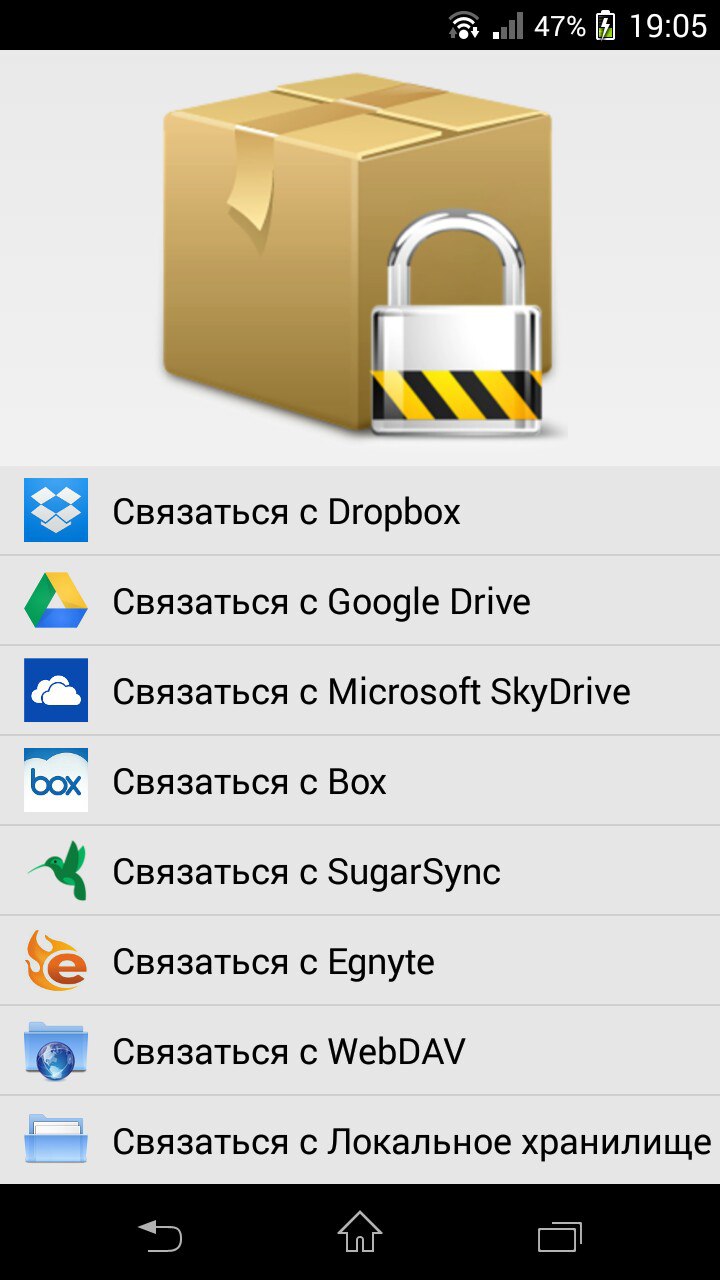
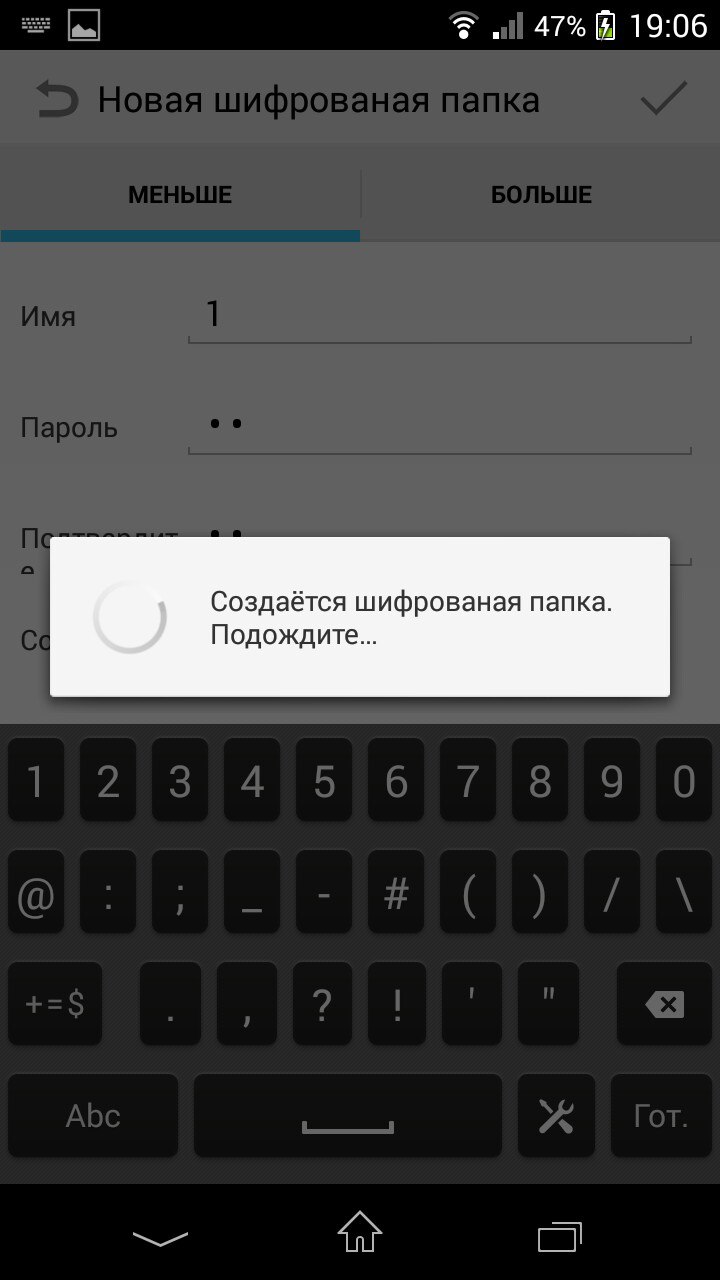
**Boxcryptor Classic**

