

А. О. Гурченко
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **М. А. Подалов**, ст. преподаватель

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ШИФРОВАНИЯ ДАННЫХ

Современный мир становится всё более зависимым от цифровых технологий, что приводит к увеличению объёма конфиденциальной информации, хранящейся и передаваемой с помощью мобильных устройств. В условиях постоянного роста угроз в лице киберпреступлений, необходимости защиты личных данных и обеспечения конфиденциальности информации, вопрос шифрования данных приобретает особую актуальность. Мобильные приложения, использующие различные методы шифрования, становятся незаменимыми инструментами для защиты информации пользователей.

Функционально это приложение работает как хранилище заметок. Поскольку необходимо было реализовать шифрование данных, то приложение шифрует саму заметку и файл внутри самого устройства. Реализовано это следующим образом:

Пользователь входит в приложение, в котором представлено окно со списком заметок, кнопкой создания новой заметки, а также настройки самого приложения.

Пользователь вводит некоторые данные и сохраняет их.

Эти данные сохраняются в файл внутри устройства и в локальной базе данных.

Алгоритм шифрует файл внутри устройства. При этом для базы данных применяется пароль, который недоступен сторонним пользователям.

Если каким-то образом стороннему пользователю удаётся получить доступ к файлу, то приложение зашифровывает текст заметки внутри устройства.

Внутри базы данных сохраняется исходный и зашифрованный тексты.

Такой алгоритм работы предоставляет пользователю полную конфиденциальность данных, несмотря на то, что внешне это обычное приложение для записи и хранения заметок.

Рассмотрим подробнее алгоритм шифрования. В качестве шифратора использовался алгоритм AES. Весомым плюсом данного алгоритма является то, что для его использования не нужно использовать фреймворки или сторонние библиотеки. Сам алгоритм работает с блоками данных. Это означает, что алгоритм разбивает исходные данные на блоки по 128 бит и заменяет их на зашифрованные блоки также по 128 бит. Стоит отметить, что размер блоков также может быть 192 или 256 бит. В проекте использовался вариант со 128 битными блоками [1].

Для реализации этого проекта были выбраны следующие инструменты:

1. **Android Studio** — интегрированная среда разработки (IDE), которая предназначена для разработки мобильных приложений. Среди преимуществ можно выделить встроенный в IDE эмулятор Android-устройства, интеграцию с некоторыми базами данных, большое сообщество разработчиков и выбор языка программирования для реализации приложения.

2. **Java** — объектно-ориентированный язык программирования со строгой типизацией. Широко используется для разработки мобильных приложений [2].

3. **Android SDK** — инструмент для работы с Java. Используется для компиляции приложений, написанных на данном языке программирования.

4. **Gradle** — инструмент автоматизации сборки проектов. Он позволяет эффективно управлять процессом компиляции кода, запуском модульных и интеграционных тестов, созданием исполняемых файлов и автоматической загрузкой необходимых библиотек [3].

5. **SQLite** — реляционная база данных, в которую происходит сохранение всех данных, внесённых пользователем. Она позволяет создавать локальные базы данных, а также предоставляет удобный функционал для работы.

На рисунке 1 приведена схема прецедентов данного приложения. На схеме отображаются все варианты действий, которые приводят к редактированию содержимого базы данных.

