УДК 004

ПРОГРАММНЫЙ КОМПЛЕКС «REMEMBER ME»

Кошеутова Н.В., Осина П.М.
Научный руководитель: Шерстнев В.С., к.т.н., доцент кафедры ВТ

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: polinaosina14@gmail.com, nat.dar@mail.ru

The article describes the importance of time management and effective planning in modern society and is devoted to an Android OS app development. It points out the main features of a mobile application such as cross-platform capability and synchronization. Much attention is given to the software architecture as well as user data protection via password hashing methods.

Key words: *time management, application, development, security, hashing, password*

Ключевые слова: *планирование, приложение, разработка, безопасность, хэширование, пароль.*

Управление временем для современного человека является основным понятием, благодаря которому достигается эффективность и продуктивность любых процессов. Тот кто добился успеха в своей жизни, много времени посвящают планированию. Ежедневное планирование просто необходимо для повышения производительности и эффективного управления временем.

В современном мире каждый первый человек имеет смартфон, на котором могут быть установлены приложения–органайзеры. Благодаря данным приложениям планирование дел становиться удобным, быстрым, а главное мобильным. Но, к сожалению не все приложения обладают полным функционалом, который необходим пользователю.

Таким образом, актуальна разработка многофункционального, кроссплатформенного комплекса, который позволит управлять делами напрямую как с мобильного устройства, так и персонального компьютера. При создании данного комплекса, необходимо учитывать множество факторов, главным из которых является безопасность персональных данных пользователя от различных злоумышленников.

Целью данной работы является разработка программного комплекса «Remember me» необходимого для управления расписанием и собственными мероприятиями. Данный комплекс позволяет управлять делами прямо с мобильного телефона, а также с персонального компьютера, синхронизируя данные между устройствами. В состав программного комплекса входит мобильное приложение под Android OS, web-приложение, а также web-сервис, и приложение администратора.

Для определения основных функций программного комплекса необходим объективный анализ рынка приложений аналогов, а также изучение слабых и сильных сторон других продуктов, их отличия от программного комплекса «Remember me», изучение будущей конкурентоспособности разрабатываемого программного комплекса и потребностей пользователей.

Проведя анализ рынка приложений-органайзеров, ежедневников, можно выделить шесть основных, наиболее популярных программных продуктов с аналогичными функциями:

- BossNote;
- Jorte;
- Помнить все;
- iStudiez.

Данные приложения совместно имеют такие функции, как: запись события/мероприятия с напоминанием, определение местоположения события на карте, синхронизация записей между устройствами, просмотр календаря с событиями, настройки формата отображения записей (сортировки, порядок отображения и т. д.), отметка о выполненном задании, мероприятии, изменение записей о событиях.

На основании проведенного анализа функций приложений аналогов были выявлены функции программного комплекса «Remember me». Для того чтобы информация, занесенная пользователем на ПК или мобильном телефоне также была доступна на других устройствах, необходима функция синхронизации. Пользователь может устанавливать для событий напоминания, указать местоположение создаваемого события на карте, а также у каждого мероприятия есть уровень приватности. Для использования системы необходима регистрация. После регистрации пользователю предоставлена возможность выбрать друзей из списка пользователей, а также просматривать список дел друга, если на них установлен, допустимы уровень приватности – для всех, или для друзей. Также в данном приложении пользователь может синхронизировать общие дела (с открытым уровнем приватности) со своими друзьями.

На основании заявленных выше функций программного комплекса, архитектура данного комплекса должна быть гибкой и обеспечивать простое и быстрое взаимодействие клиентов с сервером, а также с сервисами GoogleMap.

Архитектура изображена на рис. 1. Для осуществления возможности использовать данный комплекс на любом устройстве необходимо разработать два клиентских приложения для пользователей: мобильное приложение для Android OS и web-приложение для браузера. Для возможности управлять системой в экстренных ситуациях необходимо web-приложения для администратора системы. Для обеспечения синхронизации между устройствами вся информация должна храниться в базе данных на сервере и представлять собой облачное хранилище. Для повышения скорости взаимодействия клиентской части и базы данных все запросы от клиента к базе данных отправляются не напрямую, а при помощи web-сервиса. Web-сервис является связующим звеном между клиентской частью и базой данных.

