МИНИСТЕРСТВО ОБРАЗОВАНИЯ И МОЛОДЕЖНОЙ ПОЛИТИКИ СВЕРДЛОВСКОЙ ОБЛАСТИ

ГАПОУ СО «ЕКАТЕРИНБУРГСКИЙ МОНТАЖНЫЙ КОЛЛЕДЖ»

ДОПУЩЕН К ЗАЩИТЕ:

РУКОВОДИТЕЛЬ РАБОЧЕЙ ГРУППЫ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

ЗАЩИЩЕН: ПРОТОКОЛ\_\_\_\_\_\_ОТ\_\_\_\_\_\_\_ ПРЕДСЕДАТЕЛЬ ГАК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

**ДИПЛОМНЫЙ ПРОЕКТ**

ТЕМА: «РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ “МОБИЛЬНОЕ ПРИЛОЖЕНИЕ МЕНЕДЖЕРА ПАРОЛЕЙ”»

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 9 | 0 | 2 | 0 | 7 | - ДП - | 4 | 1 | 6 | 3 | – | И | П | 8 | 1 | – | 1 | 8 |

ОЦЕНКА: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

РУКОВОДИТЕЛЬ ДИПЛОМНОГО ПРОЕКТА: Софьина Н.А.

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

СТУДЕНТ ГР. ИП-81 Савин М.В.

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

КОНСУЛЬТАНТ:

Грибова А. В.

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

РЕЦЕНЗЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

|  |
| --- |
| 2020 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № стр. | Формат | Обозначение | Наименование | Кол.  листов | № экз. | Примеч. |
| 1 | А4 | ЕМК 09.02.04. ДП 4163-ИП-81-18 ПЗ | Пояснительная записка | 80 | - |  |
| 2 |  | ЕМК 09.02.04.ДП 4163-ИП-81-18 ИС | «Мобильное приложение менеджера паролей» | 1 |  | CD-диск |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |
| 13 |  |  |  |  |  |  |
| 14 |  |  |  |  |  |  |
| 15 |  |  |  |  |  |  |
| 16 |  |  |  |  |  |  |
| 17 |  |  |  |  |  |  |
| 18 |  |  |  |  |  |  |
| 19 |  |  |  |  |  |  |
| 20 |  |  |  |  |  |  |
| 21 |  |  |  |  |  |  |
| 22 |  |  |  |  |  |  |
| 23 |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |
|  | | | | | | |

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Раздел 1. АНАЛИТИЧЕСКАЯ ЧАСТЬ

1. Назначение, цели и задачи проекта
2. Обоснование выбора языка программирования
3. Анализ существующих разработок по данной теме
4. Обоснование необходимости разработки информационной системы
5. Руководство по стилю
6. Страницы приложения
7. Выбор и обоснование проектных решений

Раздел 2. ПРОЕКТНАЯ ЧАСТЬ

ВВЕДЕНИЕ

В современном мире электронная безопасность – это крайне важно, потому что многие жизненно необходимые на сегодняшний день сервисы, такие как онлайн банки, государственные порталы, социальные сети и многое другое, имеют системы авторизации.

Каждый день множество людей теряют свои учётные записи из-за слабого пароля или из-за использования одинаковых паролей на всех своих учётных записях. Менеджеры паролей позволяют облегчить и обезопасить процесс авторизации.

Менеджер паролей – это программное обеспечение, которое позволяет пользователю безопасно хранить и работать с паролями и pin-кодами. Безопасность хранения паролей обеспечена шифрованием данных, а возможность работы с множеством паролей позволяет пользователю использовать более сложные и разные пароли без особых усилий, что позволяет значительно снизить шансы потери учётной записи из-за слабого пароля.

РАЗДЕЛ 1. АНАЛИТИЧЕСКАЯ ЧАСТЬ

1.1. Назначение, цели и задачи проекта

Менеджер паролей хранит пароли пользователя в зашифрованном виде для их дальнейшего использования в процессах авторизации с целью упрощения управления паролями и предоставления безопасного хранения паролей на устройстве.

Цель проекта – разработать надёжное и удобное в использовании мобильное приложение менеджера паролей.

