных, раскрытие паролей пользователей	Администратор, Продвинутый пользователь
8. Пароли на мониторах, слабые пароли	Клиент	Средняя	Несанкционированный доступ к учетным записям пользователей с последующим доступом к данным	Продвинутый пользователь, уволенный сотрудник
9. Перехват информации	Клиент-Кластер, Кластер-СУБД	Минимальная	Перехват паролей с последующим доступом к данным	Высоко квалифицированный системный программист, сетевой специалист

2. Проверка на отсутствие разграничений доступа в режиме 1С:Предприятие осуществлялась путем сверки прав учетных записей пользователей и тех уровней доступа, которые должны иметь сотрудники. Угрозой считалось наличие у пользователя прав доступа к той информации, которая не должна быть ему доступна.

3. Несанкционированный доступ к данным сервера СУБД определялся по следующим критериям:

- Наличие включенного (enabled) логина sa для используемого MS SQL Server;
- Учетная запись службы MS SQL Server входит в доменные группы;
- Имеется доступ к файлам, хранящимся на компьютере, на котором запущен MS SQL Server;
- Сервер 1С:Предприятия и SQL Server запущены на одном компьютере;
- Открыт доступ к серверу учетных записей пользователей;
- Слабые пароли логинов MS SQL Server;
- Включена возможность работы с командной строкой службой MS SQL Server.

4. Проверка на использование старых логинов необходима, так как среди учетных записей, используемых системой могут оставаться те, которые принадлежали уволенным сотрудникам. В силу этого была разработана автоматизированная процедура проверки длительной неактивности учетных записей и их автоматического удаления

5. Несанкционированный доступ к файлам кластера серверов определялся по следующим признакам возможной угрозы:

- отсутствие учетных записей администраторов кластера;
- использование одной учетной записи для служб ragent, rmngr, rphost;
- файловый доступ к серверу;
- физический доступ к серверу.

Также, для защиты персональных данных от несанкционированного доступа может быть использован специальный программный комплекс 1С: Предприятие 8.3z (ЗПК). Защищенный комплекс может применяться в государственных информационных системах до 1 класса защищенности включительно и в информационных системах до 1 уровня защищенности персональных данных включительно.

1С: Предприятие 8.3z может применяться для организации безопасности персональных данных в соответствии Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными приказом ФСТЭК России от 18 февраля 2013 г. N 21, в информационных системах персональных данных всех уровней защищенности [4].

После проведения работ по обеспечению информационной безопасности [5] взаимодействие с информационной системой осуществляется следующим образом. При работе с информационной системой работодатель загружает в информационную базу список должностей с их требованиями. Заведующий кафедрой загружает учебный план и рабочие программы дисциплин (РПД) того или иного направления (специальности).

В процессе работы системы студент выбирает должность, которую он в дальнейшем планирует занимать и система автоматически ведет поиск соответствующих дисциплин, указывая конкретные разделы учебной программы, интеллектуально сравнивая компетенции и требования с помощью тезауруса.

На выходе система выдает список рекомендованных дисциплин, необходимых для получения желаемой должности, ранжированный по значимости включенных в

список дисциплин. На рисунок 1 представлена структурная схема проектируемой системы.

Система должна выполнять следующие задачи:

1. хранить данные в информационной базе: УП, РПД, должности и требования к ним, компетенции и их описание;
2. выявлять соответствия посредством соотнесения слов по смыслу с помощью тезауруса;
3. выводить темы занятий, полученные после проведения сравнения требований и компетенций.

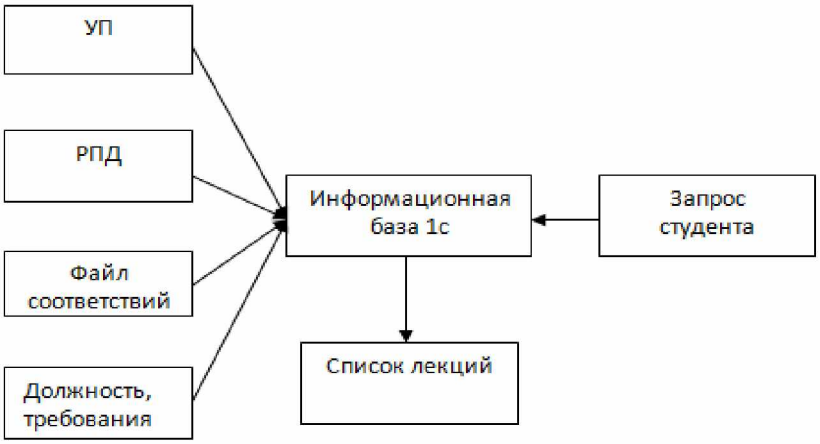

Рисунок 1. Структура информационной справочной системы трудоустройства выпускников.

