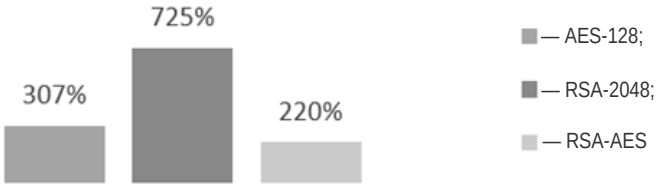

Рисунок 6 — Увеличение времени выполнения шифрования
и расшифровки при падении мощности компьютера

Заключение. Проведя тестирование распространенных алгоритмов шифрования как симметричных, так и асимметричных, мы выделили AES-алгоритм как один из оптимальных алгоритмов, обладающих как высокой скоростью, так и достаточной надежностью. Однако, как оговаривалось ранее, у него есть недостаток, который заключается в проблеме передачи ключа. Поэтому можно утверждать, что протокол RSA-AES является оптимальным, потому что включает в себя алгоритм AES, при этом лишая его главного недостатка — передачи секретного ключа. В результате исследования был разработан программный продукт, использующий стандартные библиотеки шифрования Java, а также проведены тестирования как на стандартном компьютере, так и на маломощном. Это позволяет утверждать, что сделанные выше выводы верны.

Данные исследования могут быть использованы при разработке программных продуктов, в которых необходимо реализовать защиту информации. На основе проведенных исследований будет создан программный продукт на языке программирования Java, предназначенный для передачи сообщений по зашифрованным каналам. Данный программный продукт будет использовать протокол RSA-AES, а также протокол Диффи—Хеллмана.

Список цитируемых источников

1. *Баричев, С. Г.* Основы современной криптографии / С. Г. Баричев, Р. Е. Серов, В. В. Гончаров. — М. : Горячая Линия — Телеком, 2011. — 176 с.
2. *Бернет, С.* Криптография. Официальное руководство RSA Security / С. Бернет, С. Пэйн. — М. : Бином-Пресс, 2009. — 384 с.
3. *Шнейер, Б.* Прикладная криптография / Б. Шнейер. — М. : Триумф, 2002. — 816 с.

УДК 004.657

А. В. Суряпина
Учреждение образования «Барановичский государственный университет», Барановичи

АВТОМАТИЗИРОВАННАЯ СИСТЕМА КОНТРОЛЯ ПРОХОЖДЕНИЯ ПРАКТИКИ СТУДЕНТАМИ В КОМПАНИИ “JAZZTEAM”

Введение. Проблема совершенствования процесса образования постоянно находится в центре внимания общества и государства. Одним из наиболее важных этапов учебного процесса является практика студентов на предприятиях.

Прохождение практики представляет собой планомерную и целенаправленную деятельность студентов по освоению избранной специальности, углубленному закреплению теоретических знаний, профессиональных, творческих и исполнительских навыков на каждом этапе обучения.

Целью практики является обучение студентов практическим навыкам и подготовка их к самостоятельной работе по избранной специальности. Практика должна проводиться в организациях, соответствующих профилю подготовки специалистов.

Одной из таких организаций является компания “JazzTeam” — молодая инновационная компания с офисами в Солигорске и Минске, созданная экспертами с опытом участия в проектах мирового уровня. Она является Agile-компанией, концентрируемой на всех проявлениях технологии и платформы Java (J2SE, J2EE, Android, SOA, OSGI, Automation, Open Source) и оказывающей широкий спектр инновационных услуг на ИТ-рынке.

Уже несколько лет в компании “JazzTeam” проходят практику учащиеся различных учебных заведений, в связи с этим возникла необходимость создания автоматизированной системы контроля прохождения практики студентами в данной организации.

Программный продукт работает с базой данных, так как сегодня их использование становится неотъемлемой частью функционирования любых организаций и предприятий.

База данных помогает систематизировать и хранить информацию из определенной предметной области, облегчает доступ к данным, поиск и предоставление необходимых сведений, обеспечивает их целостность и безопасность [1].

Для разработки приложения была выбрана мощная интегрированная среда разработки профессионального уровня — MS Visual Studio 2012. Для написания программы использовался объектно ориентированный язык высокого уровня C#. Для проектирования и реализации работы с базой данных была выбрана одна из самых популярных систем управления базами данных — Microsoft SQL Server 2012. Построение диаграмм проекта проходило в программе Rational Rose, которая представляет собой CASE-средство проектирования и разработки информационных систем и программного обеспечения.

