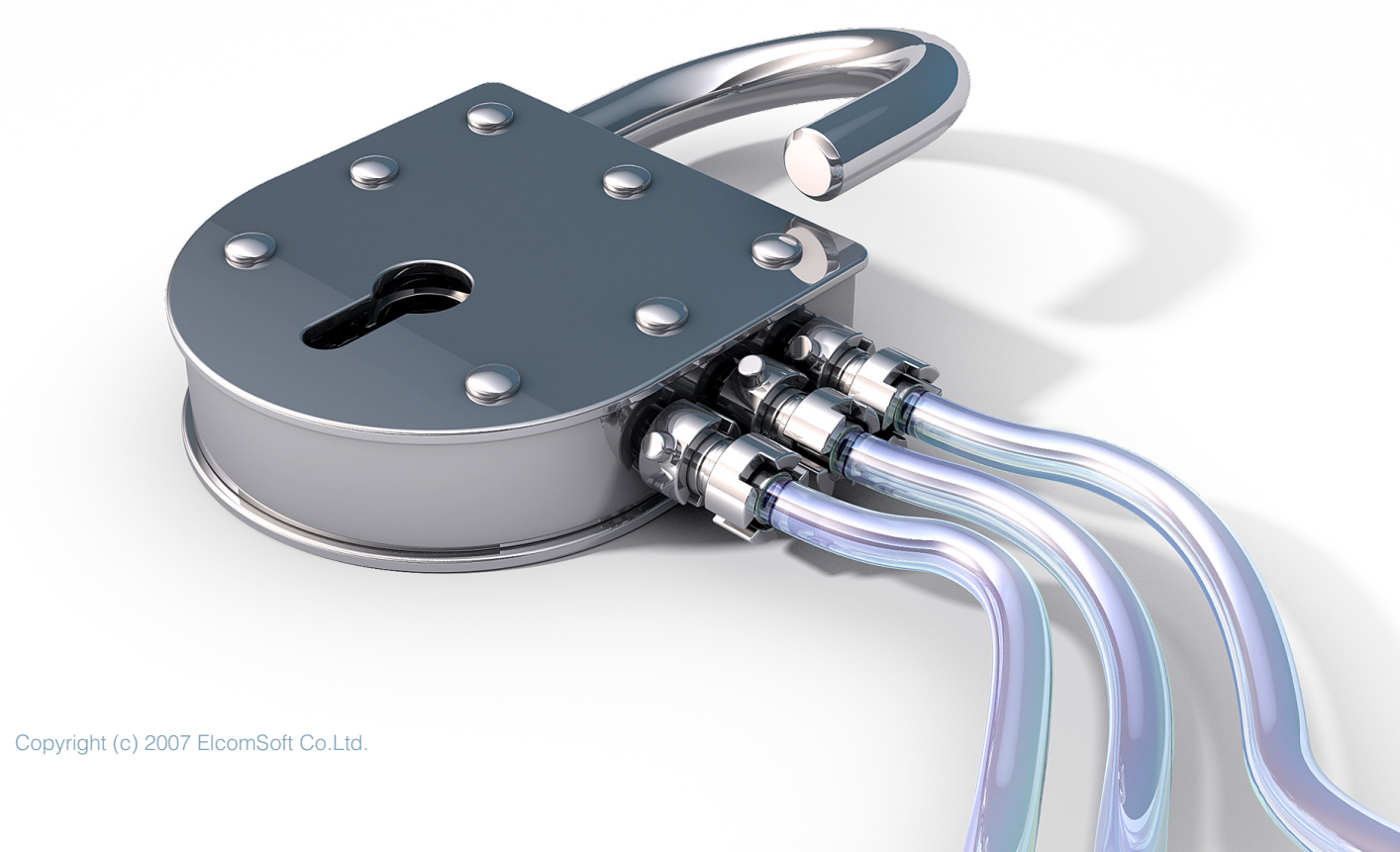
ELCOMSOFT
PROACTIVE SOFTWARE

WHITE PAPER

ПЛЮСЫ И МИНУСЫ EFS И ЭФФЕКТИВНОЕ ВОССТАНОВЛЕНИЕ ЗАШИФРОВАННЫХ ДАННЫХ



ELCOMSOFT
PROACTIVE SOFTWARE

СОДЕРЖАНИЕ

ЧТО ТАКОЕ EFS?