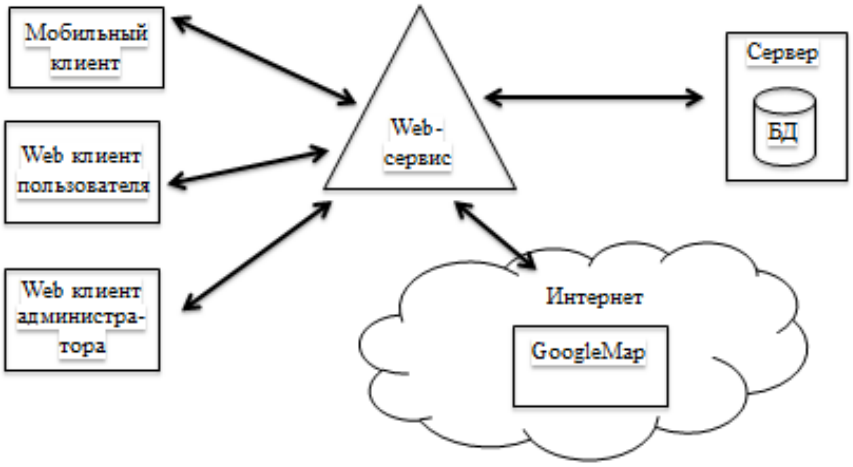

Рис. 1. Архитектура программного комплекса «Remember Me».

На основе разработанной архитектуры и основных функций будущего программного комплекса были выбраны следующие средства разработки:

- для разработки мобильного клиента: Android Studio, язык программирования Java;
- разработки базы данных: для web-сервера – MySql, для мобильного приложения – SQLite;
- разработки web-сервис – язык программирования PHP;
- разработки web-клиент – язык программирования PHP, язык разметки гипертекста HTML.

После выбора средств разработки стал вопрос обеспечения безопасности хранения и передачи данных. Для этого были исследованы основные методы, используемые в защите информации в целом, а так же какие способы реализованы в выбранных нами средствах разработки [1].

Самой главной статьей в обеспечении безопасности является хэширование паролей, данную операцию необходимо проводить при разработке приложений, которые принимают пароли от пользователей. Без хэширования пароли могут быть украдены из базы данных и все пользователи останутся без своих профилей в системе [2].

Многие разработчики хэшируют пароли пользователей с помощью популярных функций, таких как *md5()* и *sha1()*. Такие хэширующие алгоритмы как MD5, SHA1 и SHA256 очень быстрые и эффективные. Но при наличии современных технологий и оборудования, стало довольно просто выяснить результат этих алгоритмов. Из-за той скорости, с которой современные компьютеры могут «обратить» эти хэширующие алгоритмы, многие профессионалы компьютерной безопасности строго не рекомендуют использовать их для хэширования паролей [3].

Существует несколько способов наиболее надежного хэширования паролей: первый из них – использовать несколько раз функцию *md5()* или *sha1()*, например *md5(md5($password));* второй способ – совмещать две функции, например, *sha1(md5($pass));* третий – способ использовать функцию *crypt()*, которая поддерживает несколько алгоритмов хэширования в PHP 5.3 и новее. Функция *crypt()* имеет параметр *salt* – это кусочек дополнительных данных, которые делают хэши более устойчивыми к взлому.

Наиболее из распространенных уязвимостей баз данных являются SQL-инъекции. SQL-инъекция – это разновидность уязвимости, которая позволяет заменить sql-запрос инородными данными. Защититься от данной уязвимости можно несколькими способами, и самые простые из них: первый способ – не вставлять напрямую переменную, которую ввел пользователь в SQL-запрос, а пропустить ее через такие функции как, *mysql_real_escape_string(),* которая экранирует специальные символы в строке [4]; второй способ – использовать встроенные функции PHP, для подготовки SQL-запросов, например, *mysqli_prepare()* подготавливает SQL запрос и возвращает указатель на это выражение, который может использоваться для дальнейших операций с этим выражением, в случае если запрос содержит ошибку, данная функция возвращает значение false [5].

Список литературы

1. Мао В. Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 763 с.
2. Яргер Р.Д., Риз Д., Кинг Т. MySQL и mSQL. Базы данных для небольших предприятий и Интернета. – СПб.: Символ-Плюс, 2000. – 560 стр.
3. PHP, безопасное хэширование паролей [Электронный ресурс]. – Режим доступа: http://php.net/manual/ru/faq.passwords.php/, свободный (Дата обращения: 10.03.2016).
4. PHP, SQL-инъекции [Электронный ресурс]. – Режим доступа: http://php.net/manual/ru/security.database.sql-injection.php/, свободный (Дата обращения: 10.03.2016).
5. Руководство по PHP [Электронный ресурс]. – Режим доступа: http://php.net/manual/ru/mysqli.prepare.php/, свободный (Дата обращения: 17.03.2016).