



В КОРПОРАТИВНОЙ СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СОДЕРЖАНИЕ

Введение	3
Потерять информацию проще, чем кажется	4
Чем грозит потеря доступа к информации?	5
Угрозы деятельности предприятий Упущенные возможности для служб безопасности и судебных органов	
Как подстраховаться на этот случай?	6
Стоит ли покупать специальное ПО? Почему ПО, а не услуги специализированного сервиса? Некоторые типичные ситуации и их решение	
Зачем нужны продукты «ЭлкомСофт»?	9
Краткое описание продуктов «ЭлкомСофт» категории Password Recovery Краткое описание продуктов «ЭлкомСофт» для восстановления доступа	
О компании «ЭлкомСофт»	13

ВВЕДЕНИЕ

С бурным развитием информационно-вычислительных систем, которое мы наблюдаем в последние годы, доступность информации и простота работы с ней достигли небывалых высот. Информационная инфраструктура любого современного предприятия представляет собой сложный механизм, требующий постоянной поддержки.

Доступность информации, наряду с ее неоспоримой пользой, приносит с собой и негативные последствия. Информационные потоки стало гораздо сложнее контролировать. Информация и ее правообладатель стали более уязвимы и подвержены множеству различных факторов риска.

Наступившая информационная эра требует от нас принципиально другого отношения к информации и гораздо более серьезной ее защиты. Речь идет не только о таких вещах как внутренние утечки информации, ее кража, порча, но и элементарной потере доступа.

ПОТЕРЯТЬ ИНФОРМАЦИЮ ПРОЩЕ, ЧЕМ КАЖЕТСЯ

Еще не так давно, когда информация хранилась и распространялась преимущественно на бумажных носителях, ей угрожали разве что стихийные бедствия и время. В эру компьютерных технологий информация может быть утрачена куда проще. Ее можно легко потерять по следующим причинам:

1. Выход из строя деталей компьютера (утрата по вине hardware).
2. Сбой используемого программного обеспечения (утрата по вине software).
3. Кража или умышленная порча со стороны злоумышленников или нечистых на руку сотрудников компании.
4. Неквалифицированные действия персонала компании.
5. И, наконец, потеря контроля или утрата прав доступа.

Каждый из этих пунктов тянет на отдельный документ и сам по себе интересен для исследования, но сейчас мы остановимся только на последнем - потеря контроля над информацией или утрата прав доступа.

Эксперты и IT-специалисты уделяют данному классу рисков меньше внимания, чем он реально заслуживает, хотя на самом деле потеря контроля над информацией ничуть не менее опасна, чем ее порча или кража.

Мы всегда ограничиваем доступ к наиболее важной информации, производя ее шифрование или устанавливая парольную защиту на документы и компьютеры.

Таким образом, контроль над информацией может быть элементарно потерян вследствие:

1. Потери пароля к защищенным документам (Microsoft Office, почтовые базы, файлы Adobe Acrobat, архивы и т.д.).
2. Потери прав доступа к программам (например, потеря прав доступа к операционной системе Microsoft Windows).
3. Потери прав доступа к зашифрованным данным (например, зашифрованных при помощи Encrypting File System).

Понятно, что риски потери доступа к информации существуют всегда и их никогда не удастся полностью исключить. Любая внутрикорпоративная служба поддержки пользователей регулярно сталкивается с проблемами потери паролей, на решение которых уходит большое количество ресурсов.

В то же время мало кто из IT-специалистов задумывается над тем, что эти риски можно успешно контролировать, описав и отладив у себя в компании последовательность действий в случае возникновения инцидента, связанного с потерей контроля над информацией.

ЧЕМ ГРОЗИТ ПОТЕРЯ ДОСТУПА К ИНФОРМАЦИИ?

Давайте разберемся, в чем же состоят риски потери доступа/контроля над важной для нас информацией, ведь именно ее, как правило, мы защищаем паролями и подвергаем шифрованию.