Одним из нововведений в составе Microsoft Windows 2000 и файловой системе NTFS 5.0, была технология Encrypting File System (EFS), которая предназначена для быстрого шифрования файлов на жестком диске компьютера.

Файловая система NTFS по своей сути является защищенной, однако, как это часто бывает, она очень скоро потребовала дополнительной надстройки безопасности. Причиной стало широкое распространение утилит типа NTFSDos, позволяющих легко обойти систему защиты NTFS, получив к ней доступ из-под DOS, игнорируя права доступа.

Система EFS использует шифрование с открытым и закрытым ключом и архитектуру CryptoAPI. EFS может использовать любой симметричный алгоритм шифрования файлов. В Microsoft Windows 2000 использовался DESX, в Windows XP - 3DES, а в Windows XP SP1, 2003 и новой Windows Vista - AES.

Для шифрования файлов не требуется совершать какие-либо предварительные операции. При первом шифровании файла, для пользователя автоматически создается сертификат шифрования и закрытый ключ.

Значительным удобством технологии EFS является то, что файлы остаются зашифрованными при перемещении на компьютере в другую папку или диск NTFS. Если перемещение идет на диск с другой файловой системой, то файлы автоматом расшифровываются. В случае если пользователь добавляет новые файлы в зашифрованную папку, они автоматически шифруются. Нет необходимости дешифровывать файл перед использованием, так как EFS встроена в операционную систему и выполнит эту операцию автоматически с соблюдением всех мер безопасности.

Создатели EFS подстраховались также и на случай утраты пользователем закрытого ключа, например, вследствие переустановки ОС, либо при создании новых пользовательских аккаунтов. В этом случае можно воспользоваться специальным EFS Recovery Agent для дешифровки файлов (в Windows 2000 Recovery Agent создавался автоматически: на отдельной машине – создавалась запись локального админа, а домене – администратора домена, в Windows XP и выше это необходимо делать врусную).

В данной статье мы оценим плюсы и минусы технологии EFS, а также рассмотрим возможности восстановления зашифрованных с ее помощью данных, в случае потери пароля или сбоя системы.

ПЛЮСЫ И МИНУСЫ EFS

Технология EFS работает таким образом, что зашифрованные одним пользователем файлы, не могут быть открыты другим пользователем, если у него нет соответствующих прав. После активации шифрования файл остается зашифрованным в любом месте хранения на диске, независимо от его перемещений. Шифрованию могут подвергаться любые файлы, в том числе и исполняемые.

Пользователь, имеющий права на открытие зашифрованного файла, работает с ним как с любым другим, не испытывая каких-либо ограничений или сложностей. Остальные же пользователи при попытке открыть зашифрованный EFS файл, получают сообщение о том, что в доступе отказано.

Такой подход, безусловно, очень удобен. Пользователь получает возможность надежно и быстро (с использованием штатных средств) ограничить доступ к конфиденциальной информации со стороны домочадцев или коллег, также имеющих доступ к компьютеру.
Казалось бы, EFS привносит в нашу жизнь только плюсы, однако это не так. Зашифрованная при помощи этой технологии информация может быть полностью утеряна, например, при переустановке операционной системы.

Стоит помнить, что сами файлы на диске шифруются с помощью ключа FEK (File Encryption Key), который хранится в их атрибутах. FEK зашифрован master-ключом, который в свою очередь зашифрован ключами пользователей системы, имеющих доступ к файлу. Ключи пользователей, соответственно, зашифрованы хэшами паролей этих самых пользователей, а хеши паролей – еще SYSKEY.

Такая цепочка шифрования, по мнению разработчиков EFS, должна надежно обеспечить защиту данных, но на деле, как мы покажем ниже, вся защита формально сводится к старой доброй комбинации логин-пароль.

Благодаря такой цепочке шифрования, при потере или сбросе пароля, сбое или переустановке операционной системы, доступ к зашифрованным при помощи EFS файлам на диске уже получить не удастся. Наоборот, он может быть потерян безвозвратно.

Обычные пользователи в полной мере не понимают, как функционирует EFS, за что потом часто расплачиваются потерянными данными. У Microsoft созданы специальные документы по EFS, разъясняющие принципы ее работы и основные проблемы, с которыми можно столкнуться при шифровании, но они сложны для понимания обычного пользователя, и поэтому их мало кто изучает перед началом работы.

