Восстановление паролей. Ч.2

Безмалый Владимир

MVP Consumer Security

Microsoft Security Trusted Advisor

В предыдущей части мы уже говорили о восстановлении паролей учетной записи пользователя при использовании ОС Windows XP/Vista/7 и восстановлении паролей к почте и интернет-сайтам. Следующей задачей, которой часто приходится заниматься при расследовании инцидентов, является восстановление паролей к архивам, почтовым клиентам и EFS (Encrypting File System) . Вот об этом и пойдет речь в данной статье.

Методы шифрования, используемые при архивировании данных

На сегодняшний день реализовано довольно много алгоритмов криптографической защиты информации в архиваторах. Однако в подавляющем большинстве архиваторов реализован, как правило, какой-либо один метод. (Речь идет о наиболее распространенных архиваторах).

При этом необходимо признать, что на сегодня ZIP-кодирование, как и шифрование по алгоритму DES (Data Encryption Standard) сложно назвать устойчивым.

Наиболее надежным на сегодняшний день является AES, принятый в качестве стандарта в США в 2001 году.

Если посмотреть на наиболее популярные в странах СНГ архиваторы, то это, без сомнения, WinZip и WinRAR.

Рассмотрим шифрование в этих архиваторах чуть подробнее.

В архиваторе WinZip реализовано три алгоритма шифрования:

1. Standard Zip 2.0 encryption – используется по умолчанию.
2. 128-bit AES encryption – криптографический алгоритм AES с длиной ключа 128 бит.
3. 256-bit AES encryption – криптографический алгоритм AES с длиной ключа 256 бит (усиленный алгоритм шифрования).

К сожалению, как правило, пользователи используют первый алгоритм (по умолчанию), а ведь этот алгоритм является наиболее слабым. Ведь, если вы не уверены с помощью какого архиватора получатель вашего архива будет распаковывать его, вы вынуждены использовать метод по умолчанию.

Вместе с тем необходимо подчеркнуть, что какой бы алгоритм шифрования вы не использовали, стойкость вашего шифра в первую очередь будет зависеть от стойкости ключа. Т.е. при использовании шифрования необходимо использовать стойкие пароли!

К недостаткам шифрования WinZip стоит также отнести то, что WinZip не шифрует комментарии zip-файлов и такие свойства зашифрованных файлов как наименования, даты и т.д. А ведь это весьма ценная информация для аналитика. Ведь далеко не всякий пользователь переименовывает архивируемые файлы, а уж тем более изменяет остальные атрибуты (дата создания, изменения, размер и т.д.).

В архиваторе WinRAR используется алгоритм шифрования AES с длиной ключа 128 бит. Стоит отметить, что файлы, зашифрованные в WinRAR, будут открываться и в WinZip. Однако обратное будет работать лишь для алгоритма шифрования Zip 2.0.

Кроме того, стоит запомнить, что если вы решили запаковать некоторые данные в архив с шифрованием, вам необходимо позаботиться о надежном удалении файлов с носителя, на котором они находились. Однако это уже тема для совершенно другой статьи.

Итак, вы решили восстановить пароль к архиву. Чем? В данном случае на помощь вам придет программное обеспечение Advanced Archive Password Recovery.

Advanced Archive Password Recovery

Данное программное обеспечение предназначено для восстановления паролей к архивам Zip, RAR, ACE, ARJ.

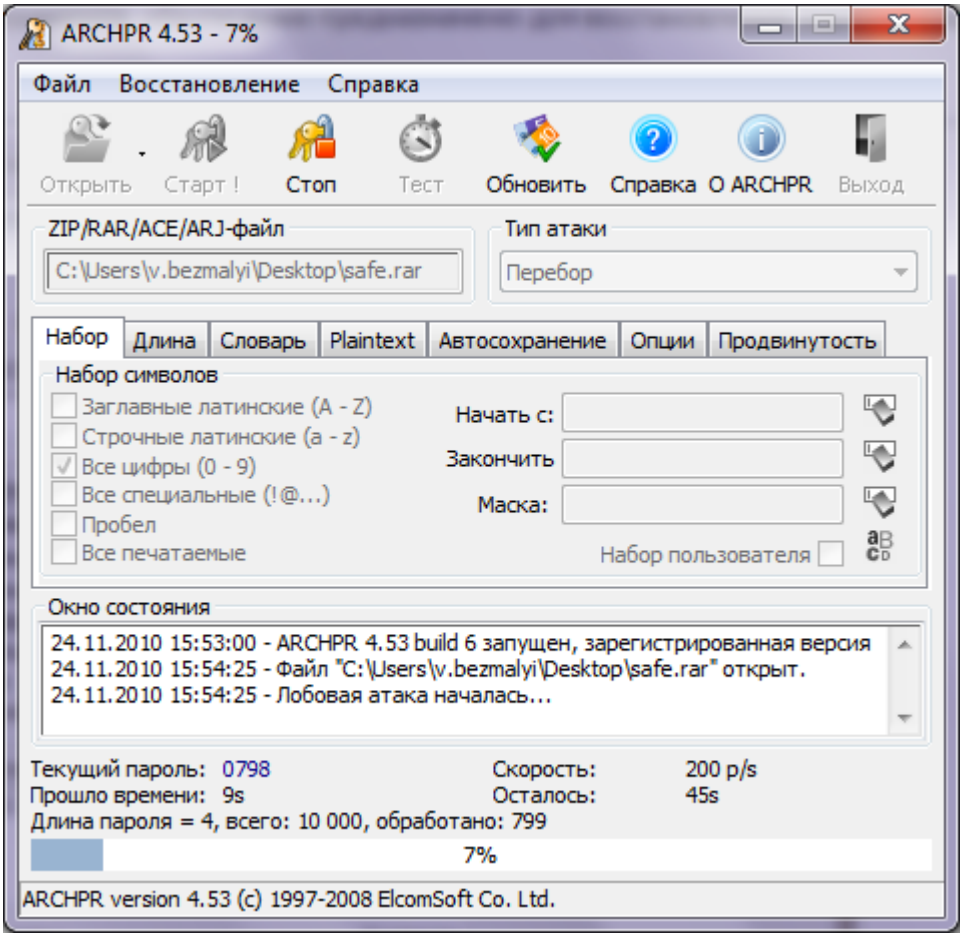

Рисунок 1 Восстановление пароля к архиву RAR

Данное программное обеспечение восстанавливает доступ к зашифрованным архивам двумя путями:

- Снимает парольную защиту
- Восстанавливает оригинальный текстовый пароль

Поддерживаемые форматы архивов ZIP/PKZip/WinZip, RAR/WinRAR, ARJ/WinARJ, а также ACE/WinACE (1.x), созданные любыми программами-архиваторами, а также самораспаковывающиеся архивы, созданные в PKZip, WinZip, RAR и WinRAR. При использовании WinZip 8.0 и более младших гарантируется снятие защиты в течение часа. Кроме того, стоит отметить, что при наличии хотя бы одного файла из архива, весь архив будет расшифрован за минуту (для архивов в формате ZIP и ARJ).

Следующим шагом в восстановлении без сомнения является восстановление пароля к почте. Так как почтовых клиентов существует огромное множество, то здесь нужно специализированное ПО.

