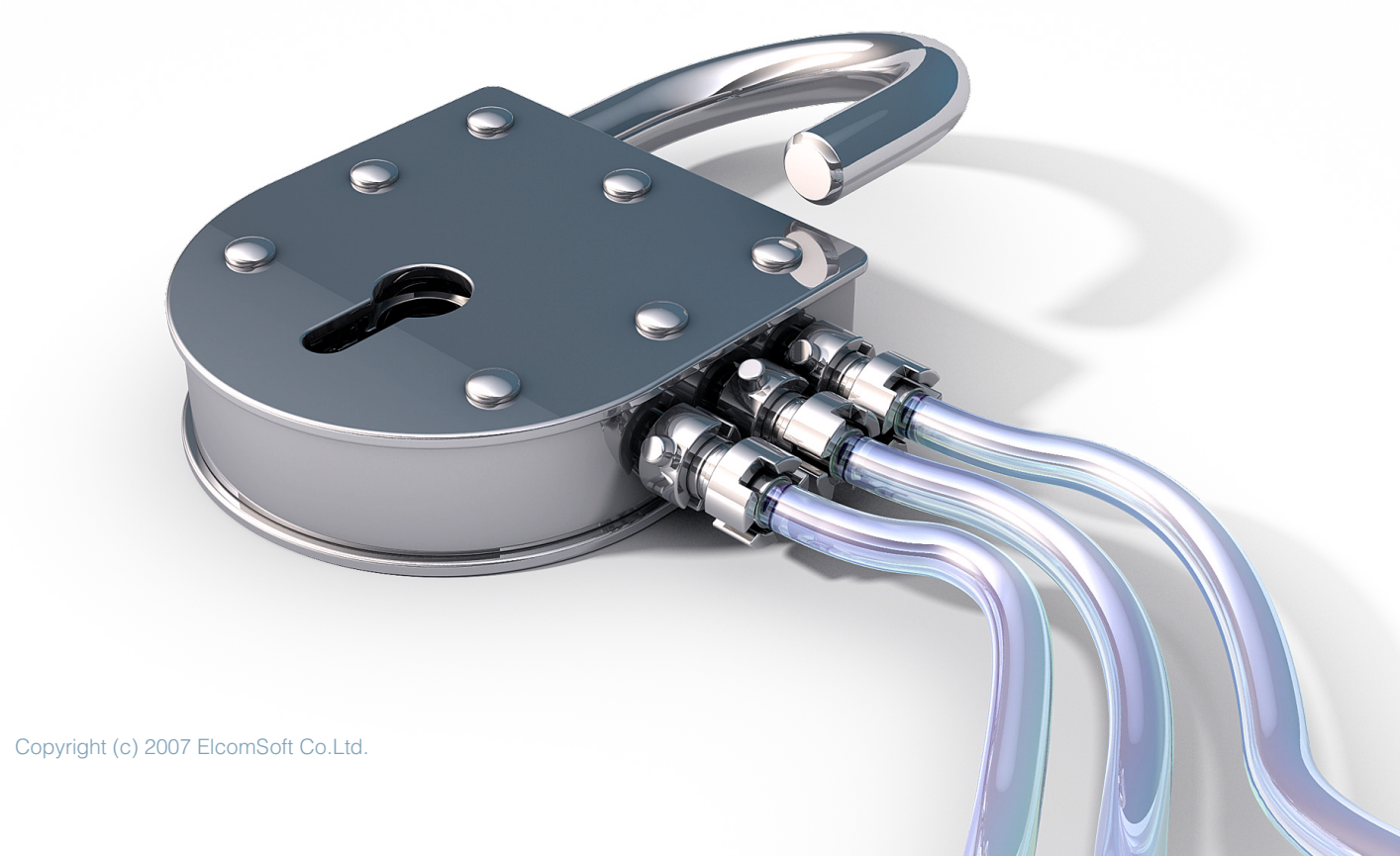
ELCOMSOFT
PROACTIVE SOFTWARE

WHITE PAPER

ЭФФЕКТИВНЫЙ СПОСОБ ВОССТАНОВЛЕНИЯ ДОСТУПА К СИСТЕМЕ ПОД УПРАВЛЕНИЕМ WINDOWS



ELCOMSOFT
PROACTIVE SOFTWARE

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Стремясь защитить важную для себя информацию, мы используем множество различных методов и технологий, особенно, если эта информация конфиденциальна или критична работы для бизнеса и принятия важных управленческих решений.