УГРОЗЫ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ

По данным исследовательской компании Gartner¹ до 30% звонков в корпоративную службу поддержки пользователей связаны с потерями паролей и необходимостью их восстановления. При этом Gartner оценивает по издержкам среднюю стоимость каждого обращения в 25\$.

Исследование компании Datamonitor² 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.

Для предприятия отсутствие доступа к информации грозит:

- полной потерей ценной информации, которую мы защитили паролем или зашифровали;
- отсутствием доступа к важным сведениям (особенно актуально для внутрикорпоративных служб безопасности);
- необходимостью собирать информацию и создавать документы заново;
- потерей ресурсов внутренних IT-служб предприятия, потраченных на бессистемное решение проблемы;
- упущенные возможности, связанные с простоем отдельных сотрудников или повторным выполнением уже сделанной ранее работы.

Как видим, возможные последствия могут создать массу дополнительных издержек, внутренних проблем и даже блокировать работу предприятия, что грозит существенными материальными и моральными издержками.

Защищенную потерянным паролем информацию придется восстанавливать заново, на что потребуется дополнительное рабочее время сотрудников. В ряде случаев это и вовсе может быть невозможно, если речь идет, например, о зашифрованном на диске архиве с документами. Все это может повлечь за собой упущенные бизнес-возможности для предприятия.

УПУЩЕННЫЕ ВОЗМОЖНОСТИ ДЛЯ СЛУЖБ БЕЗОПАСНОСТИ И СУДЕБНЫХ ОРГАНОВ

Отдельно стоит остановиться на работе служб безопасности и судебных органов. Нередко в их практике для сбора доказательств в ходе расследования возникает потребность доступа к информации, которая ранее была умышленно закрыта паролем или зашифрована для хранения или передачи третьим лицам.

¹ «Industry Identity Management with Metrics» report», Gartner, February 2004

² «The ROI case for smart cards in the enterprise», Datamonitor, November 2004

Для служб безопасности открытие доступа к этой информации могло бы оказать серьезную помощь в обнаружении следов преступной, инсайдерской или подрывной деятельности на предприятии, а для судебных органов (forensics) собрать дополнительную доказательную базу.

КАК ПОДСТРАХОВАТЬСЯ НА ЭТОТ СЛУЧАЙ?

В большинстве случаев восстановить пароли и доступ к информации, будь то закрытые паролем файлы, операционная система или зашифрованные данные можно. Для этого существует множество методов и специализированные программные средства.

На предприятиях, серьезно относящихся к информационной безопасности, такие программные продукты должны быть всегда под рукой и ими нужно уметь квалифицированно пользоваться.

СТОИТ ЛИ ПОКУПАТЬ СПЕЦИАЛЬНОЕ ПО?

Зачем покупать специальное ПО, если проблема возникает редко? Может быть, покупать такие программы стоит только в том случае, если инцидент уже произошел? Такие вопросы обычно задают IT-специалисты, не вполне понимающие риски и их возможные последствия от потери доступа к информации.

Это распространенная ошибка! Программы по восстановлению паролей и доступа к данным всегда должны быть под рукой, особенно в IT-службах крупных компаний. В противном случае, может быть потеряно драгоценное время на поиск, выбор, покупку, установку и обучение работе с программами, каждая из которых имеет свою специфику. Кроме того, в спешке трудно сделать осознанный выбор действительно эффективного решения, которое поможет решить проблему.

Может так получиться, что купленная второпях программа на деле не оправдывает ожиданий по эффективности или скорости работы, или вовсе окажется «пустышкой», неспособной решать поставленные задачи. Проверять это в критический момент, пожалуй, – преступление перед бизнесом.

Например, специальные службы во всем мире ежедневно сталкиваются проблемами восстановления доступа к данным, представляющим оперативный интерес. Имея под рукой комплекс специальных программ (для восстановления и сброса паролей, восстановления доступа к системе или зашифрованным файлам на диске), им удается эффективно решать поставленные перед ними задачи.

С подобными задачами, только применительно к расследованию внутренних инцидентов, может в любой момент столкнуться любая служба безопасности крупной компании. В IT-отделах предприятий использование специального софта для сброса/восстановления потерянных паролей и доступа к данным может кардинальным образом нивелировать последствия от потери доступа к данным и снизить издержки на их устранение (см. «Потерять информацию проще, чем кажется»).