Восстановление паролей с помощью Advanced Mailbox Password Recovery (AMBPR)

Данное ПО (рис. 2) предназначено для восстановления паролей следующих почтовых клиентов:

- Microsoft Internet Mail And News

- Eudora
- TheBat!
- TheBat! Voyager
- Netscape Navigator/Communicator Mail
- Pegasus mail
- Calypso mail
- FoxMail
- Phoenix Mail
- IncrediMail
- @nyMail
- QuickMail Pro
- MailThem
- Opera mail
- Kaufman Mail Warrior
- Becky! Internet Mail

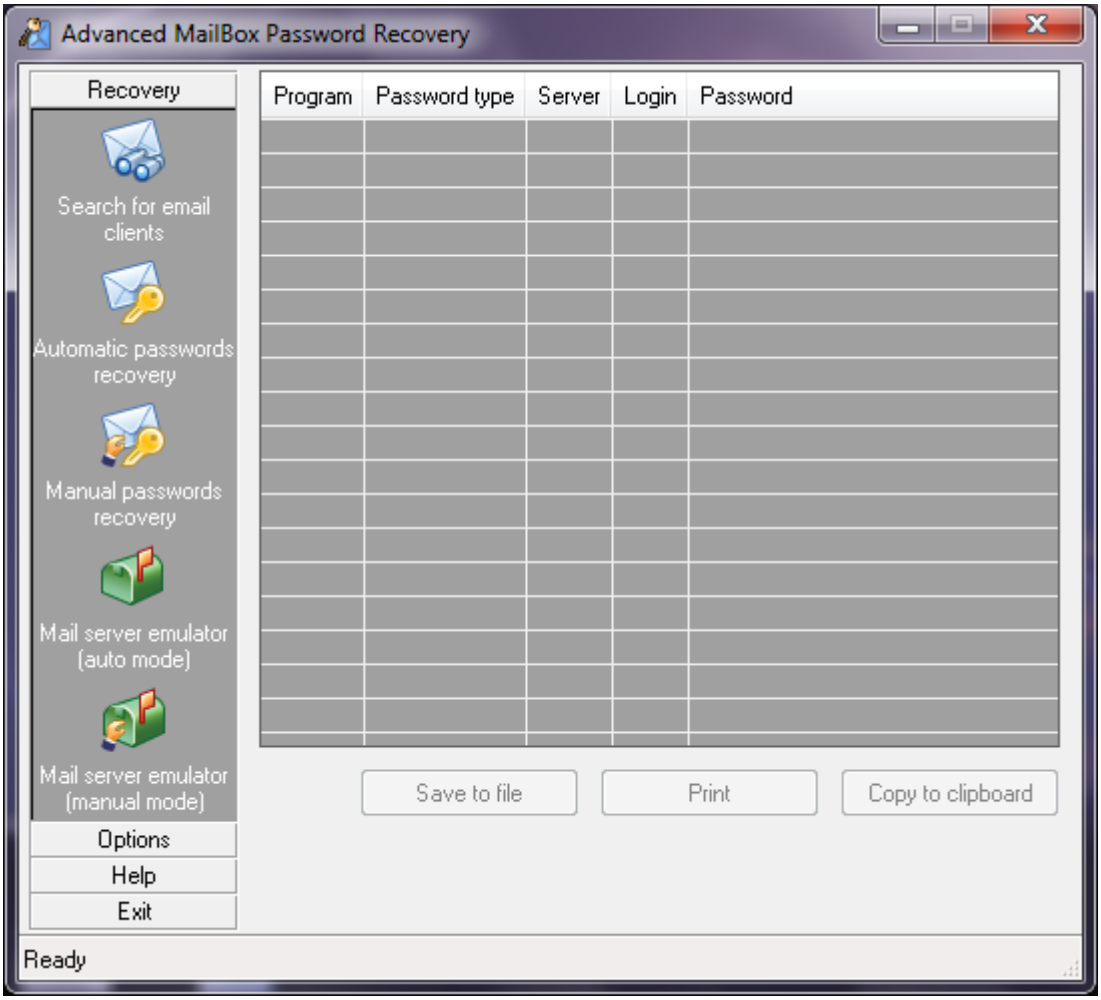

Рисунок 2 Advanced MailBox Password Recovery

Кроме того, стоит отметить что данное ПО включает в себя эмулятор серверов POP3 и IMAP, что позволяет получать пароли POP3/IMAP из любого почтового клиента.

Вместе с тем необходимо учесть, что возможно:

- восстановление паролей даже в том случае, если почтовая программа уже деинсталлирована
- Восстановление паролей из поврежденных баз данных и установок почтовых клиентов
- Автоматический режим: отображение паролей во всех установленных программах
- Ручной режим: работа с поврежденными файлами настроек и предыдущими установками программ

Отдельно хотелось бы упомянуть, что некоторые клиенты электронной почты, такие как Microsoft Internet Mail and News, Netscape Navigator/Communicator mail, IncrediMail и т.д., всю информацию, связанную с почтовым ящиком, хранят в реестре (Windows Registry), следовательно, при переустановке ОС Windows такая информация будет просто утеряна.

Отдельно хотелось бы упомянуть о мобильных почтовых клиентах. В случае утери пароля от мобильного почтового клиента, все, что вы сможете сделать, это просто заменить адрес сервера POP3/IMAP в почтовой программе, установленной на мобильном устройстве на адрес эмулятора сервера POP3/IMAP. Далее Advanced Mailbox Password Recovery перехватит и отобразит искомый пароль в тот самый миг, когда почтовая программа, запущенная на мобильном клиенте, соединится с сервером и попытается забрать новую почту.

Восстановление паролей к EFS

Очень часто мы с вами при исследовании ПК можем наблюдать картину когда по той или иной причине утрачен доступ к папкам или файлам, зашифрованным с помощью EFS (Encrypting File System). Причем зачастую пользователь сам забывает сделать сертификат для восстановления или переустанавливает систему, забыв предварительно расшифровать соответствующие файлы и папки или экспортировать сертификат. Как быть в этом случае?

Что такое EFS?

EFS (Encrypting File System) – тесно интегрированная с NTFS служба. Появилась начиная с Windows 2000. Файловые системы по состоянию на сегодняшний день не обеспечивают необходимый уровень защиты данных от несанкционированного доступа. Ведь несмотря на то что в NTFS существует разграничение доступа, можно получить доступ, загрузившись из-под сторонней ОС.

Единственным средством защиты доступа от физического чтения является шифрование файлов.

Рассмотрим подробнее как работает EFS.

Технологии шифрования

EFS использует архитектуру Windows CryptoAPI. В основе ее лежит шифрование с открытым ключом. Для шифрования каждого файла случайным образом генерируется ключ шифрования файла. При этом сам файл будет шифроваться с помощью любого симметричного алгоритма шифрования. В данный момент для этого используется алгоритм DESX, который является специальной модификацией DES.

Операции шифрования и дешифрования поддерживаются для файлов и каталогов. В том случае, если шифруется каталог, автоматически шифруются все файлы и подкаталоги этого каталога. Необходимо отметить, что если зашифрованный файл перемещается или переименовывается из зашифрованного каталога в незашифрованный, то он все равно остается зашифрованным. Операции шифрования/дешифрования можно выполнить двумя различными способами - используя Windows Explorer или консольную утилиту Cipher.

Зашифрованные файлы хранятся на диске в зашифрованном виде. При чтении файла данные автоматически расшифровываются, а при записи - автоматически шифруются.