«Кто владеет информацией, то владеет миром» – это основопогалающий постулат сегодняшнего времени, когда контроль над информацией играет важнейшую роль. Утрата доступа к важным данным может очень болезненно отразиться на бизнесе компании.

В таких условиях перед любым системным администратором в корпоративной среде периодически возникает проблема восстановления доступа к тому или иному клиентскому компьютеру, возникшая по причине потери пароля к операционной системе.

Такая проблема часто, увы, решается администратором «в лоб», без использования специальных программных средств сброса и восстановления паролей. О том, как правильнее и эффективнее решать такие задачи и пойдет речь в данной статье.

ОТ УТЕРИ ПАРОЛЯ НЕ ЗАСТРАХОВАН НИКТО

Установка пароля на вход в систему – самый распространенный и, как нам обычно кажется, надежный способ защиты информации от посторонних. Но как это часто бывает, у медали есть и оборотная сторона.

Мы стараемся установить пароль «посложнее», чтобы его было не так просто подобрать и получить несанкционированный доступ к системе, но сами же потом его забываем, попадаем в затруднительное положение, в собственноручно расставленную ловушку. После чего доступ к системе может быть полностью утрачен.

Жизнь полна непредсказуемости поворотов: пользователь системы, например, может:

- забыть пароль (переусердствовал с его сложностью и не смог вспомнить, после возвращения из командировки или отпуска);
- ошибиться при смене пароля (ошибся символом, ввел пароль не в той раскладке, выбрал изначально слишком сложный вариант);
- пойти на саботаж, сделать вид, что «потерял» пароль (например, перед увольнением в случае конфликта с руководством компании или сослуживцами);
- уволиться/исчезнуть, не оставив реквизитов доступа к системе (из-за халатности или намеренно из мести работодателю).

В случае, если в системе больше не существует других аккаунтов из соображений безопасности, а именно так обычно и происходит, доступ к ней оказывается полностью заблокирован.

Потеря системного пароля особенно неприятна тем, что доступ блокируется не к какому-то одному или нескольким файлам, программам или сервисам, а к целому рабочему месту со всеми вытекающими последствиями.

ЧЕМ ГРОЗИТ ПОТЕРЯ СИСТЕМНОГО ПАРОЛЯ?

ВОЗМОЖНЫЕ ИЗДЕРЖКИ

Исследование компании Datamonitor[1] показало, что внутренние издержки на одно обращение в корпоративную службу поддержки по вопросам, связанным с паролями, составляет от $10 до $40 (в зависимости от размеров компании). В среднем - это $25 или 57 минут рабочего времени квалифицированного IT-специалиста ежедневно. В расчете на год средние издержки превышают $150 тысяч для крупных организаций с числом сотрудников более двух тысяч.

Но это только расходы, связанные с рабочим временем наемных IT-специалистов, без учета издержек вследствие нарушения других бизнес-процессов, возможного срыва контрактов и репутационных потерь.

Проблема не столь критична, если забыт системный пароль на «пустую» рабочую станцию рядового менеджера компании. В этом случае все может обойтись потерянным временем системных администраторов на восстановление системы с чистого листа и недополучением части дохода из-за простоя работника.

Но как быть, если речь идет о потере доступа к серверу с клиентской базой данных, бухгалтерской отчетностью предприятия или ноутбуку генерального директора? Такая ситуация может создать массу внутренних проблем, блокировать работу предприятия и грозить существенными материальными и моральными издержками. Точно оценить суммарные потери для бизнеса в таких случаях невозможно, поэтому выход один – нужно постараться минимизировать подобные риски.

ПОЧЕМУ ПРОСТО НЕ ВОСПОЛЬЗОВАТЬСЯ СБРОСОМ ПАРОЛЯ?

В случае работы компьютера в домене, его персональный пароль может быть сброшен администратором сети. В этом случае проблема решится быстро, и восстанавливать пароль уже не придется. Такой простой способ – это первое, что приходит в голову при исследовании нашей темы, но этот шаг может повлечь за собой серьезные последствия.