ДАННЫЕ МОГУТ БЫТЬ ПОТЕРЯНЫ НАВСЕГДА

Итак, давайте разберемся, при каких условиях зашифрованные при помощи EFS данные могут быть потеряны? Насколько опасна та или иная ситуация? Давайте обо всем по порядку.

КАК МОЖНО ПОТЕРЯТЬ ДОСТУП К ДАННЫМ, ЗАШИФРОВАННЫМ EFS?

Почти все из нас сталкивались с ситуацией, когда необходимо полностью переустановить Windows, так как ее работоспособность нарушена из-за какого-то сбоя в работе программного обеспечения, вирусной атаки или ошибки неопытного пользователя, потерян системный пароль от учетной записи или удален профиль пользователя. В этом случае вся зашифрованная информация в старой конфигурации будет, скорее всего, утеряна.

Рассмотри подробнее следующие типовые случаи:

1. **Система не загружается из-за смены или поломки комплектующих компьютера или нарушения работоспособности ОС.** Например, вышла из строя материнская плата, поврежден загрузочный сектор, испорчены системные файлы, установлены каких-то «сырые» обновления или другой нестабильный софт. В этом случае жесткий диск можно подключить к другому компьютеру и прочитать данные, но в зашифрованном EFS виде этого сделать нельзя.
2. **Системный администратор на предприятии или сам пользователь сбросил пароль пользователя.** В этом случае доступ к зашифрованным EFS данным также будет утрачен.
3. **Удалён профиль пользователя.** В этом случае файлы (включая ключи пользователя) могут всё ещё быть на диске, но система их не видит, даже если заново создать пользователя с тем же именем, то у него будет другой ID, а он используется в процессе шифрования. В этой ситуации доступ к данным, зашифрованном EFS, также будет потерян.
4. **Пользователь переносится в другой домен (авторизуется через другой сервер).** Если при переносе его ключи шифрования хранились на сервере (обычно именно так и бывает), то при неграмотном переносе доступ к зашифрованным EFS данным может быть потерян.
5. **Переустановка системы.** В этом случае доступ зашифрованным EFS данным, естественно, будет потерян. Если при этом сделана резервная копия системного диска целиком, или хотя бы своего профиля («Documents and Settings»), то с помощью специального ПО возможно его восстановить, но только в случае сохранности ключей.

Достаточно типична ситуация, когда сама система храниться на одном диске, а зашифрованные файлы на другом диске. При переустановке системы администратор, как правило, делает бекап только диска с данными, после чего система переустанавливается. Понятно, что в этом случае теряются ключи, а вместе с ними и доступ к зашифрованным данным.

Стоит оговориться, что такой ситуации можно избежать штатными средствами, если перед использованием EFS настроить EFS Recovery Agent (далее «Агент восстановления»), но его реализация, как весь принцип работы EFS слишком сложны для рядового пользователя, что мы продемонстрируем ниже.

ЧТО ТАКОЕ EFS RECOVERY AGENT?

Агентом восстановления является пользователь, уполномоченный расшифровывать данные, зашифрованные другим пользователем, если он утратил закрытые ключи сертификата шифрования или его учетная запись была удалена, но при этом требуется восстановить зашифрованные данные.

Как правило, Агентом восстановления назначается Администратор, но это может быть и другой пользователь. Агентов восстановления может быть несколько. Чтобы назначить пользователя Агентом восстановления, необходимо сначала создать сертификаты Агента восстановления командой Cipher /R: filename, где filename - путь и имя создаваемых сертификатов без расширения.

После этого пользователю будет предложено ввести пароль для защиты закрытого ключа и подтвердить его (при вводе пароля он не будет отображаться в консоли). Затем будет создано два файла с указанным именем - *.cer и *.pfx, содержащих, соответственно, открытый и закрытый ключи сертификата. Теперь необходимо добавить сертификат в личное хранилище пользователя, назначаемого Агентом восстановления (можно пропустить этот шаг, тогда Агент восстановления может проделать это позже, когда будет необходимо использовать функции восстановления) импортировав файл *.pfx (для запуска Мастера импорта сертификатов достаточно дважды щелкнуть по значку файла). После этого необходимо от имени администратора открыть оснастку «Локальные параметры безопасности» (Пуск - Выполнить - secpol.msc), выделить пункт «Политики открытого ключа - Файловая система EFS» и в меню «Действие» выбрать «Добавить агент восстановления данных». Откроется «Мастер добавления агента восстановления», на второй странице которого необходимо нажать кнопку «Обзор папок» и указать ранее созданный файл *.cer.