Основная часть. Программа позволяет получить студенту и его руководителю всевозможные сведения о прохождении практики в компании “JazzTeam”, а также производить добавление, редактирование, удаление и поиск необходимой информации, осуществлять планирование выполняемых задач и взаимодействие практиканта со своим руководителем.

Представима физическую модель базы данных, которая определяет способы размещения информации в среде хранения и способы доступа к этим данным, которые поддерживаются на физическом уровне (рисунок 1).

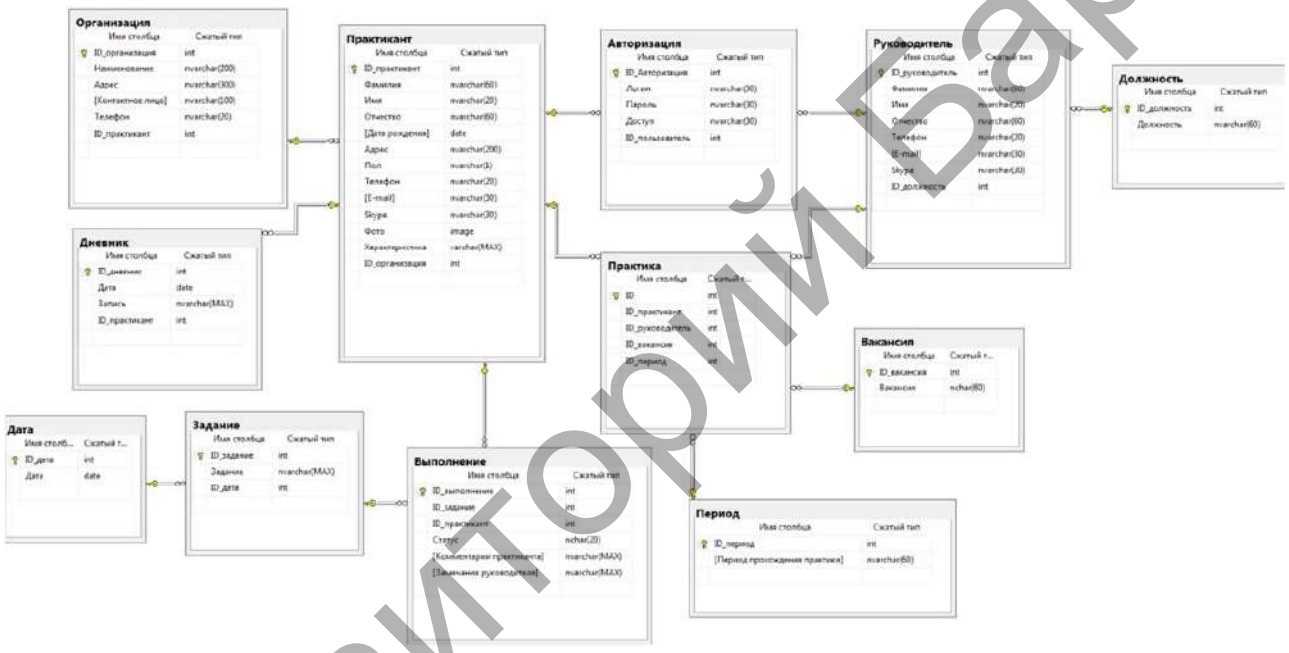

Рисунок 1 — Физическая диаграмма данных

Для запуска программы сначала необходимо пройти авторизацию пользователя, которая включает в себя ввод логина и пароля. Подключение работает в сетевом режиме.

Работать с базой данных смогут только пользователи двух типов: «руководитель», «практикант».

В зависимости от типа пользователю предоставляются те или иные права доступа и рабочий интерфейс программы. Данные меры представляют собой простой и эффективный способ защиты данных от несанкционированных действий пользователя.

Диаграммы вариантов использования (use case diagrams) являются графическим представлением взаимодействия пользователя и компьютерной системы. Каждый вариант использования охватывает некоторую очевидную для пользователей функцию системы и решает некоторую дискретную задачу пользователя. Список всех вариантов использования фактически определяет функциональные требования к системе [2]. Представим диаграммуUse Case (рисунок 2).