Например, как быть в случаях, если на компьютере использовалось шифрование EFS (Encrypted File System) или другие сервисы, напрямую привязанные к учетной записи, пароль к которой утрачен?

Проблема в том, что сами файлы на диске, защищенные EFS, шифруются с помощью ключа FEK (File Encryption Key), который хранится в атрибутах файла. FEK зашифрован master-ключом, а мастер-ключ в свою очередь – ключами пользователей (имеющих доступ к файлу). Ключи пользователей, соответственно, зашифрованы хэшами паролей этих самых пользователей. Поэтому в случае сброса пароля пользователя в домене доступ к зашифрованным EFS данным будет утрачен.

[1] «The ROI case for smart cards in the enterprise», Datamonitor, November 2004

В ситуации, когда компьютер находился не в домене, пароль локального администратора не может быть сброшен.

Не стоит решать проблему потери пароля в лоб, то есть переустановкой операционной системы. Это может привести к потерям важной информации и лишним внутренним издержкам.

При потере системного пароля гораздо разумнее попробовать восстановить утерянный пароль при помощи специального программного обеспечения, речь о котором пойдет ниже.

КАК ВОССТАНОВИТЬ ДОСТУП В СИСТЕМУ?

ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧИ

Чтобы запустить программу для восстановления системного пароля, нужно каким-то образом получить полный доступ к жесткому диску «проблемного» компьютера.

Сделать это можно следующими способами:

1. Загрузка под другой рабочей учетной записью пользователя с привилегиями Администратора (если она существует).
2. Физическое отсоединение жесткого диска и установка его на другой рабочей машине со специальной программой для расшифровки.
3. Загрузка другой операционной системы, установленной на том же компьютере, если она есть.
4. Загрузка операционной системы со специального загрузочного CD-диска.

Вариант с загрузочным CD является наиболее удобным, так как позволяет быстро произвести гарантированную загрузку компьютера с правами администратора и полным доступом к жесткому диску.

ИСПОЛЬЗОВАНИЕ ЗАГРУЗОЧНОГО ДИСКА НА ОСНОВЕ WINPE

Среди загрузочных дисков предпочтительнее использовать решения на основе Microsoft Windows Preinstallation Environment (WinPE). Это инструмент, обладающий минимальной функциональностью стандартной операционной системы класса Windows XP, который замещает DOS и позволяет осуществлять предустановку системы в автоматическом режиме.

С помощью WinPE создается загрузочный CD, настроенный под конкретную задачу, используя который администратор получает возможность автоматизировать процесс развертывания программного обеспечения или восстановления системы после сбоя, когда ее загрузка в штатном режиме становится невозможна. Это как раз наш случай!

С его помощью становится возможным быстро создать диск восстановления, после чего гарантированно загрузить проблемный компьютер, получить доступ к содержимому жесткого диска и запустить специальный софт для восстановления пароля (прямо с этого же CD).

Лучше всего использовать уже готовый диск восстановления с WinPE, в этом случае администратору нет необходимости создавать его самому и разбираться в премудростях WinPE.

Если на компьютере нет CD-привода (например, в ноутбуке), то можно использовать специально подготовленную загрузочную USB-флешку.

БЕСПЛАТНЫЕ РЕШЕНИЯ НА ОСНОВЕ LINUX/UNIX

Альтернативой WinPE могут служить бесплатные «open source» решения на основе Linux/UNIX, но их едва ли можно назвать удобными и надежными инструментами. Формат свободно распространяемого продукта не гарантирует какого-либо приемлемого качества, выпуска обновлений или технической поддержки, а внятная документация нередко вообще отсутствует.

Кроме того, существующие Linux-решения (например, Offline NT Password & Registry Editor, Bootdisk / CD (http://home.eunet.no/pnordahl/ntpasswd/bootdisk.html), в отличие от созданных на основе WinPE, не имеют нормального графического интерфейса. Их использование требует от пользователя специальных знаний. Например, необходимо знать, где расположены файлы с хэшами паролей, и совершать довольно большое количество «ручных» операций с командной строкой.

Совместимость Linux-решений также оставляет желать лучшего. В частности, для SATA/RAID/SCSI-дисков пользователям придется самостоятельно искать драйверы под Linux в Интернете, после чего подгружать их также вручную.