ПОЧЕМУ ПО, А НЕ УСЛУГИ СПЕЦИАЛИЗИРОВАННОГО СЕРВИСА?

В настоящее время существует громадное количество онлайн-сервисов по восстановлению паролей, которые работают по факту обращения к ним. Принцип их работы прост – клиент посылает файл, компания через какое-то время расшифровывает его или говорит пароль. Из-за того, что файлы с большой вероятностью содержат конфиденциальную информацию, владелец сервиса подписывает соглашение о неразглашении (Non-Disclosure Agreement).

На первый взгляд, все очень просто и удобно. Не нужно покупать программные продукты, не нужно обучать персонал. Кроме того, имеет место выигрыш в скорости, так как владелец сервиса может иметь большие ресурсы, позволяющие подобрать пароль быстрее, чем это возможно сделать своими силами внутри компании.

Однако несмотря на очевидные плюсы, такие услуги имеют следующие существенные недостатки:

- **Нет гарантии конфиденциальности.** Несмотря на подписанное соглашение о неразглашении, всё равно нет 100% гарантии, что полученные в результате подбора пароля конфиденциальные данные, например, не попадут к конкурентам.
- **Высокая цена.** Если пароли забываются или теряются относительно регулярно (в большой компании именно так и происходит), то плата каждый раз по факту обращения становится невыгодной, а имея в офисе недорогой софт, можно решать проблему самостоятельно.
- **Низкая оперативность.** Цикл работы с сервисом (даже если он работает круглосуточно и без выходных) может занять очень приличное время. Сначала нужно получить разрешение на отправку «проблемных» файлов в отделе безопасности и у руководства. Затем необходимо подписать соглашение о неразглашении и отослать файл по сети (при условии, что это позволяют сделать внутренние нормативные документы). Если задача очень критичная, то из-за отсутствия доступа к документу или системе каждая минута простоя может стоить в итоге приличных денег.
- **Узкое применение.** Онлайн-сервисы позволяют подобрать только пароль к файлам, среди которых могут быть документы Microsoft Office, Adobe Acrobat и архивы, но в случае необходимости восстановления доступа к операционной системе или зашифрованным данным на жестком диске про эти сервисы придется забыть.

Таким образом, по большинству параметров для корпоративного использования софтверные решения подходят лучше.

НЕКОТОРЫЕ ТИПИЧНЫЕ СИТУАЦИИ И ИХ РЕШЕНИЕ

Типовая ситуация №1

Потерян/забыт пароль для входа в Microsoft Windows XP на ноутбуке генерального директора. Альтернативных учетных записей по соображениям безопасности на компьютере не существуют. Требуется **срочно** восстановить доступ к компьютеру и важным документам, хранящимся на нем в единственном экземпляре.

Для разрешения ситуации наиболее удобно воспользоваться программой [ElcomSoft System Recovery](#), позволяющей быстро восстановить доступ в Windows с нужными привилегиями или сбросить потерянный пароль для входа в систему, используя только внутренние ресурсы компании.

Типовая ситуация №2

Потерян пароль к важному документу Microsoft Office 2003 (Microsoft Word или Microsoft Excel), в котором находится тендерная документация. Восстановление информации в **разумные сроки** невозможно, а ее отсутствие поставит под удар выгодную сделку и репутацию компании на рынке.

Для выхода из сложившейся ситуации лучше всего воспользоваться программой [ElcomSoft Advanced Office Password Recovery](#), позволяющей восстанавливать пароли к документам Microsoft Office всех версий, существующих на данный момент.

Типовая ситуация №3

Отсутствует доступ к важным сведениям со стороны **службы безопасности** предприятия. Искомые файлы зашифрованы при помощи Encrypted File System под операционной системой Microsoft Windows 2000. Кроме этого, на компьютере установлена парольная защита на вход в почтовую программу Outlook, доступ к которой также необходимо получить. В качестве решения задачи наиболее удобно воспользоваться набором из двух специальных программ.

