Шитикова А.С.
Научный руководитель: к.т.н., доцент каф. ФПМ А. В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: anastasiya.shitikova.96@mail.ru

Разработка системы хранения паролей с помощью шифрования

В последнее время очень актуален вопрос о защите персональных данных. Большинство людей активно пользуются сетью Интернет, регистрируются на множестве сайтов, требующих регистрацию пользователей. Как итог – большое количество паролей от различных аккаунтов сложно удержать в голове. Есть вариант использования одних и тех же данных, но это опасно, так как взломав один аккаунт, злоумышленник может получить доступ ко всем персональным данным.

При сохранении информации на первый план выходят не технические, а системные средства. К ним можно отнести также специальную процедуру ограничения доступа к информации или полный ее перенос в организованные места хранения (архивы, хранилища и др.) [1].

Целью работы является разработка системы хранения паролей в зашифрованном виде.

Для достижения цели были установлены следующие задачи:

- обзор аналогов;
- сформировать требования к разработке системы хранения паролей.

В результате выполнения работы должна быть разработана программа, позволяющая пользователю вносить в нее регистрационные данные своих аккаунтов, иметь к ним удобный доступ [2]. Храниться данные должны в зашифрованном виде в специальном файле.

Рассмотрим приложения-аналоги:

Таблица 1. Сравнение приложений-аналогов

Аналоги	Особенности			
	Генерация паролей	Шифрование паролей	Использование «соленого» хеширования	Выбор способа кодирования информации
KeePass	+	+	-	-
LastPass	+	+	+	-
Реализуемая система	+	+	+	+

После обзора аналогов можно увидеть, что реализуемая система включает в себя все особенности рассмотренных программ.

Хранение данных удобно производить в специализированной базе данных, но ввиду того, что объем данных приложения не будет очень большим (маловероятно, что у пользователя будет несколько сотен или тысяч данных авторизации), использование БД необоснованно и лишь затрудняет разработку программы и ее сопровождение, так как практически все БД требуют установки на компьютере сервера баз данных. Поэтому в программе будет использован бинарный файл. Данный тип файлов по умолчанию не открывается обычными программами редактирования и, соответственно, обеспечивается его сохранность от доступа посторонних лиц.

Требования к разработке системы хранения паролей:

1. Необходимо предусмотреть аутентификацию, для того, чтобы пользователь идентифицировался в системы со своим логином и паролем.

2. Возможность обработки довольно большого количества авторизационных данных пользователя.

3. Также пользователю необходимо вводить название сайта или аккаунта, логин и пароль от него, а также нужно предусмотреть поле для ввода какой-либо дополнительной информации.

Для обеспечения выбора метода кодирования [3] отлично подойдут переключатели, позволяющие пользователю осуществить выбора одного варианта из нескольких.

В ходе исследовательской деятельности были сформулированы требования к разработке системы хранения паролей на основе обзора особенностей приложений аналогов.

Литература

1. Зубкова, Т.М. Технология разработки программного обеспечения: Учебное пособие /Т.М. Зубкова. - Оренбург: ГОУ ОГУ, 2004. - 101 с.

2. Степанченко, И.В. Методы тестирования программного обеспечения: Учебное пособие /И.В. Степанченко. - Волгоград: ВолгГТУ, 2006. - 74 с.

3. Левин М.: PGP: Кодирование и шифрование информации с открытым ключом. - М.: Майор, 2001.