Каждый пользователь может осуществлять просмотр, сортировку и поиск необходимой информации. Руководители могут также добавлять, удалять и редактировать различные данные. Они отвечают за внесение новой информации о студентах и организациях, заполнение плана прохождения практики, проверку выполненных заданий, оценку и характеристику практикантов. Кроме этого руководитель может осуществлять управление другими пользователями: добавлять, назначать им права доступа и удалять уже существующих.

Практикант помимо основных функций может изменять статус выполнения задания, оставлять комментариии, просматривать свою характеристику и вести дневник практики.

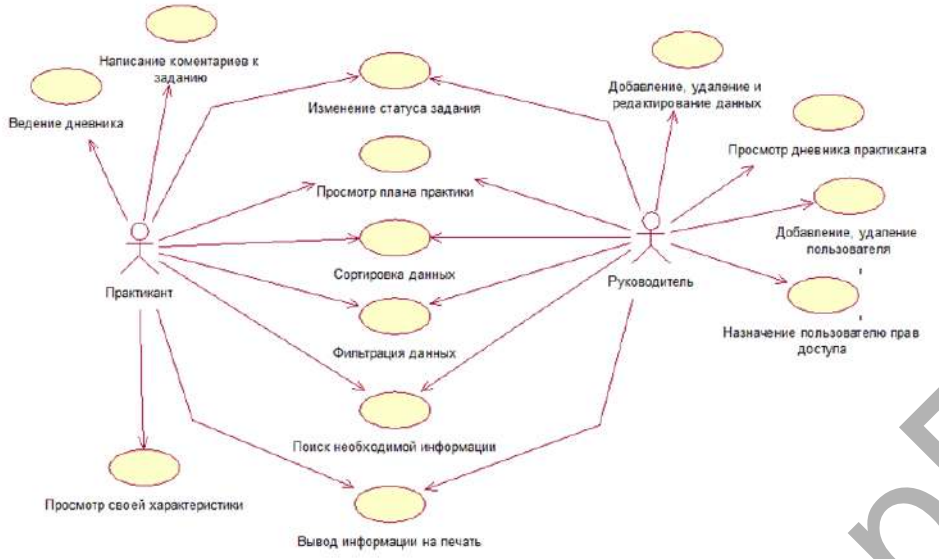

Рисунок 2 — Диаграмма Use Case

При одновременной работе с базой данных нескольких пользователей происходит автоматическое обновление данных, поэтому каждый из пользователей может видеть все изменения, произведенные на другом компьютере.

Заключение. В результате изучения новых технологий в разработке приложений баз данных была создана программа, позволяющая упростить работу с практикантами на предприятии “JazzTeam”. Полученное программное средство позволяет управлять хранящейся информацией, обеспечивает простоту и легкость использования данных, осуществляет их поиск и защиту, организовывает работу с учетными записями пользователей приложения, а также обладает приятным интерфейсом, понятным пользователю.

Список цитируемых источников

1. *Петкович, Д.* Microsoft SQL Server 2012. Руководство для начинающих : пер. с англ. / Д. Петкович. — СПб. : БХВ-Петербург, 2013. — 816 с.
2. *Боггс, У.* UML и Rational / У. Боггс, М. Боггс. — М. : Лори, 2001. — 582 с.

УДК 004.85

Е. И. Сушко
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск

ПРИМЕНЕНИЕ МОДЕЛИ ЛИЧНОСТИ ЧЕЛОВЕКА В РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМАХ

Введение. Рекомендательные системы помогают пользователям в выборе нужных товаров или услуг, предоставляя среди огромного объема имеющейся информации персонализированные предложения, которые соответствуют их потребностям и ограничениям. В последние годы наблюдается повышенный исследовательский интерес к ориентированным на пользователя подходам в рекомендательных системах, в которых были исследованы различные психологические аспекты (например, индивидуальность и эмоции) по сравнению с классическими подходами в рекомендательных системах [1; 2]. Важной функцией рекомендательной системы является помощь людям в принятии более обоснованных решений. Так как личностные черты пользователя играют важную роль в принятии решений, их следует учитывать при построении рекомендательных систем [3].

Основная часть. Индивидуальность (личность) показывает, как различные индивидуумы отличаются друг от друга своими устойчивыми эмоциональными, межличностными, эмпирическими, поведенческими и мотивационными стилями. В терминологии рекомендательных систем личность можно рассматривать как профиль пользователя, который не зависит от контекста (она не изменяется со временем, местоположением или каким-либо другим контекстом) и не зависит от домена (она не меняется в разных доменах, например, в книгах,