Немного теории

Для шифрования в EFS используется схема с общим ключом. При этом данные шифруются симметричным алгоритмом при помощи сгенерированного случайным образом ключа FEK определенной длины.

FEK шифруется одним или несколькими общими ключами шифрования, в результате чего получается список зашифрованных ключей FEK. Список зашифрованных ключей FEK хранится в специальном атрибуте EFS, который называется DDF (data decryption field - поле дешифрования данных). Информация, при помощи которой производится шифрование данных, жестко связана с этим файлом. Общие ключи выделяются из пар пользовательских ключей сертификата X509 с дополнительной возможностью использования "File encryption". Личные ключи из этих пар используются при дешифровке данных и FEK.

FEK также шифруется при помощи одного или нескольких ключей восстановления (полученных из сертификатов X509, записанных в политике восстановления зашифрованных данных для данного компьютера, с дополнительной возможностью "File recovery").

Восстановление ключей EFS

На самом деле наиболее правильным будет восстановить пароль пользователя (см. часть 1). В таком случае расшифровать EFS будет значительно проще, мы об этом еще поговорим ниже. Однако необходимо понимать, что даже если у вас нет соответствующего пароля, все равно можно попробовать расшифровать соответствующие файлы и папки. Для этого служит программное обеспечение **Advanced EFS Data Recovery**.

В данном ПО для удобства пользователя создан соответствующий Мастер Advanced EFS Data Recovery с помощью которого вы сможете пошагово пройти весь процесс расшифровки. Или можно воспользоваться «Режимом эксперта» для того чтобы выполнять действия самому.

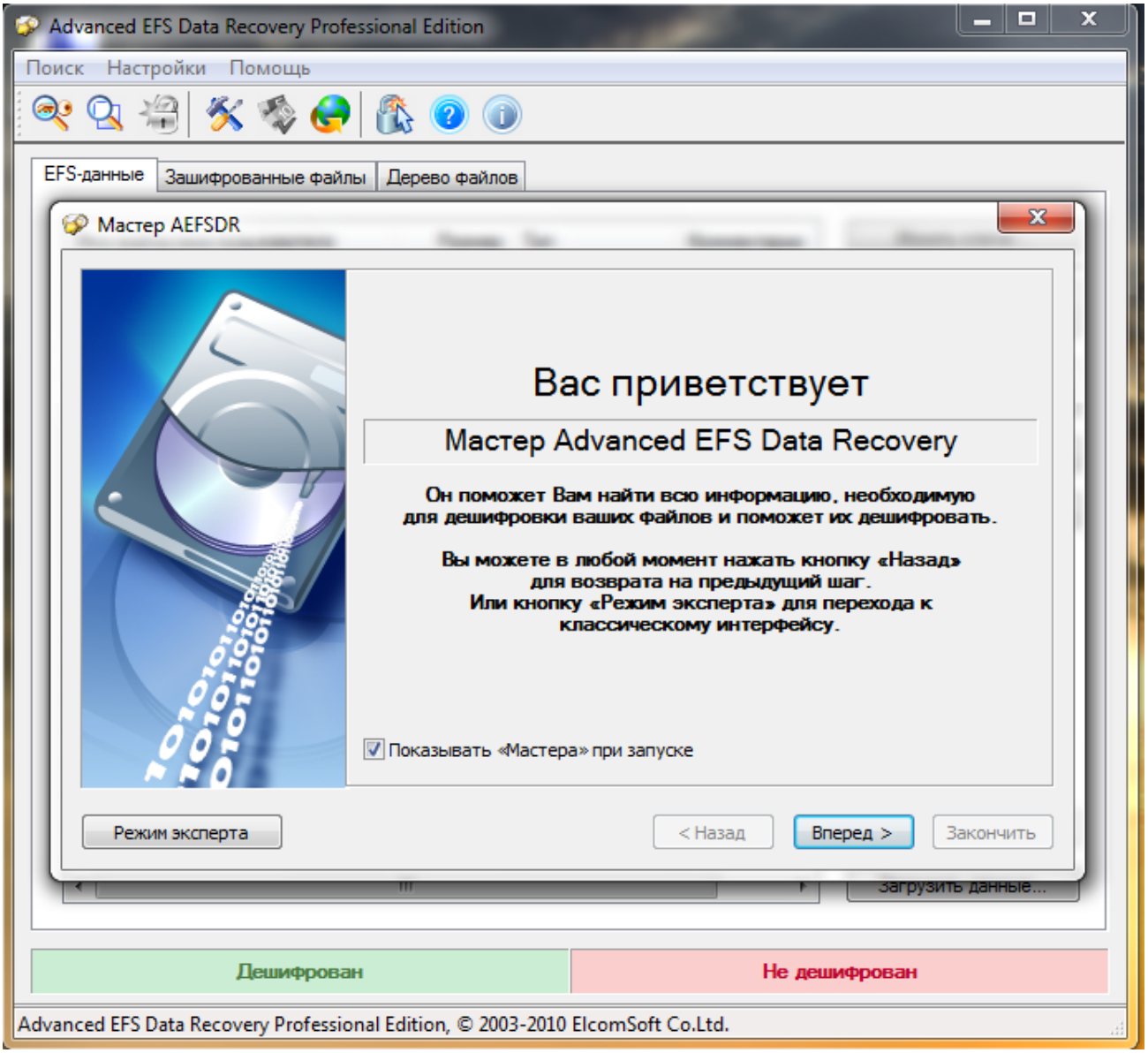

Рисунок 3 Мастер Advanced EFS Data Recovery

На мой взгляд, если человек, использующий Advanced EFS Data Recovery, не чувствует себя уверенно, гораздо удобнее использовать Мастер Advanced EFS Data Recovery. Рассмотрим этот режим чуть подробнее.

Мастер Advanced EFS Data Recovery

На первом этапе у вас будет запрошен персональный сертификат использовавшийся для EFS (рис.4).