В задачи проекта входит:

1. спроектировать базы данных для приложения;
2. изучить различные способы шифрования паролей;
3. создать мобильное приложение, выполняющее функции менеджера паролей;

1.2. Обоснование выбора языка программирования

Для разработки мобильного приложения, был выбран язык программирования C# на платформе Xamarin.Forms из-за возможности быстро и качественно разработать дизайн приложения, благодаря удобной XAML вёрстке и возможности точно настроить дизайн элементов. Язык программирования C# благодаря статической типизации, строгой структуре написания кода и системе IntelliCode в ide VisualStudio позволяет избежать множества проблем и ошибок, ещё на моменте написания кода, что значительно увеличивает скорость и качество написания кода. Также язык программирования C# имеет большое количество встроенных библиотек, способное оптимально обеспечить работоспособность всех модулей менеджера паролей.

В качестве базы данных была выбрана Microsoft SQL благодаря удобной работе с приложениями, написанными на языке программирования C#, и удобного инструмента для работы с базой данных Manager Studio.

1.3. Анализ существующих разработок по данной теме

Существует несколько видов алгоритмов шифрования данных:

* + 1. Необратимое (Хеширование):

При необратимом шифровании применяются необратимые функции шифрования.

Необратимое шифрование отлично подходит для подсчёта контрольной суммы данных, для проверки целостности данных или для хранения данных в которых нет необходимости проводить расшифровку.

Такой вид шифрования не подходят для менеджера паролей по причине необратимости шифрования шифруемых данных.

* + 1. Ассиметричное (с открытым ключом)

В системах шифрования с открытым ключом используются два ключа — открытый и закрытый, связанные определённым математическим образом друг с другом. Данные шифруются открытым ключом и расшифровываются при помощи закрытого ключа.

Основным достоинством таких видов шифрования является то, что при зашифровывании данных отправитель не знает ключа для расшифровки данных, из-за чего нет необходимости для передачи ключа для расшифровки данных, что повышает безопасность данных необратимого шифрования при передаче, при этом позволяя расшифровать данные только назначаемому получателю.

Такой вид шифрования не подходит для облачного менеджера паролей, по причине того, что использование закрытого ключа не позволит пользоваться пользователю одной учётной записью менеджера паролей на разных устройствах, без проблем с безопасностью.

* + 1. Симметричное

В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ.

Такой вид шифрования удовлетворяет потребностям менеджера паролей. Возможность расшифровки позволяет хранить данные в базе данных безопасно и один ключ для шифрования и расшифровки позволяет пользоваться менеджером паролей на разных устройствах.

Алгоритмы симметричного шифрования:

* ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» — устаревший государственный стандарт союза ССР (а позже межгосударственный стандарт СНГ), описывающий алгоритм симметричного блочного шифрования и режимы его работы.
* Twofish — симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа до 256 бит. Отличительными особенностями алгоритма являются использование предварительно вычисляемых и зависящих от ключа узлов замены и сложная схема развёртки подключей шифрования. Половина n-битного ключа шифрования используется как собственно ключ шифрования, другая — для модификации алгоритма.
* XXTEA — криптографический алгоритм, реализующий блочное симметричное шифрование и представляющий собой сеть Фейстеля.

Исходный текст разбивается на слова по 32 бита каждый, из полученных слов формируется блок. Ключ также разбивают на 4 части, состоящие из слов по 32 бита каждый, и формируют массив ключей. В ходе одного раунда работы алгоритма шифруется одно слово из блока. После того, как были зашифрованы все слова, заканчивается цикл, и начинается новый. Количество циклов зависит от количества слов и равно 6+52/n, где n — количество слов.

Этот алгоритм не подходит для данной реализации менеджера паролей, так как зная пару текстов с одинаковыми ключами, для восстановления ключа достаточно прогнать алгоритм в обратном порядке, так как теперь нам известно все кроме ключа.

