

СИМ-СИМ, ОТКРОЙСЯ!

ЛЕГКИЙ СПОСОБ ВОССТАНОВИТЬ ПАРОЛИ ДОСТУПА К ФАЙЛАМ,
ПРИЛОЖЕНИЯМ И БАЗАМ ДАННЫХ



СОДЕРЖАНИЕ

Информация – ключ к верным решениям	3
В доступе отказано...	4
Как решить головоломку?	5
Пароли: хорошие и разные	
И тебя вылечим...	
Выбираем лучшее	
«ЭлкомСофт» начинает и выигрывает	9
Документы Microsoft Office	
Почтовые клиенты и инстант-мессенджеры	
Документы Adobe Acrobat и Intuit Quicken	
Архивы	
Другие офисные приложения	
Распределенные вычисления	
О компании «ЭлкомСофт»	16

ИНФОРМАЦИЯ – КЛЮЧ К ВЕРНЫМ РЕШЕНИЯМ

Сегодня мы постоянно слышим такие слова, как «информационная эра», «информационные технологии», «кто владеет информацией, тот владеет миром» и т.д. В нашем сознании прочно поселилась мысль о том, что информация – это наше все.

Что это означает и так ли важна информация сама по себе? Это не совсем верно. Информация нужна нам для принятия решений. Вот, что действительно важно. Правильное решение – это путь к успеху в любом деле. Поэтому владение информацией является конкурентным преимуществом в современной бизнес-среде.

Неудивительно, что защите информации уделяется повышенное внимание. На рынке программных и аппаратных средств сегодня представлены многочисленные решения, ограничивающие доступ к информации и предотвращающие ее утечку: инструменты контроля доступа и аутентификации, системы предотвращения вторжений, программы резервного копирования, антивирусные приложения и другие.

Но самым простым и доступным любому пользователю инструментом по-прежнему остается парольная защита, которая позволяет предотвратить несанкционированный доступ к системам, документам и базам данных. Каждый из нас, приходя на работу, использует пароль для входа в систему, просмотра базы данных и т.п.

Известно, что в любой информационной системе самым уязвимым местом остается человек. И ситуация с парольной защитой – не исключение. Сколько раз вы сами забывали тот или иной пароль? Вот-вот... Однако при том количестве паролей, которые должен держать сегодня в голове любой компьютерный пользователь, это немудрено.

А если пароль утерян по той или иной причине, нет и доступа к информации.

В ДОСТУПЕ ОТКАЗАНО...

Данные о продажах и финансовых потоках, клиентская база данных, бухгалтерская и управленческая отчетность, аналитические отчеты и прогнозы – вся эта информация необходима как для успешного ведения операционной деятельности компании, так и для принятия стратегических решений о развитии бизнеса.

Доступ без пароля к большей части подобной информации, как правило, невозможен. Такова элементарная политика безопасности в любой компании. Однако что делать в том случае, когда доступ к информации необходим, а пароль неизвестен? А такие ситуации случаются сплошь и рядом.

Во-первых, вы сами можете забыть пароль. Признайтесь, ведь было? Как человек разумный, вы его не записали на последней обложке своего ежедневника, а предпочли запомнить, используя простую ассоциацию. Например, любимое блюдо + год вашего рождения. С годом рождения все ясно, но вот блюдо... После недавнего отпуска на Крите в голове маячит только греческий салат. Но авторизоваться в системе с ним не получается.

Бывает и так, что менеджер по продажам уволился, а пароль для просмотра отчетов о поставках вам не оставил. Связи с ним в данный момент нет, так как он решил воплотить в жизнь свою давнюю мечту и отправился в 90-дневный паломнический тур на Тибет. Контрагенты грозятся разорвать с вами все договора, если вы немедленно не расплатитесь с ними, а на основе каких данных это сделать, не вполне ясно. Знакомо?

Нередки и ситуации, когда сотрудника увольняют за участие в финансовых махинациях или работу на конкурирующую компанию. В таком случае рассчитывать на то, что человек добровольно сообщит пароль к своим документам, бессмысленно. А доступ к этой информации нужен. Причем срочно.

Итак, проблема очевидна: чтобы получить доступ к информации и решить текущие бизнес-задачи, необходимо восстановить утерянный пароль. И в большинстве случаев это сделать можно.