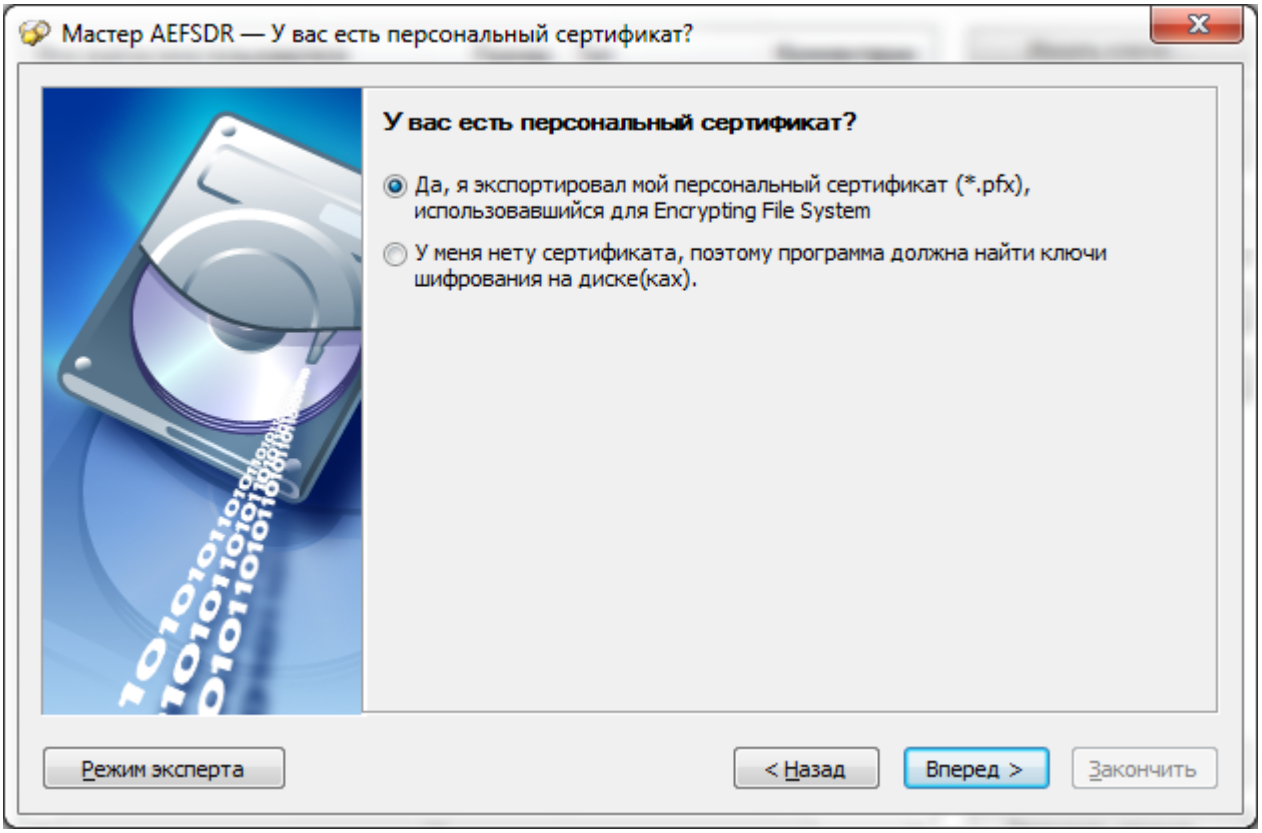

Рисунок 4 Первый шаг мастера

Предположим что у вас есть данный сертификат (ситуация крайне редкая, ведь пользователи почему-то либо пренебрегают экспортировать сертификаты либо просто забывают а куда же его экспортировали).

В этом случае все достаточно просто. От вас требуется выбрать файл сертификата (рис.5) и ввести пароль сертификата.

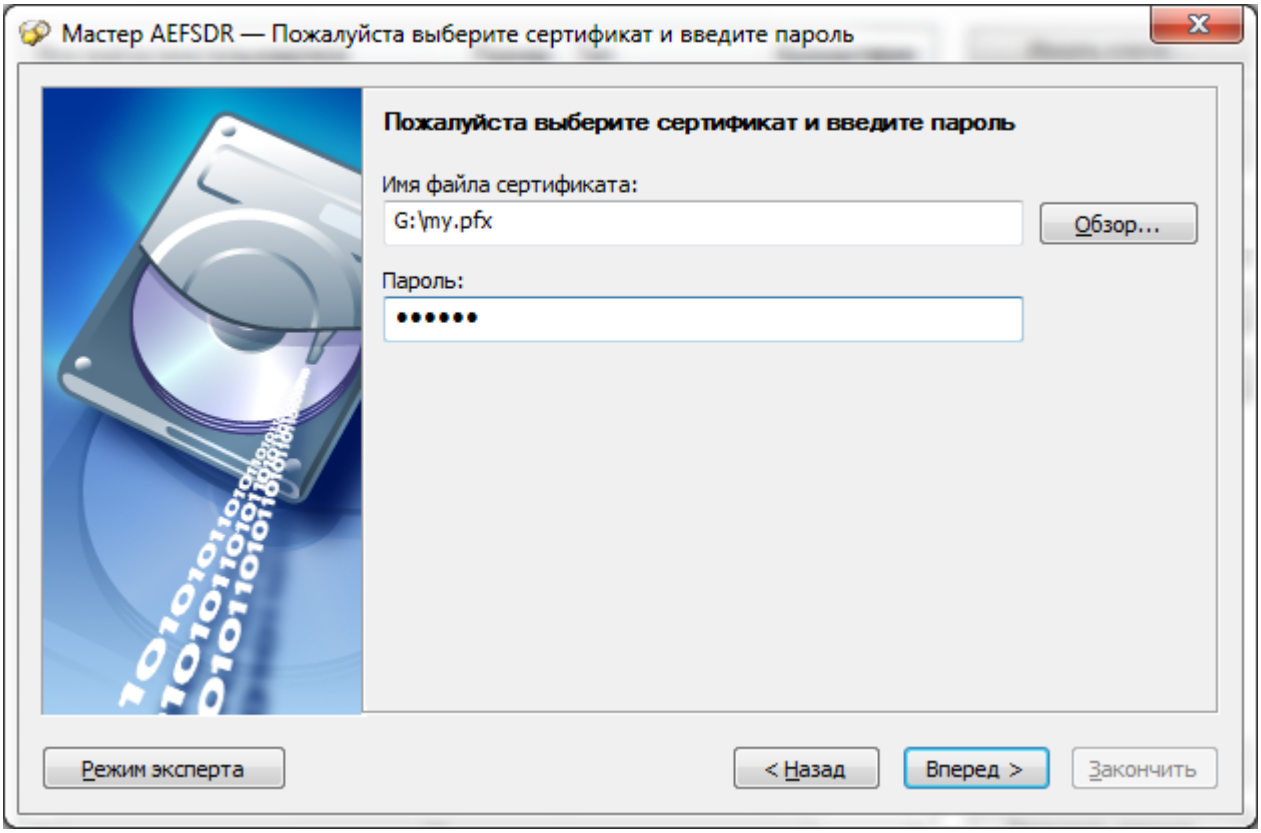

Рисунок 5 Выбор файла сертификата

Далее производится поиск всех зашифрованных с его помощью папок и файлов на локальных разделах (рис.6).

