**Цель работы**: разработка мессенджера.

**Состав команды**: студенты группы 3651001/60201:

1. Бурмистров П. А.
2. Гильман А. В.
3. Кротов Н. Д.
4. Никулкин В. А.
5. Облогина А. Ю.

В качестве темы проекта предлагается взять разработку мессенджера. Для разработки мессенджера предполагается использование языка программирования Python 3. Для разработки фронтенда предполагается использование фреймворка Django, который также поддерживает язык Python 3.

Рассмотрим функционал, который предоставляет пользователям мессенджер:

1. Отправка сообщений между клиентами;
2. Групповые чаты;
3. Поддержка отправки пользователей документов (например, текстовые файлы, видео файлы или картинки);
4. Сохранение истории переписки;
5. Возможность пользователю заводить личную страницу и размещать там некоторую информацию (например, фотографии или видеозаписи).

Для сохранения истории переписки требуется использование базы данных. В данной работе для этой цели предполагается использование базу данных PostgreSQL.

Также требуется разработка легковесного мобильного приложения, которое позволит использовать разрабатываемый мессенджер на мобильных устройствах. Разработка будет производиться с использованием языка Kotlin под платформу Android.

Отличительной особенностью данного мессенджера является способ шифрования. В качестве метода шифрования предлагается использовать отрицаемое шифрование. Отрицаемое шифрование – способ криптографического преобразования, в котором зашифровываются совместно два или более различных сообщений на двух или более различных ключах. С помощью такого метода можно правдоподобно отрицать наличие сообщения. Рассмотрим на примере алгоритм работы отрицаемого шифрования:

1. Клиент1 хочет передать сообщение Клиенту2, при этом известно, что трафик Клиента1 прослушивается. Для этого Клиент1 создает два ключа: один, который хранится в секрете, а другой, который может быть передан третьей стороне в критической ситуации. Затем настоящий ключ передается Клиенту2 (передача ненастоящего ключа не является обязательной);
2. Создается два сообщения М1 и М2. М1 не содержит конфиденциальной информации, а М2 содержит. Эти два сообщения комбинируются и отправляются;
3. Клиент2 расшифровывает сообщение М2;
4. При прослушивании трафика обнаруживается факт отправки сообщения. После этого к Клиенту1 приходят и требуют расшифровать сообщение, но Клиент1 использует ненастоящий ключ и расшифровывает сообщение М1, которое не содержит важной информации.

Тогда план работы может иметь следующий вид:

1. Разработка серверной части приложения, отвечающей за пересылку сообщений между узлами;
2. Создание фронтенда веб-приложения;
3. Внедрений криптографической защиты информации;
4. Внедрение базы данных для хранения истории переписки;
5. Тестирование разработанного приложения;
6. Поиск уязвимостей в безопасности (например, таких как XSS);
7. Устранение уязвимостей;
8. Разработка легковесного мобильного приложения;
9. Тестирование приложения;
10. Оформление отчета о проделанной работе, а также составление презентации.