Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.55

ПАЖИТНЫХ
Иван Павлович

РАЗРАБОТКА ПЛАТФОРМЫ КОРПОРАТИВНЫХ СКИДОК

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра информатики и вычислительной техники

по специальности 1-40 81 01 – Информатика и технологии разработки
программного обеспечения

Минск 2020

Работа выполнена на кафедре информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **СТЕРЖАНОВ Максим Валерьевич,**
кандидат технических наук, доцент кафедры информатики учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **БУЛОВА Александр Дмитриевич,**
кандидат технических наук, доцент кафедры экономической информатики учреждения образования «Белорусский государственный экономический университет»

ВВЕДЕНИЕ

За последние десятилетия во всем мире наблюдается колоссальный технологический рост. Тем не менее, только несколько секторов индустрии стали свидетелями беспрецедентного роста, одной из которых является индустрия разработки мобильных приложений. Рынок мобильных приложений развивается быстрыми темпами и по прогнозам аналитиков рост будет увеличиваться. Согласно статистическим данным, в 2020 году доходы приложений достигнут 189 миллиардов долларов, а в 2021 прогнозируется рост на 375%.

Диссертационная работа посвящена разработке алгоритмов и программного обеспечения в виде кроссплатформенного мобильного приложения, которое будет обеспечивать взаимодействие представителей услуг и корпоративных клиентов.

Актуальность работы обусловлена тем, что в настоящее время все больше компаний, как больших, так и маленьких в борьбе за сотрудников предоставляют им различные преференции, называемые “социальным пакетом”. Они включают в себя различные скидки и акции в заведениях сферы услуг и здравоохранения: медицинские центры, тренажерные и фитнес залы, кофейни, рестораны, магазины и так далее.

Для получения скидки сотруднику необходимо как-то идентифицировать себя и подтвердить свою принадлежность к данной компании. В данный момент в большинстве компаний для этого используются следующие способы:

- пропуски, но не во всех компаниях они именные и с логотипом или как-то защищены от подделки;
- предоставление списка сотрудников в заведение и идентификация по документам (паспорту);
- вера на слово: то есть, если кто-то знает о этой акции, будем считать, что это сотрудник компании.

Все вышеперечисленные методы не идеальны и зачастую связаны с неудобствами для всех сторон: сотрудника, компании и представителя услуг.

Компании больших размеров имеют свои собственные разработки для решения данной проблемы, но, зачастую, ими неудобно пользоваться, они редко обновляются или имеют ограниченный функционал, так как реализуются как внутренние проекты с малым приоритетом. Малые компании, наоборот, не имеют ресурсов на подобные разработки.

Единое приложение как сервис-посредник решило бы все эти проблемы. Компаниям выгодно пользоваться таким приложением, без затрат на собственную разработку и поддержку. Представителям услуг выгодно привлекать новую аудиторию и наращивать клиентскую базу. Также формируется единая база партнерских сервисов, компаниям не нужно связываться с ними напрямую и разрабатывать собственные скидочные программы. Конечный пользователь-сотрудник получает удобное приложение с нужным функционалом.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель диссертационной работы заключается в разработке платформы на основе мобильного приложения, которая позволит представителям услуг и бизнеса производить идентификацию и аутентификацию корпоративных клиентов и на основе этого предоставлять им скидки и преференции.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Сформулировать и поставить требования к разрабатываемой платформе, обозначить варианты использования, продумать функции и интерфейс мобильного приложения.
2) Разработать архитектуру программной платформы, состоящей из мобильного приложения, сервера, базы данных и админ интерфейса.
3) Реализовать систему шифрования и защиты пользовательских данных.
4) Реализовать интеграцию с сервисом поиска заведений по локации.
5) Провести тестирование и проверку разработанной системы.

Объектом исследования являются системы мобильной идентификации и аутентификации пользователей.

Предметом исследования программное обеспечение для решения задачи удобной и надежной авторизации пользователей, методы и алгоритмы шифрования и защиты пользовательских данных.

Основной *гипотезой*, положенной в основу диссертационной работы, является возможность разработки мобильного приложения улучшающего

пользовательский опыт взаимодействия с представителями услуг, а также предоставляющего компаниям решение для поощрения сотрудников.

Связь работы с приоритетными направлениями научных исследований и запросами реального сектора экономики

Работа отвечает запросам реального сектора экономики, так как предоставляет новое решение в сфере взаимодействия корпоративных клиентов и представителей услуг.

С точки зрения научных исследований данная работа охватывает такие разделы науки как компьютерная безопасность и криптография, а также передовые технологии и методы разработки программного обеспечения.

Личный вклад соискателя

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя М. В. Стержанова, заключается в формулировке целей и задач исследования.

Опубликованность результатов диссертации

По теме диссертации опубликована статья в научном журнале.

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, трех глав, заключения, списка использованных источников, списка публикаций автора и приложений. В ведении представлен анализ предметной области, выявлены основные существующие проблемы в рамках тематики исследования, показаны направления их решения. Первая глава посвящена разработке архитектуры программной платформы. Во второй главе проводится обзор и сравнительный анализ алгоритмов шифрования для рассматриваемой системы. Третья глава включает в себя этапы разработки платформы, описание методов, инструментов и проведенных экспериментов.