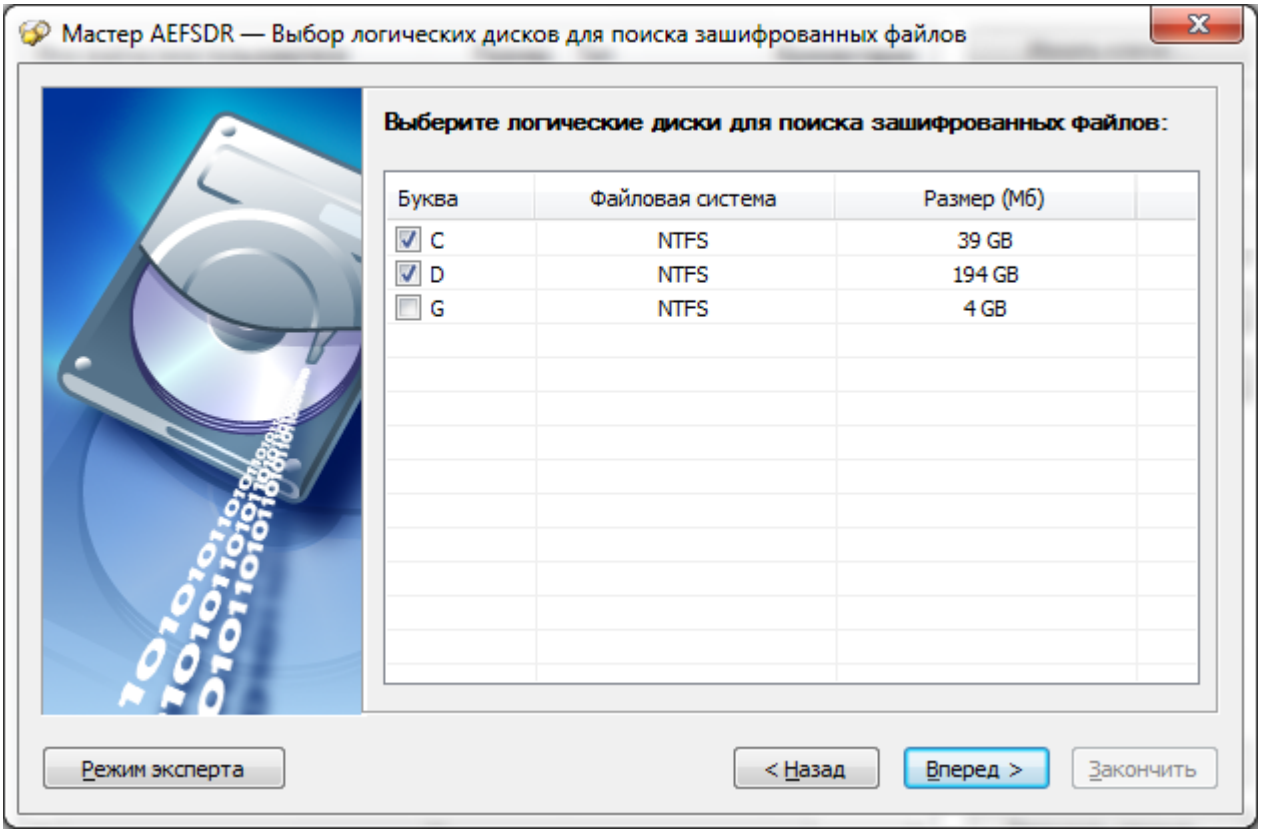

Рисунок 6 Поиск зашифрованных файлов

И вы получаете список найденных зашифрованных данным сертификатом файлов, которые можете расшифровать (рис.7).

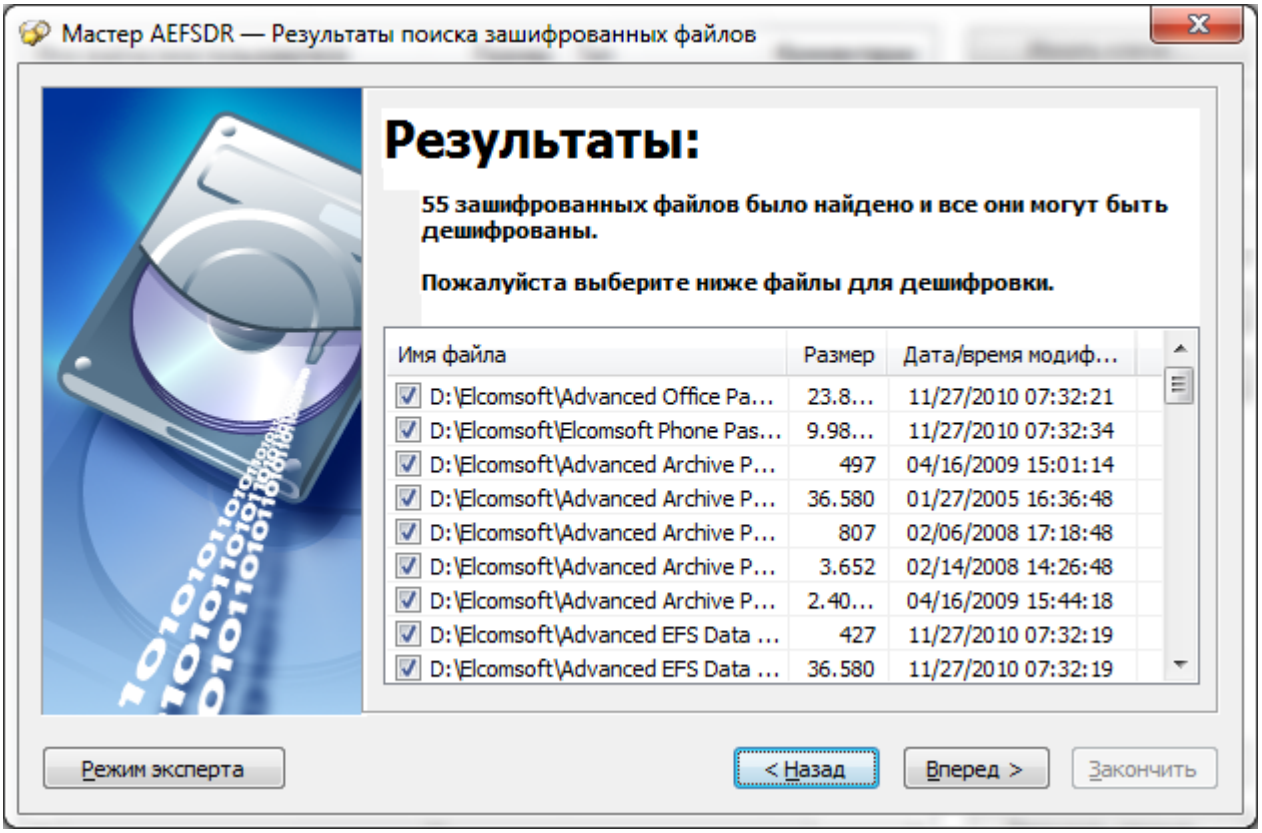

Рисунок 7 Результаты поиска зашифрованных файлов

Естественно, вы понимаете, что в случае исследования ПК расшифровывать вы должны на другой жесткий диск или внешний носитель, дабы ничего не повредить (рис.8).