КАК РЕШИТЬ ГОЛОВЛОМКУ?

ПАРОЛИ: ХОРОШИЕ И РАЗНЫЕ

Поскольку проблема утраченных паролей существует с тех пор, как была изобретена парольная защита, производители ПО уже давно озаботились этим вопросом. В результате сегодня на рынке представлен ряд программных решений для восстановления паролей.

Однако отложим на некоторое время в сторону рассказ о методах, которые используются этими программами для решения проблемы утраченных паролей. Для начала давайте разберемся, какими бывают пароли в принципе и какая дополнительная информация может пригодиться нам при поиске пароля.

Итак, в общем случае в пароле могут быть использованы следующие символы: 26 строчных латинских букв (a...z), 26 прописных латинских букв (A...Z), 10 цифр (0...9), 33 спецсимвола (!@#\$%^ и т.п.), то есть всего 95 символов в любых комбинациях. В некоторых случаях из числа допустимых исключены специальные символы, что сокращает число возможных вариантов пароля. При этом не будем забывать, что пароли могут быть разной длины, что может быть критично в том случае, когда пароль невозможно восстановить или сбросить, а только лишь найти методом прямого перебора.

Кроме того, большим подспорьем в деле поиска пароля может стать знание человеческой психологии. Несмотря на многочисленные ограничения, призванные усилить стойкость парольной защиты (минимальная длина пароля, регулярная смена пароля и пр.), многие пользователи пренебрегают элементарными правилами безопасности, лишняя раз доказывая существование уже упомянутого феномена «слабого звена», которым в данной ситуации является человек.

Большая часть используемых паролей состоит из слов и символов на родном или знакомом человеку языке. Эти слова часто имеют отношение к личной жизни пользователя: год рождения, имя любимой собаки, номер телефона или банковской карты и т.д. Новый пароль может быть незначительной модификацией старого пароля. Именно таким образом большая часть пользователей решает для себя проблему регулярной смены пароля, предусмотренной политикой безопасности компании. И последнее, но важное замечание: люди очень часто держат записку с паролями прямо на рабочем столе или хранят их на своем компьютере в отдельном файле, хотя такое лекарство от забывчивости ставит крест на самой идее парольной защиты.

Таким образом, знание требований к паролю (возможные состав и длина) и наличие некоторых сведений о пользователе могут значительно упростить задачу нахождения неизвестного пароля. И технологии, применяемые специализированным ПО для восстановления паролей, предусматривают возможность использования подобной информации.

И ТЕБЯ ВЫЛЕЧИМ...

На сегодня основными методами поиска паролей программными средствами являются простой перебор, перебор по маске, атака по словарю, перебор ключей шифрования (вариантов здесь может быть меньше, чем при переборе паролей) и так называемая rainbow-атака. В некоторых случаях применяются и другие виды восстановления доступа к файлу – например, так называемая plaintext-атака (на основе известного содержимого). Давайте рассмотрим некоторые из этих методов.

Простой перебор

Суть метода прямого перебора (brute force) проста: программа перебирает все возможные комбинации символов, пытаясь подобрать подходящий пароль. Поиск можно несколько ограничить, указав количество символов в пароле, их тип (буквы, цифры, другие знаки), а также если задать символы, с которых должен начаться поиск.

Сколько же времени может потребоваться, чтобы восстановить утерянный пароль методом «грубой силы»? Это зависит от длины пароля, набора использованных в нем символов, мощности компьютера, а также типа документа, к которому пароль подбирается.

Конечно, может случиться так, что правильный пароль встретится быстро, и все возможные комбинации перебирать не придется. Но вряд ли стоит на это рассчитывать. При решении задачи на обычном компьютере счет может идти на годы! Метод прямого перебора самый трудоемкий, поэтому прибегать к нему рекомендуется лишь при отсутствии других альтернатив.

Перебор по маске

В случае, если пароль создавали вы сами, всегда есть шанс попробовать восстановить его по маске, сильно сузив область поиска. Возможно, вы помните длину пароля и некоторые символы из него. Пригодится любая информация.

Например, вы уверены, что использовали лишь цифры и строчные латинские буквы. Тогда при поиске можно исключить спецсимволы и прописные латинские буквы. Неплохо, если вы знаете, что тот или иной символ стоял на определенной позиции в пароле. Например, зная, что пароль имеет длину 10 символов, начинается с буквы «а» и заканчивается «2007», для поиска можно задать шаблон «а?????2007». Неизвестные символы обозначены в шаблоне вопросительными знаками.

