УДК 004.42

ИСПОЛЬЗОВАНИЕ ФУНКЦИЙ ШИФРОВАНИЯ ПРИ ПЕРЕДАЧЕ СООБЩЕНИЙ В РАСПРЕДЕЛЕННОМ ПРИЛОЖЕНИИ

А. С. БАРЫГИН, Е. А. ЗАЙЧЕНКО
Белорусско-Российский университет
Могилев, Беларусь

Применение компьютерных сетей и кластерных систем для организации распределённых вычислений получило широкое распространение. В качестве примера распределенного приложения был реализован обмен сообщениями между множеством пользователей (чат).

В качестве средства реализации программного обеспечения выбран механизм сокетов Python и СУБД PostgreSQL. Сокеты представляют собой классическое средство межпроцессного взаимодействия, обеспечивающее возможность организации обмена сообщениями между задачами, выполняющимися на различных компьютерах сети, с разнородными операционными системами. Важным фактором является способность сокетов работать в реальном времени.

Разработанное распределенное приложение состоит из серверной и клиентской части. Информация о пользователях и чатах организована в виде объектно-реляционной базы данных и хранится в серверной части приложения. Задачи серверной части – создание сокета, прослушивание определенного порта в ожидании подключения клиента, идентификация клиента и чата. После установления соединения начинается обмен данными. Функция регистрации пользователей принимает два аргумента: логин и пароль, которые находятся в запросе, поступившем от клиентской части распределенного приложения. Функция авторизации пользователей отправляет запрос на извлечение записи о пользователе с логином, который был передан как аргумент, и последующей проверке пароля. На клиентской части приложения реализован пользовательский интерфейс, выполняется шифрование и дешифрование паролей и сообщений пользователей. Таким образом, передача информации по сети происходит в зашифрованном виде.

Для защиты от несанкционированного доступа паролей пользователей и чатов, а также всех отправляемых сообщений, был разработан ряд алгоритмов шифрования. Функции шифрования реализованы с использованием модуля Pickle, который преобразует сложные объекты в поток байтов. В предложенных алгоритмах использованы операции побитового сдвига и ряд других последовательностей логических преобразований. В качестве уникального ключа шифрования используется идентификатор клиента, который отправляет сообщения.

Тестирование приложения проводилось с различным числом клиентов. Выполнена сравнительная оценка производительности и надежности работы предложенных функций шифрования. В результате была доказана высокая эффективность разработки.