|  |
| --- |
| Описание: https://lh6.googleusercontent.com/QcftzNtI05T0Y6fjdSh1Rr2rt8oqZ1IvnLvbn1jLJ7CCyteVir3k-xBLv4SL1wAgWJsRhmmJSR0UW-RP63_GQenE4vVWv05BRoZTsmIcBccVTnfxwmsnNMvjg599x9SqZd8E3dkd |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждениевысшего образования"МИРЭА - Российский технологический университет"РТУ МИРЭА |

Институт информационных технологий

Кафедра вычислительной техники

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

**по дисциплине**

**«Защита информации»**

Студент группы ИВБО-07-15 Попов Н.С.

Принял Воронков С. О.

Москва 2018

Постановка задачи:

Разработать программу, реализующую алгоритм Диффи-Хеллмена.

Ход выполнения работы:

1. Создаются два объекта класса Пользователь (Алиса и Боб), один объект класса Подслушивающий (Ева) и один объект класса Канал.
2. Алиса и Боб генерируют параметры p и g и обмениваются ими между собой по каналу передачи данных. Ева подслушивает канал и сохраняет себе эти параметры.
3. Алиса и Боб создают свои закрытые ключи.
4. Ева пытается отправить Бобу свой публичный ключ, безуспешно. Алиса генерирует и отсылает Бобу свой публичный ключ. Ева подслушивает канал и сохраняет себе этот ключ.
5. Боб генерирует и отсылает Алисе свой публичный ключ. Ева подслушивает канал и сохраняет себе этот ключ.
6. Алиса и Боб генерируют у себя общий секретный ключ.

Вывод:

Алгоритм работает корректно, общие секретные ключи пользователей сходятся.