Первая из них – [ElcomSoft Advanced EFS Data Recovery](#), предназначена специально для восстановления (расшифровки) файлов, расположенных на партициях NTFS и зашифрованных при помощи Encrypted File System (EFS) под операционными системами Windows 2000 и Windows XP, Windows 2003 Server и **Windows Vista**.

Вторая – [ElcomSoft Advanced Outlook Password Recovery](#), которая восстанавливает забытые пароли к файлам с персональной информацией Microsoft Outlook (расширение PST). Также программа восстанавливает пароли к E-Mail аккаунтам, созданным в Microsoft Outlook и сохраненным на локальной машине. Все пароли восстанавливаются мгновенно, прямым декодированием.

ЗАЧЕМ НУЖНЫ ПРОДУКТЫ ELCOMSOFT?

Компания ElcomSoft предлагает полный набор программных продуктов для восстановления паролей и данных в различных приложениях.

Продукты ElcomSoft признаны экспертами во всем мире и являются действительно эффективными и надежными решениями в своем классе.

Используя весь комплекс программ ElcomSoft можно с высокой степенью вероятности восстановить даже те пароли, которые считаются очень стойкими, например, PGP.

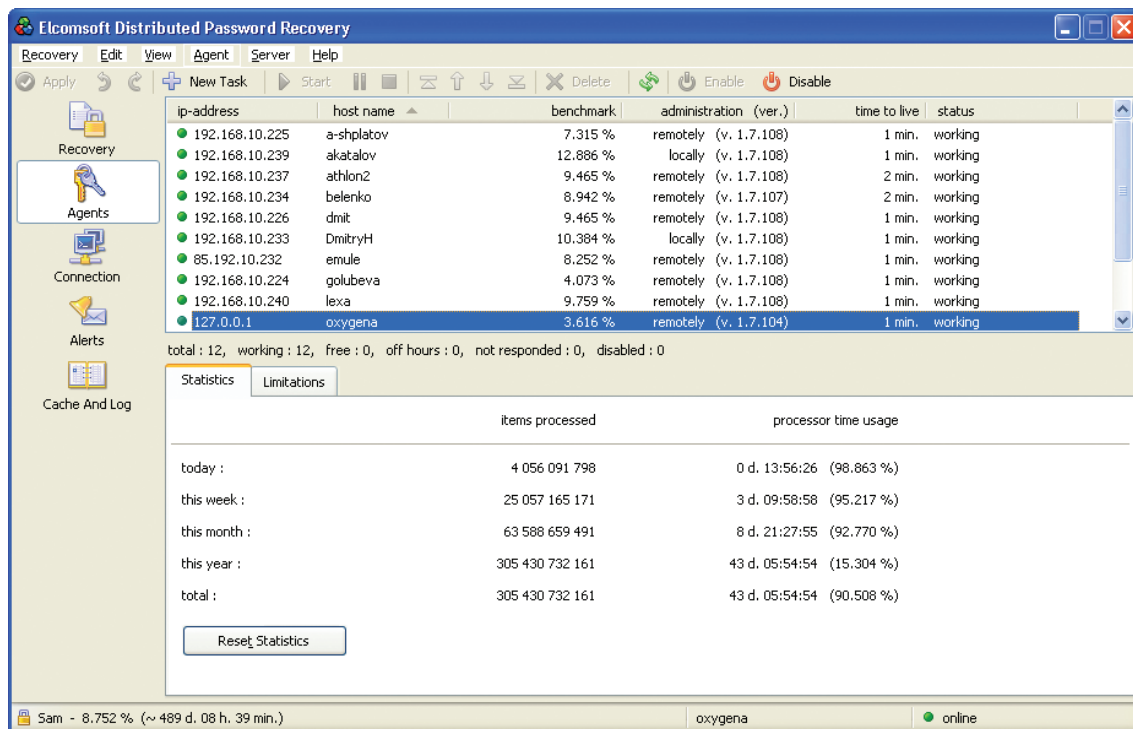
Обычным перебором решить такую задачу нельзя, однако, очень велика вероятность того, искомый пароль мог использоваться и в другой программе, например, ICQ или WordPerfect. Откуда он может быть восстановлен очень быстро.