Смысл использования маски очевиден: программе приходится перебирать меньшее количество возможных комбинаций, а значит, срок, за который может быть найден пароль, значительно сокращается.

К сожалению, не так часто о пароле известны какие-либо подробности, поэтому использовать маску удается редко. К счастью, существует еще один метод восстановления пароля, который дает очень и очень хорошие результаты.

Атака по словарю

Предположим, у вас есть информация о возможных словах или именах, используемых в пароле. В этом случае можно воспользоваться методом поиска по словарю.

Дело в том, что часто пользователи используют в качестве пароля обычные слова. Как правило, это слова из английского языка: open, access, password и т.д. Ведь такой пароль запомнить значительно проще, чем бессмысленные комбинации букв и цифр. На самом деле забывается такой пароль точно так же, как и любые другие, зато восстанавливается довольно легко.

Где взять такой словарь (а если быть более точным, то список слов)? Во-первых, он может входить в поставку программы. Во-вторых, его можно поискать в сети – на FTP-серверах можно найти самые разнообразные списки общеупотребимых слов и их модификаций, тематические списки (животные, футбольные команды и пр.), аббревиатур и т.д. В-третьих, словарик можно составить и самостоятельно.

Преимущества этого метода очевидны. Список слов, которые пользователи вводят в качестве пароля, весьма и весьма ограничен и редко превышает сто тысяч. А перебрать сотню тысяч вариантов для современного компьютера – сущий пустяк. Вот и получается, что метод перебора по словарю стоит попробовать раньше всех остальных. Вполне возможно, что он быстро принесет удачу.

Rainbow-атака

Как видим, самым важным параметром при восстановлении пароля является срок, за который его можно найти. Мы уже знаем, что при простом переборе выполняется проход по всем возможным вариантам пароля, а для сложных комбинаций это требует слишком много времени. Если речь идет о месяцах или годах вычислений, то целесообразность такого мероприятия стремится к нулю.

Для решения именно этой проблемы и была изобретена так называемая rainbow-атака (rainbow attack), основная идея которой состоит в использовании предвычислений при поиске пароля. Мысль о замене ресурсоемких вычислений обычным поиском по предварительно подготовленной таблице поиска (lookup table), не нова. Таблицы поиска применяются в тех случаях, когда данные гораздо проще извлекать из памяти, чем создавать.

При проведении rainbow-атаки используют результаты предварительных вычислений возможных вариантов пароля для некоторого набора символов. За время, сравнимое со взломом одного пароля методом простого перебора, получают таблицы, по которым с очень высокой вероятностью можно в тысячи раз быстрее найти любой пароль из проверенного диапазона. А построение радужных таблиц не по набору символов, а по набору словарей, позволяет восстанавливать пароли практически неограниченной длины.

Размер радужных таблиц на порядок меньше, чем обычных таблиц поиска: речь идет уже не о терабайтах, а о гигабайтах памяти. Сокращение размера таблицы достигается за счет их оптимизации. Справедливости ради стоит признать, что время восстановления пароля при этом возрастает, а вероятность несколько снижается, но результат того стоит. Например, при использовании таблицы для семи алфавитно-цифровых символов (на ее создание потребуется около недели), метод rainbow-атаки позволит восстановить практически любой пароль из семи алфавитно-цифровых символов за 20-30 секунд. А вот прямой перебор в этом случае займет уже более суток. Выгода – налицо.

Поскольку подготовка таких таблиц сильно удорожает стоимость программы, метод rainbow-атаки применяют в основном в корпоративных решениях. Также надо помнить, что вероятность восстановления пароля в результате rainbow-атаки ниже, чем при использовании обычных методов. Такова цена скорости.

ВЫБИРАЕМ ЛУЧШЕЕ

Итак, вопрос о целесообразности покупки программы для быстрого восстановления паролей не стоит. Такой инструмент должен иметь под рукой каждый системный администратор. Затраты на его приобретение с лихвой окупятся при первом же инциденте утраты пароля.

На что стоит обратить внимание при выборе решения класса password recovery?