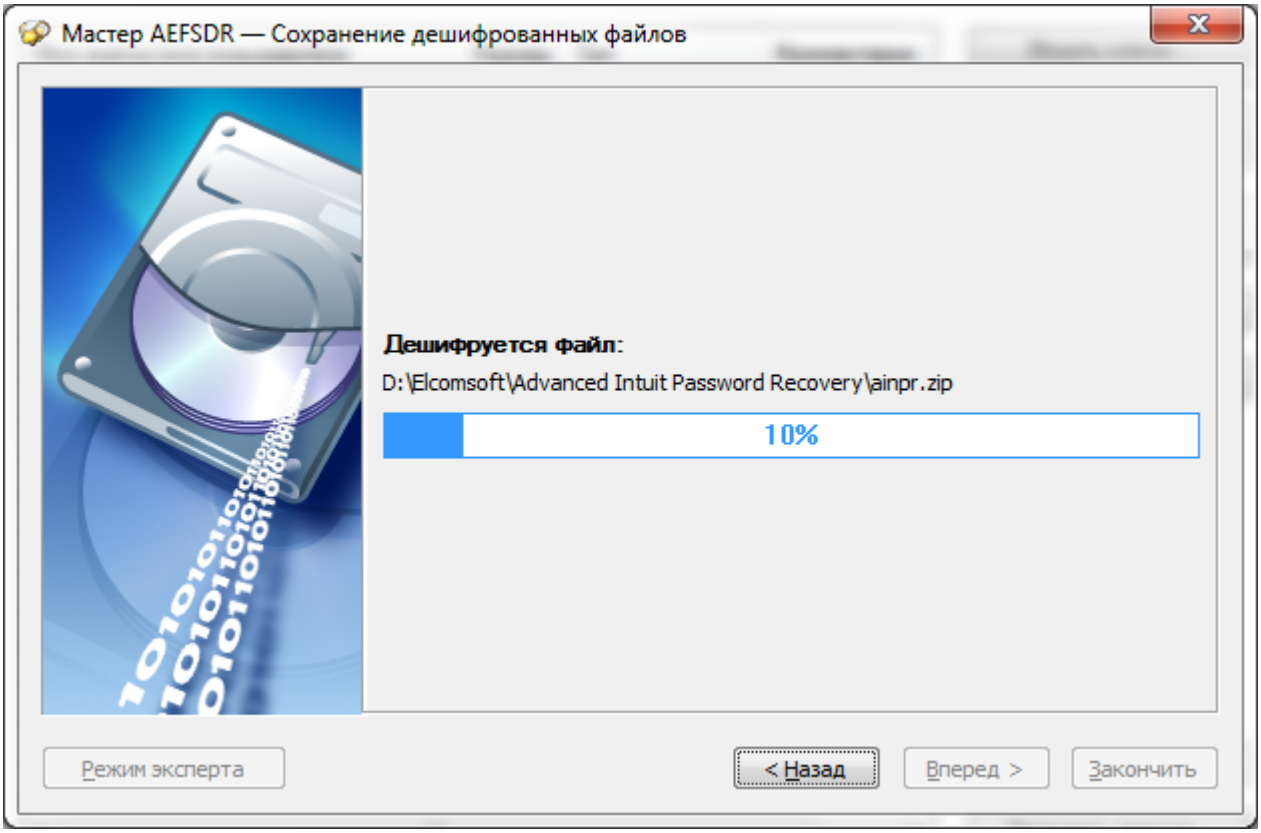

Рисунок 8 Дешифрование файлов

Но как быть если у вас нет сертификата?

В этом случае Мастер Advanced EFS Data Recovery предложит вам его поискать на жестком диске. Учтите, что вы сможете искать сертификат не только среди существующих файлов, но и среди удаленных. Но для этого вам необходимо включить флажок «Сканировать посекторно» (рис.9). Рекомендуется включать данный режим при повторном сканировании, если на первом проходе вы не обнаружили искомые сертификаты.

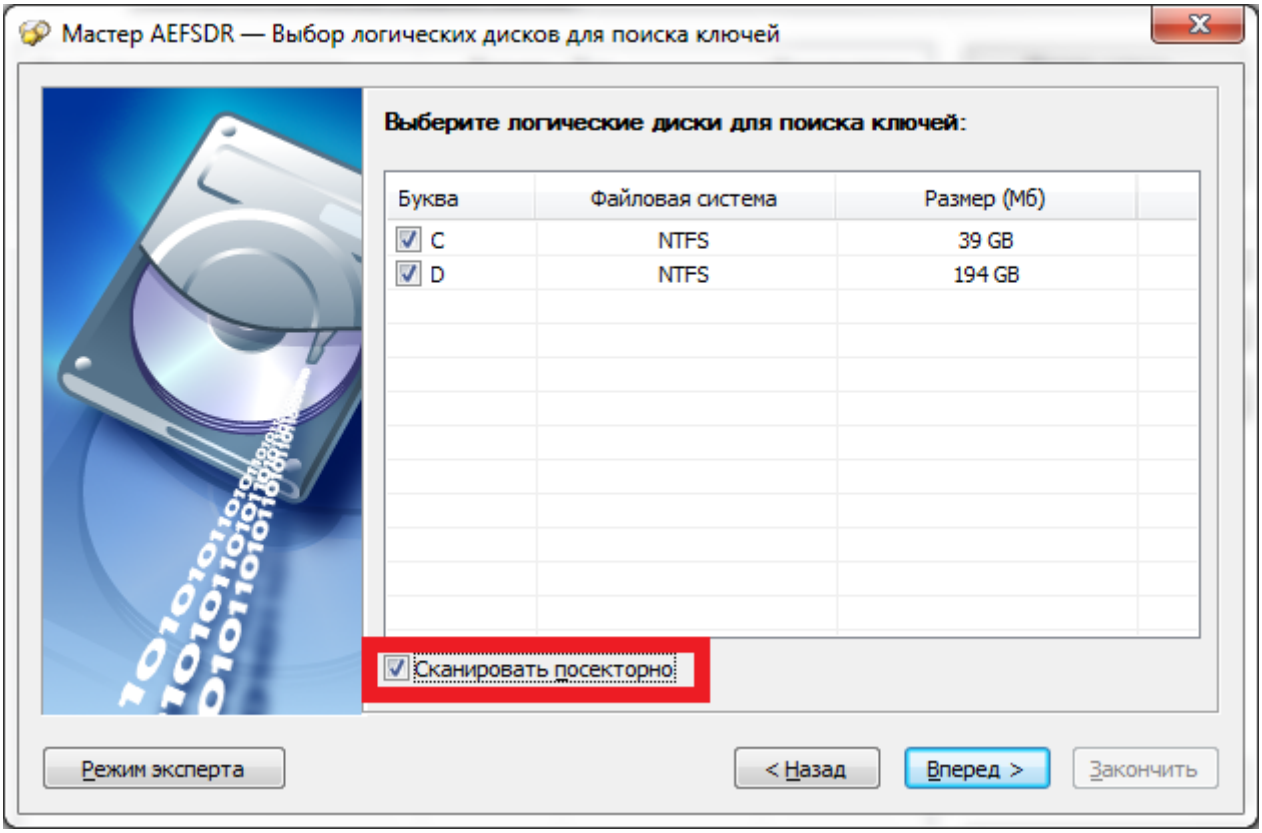

Рисунок 9 Выбор логических дисков для поиска ключей

Далее некоторое время у вас займет сам поиск ключей (рис.10).