Бесплатная программа для Android. Разработчики позиционируют ПО как приложение, оптимизированное для работы с удалёнными облачными хранилищами, такими как Google drive, Dropbox, Microsoft SkyDrive и.т.д.

В Boxcryptor Classicиспользуется симметричное шифрование по стандарту AES-256, так-же доступны варианты AES-192 и AES-128, Все операции шифрования и дешифрования производятся непосредственно на устройстве, таким образом, секретный ключ не подвергается опасности перехвата при передаче по открытым каналам связи.

Само приложение на телефоне блокируется ПИН-кодом, таким образом не зная пин-кода доступа будет невозможно запустить приложение.

Интерфейс программы можно увидеть на рисунках №**(№ РИСУНКОВ)**

Способ взаимодействия с файловой системой: Создание зашифрованного хранилища. Все файлы, помещённые в хранилище будут зашифрованы с применением выбранного алгоритма.

Плюсы:

* Встроенная поддержка AES-256 шифрования.
* Интеграция с популярными Облачными хранилищами.
* Не требует ROOT доступа.

Минусы:

* Не удаляет оригинал файла после шифрования.
* Не ведёт историю операций.
* Не очищает КЭШ приложения.
* Частота Обновлений.

Из минусов особенно хотелось бы отменить отсутствие очищения кэша приложения – таким образом, дешифрованные файлы какое-то время хранятся на устройстве в незащищённом виде.

(<https://play.google.com/store/apps/details?id=com.boxcryptor.android>)

**Encryption Manager**

Приложение являющееся файловым менеджером с возможностью шифрования файлов. Защита осуществляется с помощью алгоритмов AES или Twofish шифрования.Для доступа к приложению необходимо знать мастер-пароль, который задаётся при первом запуске. Ключи шифрования для каждого файла генерируются отдельно, без участия пользователя, однако сами ключи шифруются при помощи Мастер-Пароля, и именно в этом проявляется главное узкое место программы.

Плюсы:

* Низкие системные требования.
* Проста в использовании.
* Поддержка двух различных алгоритмов шифрования.
* Частота Обновлений.

