|  |  |  |
| --- | --- | --- |
|  | |  |
| 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 | Камаев А. А.  Воронков С. О. |
|  |  |

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

Москва 2018

Постановка задачи

Разработать клиент-серверное приложение, реализующую алгоритм авторизации без передачи пароля - SRP.

Ход выполнения работы

1. Клиент
   1. Клиентское приложение состоит из двух окон – регистрация и авторизация. При регистрации клиент высчитывает соль и верификатор. Далее он отправляет на сервер 4 сообщения:

- команда «REGISTRATION»

- идентификатор, записанный в поле «Имя пользователя»

- соль

- верификатор

1.2) При авторизации вычисляет ключи (A, a), отправляет команду «AUTH», идентификатор пользователя и открытый ключ A. Далее, начинается обмен данными с сервером и вычисления, необходимые для подтверждения. Последним этапом является вычисление подтверждения M, отправка его на сервер, получение от сервера подтверждения R и сравнивание результатов.

2) Сервер

1.1) Сервер может принимать одну из двух команд – «REGISTRATION» и «AUTH». С первой он заносит в список пользователей нового пользователя. Со второй начинает аутентификацию, после чего происходят необходимые вычисления и обмен данными с клиентом. В конце сервер получает от клиента подтверждение M, сравнивание, вычисление подтверждения R и отправка его клиенту.

Вывод

Разработано клиент-серверное приложение, реализующее алгоритм авторизации без передачи пароля - SRP. Программа работает корректно:

- при регистрации все пользователи заносятся в список без потерь;

- при попытке зарегистрировать пользователя с существующим именем, сервер присылает сообщение о существовании такого пользователя;

- при попытке зайти под несуществующим именем пользователя, сервер присылает соответствующее сообщение об ошибке аутентификации;

- при попытке зайти с неправильным паролем, сервер присылает соответствующее сообщение о неправильности пароля;

- при корректно введенной паре логин-пароль выводится сообщение об успешном входе.