Такой комплексный подход особенно актуален в случае полной утери контроля над данными, например, в случае умышленного сокрытия информации, что часто встречается в практике органов безопасности.

Линейку программных средств от ElcomSoft можно условно разбить на две части: для восстановления паролей к содержимому файлов и для восстановления доступа к системе или данным.

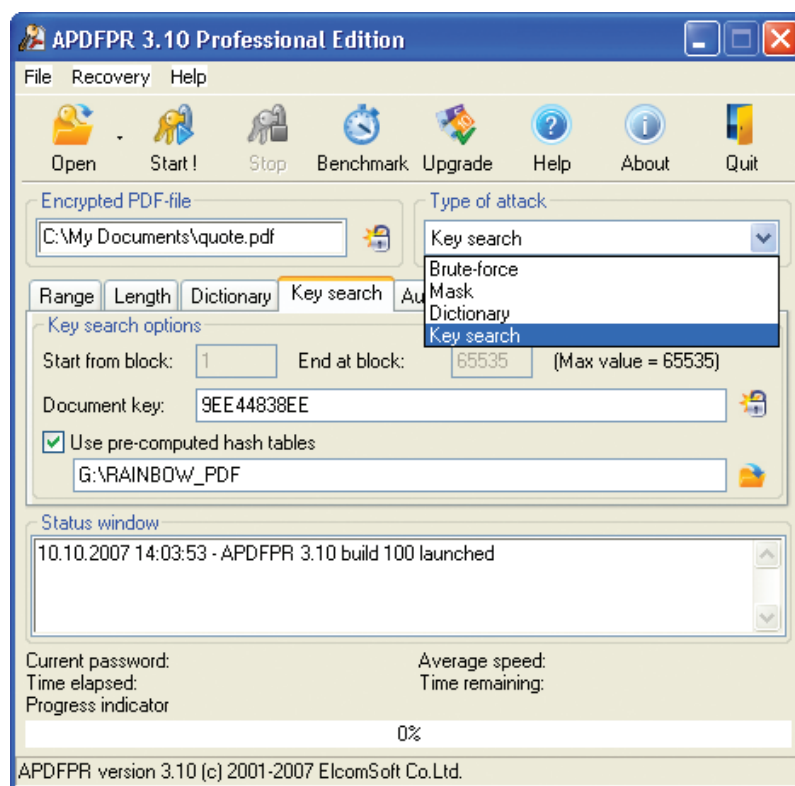
КРАТКОЕ ОПИСАНИЕ ПРОДУКТОВ ELCOMSOFT КАТЕГОРИИ PASSWORD RECOVERY

- 1. Elcomsoft ElcomSoft Distributed Password Recovery** – флагманский продукт компании. Программа предназначена для распределенного нахождения забытых паролей к различным типам документов. Поддерживаются форматы Microsoft Office (Word, Excel, PowerPoint), Microsoft Money, Microsoft OneNote, PGP (*.skr, *.pgd, *.pgp, PGP whole disk encryption), сертификаты PKCS #12 (*.pfx), Adobe Acrobat PDF, пароли пользователей Windows 2000/XP/2003/Vista, Intuit Quicken, ID файлы Lotus Notes, хеши MD5. Подробнее о продукте можно узнать [здесь](#).
- 2. Elcomsoft Advanced Office Password Recovery** – программа для восстановления забытых паролей к документам Microsoft Office всех версий, существующих на данный момент (Office 95, Office 97, Office 2000, Office XP, Office 2003 Beta, Office 2003). Также программа позволяет восстанавливать пароли MS Money, MS Visio, MS Backup и пароль IE Content Advisor. Программа поставляется в трех редакциях - Home, Standard и Professional. Большинство паролей находятся мгновенно, прямым декодированием. Подробнее о продукте можно узнать [здесь](#).
- 3. Elcomsoft Advanced Office Password Breaker** – программа для расшифровки документов Word 97/2000 и Excel 97/2000, защищенных паролем на открытие документа. Программа обеспечивает **гарантированное** вскрытие документа независимо от сложности пароля и его длины. Подробнее о продукте можно узнать [здесь](#).