Минусы:

* Использование Мастер-пароля.
* Невозможность передать зашифрованные файлы по каналу связи БЕЗ сообщения мастер пароля получателю.
* В бесплатной версии возможно зашифровать не более 5 файлов.

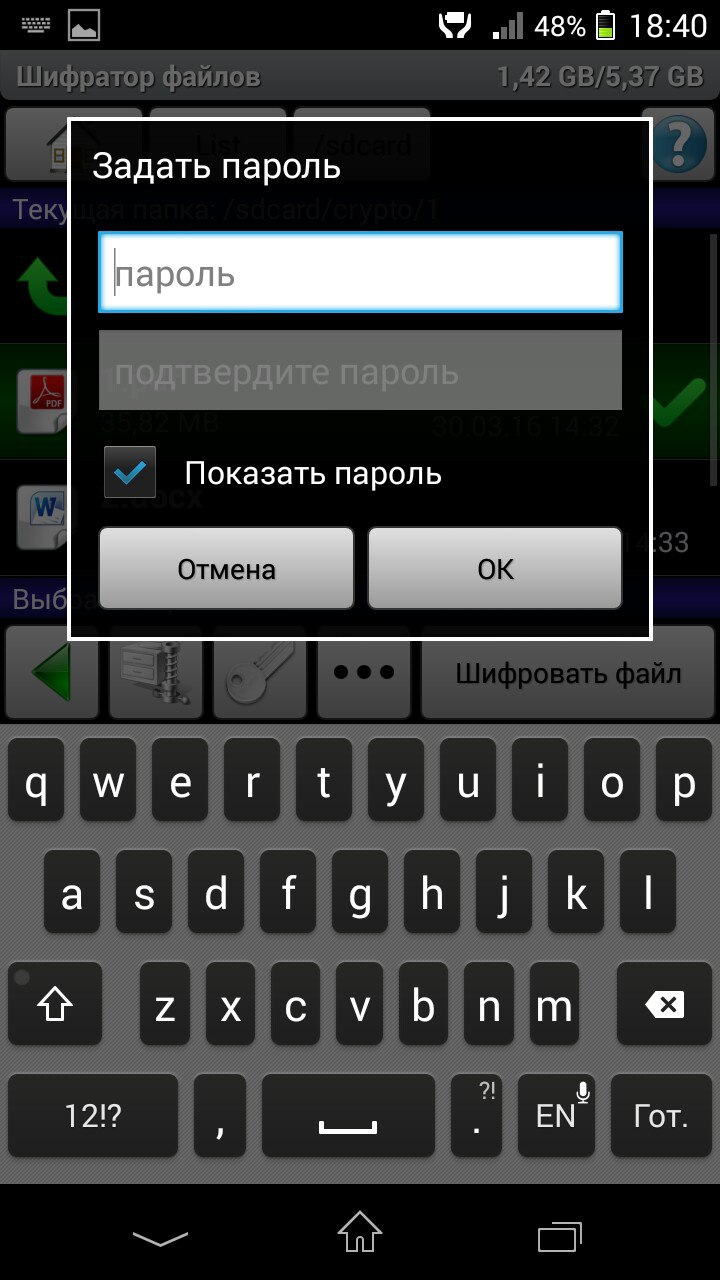
**SSE Шифрование**

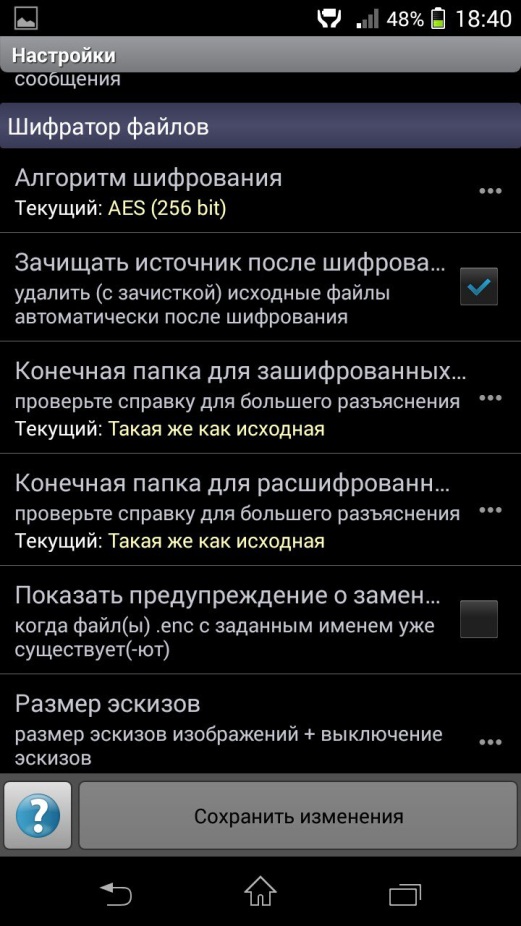
Данное приложение сочетает в себе функции менеджера паролей, шифратора текста и шифратора файлов. В нашем случае целесообразно подробнее разобрать возможностиданного приложения в области шифрования файлов.