Во-первых, какова вероятность восстановления пароля, заявляемая производителем? Собственно, это главный критерий оценки эффективности решения. Ведь именно для этого вы его и покупаете. Шансы на успех зависят от типа документа, к которому подбирается пароль и от производительности компьютера. К тому же пользователи становятся все более осторожными и выбирают все более стойкие пароли. Но все же обычно речь идет о вероятности около 80%. Это считается приемлемым показателем. Однако для некоторых видов паролей и документов производители ПО могут гарантировать и 99% вероятность.

Во-вторых, стоит обратить внимание на спектр поддерживаемых ОС и версий приложений, форматов файлов, языков и кодировок. Трудно предсказать, с документом какой версии Microsoft Word или Adobe Acrobat вам придется столкнуться при восстановлении пароля, не говоря уже о кодировке (возьмите, например, иероглифические или арабские языки). Узнайте также, как быстро добавляется поддержка новых версий приложений. Ведь если в программе будет отсутствовать поддержка, к примеру Office 2007, она может оказаться бесполезной – время не ждет.

В-третьих, поинтересуйтесь скоростью восстановления пароля. Конечно, в зависимости от мощности вашего компьютера время нахождения пароля может варьироваться, но обычно производители сообщают некоторые усредненные данные. Важно понимать, о каком сроке идет речь – минуты, дни, недели или месяцы?

И последнее – предоставляет ли программа возможность организации распределенных вычислений? Этот способ решения трудоёмких вычислительных задач предполагает использование мощностей целой группы компьютеров – как в локальной сети, так и удаленных. Применяют его и при решении задачи взлома паролей. Ведь если доступ к некоторым документам и приложениям можно восстановить за короткий срок на обычном компьютере (например, пароль к ICQ или Google Talk, сохраненный локально), то для взлома других паролей ресурсов одного компьютера будет недостаточно – о каком бы сроке ни шла речь. Например, пароли PGP настолько стойкие, что их подбор возможен только при использовании распределенных вычислений.

Таковы, пожалуй, основные критерии выбора решения для восстановления утраченных паролей.

«ЭЛКОМСОФТ» НАЧИНАЕТ И ВЫИГРЫВАЕТ

Российская компания «ЭлкомСофт» предлагает клиентам целый спектр решений для восстановления паролей практически к любым системам: от офисных приложений и инстант-мессенджеров до системных паролей Windows и архивов.

Уникальные технологии и штат специалистов с многолетним опытом работы в области криптографии позволяют компании «ЭлкомСофт» создавать высококлассные программы класса password recovery. Вероятность нахождения пароля в зависимости от его длины, сложности и технологии шифрования, используемой в приложении, составляет не менее 80%. В большинстве же случаев гарантируется 100% восстановление пароля.

Выбор продуктов способен удовлетворить потребности любых клиентов: от домашнего пользователя, которому может потребоваться найти забытый пароль ICQ, до крупных корпоративных заказчиков, в задачи которых может входить восстановление системных паролей Windows, доступ к зашифрованным документам Microsoft Office или снятие ограничений с файлов Adobe Acrobat. Объединение отдельных приложений в пакеты позволяет выбрать несколько продуктов одновременно по привлекательной цене.

Для нахождения паролей к большому количеству документов, а также длинных и сложных паролей в разумные сроки, предусмотрена возможность организации распределенных вычислений с привлечением как локальных, так и удаленных ресурсов.

Давайте посмотрим на основные продукты компании «ЭлкомСофт», чтобы составить представление о возможностях этих приложений и сложности решаемых задач.

ДОКУМЕНТЫ MICROSOFT OFFICE

Advanced Office Password Recovery

Для восстановления паролей к документам, созданным с помощью программ из пакета Microsoft Office, компания предлагает решение Advanced Office Password Recovery (рис.1).

Большинство паролей находятся мгновенно, прямым декодированием. При этом неважно, о какой версии Microsoft Office идет речь – Advanced Office Password Recovery поможет восстановить пароль к документам, созданным в любой из существующих на данный момент: Office 95, Office 97, Office 2000, Office XP, Office 2003 Beta, Office 2003, Office 2007. Кроме этого, вы сможете найти пароли Microsoft Money, Microsoft Visio, Microsoft Backup и пароль Internet Explorer Content Advisor.

Программа поставляется в трех вариантах: Home, Standard и Professional, которые отличаются набором поддерживаемых приложений. Версия Professional, предназначенная для крупных организаций, позволяет восстанавливать более 30 типов паролей в 14 различных приложениях.