* IDEA (англ. International Data Encryption Algorithm, международный алгоритм шифрования данных) — симметричный блочный алгоритм шифрования данных. Так как IDEA использует 128-битный ключ и 64-битный размер блока, открытый текст разбивается на блоки по 64 бит. Если такое разбиение невозможно, последний блок дополняется различными способами определённой последовательностью бит. Для избежания утечки информации о каждом отдельном блоке используются различные режимы шифрования. Каждый исходный незашифрованный 64-битный блок делится на четыре подблока по 16 бит каждый, так как все алгебраические операции, использующиеся в процессе шифрования, совершаются над 16-битными числами. Для шифрования и расшифрования IDEA использует один и тот же алгоритм.

1.4. Обоснование необходимости разработки информационной системы

В современной интернет среде необходимо использовать менеджер паролей для сохранения безопасности учётных записей, так как это не только самый удобный, но и самый безопасный способ хранить пароли по нескольким причинам:

* Простота использования:

Используя менеджер паролей от пользователя не требуется запоминать пароли от каждой из учётных записей и некоторые из них позволяют напрямую заполнять поля ввода данных авторизации.

* Безопасность:

При использовании эффективного способа шифрования паролей менеджер паролей становится самым безопасным способом хранения их хранения, так как, не требуя запоминать их или записывать на сторонние носители, не даёт доступ к паролям нежелательным пользователям.

1.5. Руководство по стилю

В качестве основных цветов в приложении используются

(приложение 1):

1. #372EA3 – Цвет привлечения внимания
2. #7366FF – Основной цвет фона
3. #C9C4FF – Дополнительный цвет фона

Для всего текста мобильного приложения используется шрифт Ubuntu.

В приложении менеджера паролей используются три вида кнопок

(приложение 2).

Для ввода данных используются поле для ввода текста и выпадающие меню (приложение 3).

В качестве переключателей значений в настройках используются слайдеры (приложение 4).

1.7. Выбор и обоснование проектных решений

База данных

Для хранения данных о пользователях, их учётных записях и настройках используется база данных Microsoft SQL Server (приложение 12). Для этого в бд используются следующие таблицы:

* Users – в этой таблице находятся данные авторизации (email и пароль от менеджера паролей) пользователей;
* Accounts – в этой таблице находятся данные об учётных записях, привязанные к пользователю;
* Services – в этой таблице хранятся данные о сервисах;
* Settings – в этой таблице хранятся настройки пользователя (для передачи между устройствами пользователя);

Алгоритм шифрования

Для шифрования хранимых в базе данных, мной был выбран симметричный алгоритм шифрования IDEA (приложение 13), из-за относительной простоты реализации на языке программирования C# и достаточного уровня защиты данных для менеджера паролей. В качестве ключа шифрования планируется использовать пароль пользователя от учётной записи менеджера паролей.

РАЗДЕЛ 2. ПРОЕКТНАЯ ЧАСТЬ

2.1. Структура информационной системы

Информационная система состоит из следующих модулей:

1. База данных (MSSQL) – осуществляет хранение всех данных информационной системы;
2. API приложение (ASP.Net Core Веб-Приложение) – осуществляет обмен данных между базой данных и мобильным приложением;
3. Мобильное приложение (приложение Xamarin.Forms) – осуществляет интерфейс пользователя;

Схема взаимодействия модулей информационной системы в приложении 14.

2.2. Разделы информационной системы и система навигации

Мобильное приложение состоит из следующих разделов:

1. Страница авторизации – предназначена для авторизации в приложении и идентификации пользователя (приложение 5);
2. Страница регистрации – предназначена для регистрации новых пользователей в системе (приложение 6);
3. Главная страница – на ней расположен список учётных записей пользователя, кнопка перехода к настройкам и кнопка добавления учётной записи (приложение 7);
4. Страница учётной записи – на ней расположена расшифрованная информация об учётной записи (приложение 8);
5. Страница редактирования учётной записи – предназначена для изменения данных об учётной записи (приложение 9);
6. Страница настроек – на ней расположены настройки приложения (приложение 10);
7. Страница добавления учётной записи – предназначена для добавления новых учётных записей (приложение 11);

Навигация в приложении осуществлена с помощью встроенной в Xamarin.Forms системы навигации NavigationPage.

Схема навигации находится в приложении 15.

