

Шатохин В.С.

студент Магистрант

кафедра «Информационно вычислительная техника»

2 курс, факультет «Магистратуры и Аспирантуры»

Поволжский Университет Телекоммуникаций и Информатики

Россия, г. Самара

Научный руководитель: Макаров М.И.

старший преподаватель

**ИССЛЕДОВАНИЕ МЕТОДОВ ХРАНЕНИЯ ПАРОЛЕЙ НА OS
ANDROID**

STUDY OF PASSWORD STORAGE TECHNIQUES FOR OS ANDROID

Аннотация: в статье рассматриваются три приложения, которые являются наиболее часто используемыми в отношении хранения паролей в операционной системе Android. В частности, в статье приведены данные о функционале приложений RoboForm, mSecure Password Manager, Safebox. Автором приведена их емкая характеристика, позволяющая выбрать пользователю то приложение, которое ему подойдет.

Ключевые слова: пароль, безопасность, Android, RoboForm, mSecure Password Manager, Safebox.

Shatokhin V.S.

Student Magistrate

Department of «Information and computing technology»

2 year, Faculty of «Master and Postgraduate»

Povolzhsky University of Telecommunications and Informatics

Russia, Samara

Supervisor: Makarov M.I.

Senior Lecturer

Abstract: Three applications are considered in the article, which are the most frequently used for storing passwords in the Android operating system. In particular, the article contains data on the functionality of RoboForm applications, mSecure Password Manager, Safebox. The author shows their capacious characteristics, which allows you to select the application that suits the user.

Key words: password, security, Android, RoboForm, mSecure Password Manager, Safebox.

В настоящее время количество пользователей операционной системы Android достигло 1,5 млрд. человек. В общем, это 88,5% популярности операционных систем на мировом рынке, однако в США этот показатель достигает отметки в лишь 53,3%, учитывая приверженность американцев к «яблочной» технике. Однако стоит отметить, что мобильные телефоны, неважно какая операционная система, на 100% не являются программно совершенными, поэтому вся та информация, которая содержится в нем, должна быть защищена различными методами, например, паролями¹.

Сейчас большую популярность получили приложения, которые помогают пользователю хранить пароли, поэтому стоит рассмотреть именно эти предложения, как один из самых распространенных методов хранения паролей на операционной системе Android. Самым первым хотелось бы рассмотреть приложение RoboForm. Оно выпущено компанией Siber Systems Inc и постоянно выпускает обновление, учитывая меняющуюся конъюнктуру опасностей в отношении взлома паролей и общей безопасности информации. В частности, это приложение очень старое, однако по-прежнему очень популярное и среди пользователей, и среди разработчиков. В его функционал входит широчайший набор опций, среди которых такие, как хранение паролей и их автоматическая генерация, синхронизация с облачным

¹ Приложения для хранения паролей на Android [Электронный ресурс], - <http://android4all.ru/soft/comparative/1451-prilozheniya-dlya-khraneniya-parolej>

хранилищем и деление информации на различные категории. Более того, значительным плюсом является то, что приложение бесплатно².

Еще одним методом для хранения паролей в OS Android является приложение mSecure Password Manager, которое отличается от своего предшественника. К примеру, в него вмещается попросту огромный функционал и структурированный интерфейс. Это создает удобство в определении доступа к этому приложению не только с мобильного телефона, но также и с планшетного компьютера. Как только пользователь скачивает данное приложение, заплатив за него 10\$, то оно сразу же предложит придумать пароль к нему, чтобы доступ имел лишь тот, кто осведомлен о пароле³. Это приложение позволяет создавать резервные копии данных, синхронизировать устройства, например, мобильный телефон и компьютер, а также позволяет отправлять копию сохраненных данных по электронной почте. В mSecure Password Manager используется 256-битное шифрование по алгоритму Blowfish, что позволяет хранить пароли и прочие данные под надежной защитой. Также приложение работает быстро и стабильно, поэтому пользователь может быть спокоен за свои данные.

Последнее приложение для рассмотрения – Safebox – один из самых популярных методов хранения паролей на операционной системе Android. Говоря о функционале данного мобильного инструмента, подчеркнем, что большинство функций бесплатно, однако расширенный доступ нужно приобрести за 3\$, но, несмотря на это, обладает так же широким набором возможностей⁴. К примеру, к основным функциям приложения относятся возможность криптования и хранения абсолютно любых файлов, встроенный

² RoboForm [Электронный ресурс], -
<https://www.roboform.com/ru>

³ mSecure Password Manager [Электронный ресурс], -
<https://www.msecure.com>

⁴ Приложения для хранения паролей на Android [Электронный ресурс], -
<http://android4all.ru/soft/comparative/1451-prilozheniya-dlya-khraneniya-parolej>

генератор паролей, поиск нужной информации и многое другое, что делает его незаменимым для обеспечения конфиденциальности информации. Более того, все данные проходят через механизм шифрования с помощью 256-битного алгоритма AES, обеспечивающего максимальную защиту для всех данных.

Таким образом, можно сделать вывод, что сейчас основным инструментальным методом для хранения паролей является мобильное приложение. Их сейчас в Google Play можно найти огромное множество, однако в нашей статье мы рассмотрели три самых популярных варианта, которые чаще всего используются. Можно использовать и бесплатное приложение, так и платное, поэтому пользователь должен сам решить, какое лучше ему выбрать. Самое главное, чтобы функционал его был надежным.

Использованные источники:

1. Приложения для хранения паролей на Android [Электронный ресурс], -
<http://android4all.ru/soft/comparative/1451-prilozheniya-dlya-khraneniya-parolej>
2. mSecure Password Manager [Электронный ресурс], -
<https://www.msecure.com>
3. RoboForm [Электронный ресурс], -
<https://www.roboform.com/ru>