Подробнее об Advanced Office Password Recovery можно прочитать на [сайте](#) «Элком-Софт». Доступна и [пробная версия](#) программы.

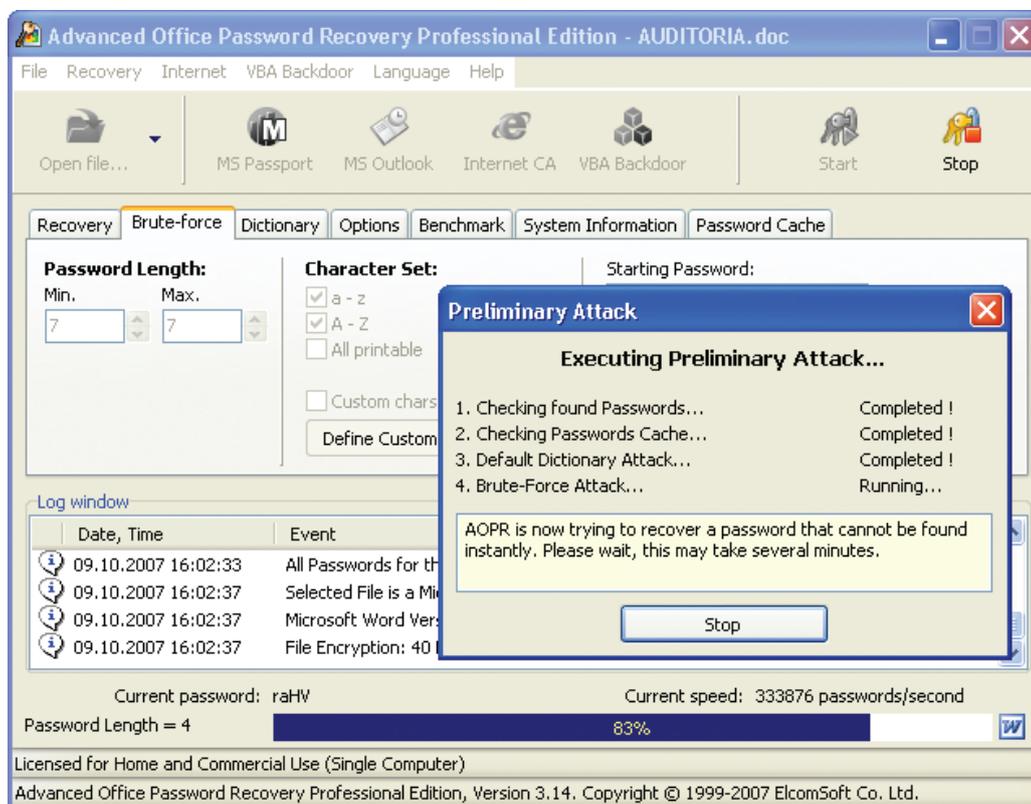


Рис.1. Предварительная атака по восстановлению пароля на открытие документа Microsoft Word 2003.

Advanced Office Password Breaker

Если речь идет о восстановлении паролей только к текстовым документам и таблицам, стоит обратить внимание на программу [Advanced Office Password Breaker](#). С ее помощью можно расшифровать документы Word 97/2000 и Excel 97/2000, защищенные паролем на открытие документа.

Благодаря тому, что в Microsoft Office 97/2003 используются 40-битные ключи шифрования, программа обеспечивает гарантированное вскрытие документа. При этом сложность пароля и его длина не имеют значения. Время нахождения ключа на среднем компьютере составит около двух недель.

Пробная версия программы [доступна](#) для скачивания.

Обратите внимание, что для расшифровки документов Microsoft Office XP, защищенных с помощью криптопровайдеров, необходимо использовать Advanced Office Password Recovery, так как для таких документов возможен только подбор пароля.

ПОЧТОВЫЕ КЛИЕНТЫ И ИНСТАНТ-МЕССЕНДЖЕРЫ

Advanced Mailbox Password Recovery

Другой распространенный случай утраты пароля – это потеря доступа к электронной почте. Легкое и быстрое решение этой проблемы – продукт [Advanced Mailbox Password Recovery](#) компании «ЭлкомСофт». Программа помогает восстановить сохраненные локально пароли к учетным записям электронной почты.