Опытный пользователь, возможно, со всем этим справится, но большинство, увы, нет. Мало того, под Linux могут возникнуть проблемы не только с жестким диском, но даже с USB-клавиатурой.

Таким образом, для решения задач по восстановлению доступа к системе Windows больше подходят платные решения на основе WinPE, которые имеют более высокое качество, знакомый интерфейс Windows, не требует длительной «доводки» перед использованием. Кроме этого, в случае WinPE гарантируется техническая поддержка продукта со стороны производителя.

ELCOMSOFT SYSTEM RECOVERY – ПРОСТОЙ СПОСОБ ВОССТАНОВИТЬ ДОСТУП К СИСТЕМЕ

ОСНОВНЫЕ ВОЗМОЖНОСТИ И ПРИНЦИП РАБОТЫ

Среди специальных программных средств для восстановления системых паролей Windows можно выделить продукт ElcomSoft System Recovery (ESR), позволяющий в предельно сжатые сроки получить доступ к компьютеру под управлением Windows с нужными вам правами.

При этом системному администратору не придется тратить много времени на восстановление работоспособности системы и доступа к данным. Достаточно загрузиться с CD под управлением WinPE, запустить ElcomSoft System Recovery и можно заниматься другими делами.

По желанию с помощью специальной утилиты, которая есть на загрузочном диске, можно создать загрузочную USB-флешку. Это может быть очень полезно в тех случаях, когда у «проблемного» компьютера нет CD-привода (например, в ноутбуке).

Также загрузочная USB-флешка может быть очень удобна, если надо не сбросить пароли, а с помощью ESR переписать файлы с хэшами паролей для дальнейшего восстановления на другом компьютере.

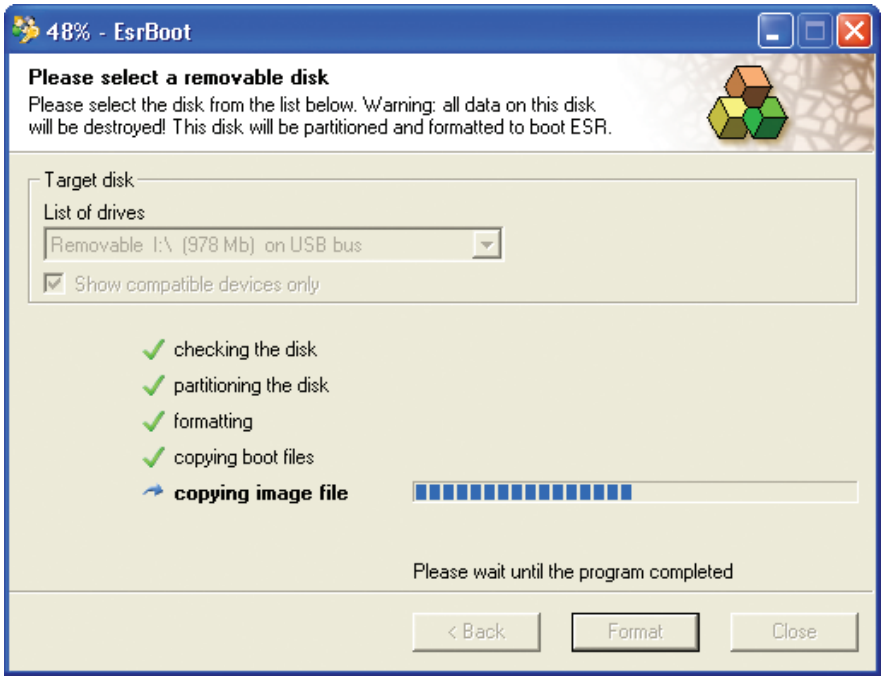


Рис.1. Создание загрузочной USB-флешки.

ESR сначала пытается восстановить пароли с помощью predefined атак (по словарю и прямым перебором). Кроме того, некоторые пароли вытаскиваются из кэша, системных служб, autologon (если он сконфигурирован) и т.д. Пробуются различные комбинации (атака по словарю), например, когда пароль эквивалентен имени пользователя в сочетании с одной-двумя цифрами в конце.

