**МИНОБРНАУКИ РОССИИ**

**Санкт-Петербургский государственный**

**электротехнический университет**

**«ЛЭТИ» им. В.И. Ульянова (Ленина)**

**Кафедра информационной безопасности**

отчет

**по лабораторной работе №6**

**по дисциплине «Криптография и защита информации»**

Тема: **Изучение хэш-функций**

|  |  |  |
| --- | --- | --- |
| Студент гр. 8383 |  | Киреев К.А. |
| Преподаватель |  | Племянников А.К. |

Санкт-Петербург

2021

**Выводы.**

* Проведено исследование лавинного эффекта для представленных хэш-функций.

Для каждой функции замена, добавление, удаление одного символа в прообразе приводило в среднем к изменению 50% битов значения дайджеста. Кроме того, при любом изменении текста хэш-значения модифицированного файла абсолютно не совпадали с исходными. Следовательно, представленные функции обладают лавинным эффектом.

* Проведено исследование лавинного эффекта для хэш-функции Keccak (SHA-3).

Выявлено, что данная функция им обладает – при модификации одного символа в сообщении происходило изменение в среднем 48% бит в хэше. Также, дайджест модифицированного файла не совпадал с исходным. Сравнивания количество измененных бит дайджеста для каждого из типов изменений у всех исследуемых функций, было обнаружено, что наибольший процент получается при замене символа.

* Изучен HMAC – один из механизмов проверки целостности информации.

HMAC вычисляется по формуле:

Для создания секретного ключа используется генерация на основе пароля. Секретный ключ – результат повторного использования хэш-функции над заданным паролем. Количество итераций хэша значительно увеличивает количество усилий, необходимых для успешной атаки.

* Изучена атака дополнительной коллизии.

Выявлено, что для двух сообщений и временная сложность атаки вычисления 48 и более бит растет экспоненциально для SHA-1. Цель атаки – получение полностью одинакового дайджеста для двух сообщений (пары ) – занимает 1.9e+003 лет. Следовательно, данные хэш-функции устойчивы к коллизиям.