SSE использует алгоритмы шифрования: AES (Rijndael) 256bit, RC6 256bit, Serpent 256bit, Blowfish 448bit, Twofish 256bit, GOST 256bit. Так же в случае приобретения платной версии программы есть возможность использовать алгоритмы Threefish 1024bit, SHACAL-2 512bit .

Приложение не требует ROOT доступа на устройстве. Имеется функция затирания исходного файла после его Шифрования. SSE – кроссплатформенное решение, имеются версии для десктопных операционных систем семейств Windows, Linux, Mac OS X.

Интерфейс программы можно увидеть на рисунках №**(№ РИСУНКОВ)**



Плюсы:

* Кроссплатформенное.
* Наличие нескольких алгоритмов шифрования.
* Затирание файлов.
* Много возможностей в одном приложении.
* Частота обновлений.

Минусы:

* Полный функционал доступен только при покупке платной версии.

Анализ и сравнение существующих решений

В следующей таблице представлены данные о функциональности протестированных приложений.

Таблица 1 Характеристики Приложений

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Название | Количество доступных алгоритмов шифрования | Дополнительный функционал | Наличие Платной версии | User Friendly интерфейс | Кросс-Платфор-менность | Частота Обновления |
| Boxcryptor Classic | 3 | - | - | - | - | Очень редко |
| Encryption Manager | 2 | - | + | + | - | Постоянно |
| SSE Шифро-вание | 6 в бесплатной версии,  8 в платной | + | + | + | + | Постоянно |

После первоначальной оценки приложений была произведена проверка работоспособности и быстродействия приложений. В качестве Android-устройства выступал смартфон Sony Xperia SP - модель C5303 с основными характеристиками:

* SoC Qualcomm Snapdragon S4 Pro (MSM8960T), 1,7 ГГц, 2 ядра Krait (ARMv7)
* GPU Adreno 320
* Оперативная память (RAM) 1 ГБ
* внутренняя память 8 ГБ
* Операционная система Android 4.3 (Jelly Bean)

Тестирование приложений производилось на трёх различных файлах:

* Pdf файл размером 37 560 320 байт.
* Docx файл размером 6 770 688 байт.
* Png файл размером 2 494 464 байт.

Шифрование осуществлялось при использовании алгоритма AES-256, присутствующего во всех представленных приложениях.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Название | Время, секунды, Pdf | Время, секунды, Docx | Время, секунды, Png | Время, Затирание, PDF |
| Boxcryptor Classic | 54.350 | 5.300 | 3.000 | - |
| Encryption Manager | 40.500 | 4.100 | 1.950 | - |
| SSE Шифро-вание | 14.350 | 2.350 | 1.100 | 17.400 |

Заключение из Анализа.

Таким образом, проанализировав существующие на платформе Android приложения, осуществляющие шифрование данных, были выявлены следующие требования и критерии, которые необходимо учитывать при разработке приложения.

При проектировании и создании приложения необходимо учитывать:

* Скорость работы.
* Удобство интерфейса для конечного пользователя.
* Наличие встроенного файлового менеджера.
* Отсутствие критически узких мест, например- использования 1-го Мастер пароля для последующего шифрования всех данных.
* Возможность Передачи защищённых файлов по открытым каналам, и возможность использовать эти файлы различных устройствах.