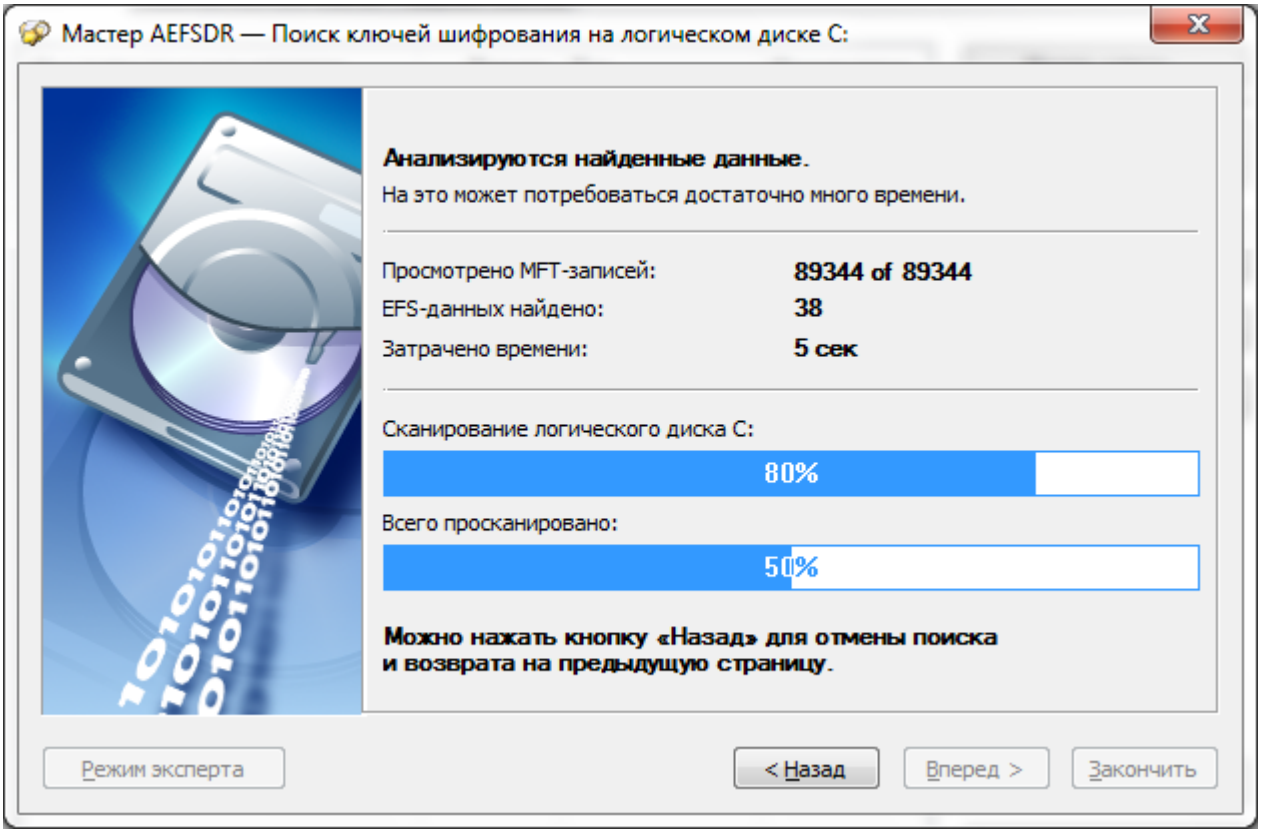

Рисунок 10 Поиск ключей шифрования на логическом диске C:

В результате поиска вам будет выведено окно мастера (рис.11).

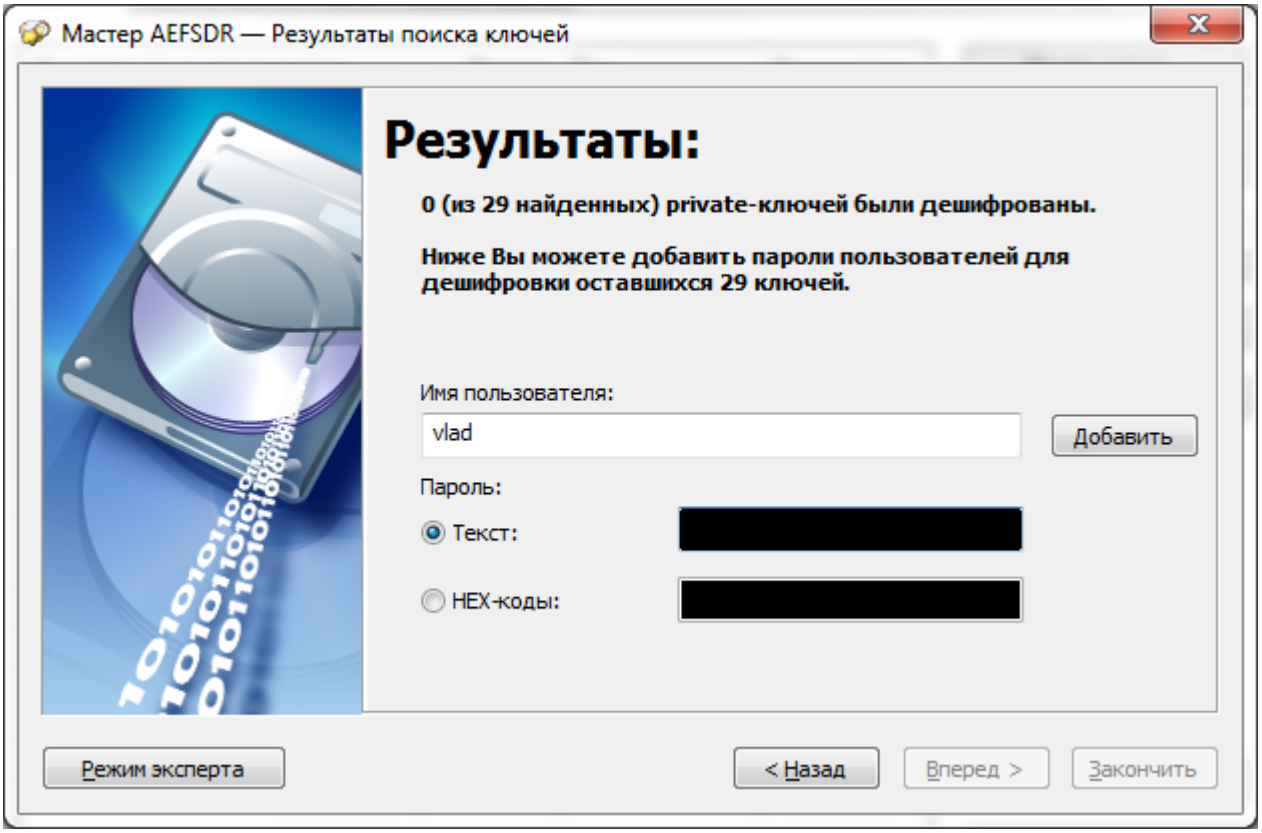

Рисунок 11Результаты поиска ключей

Если ключи не найдены, вам необходимо ввести имя пользователя (владельца EFS) и его пароль или в крайнем случае HEX-код. Как получить пароль пользователя мы уже описали в части 1 нашего цикла.

Если вам известен пароль требуемого пользователя, то вы вводите имя соответствующей учетной записи и ее пароль и нажимаете кнопку «Вперед». Далее происходит дешифрование найденных папок и файлов, зашифрованных с помощью EFS. Как видите, даже если вы переустановили вашу операционную систему, вовсе не факт, что вы потеряли данные, зашифрованные с помощью EFS.