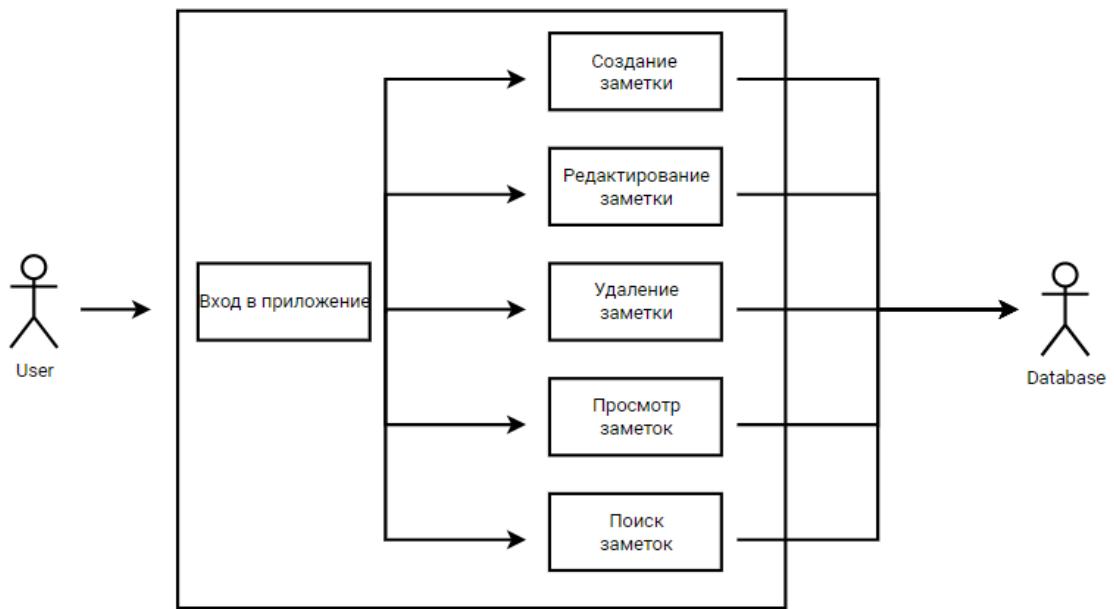


Рисунок 1 – Схема прецедентов

Варианты взаимодействия, представленные на схеме:

1. Создание заметки, которое запускается при помощи отдельной кнопки.
2. Редактирование заметки из уже созданной.
3. Удаление существующей заметки из памяти и базы данных.
4. Просмотр списка созданных заметок.
5. Поиск заметок по заголовку.

На рисунке 2 приведён дизайн приложения. Поскольку базовый функционал, который связан исключительно с работой с заметками, довольно простой, то и дизайн приложения выглядит минималистично. На верхней панели помещены три кнопки. Первая отвечает за поиск нужной заметки по её заголовку. Вторая отвечает за сортировку по названию или дате добавления. Третья кнопка открывает экран настройки приложения. Данные настройки предназначены исключительно для изменения внешнего вида приложения. Основную часть экрана занимает список созданных заметок. На данном рисунке показывается сообщение, которое подсказывает, что нужно делать для создания новой заметки. Сообщение выводится в том случае, если нет никаких записей, в противном случае вместо сообщения выводится список заметок. В правой нижней части экрана располагается кнопка создания новой заметки.

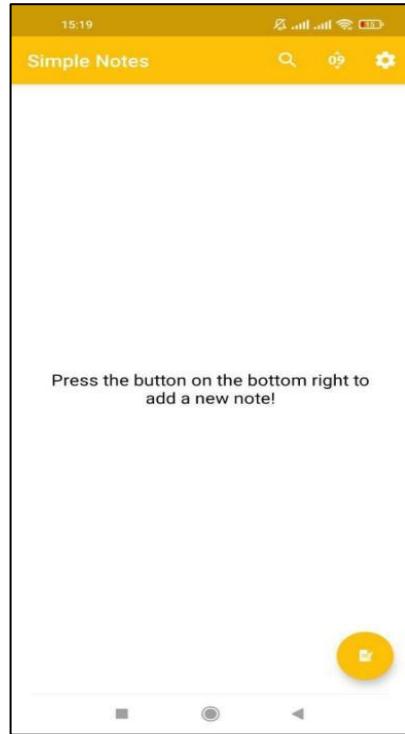


Рисунок 2 – Дизайн приложения

Мобильное приложение успешно запускается на операционной системе Android. Тесты были проведены на эмуляторе и на реальном устройстве.

По итогам этот проект успешно справляется с заданным функционалом: записывает и хранит заметки, шифрует данные, сохраняет всю информацию в базе данных.

Литература

1. Habr.com [Электронный ресурс] : Как устроен AES. – Режим доступа: <https://habr.com/ru/articles/112733/>. – Дата доступа: 25.03.2025.
2. Metanit.com [Электронный ресурс] : Язык Java. – Режим доступа: <https://metanit.com/java/tutorial/>. – Дата доступа: 25.03.2025.
3. Javarush.com [Электронный ресурс] : Краткое знакомство с Gradle. – Режим доступа: <https://javarush.com/groups/posts/2126-kratkoe-zнакомство-s-gradle>. – Дата доступа: 25.03.2025.