В целях восстановления доступа к зашифрованным файлам после переустановки системы или вследствие утраты закрытого ключа следует сохранить в надежном месте закрытые ключи Агентов восстановления или (если они не назначены), закрытые ключи всех пользователей, использующих EFS, экспортировав их из хранилища «Личные» оснастки «Сертификаты» (certmgr.msc). В Windows Vista, наконец то появилась возможность хранения ключей на смарт-карте, что гораздо надежнее с точки зрения безопасности.

Как видно, такая подстраховка при помощи EFS Recovery Agent противоречит заложенному в ней принципу простоты, требует нетривиальных с точки зрения массового пользователя (рутинных для администратора) действий и манипуляций. Немудрено, что этим мало кто пользуется.

Стоит заметить, что если для локального пользователя администратор попытается удалить пароль учетной записи, то пользователь потеряет все личные сертификаты, а соответственно и доступ к зашифрованным EFS файлам (при такой попытке будет выдано соответствующее предупреждение). Тоже самое произойдет, если локальный администратор, используя специальные средства, попытается сбросить пароль «насильно» (т.е. без ввода старого).

Как следствие, риск потерять самые важные данные, зашифрованные EFS, при сбое операционной системы или ошибки администратора/пользователя довольно высок и его обязательно нужно учитывать.

ЧТО ДЕЛАТЬ, ЕСЛИ ПРОИЗОШЕЛ СБОЙ?

Типичной ситуацией, когда пропадает доступ к зашифрованным EFS данным, является потеря связи между операционной системой и имеющимися физически на диске ключами (см. ситуации, описанные в пункте «Как можно потерять доступ к данным, зашифрованным EFS?»). В этом случае не стоит отчаиваться, выход есть, доступ к данным может быть восстановлен с высокой степенью вероятности. Но если ключи удалены с диска и не была сделана резервная копия профиля пользователи или его сертификатов, то данные, увы, будут потеряны навсегда.

Как показывает практика, очень часто не помогает даже экспорт/импорт профиля или сертификатов – ключи в системе появляются, но доступ к зашифрованным данным при этом не восстанавливается.

Если все-таки произошла неприятность и зашифрованные EFS данные оказались недоступны при сохранении ключей, то можно воспользоваться специальным программным обеспечением, которое поможет с высокой степенью вероятности восстановить доступ к данным.

ВОЗМОЖНЫЕ ВАРИАНТЫ ДЕЙСТВИЙ

Далее попробуем описать возможные варианты действий в этой ситуации, их существует несколько:

1. Загрузка под рабочей учетной записью пользователя с привилегиями Администратора, если она существует, с последующей установкой специальной программы для расшифровки.

2. Физическое отсоединение жесткого диска и установка его на другой рабочей машине со специальной программой для расшифровки.

3. Загрузка другой операционной системы, установленной на той же машине, если она установлена, либо ее установка специально для этой цели.

Главное, что должно быть сделано – это получение прямого доступа к диску. Если идти по первому пути, то это возможно только у пользователей с правами администратора. Поэтому если прав у резервной/рабочей учетной записи не достаточно, то их можно попытаться расширить каким-либо способом.

СХЕМА РАСШИФРОВКИ ДАННЫХ

Когда прямой доступ к диску получен, то можно переходить к следующему этапу – непосредственно расшифровке и восстановлению данных. Это можно сделать по следующей схеме:

1. Поиск и попытка расшифровки всех ключей на жестком диске проблемного компьютера.

2. Поиск зашифрованных файлов на жестком диске и попытка их расшифровки.

Одним из наиболее эффективных средств, предназначенных для расшифровки защищенных EFS данных, является программный продукт Advanced EFS Data Recovery. Он позволяет расшифровать данные на проблемном компьютере, даже в случае, если повреждены некоторые записи о ключах пользователя.