Для реализации информационной системы трудоустройства на базе платформы 1С:Предприятие 8 были созданы объекты конфигурации.

Для хранения всей необходимой информации используется шесть справочников:

- «Дисциплины» - содержит наименования дисциплин;
- «Должности» - содержит наименования должностей;
- «Компетенции» - содержит информацию о наименованиях компетенций, о их содержании и соответствующих направлениях
- «Организации» - содержит наименование организации, адрес ее местоположения, номер телефона и ИНН;
- «Направления» - содержит наименования направлений подготовки;
- «Требования» - содержит требования работодателей к принимаемым работникам в разрезе должностей.

В информационной базе документ «Требования к должностям» предназначен для внесения данных об организации, должности и требованиях к ней. Документ совершает движение по регистру сведений «Требования». Процедура проведения данного докумета позволяет не только провести документ по регистру сведений «Требования», но и исключает возможность повторного внесения одинаковых данных.

Разработана внешняя обработка «Загрузка информации», которая предназначена для автоматической загрузки данных из Учебного плана и «Файла соответствий» в информационную базу. Обработка «Получение дисциплин» предназначена для автоматического вывода списка дисциплин, изучение которых необходимо для получения указанной студентом должности по его направлению. Непериодический регистр сведений «Компетенции» предназначен для хранения наименований дисциплин, соответствующих им компетенций, для определенного направления.

Система имеет несколько интерфейсов, определенных для каждого типа пользователей, а именно: Администратор, Студент, Работодатель, Заведующий [6, 7]. Администратор-пользователь, обладающий всеми правами, который может производить изменения в самой конфигурации. Студент – пользователь, который не производит никаких изменений, а лишь получает необходимую ему информацию. Работодатель – пользователь, который заносит в систему данные о должностях. Заведующий – пользователь, который загружает в базу данных учебные планы.

Студент входит в систему, выбирает должность, которую в будущем он хочет занимать, система автоматически выводит список лекций определенных дисциплин, необходимых для ее получения.

Таким образом, разработанная информационная система на данный момент времени позволяет автоматически загружать необходимые данные в базу данных 1С и производить автоматическое сравнение требований и компетенций. В результате формируется список необходимых дисциплин, на изучение которых студент должен обратить особое внимание.

Также следует отметить, что для обеспечения требований безопасности были удовлетворены следующие требования к защите системы:

- идентификация, проверка подлинности и контроль доступа субъектов;
- регистрация и учет (входа/выхода субъектов в/из системы; выдачи печатных выходных документов; запуска/завершения программ и процессов; доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи).

Библиографический список.

1. Информация о системе АИСТ. [Электронный ресурс] // URL: http://aist.magtu.ru.
2. Введение в АИСТ. [Электронный ресурс]// URL: http://aist.elsu.
3. Радченко М.Г., Ажеронок В.А., Габец А.П., Гончаров Д.И., Козырев Д.В., Кухлевский Д.С., Островерх А.В., Хрусталева Е.Ю. Профессиональная разработка в системе 1С: Предприятие 8, Издание 2. - 1С-Паблишинг. - 2012. - Т.1 - 704 с., Т. 2 - 704 с.
4. Габец А.П., Гончаров Д. И. 1С: Предприятие 8.1. Простые примеры разработки. // 1С-Паблишинг. – 2008. – 383 с.
5. Минакова Н.Н., Поляков В.В., Толстошеев С.Н. Методы технической и правовой защиты информации в сети Интернет //Барнаул: Изд-во Алтайского ун-та, 2015. – 155с.
6. Радченко М.Г. 1С: Предприятие 8.1. Практическое пособие разработчика. Примеры и типовые приемы //1С-Паблишинг. – 2008. – 330 с.
7. Примеры и советы по программированию в системе 1С:Предприятие 8.1. [Электронный ресурс] // URL: http://kod1c.narod.ru/Index.html.