2.3. Макет приложения

Изображения макета страниц находится в приложении 5-11.

Ссылка на прототип страниц приложения в фигме

<https://www.figma.com/proto/7kI0WbLQAVUY0DGkGy3Pdi/%D0%9C%D0%B5%D0%BD%D0%B5%D0%B4%D0%B6%D0%B5%D1%80-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D0%B5%D0%B9?node-id=5%3A40&scaling=scale-down&page-id=0%3A1>

2.4. Описание разработки программных модулей

В ПРОЦЕССЕ

РАЗДЕЛ 3. ТЕСТИРОВАНИЕ ИНФОРМАЦИОННОЙ СИСТЕМЫ

РАЗДЕЛ 4. РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

1. Авторизация:

Страница авторизации – первое, что видит пользователь при входе в приложение (если при последнем входе не была установлена настройка запоминания пользователя или был произведён выход из приложения).

Если у пользователя есть учётная запись в информационной системе (если нет, то см. “2. Регистрация”), то пользователь может авторизоваться со своими логином и паролем, для этого:

1. В поле “Email” введите свой логин от информационной системы;
2. В поле “Пароль” введите свой пароль от информационной системы;
3. Нажмите на кнопку “Войти”

При успешной авторизации произойдёт переход на главную страницу приложения.

1. Регистрация:

Страница регистрации – позволяет новым пользователям создать свою учётную запись в информационной системе.

Для перехода на страницу регистрации, на странице авторизации нужно нажать на кнопку “Регистрация”.

На странице регистрации, для того, чтобы зарегистрироваться в информационной системе:

1. В поле “Email” введите свой email, который будет выступать в роли логина при авторизации;
2. В поле “Пароль” введите свой пароль от информационной системы;
3. В поле “Повторите пароль” снова введите свой пароль;
4. Нажмите на кнопку “Зарегистрироваться”;

При успешной регистрации будет создана новая учётная запись и произойдёт переход на главную страницу приложения.

# ЗАКЛЮЧЕНИЕ

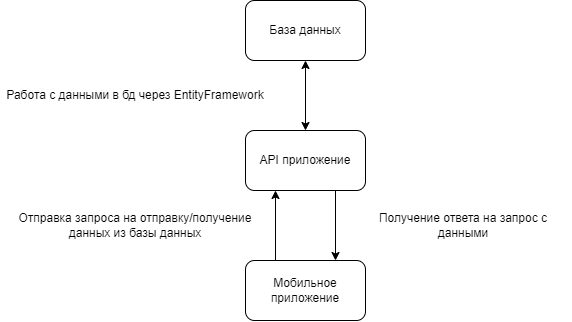
# СПИСОК ЛИТЕРАТУРЫ

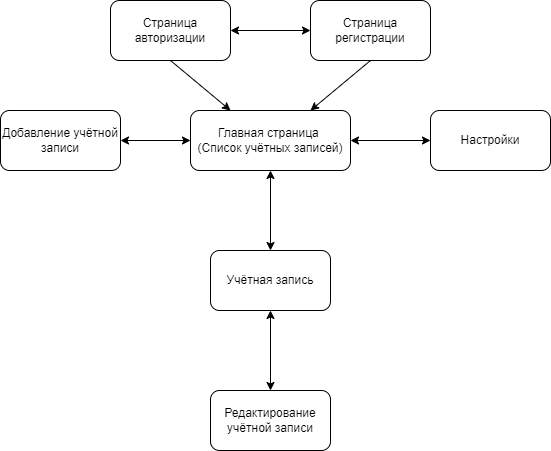
1. Основы CSS [Электронный ресурс]. – Режим доступа: <https://html5book.ru/osnovy-css/>.
2. Гарретт, Д. Веб-дизайн. Элементы опыта взаимодействия / Д. Гарретт. – СПб.: Символ-плюс, 2015. – 192 c.

НЕ МЕНЕЕ 20 ИСТОЧНИКОВ

ИСТОЧНИКИ НЕ СТАРШЕ 2015г.

# ПРИЛОЖЕНИЕ А





# ПРИЛОЖЕНИЕ Б