Все это позволяет достаточно эффективно восстановить утерянный пароль. По времени вся процедура занимает не больше нескольких минут. Таким образом, во многих случаях сбрасывать пароль нет необходимости, что гарантирует сохранность всех данных на компьютере.

ОСОБЕННОСТИ ELCOMSOFT SYSTEM RECOVERY

Среди особенностей ElcomSoft System Recovery можно выделить следующее:

- В комплекте ESR поставляется готовый загрузочный диск (CD или USB flash drive), который подходит к любому компьютеру с установленной операционной системой Windows.
- ESR базируется на системе Windows PE (Preinstallation Environment), лицензированной у Microsoft.
- ESR совместима с Windows NT 4.0, Windows 2000, Windows XP и Windows Server 2003.
- ESR поддерживает все американские и неамериканские версии Windows, а также имена пользователей и пароли на разных языках.
- ESR поддерживает все RAID-массивы и SCSI-накопители (используя Windows-драйверы).
- ESR автоматически определяет все операционные системы, установленные на компьютере – достаточно просто выбрать нужную из списка.
- Существует возможность повышения привилегий другого пользователя системы, пароль которого известен, до статуса администратора. При этом можно уже не сбрасывать/восстанавливать потерянный пароль.
- ESR извлекает хэши паролей из файлов SAM/SYSTEM или базы данных Active Directory как администратора домена, так и доменных пользователей. Такой возможности **нет ни у кого из конкурентов**. Собранные хэши записываются в текстовый файл для дальнейшего анализа и восстановления при помощи более продвинутых атак типа rainbow, и в течение более значительного времени, например, используя другой продукт ElcomSoft Proactive Password Auditor.

С помощью ESR вы легко сможете:

- Получить список всех локальных учетных записей и их свойств; узнать, у каких из них есть права администратора.
- Просмотреть привилегии учётных записей (за исключением установленных через локальные или групповые политики безопасности).
- Обнаружить записи с пустыми паролями.
- Предоставить права администратора любой учетной записи.
- Разблокировать заблокированные учетные записи.
- Мгновенно восстановить пароли для специальных / системных учетных записей (таких как IUSR_, HelpAssistant и др.)
- Сбросить и изменить пароли для любых локальных учетных записей.

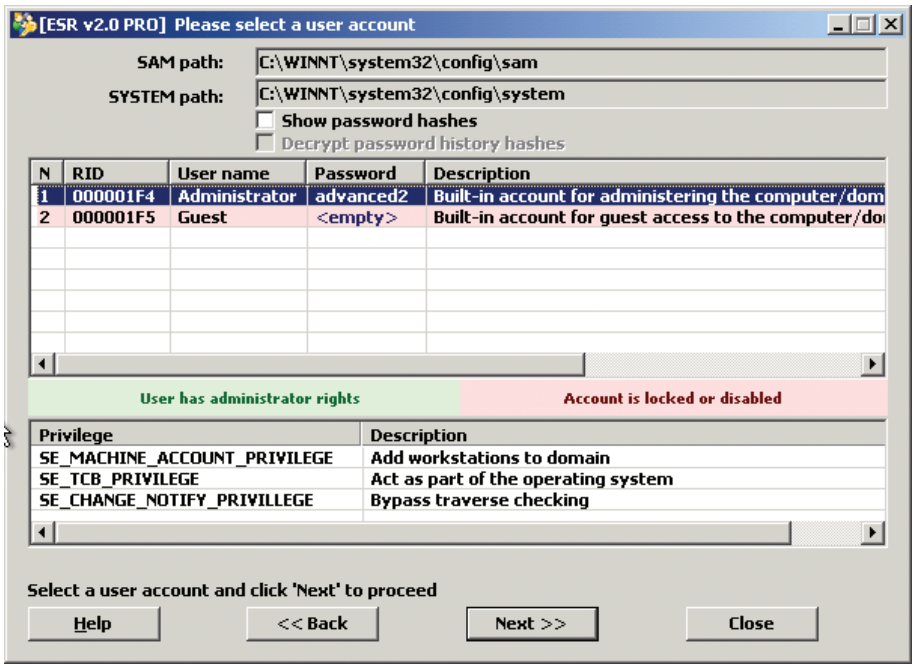


Рис.2. Выбор аккаунта из списка для восстановления пароля.