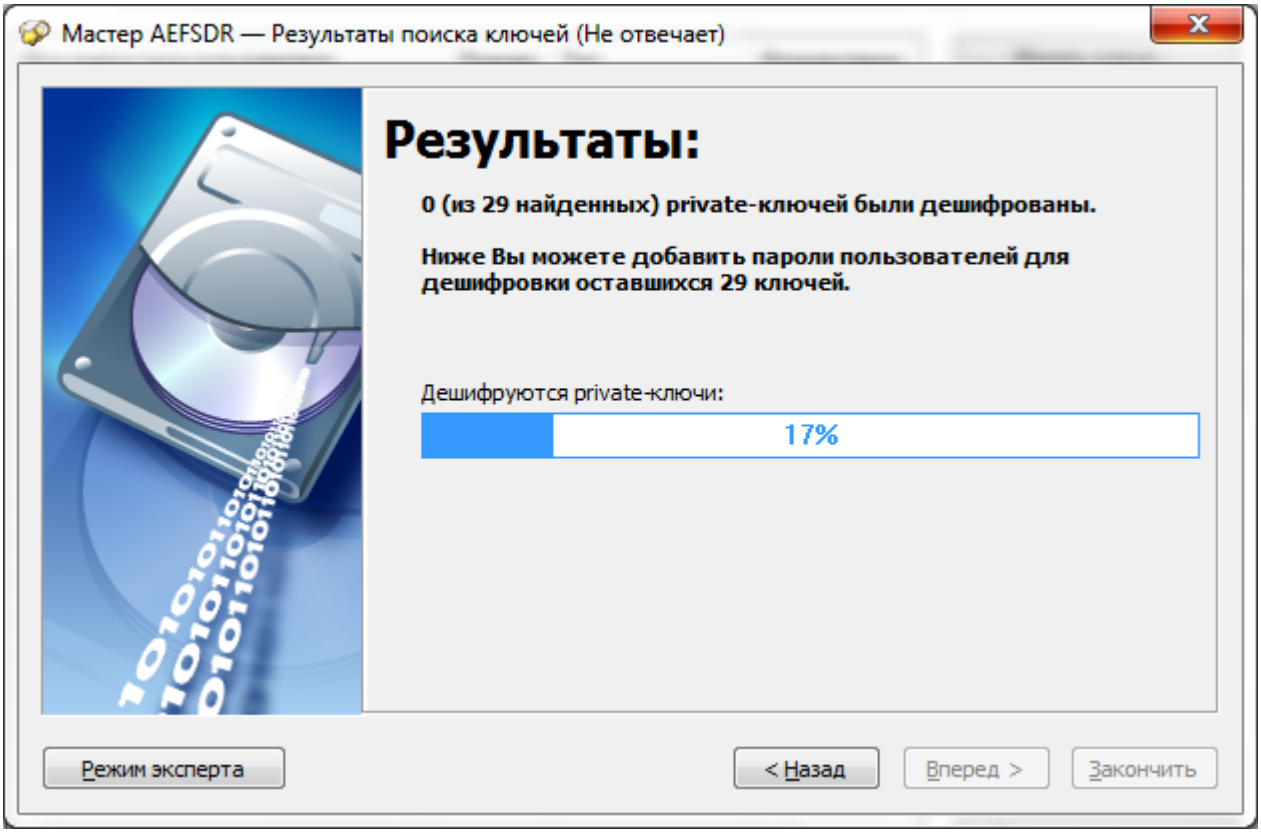

Рисунок 12 Результаты поиска ключей

Не забудьте, что зная имя и пароль учетной записи под которой осуществлялось шифрование, процесс расшифровывания займет у вас куда меньше времени. Однако как быть, если вы не знаете этого?

В таком случае можно попытаться осуществить расшифровывание с помощью режима эксперта. Хотя стоит честно признать, что вероятность положительного результата в данном случае заметно ниже.

Вам будет предложено добавить пароль из словаря (рис.13). Естественно, считается, что файлы словарей у вас уже есть.

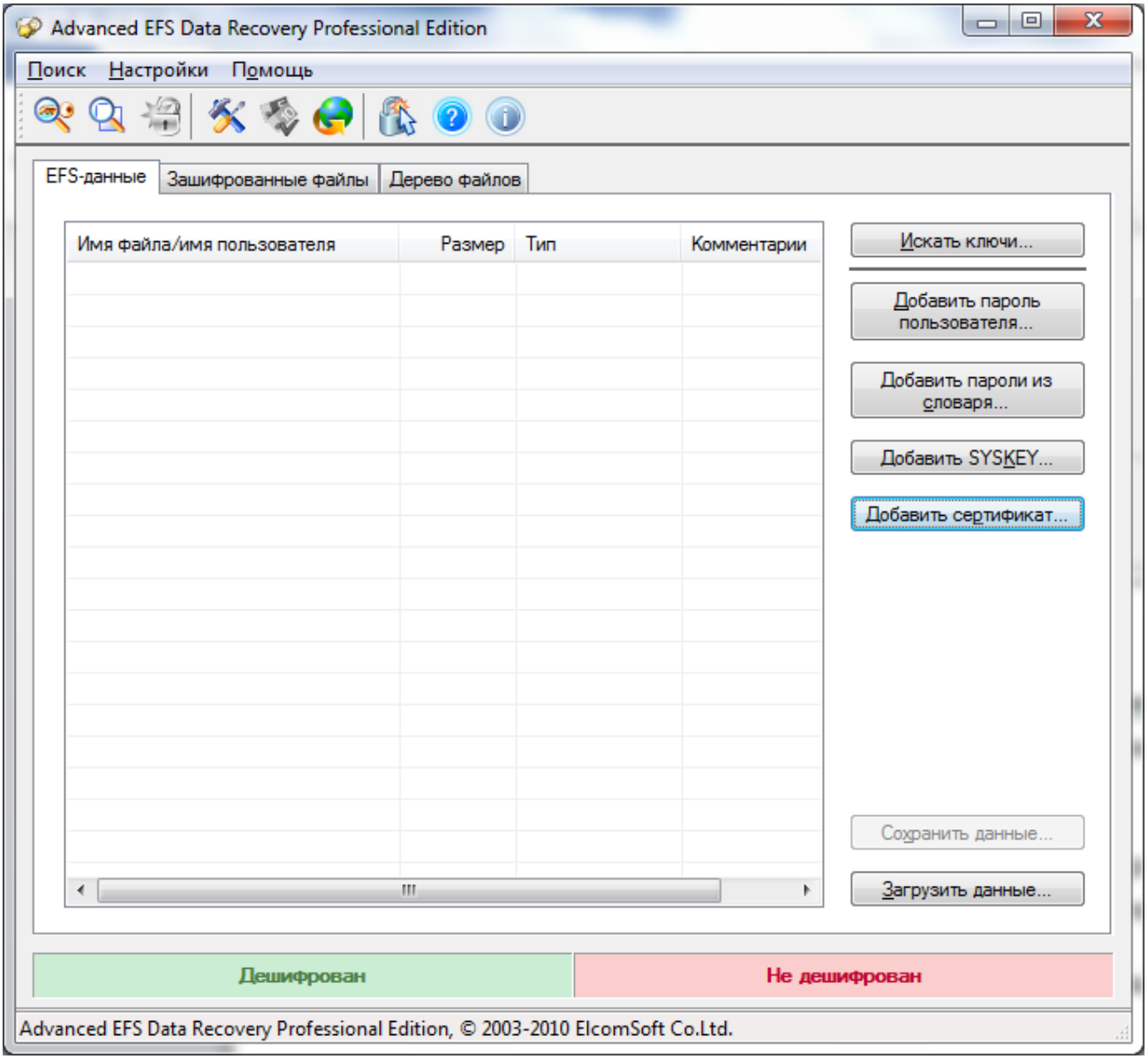

Рисунок 13 Режим эксперта

Заключение

Хотелось бы отметить следующее. Как видите, сегодня существуют достаточно мощные средства восстановления (взлома) паролей. Следовательно, для обеспечения их стойкости у нас есть два пути:

1. Дальнейшее наращивание их длины и сложности (на мой взгляд путь тупиковый, потому что рано или поздно пользователи начинают путаться, забывать пароли, использовать один и тот же на все случаи жизни и т.д.).
2. Использование биометрических средств аутентификации.
3. Использование многофакторной аутентификации и сертификатов. Данный путь, опять таки, на мой взгляд, значительно перспективнее, однако стоит учесть, что предлагаемые решения, конечно же, стоят денег и порой немалых.

Выбор, естественно, за вами.

Какой выбор примете вы? Не знаю.

Литература

1. Станислав Коротыгин Шифрующая файловая система (EFS) http://www.ixbt.com/storage/efs.html