|  |  |  |
| --- | --- | --- |
|  | |  |
| МИНОБРНАУКИ РОССИИ | |  |
| Федеральное государственное бюджетное образовательное учреждениевысшего профессионального образования"Российский технологический университет"МИРЭА | |  |
|  | Факультет информационных технологий (ИТ) | |
|  | Кафедра вычислительной техники (ВТ) | |

|  |  |
| --- | --- |
| **ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3** | |
| **по дисциплине** | |
| «Защита информации» | |
|  | |
| Выполнил студент группы ИВБО-04-15  Принял | Афатов Д. В.  Воронков С. О. |
|  |  |

|  |  |  |
| --- | --- | --- |
| Лабораторная работа выполнена | «\_\_»\_\_\_\_\_\_\_201\_\_ г. | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
|  |  |  |
| «Зачтено» | «\_\_»\_\_\_\_\_\_\_201\_\_ г. | *\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |

Москва 2018

Постановка задачи:

Разработать клиент-серверное приложение, реализующую алгоритм SRP-6a.

Ход выполнения:

Для реализации алгоритма SRP-6a было использовано клиент-серверное приложение из второй лабораторной. Для этого было добавлена возможность выбора используемого алгоритма шифрования при общении и добавлены механики взаимодействия клиентов, если их выбранный алгоритм не совпадает. В интерфейсе каждого клиента при использовании алгоритма SRP был добавлен интерфейс ввода логина и пароля и выбор регистрации и входа. Клиент, который инициирует соединении играет роль клиента, а тот к которому происходит подключение – сервера. Сервер хранит список пользователей в формате txt и загружает данные при запросе на подключение. В результате работы алгоритма при успешном соединении каждый из клиентов имеет секретный ключ, который используется при шифровании текстовых сообщений алгоритмом Цезаря.

Вывод:

Разработанная программа работает корректно. Закрытые ключи сходятся.