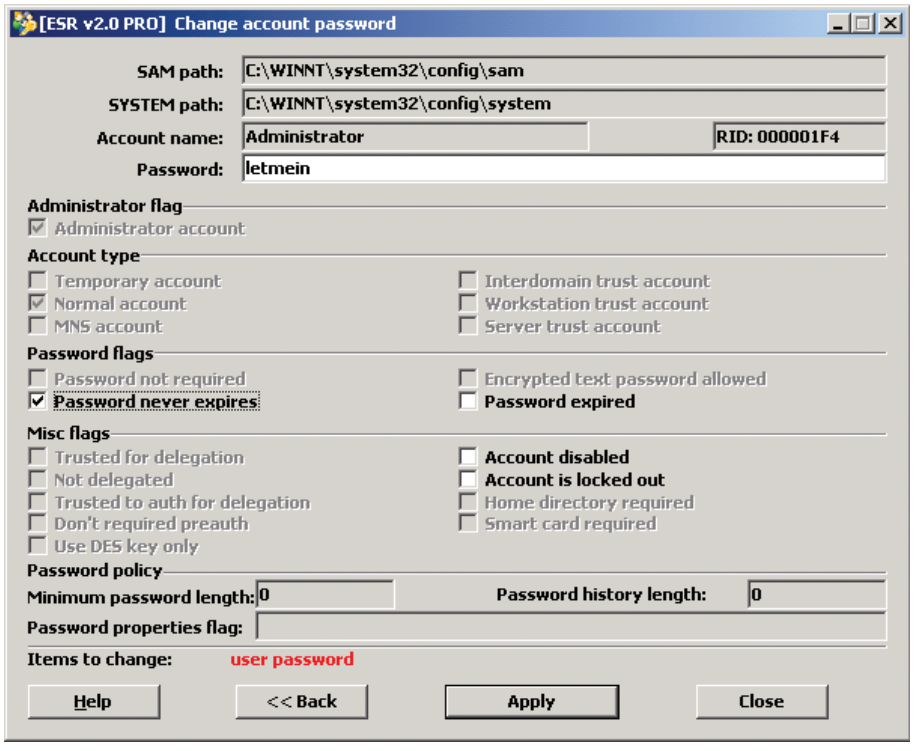


Рис.3. Сброс пароля пользователя.

ESR продается в трех различных версиях: Basic, Standard и Professional, отличия которых представлены в таблице ниже:

	ESR Basic	ESR Std	ESR Pro
Windows versions support			
Supports Windows Vista	●	●	●
Supports Windows NT/2000/XP workstations	●	●	●
Supports Windows NT/2000/XP servers	●	●	●
Supports non-US Windows versions	●	●	●
General features			
Multilingual user interface	●	●	●
Based on Windows PE	●	●	●
Supports all RAID/SCSI/SATA devices	●	●	●
Automatic mode (list of installed systems)	●	●	●
Manual mode (browse for Registry files)	●	●	●
Password reset CD	●	●	●
Creates a password reset USB flash drive	●	●	●
Reset local Administrator password	●	●	●
Enable/unlock Administrator account	●	●	●
Advanced features			
Reset password to other user accounts	●	●	●
Highlight accounts with Administrator rights	●	●	●
Look up account privileges	●	●	●
Enable/unlock disabled/locked accounts	●	●	●
Give Administrator privileges to any user account	●	●	●
Recover passwords for some system accounts	●	●	●
Reset Domain Administrator password	●	●	●
Reset AD users password	●	●	●
Dump password hashes for local accounts	●	●	●
Dump password hashes for AD accounts	●	●	●
Show LM/NTLM hashes	●	●	●

Advanced features			
Show password history hashes	●	●	●
Test short and simple passwords	●	●	●
SAM database editor	●	●	●
License, maintenance, delivery, price			
Licensed for business use	●	●	●
One year of free updates	●	●	●
Delivery	Download (ISO)	Express mail	Express mail
Price	US $49	US $199	US $599

Версия Basic распространяется через Интернет без готового загрузочного CD, который можно создать из архива при помощи образа диска ISO-9660. Версии Standard и Professional поставляются уже с готовым загрузочным CD и позволяют создавать загрузочный USB-флешки.

Подробности о программе ElcomSoft System Recovery можно прочитать здесь.

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