Список поддерживаемых почтовых клиентов впечатляет: Microsoft Internet Mail And News, Eudora, TheBat!, Netscape Navigator/Communicator Mail, Pegasus mail, Calypso mail, FoxMail, Phoenix Mail, IncrediMail, @nyMail, QuickMail Pro, MailThem, Opera mail, Kaufman Mail Warrior, Becky! Internet Mail. Помимо этого в программу включен эмулятор POP3/IMAP-сервера, позволяющий восстановить пароль к любому почтовому клиенту.

Пробная версия доступна для скачивания [здесь](#).

Advanced Instant Messengers Password Recovery

Одним из самых распространенных кейсов в области аутентификации является забытый пароль к инстант-мессенджеру типа ICQ. Поскольку этот способ коммуникации для большинства людей связан в первую очередь с общением личного характера, то и отношение к конфиденциальности тут более вольное. Ведь ответственность за потерю пароля нести ни перед кем, кроме себя, не придется. Но потерять «красивый» номер ICQ и историю переписки все же не слишком приятно.

Как раз для таких случаев компания «ЭлкомСофт» и предлагает продукт [Advanced Instant Messengers Password Recovery](#), позволяющий восстановить забытые логины и пароли к более чем 30 инстант-мессенджерам, включая такие популярные, как ICQ, Miranda, QIP, Google Talk, Trillian, Mail.Ru Agent.

Все пароли находятся мгновенно, прямым декодированием (для этого пароль должен быть сохранен локально). Искомый пароль может состоять не только из латинских символов – можно найти пароли и на других языках. [Пробная версия](#) программы имеет некоторые ограничения, однако составить представление о ее возможностях вы, безусловно, сможете.

ДОКУМЕНТЫ ADOBE ACROBAT И INTUIT QUICKEN

Advanced Intuit Password Recovery

Программы семейства Quicken, разработанные фирмой Intuit, предназначены для обработки и хранения информации о финансовых операциях. Эти приложения используются банками, аудиторскими и бухгалтерскими компаниями, позволяют вести налоговый учет и контролировать личные финансы. Нужно ли объяснять, насколько серьезна утрата пароля к этой информации?

Программа [Advanced Intuit Password Recovery](#) поможет восстановить пароли к документам, созданным в приложениях Intuit Quicken версий от 4 до 2008, а также Quicken Lawyer (Portfolios, *.PFL) и QuickBooks (*.QBW, *.QBA) версий от 3 до 2007 (рис.2).

Для документов, созданных в 2003 и более поздних версиях приложения, Intuit применяет усовершенствованные алгоритмы шифрования. И если альтернативные продукты используют только технологию перебора, то Advanced Intuit Password Recovery предлагает мгновенную расшифровку документов.

Пробная версия программы доступна [здесь](#).

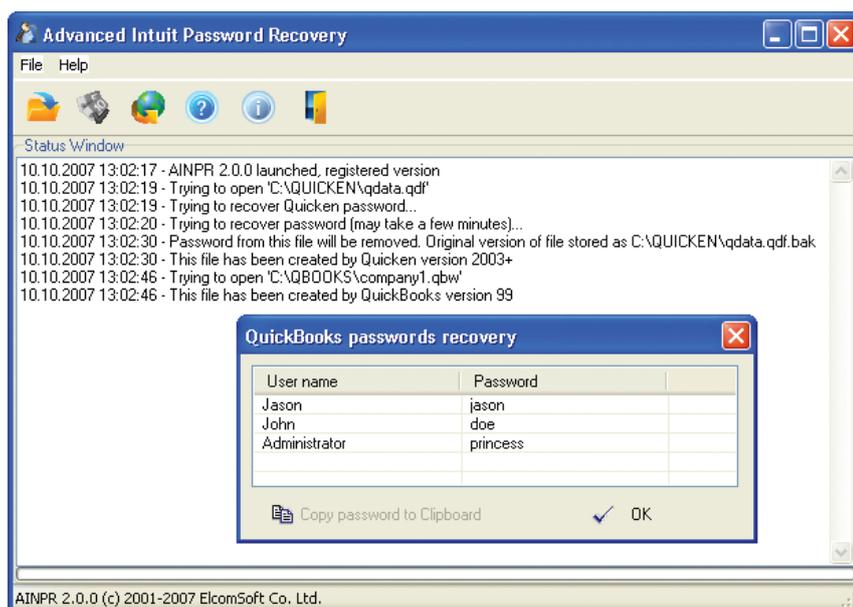


Рис.2. Результат поиска паролей пользователей QuickBooks.