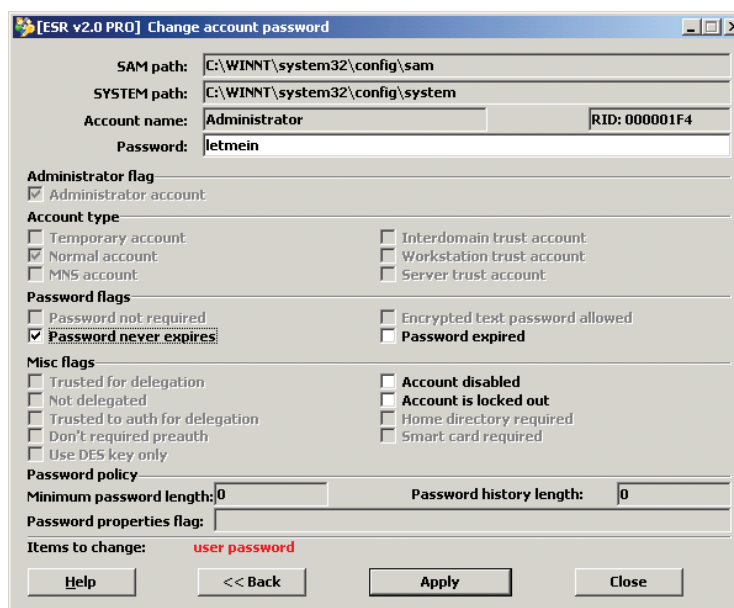
- 4. Elcomsoft Advanced Archive Password Recovery** – программа для восстановления забытых паролей к архивам ZIP (PKZIP, WinZIP), ARJ/WinARJ, RAR/WinRAR и ACE/WinACE. Программа объединяет в себе все возможности Advanced ZIP Password Recovery, Advanced ARJ Password Recovery, Advanced ACE Password Recovery и Advanced RAR Password Recovery. Кроме этих возможностей в ARCHPR возможно гарантированное восстановление содержимого WinZIP архивов, если они содержат больше пяти файлов. Подробнее о продукте можно узнать [здесь](#).
- 5. Elcomsoft Advanced PDF Password Recovery** – программа, позволяющая расшифровывать PDF-файлы, защищенные паролем, либо имеющие ограничения, предусмотренные форматом PDF. Ограничения PDF-формата снимаются мгновенно, независимо от сложности установленного owner-пароля. Для нахождения user-пароля может использоваться прямой перебор, атака по словарю, а также поиск ключа шифрования. Программа также позволяет конвертировать файлы формата Kinko's Document Format (KDF) в формат PDF со снятием всех ограничений. Подробнее о продукте можно узнать [здесь](#).
- 6. Elcomsoft Advanced Intuit Password Recovery** – программа для восстановления паролей к документам, созданным в приложениях фирмы Intuit - Quicken (*.QDT, *.QDB, *.QDF) версий от 4 до 2007 включительно, Quicken Lawyer (Portfolios, *.PFL) и QuickBooks (*.QBW, *.QBA) версий от 3 до 2007 включительно. Подробнее о продукте можно узнать [здесь](#).

Кроме того, в линейку компании ElcomSoft входят и другие продукты для восстановления и снятия паролей на документы, например, ACT!, WordPerfect или Lotus SmartSuite, интернет-мессенджерам (различные версии ICQ, AOL Instant Messenger, Yahoo! Messenger, MSN Messenger, Google Talk, Trillian, Miranda, Mail.Ru Agent и многие другие), а также E-Mail клиентам (Eudora, TheBat!, Netscape Mail, Opera Mail и многие другие) и Microsoft Internet Explorer и Outlook Express.