Общий объем работы составляет 58 страниц, 10 рисунков, список использованных источников из 30 наименований и 4 приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** определена область и указаны основные направления исследования, показана актуальность темы диссертационной работы, дана краткая характеристика исследуемых вопросов, обозначена практическая ценность работы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе описана структура, предъявляемые требования и функционал разрабатываемой системы. Детально рассмотрена структура и архитектура приложения.

Система состоит из нескольких сервисов, включающих в себя: облачную базу данных Firebase, сервис по регистрации и администрированию пользователей и интеграции с социальными сетями, сервис по интеграции с представителем данных о заведениях Foursquare, сервис отправки смс сообщений и кроссплатформенное мобильное приложение в двух интерфейсах: для клиентов и для представителей услуг.

Также описаны модели базы данных, такие как: User, UserGroup, Place, Company и Discount.

Конечными пользователями мобильного приложения с одной стороны будут сотрудники компаний, получающие скидки и услуги и представители услуг: администраторы, кассиры, бариста. Соответственно приложение должно работать в двух интерфейсах: назовём их “пользовательский” и “сервисный” соответственно. Должна быть удобная авторизация в приложении через социальные сети в один клик.

Идентификацию пользователей производится с помощью сгенерированного QR-кода: для каждого сотрудника компании генерируется уникальный код, в котором зашифрована информация о скидке. Сотрудник сервиса с помощью приложения сканирует QR-код, происходит расшифровка и проверка данных и отображается информация о предоставляемых скидках.

Во **второй** рассмотрены основные алгоритмы шифрования текста, принципы их работы и применяемые к ним методы криптоанализа. Криптографические алгоритмы применяются для обеспечения безопасности использования приложения и предотвращения утечек информации.

Рассмотрены методы простой подстановки, симметричные и асимметричные криптосистемы, приведены примеры криптоатак используемых для взлома шифра. Проведен сравнительный анализ таких алгоритмов как IDEA, AES, Serpent и RSA.

В **третьей главе** приведены этапы разработки программной платформы, принятые решения и технические подробности. Детально рассмотрены использованные технологии и обоснование их выбора. Для разработки мобильного приложения использовалась платформа React Native и набор инструментов Expo.

Для реализации шифрования используется симметричный алгоритм блочного шифрования AES, а также асимметричная криптосистема RSA для передачи секретного сеансового ключа по открытому каналу связи. Реализации этих алгоритмов на языке Python приведены в приложениях А и Б.

В ходе разработки алгоритма была предложена следующая схема обработки запроса:

1. Серверная часть программы хранит идентификаторы пользователей и информацию о предоставляемых скидках.
2. По запросу клиента генерирует случайный сеансовый ключ.
3. Генерирует QR-код с идентификатором клиента и шифрует его сеансовым ключом.
4. Отправляет клиенту зашифрованный открытым ключом RSA сеансовый ключ и QR-код.
5. Клиентская часть генерирует и отправляет серверу открытый ключ RSA.
6. Запрашивает временный зашифрованный QR-код для данного заведения.
7. Расшифровывает сеансовый ключ с помощью закрытого ключа RSA.
8. Расшифровывает QR-код при помощи сеансового ключа.
9. Отображает информацию о предоставляемой скидке для данного идентификатора пользователя.

Приведен обзор разработанного приложения и предоставляемого функционала. Кроме механизма авторизации на основе QR кода, приложение предоставляет информацию о предоставляемых скидках и акциях, список заведений с местоположением, отзывами, фотографиями и статистику использования.

ЗАКЛЮЧЕНИЕ

Основные результаты диссертации

1. Спроектирована и реализована программная платформа обеспечивающая удобную, быструю и безопасную аутентификацию клиентов посредством кроссплатформенного мобильного приложения.

2. Построены сценарии пользовательского взаимодействия, продуман и разработан пользовательский интерфейс для поиска, навигации, авторизации и предоставления / получения скидок для корпоративных клиентов.

3. Проведен сравнительный анализ современных алгоритмов шифрования текста, а также рассмотрены методы используемых криптоатак на них.

4. Предложен алгоритм шифрования для обеспечения безопасности пользовательских и корпоративных данных.

5. Разработан и реализован бэкэнд сервис для регистрации, управления и обслуживания программной платформы, а также выполняющий интеграции с внешними сервисами и базами данных.

Рекомендации по практическому использованию результатов

1. Полученные результаты формируют теоретическую и практическую базу для разработки мобильных и серверных приложений для решения задач удобной и безопасной авторизации пользователей.

2. Результаты работы могут использоваться как единая программная платформа для коммуникации корпоративных клиентов и представителей сервиса услуг.

3. Некоторые IT компании проявляли заинтересованность в использовании разработанной программной платформы для своих сотрудников.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Пажитных, И. П. Алгоритмы шифрования текста // Международный научный журнал “Научные вести”. – 2020. – №6 (23). – С. 199–204.