МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное автономное бюджетное образовательное учреждение высшего образования

«**Севастопольский государственный университет**»

кафедра Информационных систем

Институт информационных технологий и управления в технических системах

Лисянский Александр Игоревич

курс 4 группа ИС/б-42-о

09.03.02 Информационные системы (уровень бакалавриата)

**ОТЧЁТ**

о лабораторном практикуме №6

ПАРОЛЬНАЯ ЗАЩИТА.

по дисциплине «Основы защиты информации»

Отметка о зачёте \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

(дата)

Руководитель практикума

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(должность) (подпись) (инициалы, фамилия)

Севастополь

2016

**Цель работы**: изучение принципов организации парольной защиты программ, ознакомление с видами паролей, реализация парольной защиты.

**Простой пароль**: Простой пароль - вводимая пользователем с клавиатуры строка символов. В схеме с простым паролем пользователю разрешается самому выбирать пароль таким образом, чтобы его было легко запомнить. Иногда в ряду символов пароля и в конце его оставляют пробелы. Отличие действительного пароля от кажущегося (без пробелов) повышает защищенность системы.

Подбор пароля путем простого перебора комбинаций предполагает перебор всех возможных сочетаний символов в пароле. Время, необходимое для разгадывания пароля методом простого перебора, является геометрической прогрессией от длины пароля, но есть различные кривые, зависящие от размера алфавита, на основе которого был создан пароль и от размера набора символов, по отношению к которым рассматриваются различные пароли.

Согласно формуле Андерсена:



где R - скорость передачи в линии связи (симв./с);

E - число символов в каждом передаваемом сообщении при попытке получить доступ;

S - длина пароля;

A - число символов в алфавите, из которого составлен пароль;

P - вероятность правильного отгадывания пароля.

Наибольшее влияние на вероятность P раскрытия пароля оказывает величина S. Увеличение пароля на один символ значительно увеличивает время для раскрытия этого пароля. Поэтому применение очень длинных паролей может быть обосновано. Борьба с перебором комбинаций заключается в использовании программного обеспечения, ограничивающего минимальную длину пароля и использовании более обширного алфавита (256 символов).

**Ход работы**: В соответствии с вариантом задания был разработан алгоритм проверки идентификации и авторизации пользователя методом простого пароля.

В результате проверки было получено заключение, что программа работает правильно, проверка пароля и авторизация удается.

Код программы:

<?php

class Login {

public function \_\_construct()

{

# code...

}

public function login(){

if(isset($\_POST['logined'])){

$log = $\_POST['login'];

$pass = $\_POST['password'];

include\_once "/../models/model\_user.php";

$user = get\_user($log);

if($user['password'] == $pass){

$\_SESSION['login'] = $log;

$\_SESSION["autorised"] = true;

$\_SESSION['user\_id'] = $user['id'];

if($log == 'admin')

$\_SESSION['administration'] = true;

else

$\_SESSION['administration'] = false;

header('Location: '.$\_SESSION['base\_url'].'/home');

}

else{

header('Location: '.$\_SESSION['base\_url'].'/login');

}

}

}

public function view(){

if(isset($\_SESSION["autorised"]))

header('Location: '.$\_SESSION['base\_url'].'/home');

include\_once "/../pages/login.php";

}

public function classname()

{

return "Login";

}

}

Вывод: В результате выполнения лабораторной работы были получены навыки по разработке алгоритмов проверки данных пользователя, аутентификации и авторизации пользователя на сайте.