Advanced PDF Password Recovery

Формат документа PDF настолько популярен, что вряд ли найдется человек, который ни разу не работал с документами Adobe Acrobat. А раз так, то вы прекрасно знаете, с какой проблемой здесь чаще всего сталкиваются пользователи: это защита на редактирование и печать. Часто пароль установлен и на открытие документа.

«ЭлкомСофт» разработал специальную программу для решения этой проблемы: Advanced PDF Password Recovery. Приложение поддерживает все версии и все алгоритмы шифрования Adobe Acrobat от 3.x до 8.x и позволяет вскрывать PDF-файлы, а также снимать ограничения, предусмотренные форматом PDF. Ограничения снимаются мгновенно, независимо от сложности установленного пароля. Для нахождения пароля на открытие файла может использоваться прямой перебор, атака по словарю, а также поиск ключа шифрования.

Программа поставляется в трех версиях: Standard, Professional, Enterprise. Базовая редакция программы, позволяет снимать с документа ограничения на редактирование и печать. Версия Professional позволяет также находить пароль на открытие файла. Enterprise-версия может подобрать ключа шифрования методом rainbow-атаки за несколько минут с помощью поставляемых на отдельном DVD-диске радужных таблиц.

Возможности программы можно оценить на примере пробной версии.

АРХИВЫ

Для восстановления паролей к архивам «ЭлкомСофт» предлагает несколько отдельных решений: Advanced ZIP Password Recovery, Advanced ARJ Password Recovery, Advanced ACE Password Recovery и Advanced RAR Password Recovery. Однако все они могут быть приобретены в рамках пакета Advanced Archive Password Recovery, что позволит находить пароли ко всем распространенным видам архивов: ZIP (PKZIP, WinZIP), ARJ/WinARJ, RAR/WinRAR и ACE/WinACE.

На сегодняшний день это самый мощный из имеющихся на рынке продуктов для восстановления паролей к архивам. В числе преимуществ программы гарантированное восстановление содержимого большинства запароленных WinZIP архивов независимо от сложности установленного пароля, самый быстрый в мире перебор паролей к ZIP, ARJ и RAR архивам (около 15 млн. паролей в секунду на современных процессорах P-IV Prescott), расшифровка WinZIP архивов со стойким шифрованием (AES). Для ZIP и ARJ архивов предусмотрена так называемая known plaintext attack, или атака по известному содержимому. Если известно содержимое хотя бы одного файла в ZIP-архиве, восстановление пароля происходит за несколько часов независимо от его сложности и длины.

Пробная версия программы доступна здесь.

ДРУГИЕ ОФИСНЫЕ ПРИЛОЖЕНИЯ

Линейка продуктов «ЭлкомСофт» включает программы для восстановления паролей и к другим офисным приложениям.

Например, [Advanced Lotus Password Recovery](#) поможет получить доступ к файлам и документам, созданным в следующих приложениях IBM Lotus: Organizer, WordPro, 1-2-3, Approach и Freelance Graphics. Поддерживаются все версии приложений IBM Lotus. Кроме этого, программа восстанавливает доступ к FTP и прокси-сайтам. Все пароли находятся мгновенно, прямым декодированием независимо от языка. Пробная 30-дневная версия продукта доступна [здесь](#).

Если вы используете для работы Corel WordPerfect Office, то стоит подумать о приобретении [Advanced WordPerfect Office Password Recovery](#). Программа восстанавливает утраченные пароли к документам Corel WordPerfect Office следующих форматов: *.wp, *.wpd, *.qpw, *.wb?, *.wq?, *.db. Поддерживаются все версии приложения. Все пароли находятся в считанные минуты, прямым декодированием независимо от языка.

Пробная 30-дневная версия продукта доступна [здесь](#).

РАСПРЕДЕЛЕННЫЕ ВЫЧИСЛЕНИЯ

О пользе распределенных вычислений при восстановлении сложных паролей мы уже говорили выше. Решение Elcomsoft Distributed Password Recovery позволяет задействовать вычислительные мощности всех компьютеров, объединенных в сеть – как локальную, так и глобальную.