Возможности и особенности Advanced EFS Data Recovery мы подробно рассмотрим ниже.

ADVANCED EFS DATA RECOVERY

Advanced EFS Data Recovery (AEFSDR) – специализированная программа для расшифровки файлов, зашифрованных при помощи технологии EFS под операционными системами Microsoft Windows 2000 и Windows XP, Windows 2003 Server и новой Windows Vista.

Программа позволяет в сжатые сроки расшифровывать файлы даже в том случае, если система не грузится или повреждены некоторые записи о ключах шифрования.

Даже если база пользователей системы защищена при помощи SYSKEY, Advanced EFS Data Recovery все равно позволяет расшифровать файлы. Под Windows 2000 возможна расшифровка всех файлов, даже если неизвестны пароли администратора и пользователей.

Advanced EFS Data Recovery работает в два этапа:

1. На первом этапе производится поиск всех ключей EFS (персональных и master) и попытка их расшифровки. На первом этапе должен быть расшифрован хотя бы один ключ, это требуется для дальнейшей расшифровки файлов. В Windows XP и выше для этого может понадобиться ввести в AEFSDR пароль пользователя, шифровавшего файлы, или пароль Recovery Agent. Сперва программа пытается сделать это автоматом – например, вытаскивая пароль из кэша или системных файлов, проверяя простые варианты (типа пароль = имя пользователя) и проводит атаку по небольшому встроенному словарю.

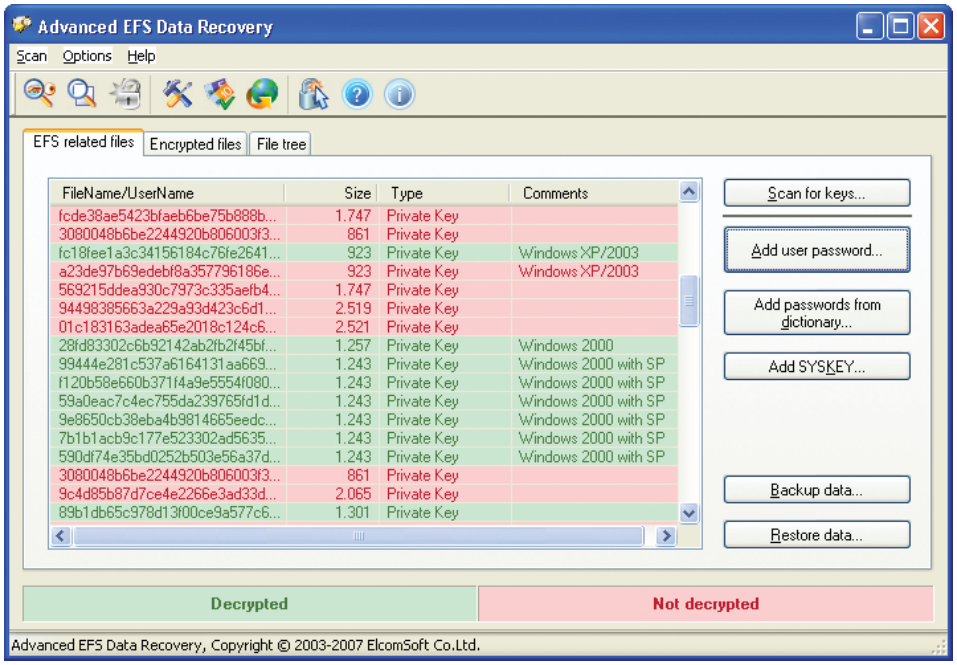


Рис.1. Закладка поиска на компьютере и расшифровки персональных ключей EFS.

2. На втором этапе происходит поиск зашифрованных при помощи файлов EFS на жестком диске и также делается попытка расшифровки. Если зашифрованных файлов немного и известно, где они находятся, то для экономии времени можно и выбрать эти файлы вручную в закладке программы «File tree».

На практике может оказаться, что ключи лежат на сервере в сети, а зашифрованные ими файлы находятся на локальной машине. В этом случае с помощью AEFSDR можно сначала найти и расшифровать ключи на сервере, а потом воспользоваться опцией «Backup data», сохранить результаты в файл и перенести их на локальную машину. Таким образом, результаты работы на первом этапе, можно будет перенести уже на машину с зашифрованными данными для начала второго этапа работы.