КРАТКОЕ ОПИСАНИЕ ПРОДУКТОВ ELCOMSOFT ДЛЯ ВОССТАНОВЛЕНИЯ ДОСТУПА

- 1. Elcomsoft System Recovery** – это решение, которое позволяет очень быстро получить доступ в Windows с нужными привилегиями. Оно представляет собой загрузочный диск на базе Windows PE (CD или USB flash drive), который подходит для работы с любым компьютером с установленной операционной системой Windows NT 4.0, Windows 2000, Windows XP и Windows Server 2003. Подробнее о продукте можно узнать [здесь](#).



- 2. Elcomsoft Advanced EFS Data Recovery** – программа для расшифровки файлов, расположенных на партициях NTFS и зашифрованных при помощи Encrypted File System (EFS) под операционными системами Windows 2000 и Windows XP, Windows 2003 Server и Windows Vista. Программа позволяет расшифровывать файлы даже в том случае, если система не грузится или повреждены некоторые записи о ключах шифрования. Даже если база пользователей системы защищена SYSKEY, программа все равно позволяет расшифровать файлы. Под Windows 2000 возможна расшифровка всех файлов, даже если неизвестны пароли администратора и пользователей! Подробнее о продукте можно узнать [здесь](#).
- 3. Elcomsoft Proactive System Password Recovery** – программа, позволяющая восстанавливать забытые пароли, установленные в ОС Microsoft Windows, например: пароль для входа в систему [Windows 95/98/Me/NT4/2000]; пароли .NET Passport; пароль на SYSKEY, пароли WiFi WEP и WPA-PSK (сохраненные в WZC); пароли, сохраненные в Windows XP (multiple credentials); пароли к Интернет-провайдерам (RAS и Dial-Up); пароли на VPN соединения; LSA Secrets; пароли на PWL-файлы и т.д. Подробнее о продукте можно узнать [здесь](#).

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:

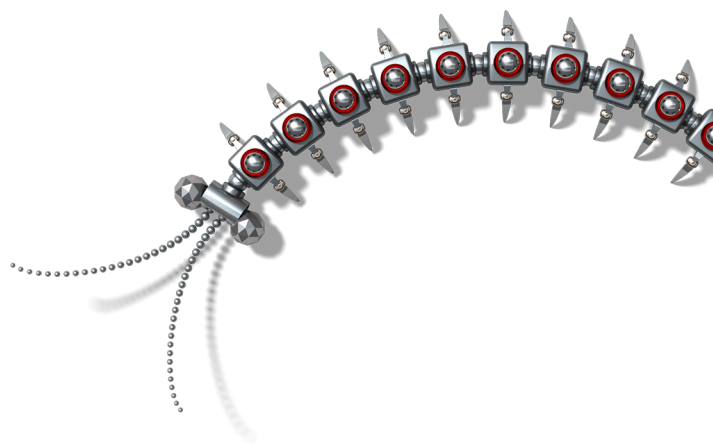
ООО «ЭлкомСофт»
Звездный б-р, 21, офис 541
129085 Москва

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>



Copyright (c) 2007 ElcomSoft Co.Ltd.
Все права защищены.

Данный документ предоставлен исключительно в информационных целях и его содержание может быть изменено без предварительного уведомления. Документ не гарантирует отсутствие ошибок и не подразумевает никаких гарантий или условий, выраженных явно или подразумеваемых законом, включая косвенные гарантии и условия окупаемости или пригодности для решения конкретной задачи. Мы отказываемся от любой ответственности, связанной с этим документом, и никакие договорные обязательства не могут быть оформлены, прямо или косвенно, на основании данного документа. Этот документ не может быть воспроизведён или передан в любой форме и любыми средствами, электронными или механическими, для любых целей, без письменного разрешения компании ElcomSoft.

Microsoft и Windows являются зарегистрированными торговыми знаками Microsoft Corporation. Intel и логотип Intel являются зарегистрированными торговыми знаками Intel Corporation. Elcomsoft и логотип Elcomsoft являются товарными знаками или зарегистрированными товарными знаками ElcomSoft Co.Ltd. Другие названия являются товарными знаками их соответствующих владельцев.