С ее помощью вы сможете восстановить пароль практически к любому документу формата Microsoft Office, а также пароли Microsoft Money, Microsoft OneNote, Adobe Acrobat, Intuit Quicken, Lotus Notes, пароли пользователей Windows 2000/XP/2003/Vista, секретные ключи PGP (*.skr), PGP Disk (*.pgd) и др.

Программа состоит из трех компонентов: сервер, агент и консоль. Сервер (рис.3) устанавливается на один из компьютеров в сети и управляет процессом перебора паролей. На любые компьютеры в сети может быть установлен агент, который перебирает порции паролей, выдаваемые сервером. С любого компьютера может быть запущена консоль, которая позволяет управлять сервером перебора, добавлять новые задачи и просматривать статистику. Для сервера и агента доступны пробные версии.

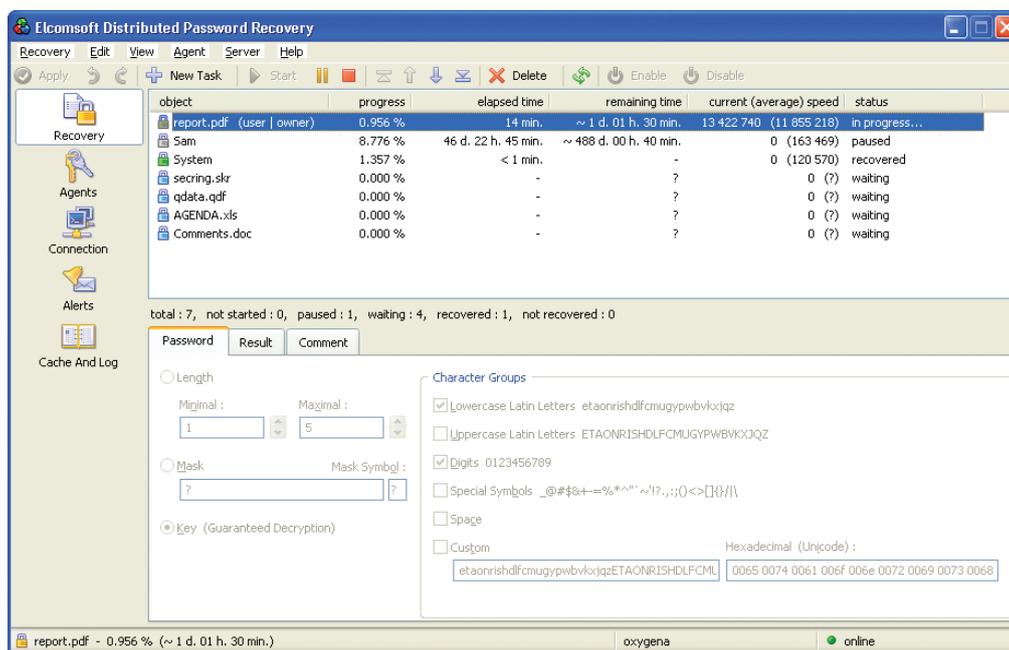


Рис.3. Главное окно Elcomsoft Distributed Password Recovery (компонент «сервер»).

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:

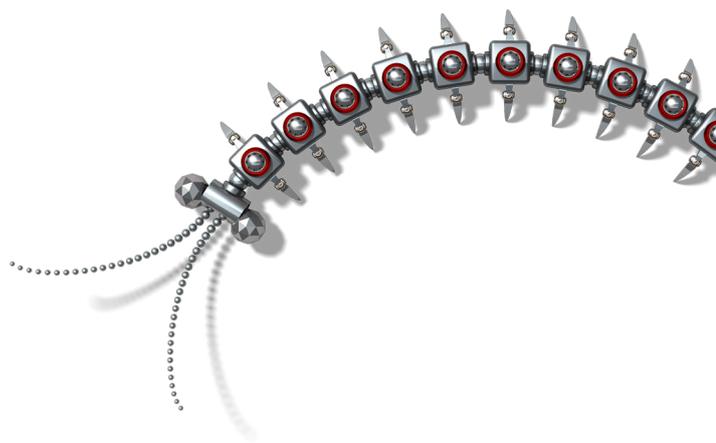
ООО «ЭлкомСофт»
Звездный б-р, 21, офис 541
129085 Москва

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.