Процесс расшифровки файлов может занять значительно время, поэтому важным достоинством Advanced EFS Data Recovery является возможность установки уровня нагрузки на систему. Пользователь может выбрать между тремя уровнями нагрузки: High, Normal и Low.

Немаловажным является и полная поддержка новейшей операционной системы Microsoft Windows Vista и Windows Server 2008, которая реализована в Advanced EFS Data Recovery.

В завершении необходимо сказать об эффективности работы продукта, т.е. о вероятности успешной расшифровки данных. По оценке экспертов компании Elcomsoft при условии обнаружения ключей пользователя продукт Advanced EFS Data Recovery позволяет успешно восстановить **до 99%** зашифрованных при помощи EFS данных, что является очень высоким результатом.

Скачать пробную версию Advanced EFS Data Recovery можно здесь.

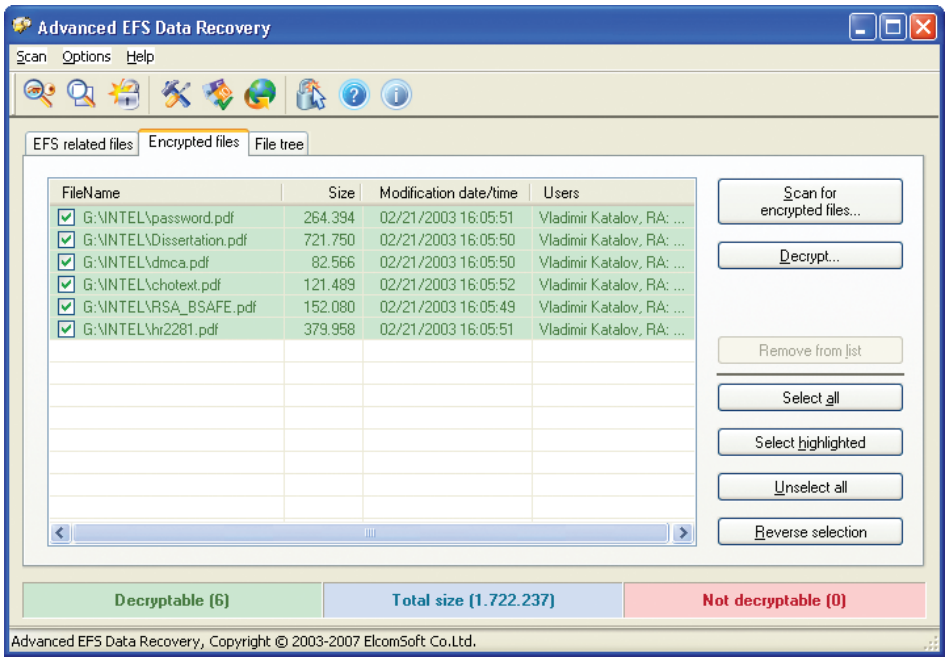


Рис.2. Закладка поиска и расшифровки файлов.

ELCOMSOFT
PROACTIVE SOFTWARE

О КОМПАНИИ «ЭЛКОМСОФТ»

Основанная в 1990 году, российская компания «ЭлкомСофт» является одним из лидеров рынка программного обеспечения для восстановления доступа к системам, приложениям и документам. Благодаря уникальным технологиям, продукты компании получили широкое признание как в России, так и за рубежом.

В число клиентов «ЭлкомСофт» входят многие известные в мире из следующих отраслей:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

Компания имеет статусы Microsoft Gold Certified Partner, Intel Software Partner, а также является членом Российской криптографической ассоциации, Computer Security Institute (CSI), Association of Shareware Professionals (ASP).

Компания «ЭлкомСофт» является признанным экспертом на рынке, на ее технологические разработки ссылаются во многих известных книгах, например, «Microsoft Encyclopedia of Security», «The art of deception» (Kevin Mitnick), «IT Auditing: Using Controls to Protect Information Assets» (Chris Davis), «Hacking exposed» (Stuart McClure).

Чтобы узнать больше, посетите сайт компании.

АДРЕС:

ООО «ЭлкомСофт»
Звездный б-р, 21, офис 541
129085 Москва

ФАКСЫ:

US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

ВЕБ-САЙТЫ:

http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr