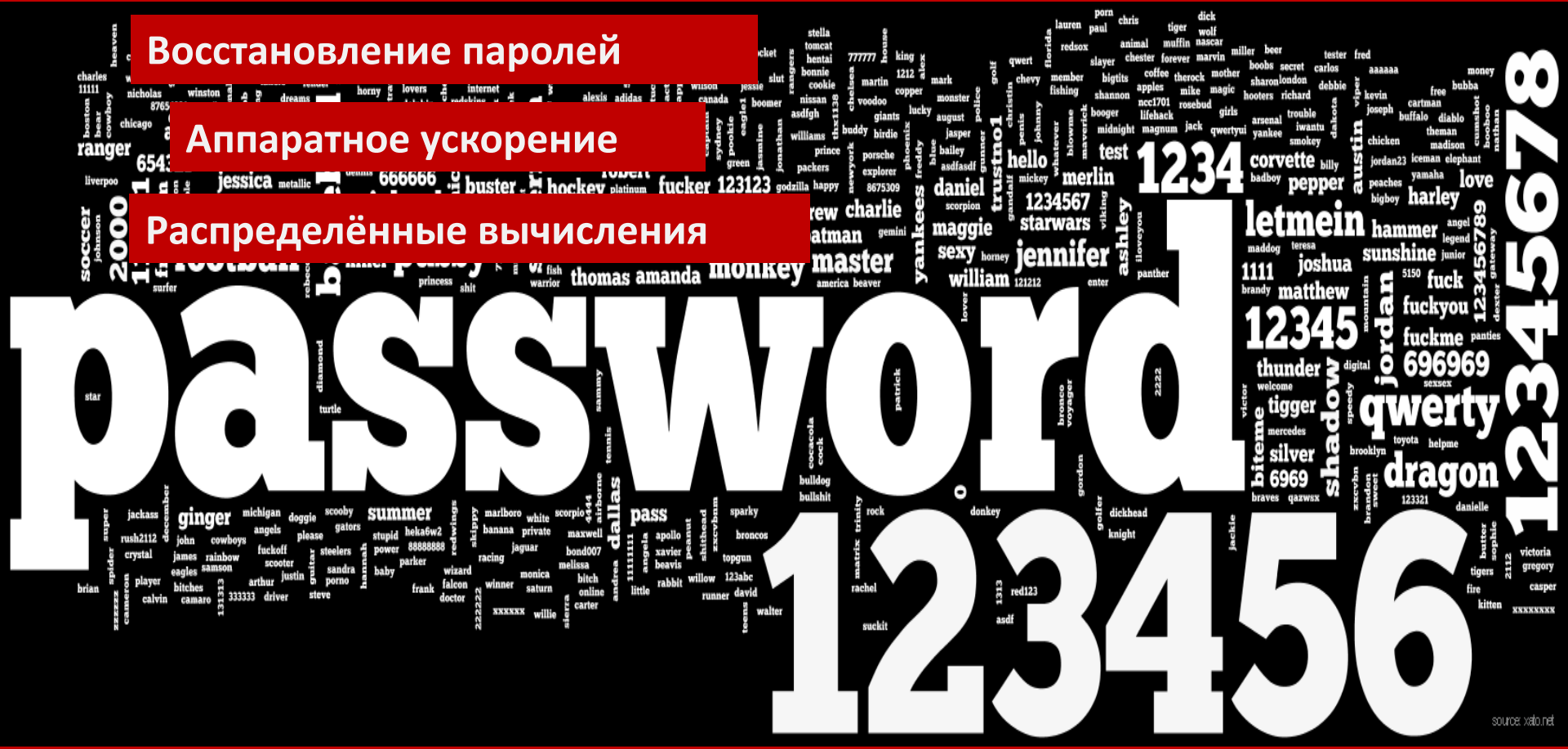
Особенности технического обеспечения решения экспертной задачи преодоления парольной защиты файлов, созданных офисными программами

Компьютерно-техническая экспертиза

- Восстановление паролей
- Аппаратное ускорение
- Распределённые вычисления



Восстановление паролей

- **Пароли для ограничения доступа**
  - Обычно восстанавливаются моментально
- **Слабое шифрование**
  - Возможно моментальное восстановление с Thunder Tables
- **Сильное шифрование**: требуется перебор
  - Начальная атака по списку часто употребляемых паролей
  - Атака по словарю с использованием мутаций
  - Аппаратное ускорение
  - Распределённые вычисления без потерь

Часто употребляемые пароли

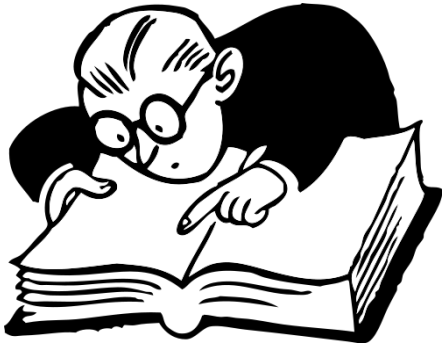
- **Всего 25 распространённых паролей используются в 2.2% случаев**
- **500 самых популярных паролей используются в 9.1% случаев**
- Компактный словарь на 10,000 популярных паролей срабатывает в 30% случаев
- 59% пользователей использует одинаковые или похожие пароли
- **Пароль зависит от языка пользователя**

Часто употребляемые пароли

- **Подход к решению задачи:**
  - Предварительная атака с использованием популярных паролей
  - Использовать ранее найденные пароли в предварительной атаке
- **Наши рекомендации:**
  - В первую очередь работайте с файлами со слабой защитой
  - Используйте **Proactive System Password Recovery** для моментального извлечения паролей и составления пользовательского словаря

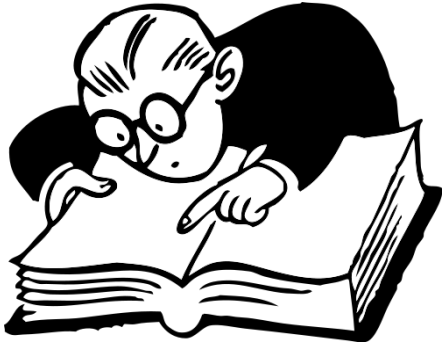
Атака по словарю

- **Большая часть паролей основана на словарных фразах**
  - Иногда с добавлением цифр
- **Словарные пароли редко блокируются политиками безопасности**
  - Вместо этого, политики устанавливают требования к минимальной длине пароля, использованию цифр и специальных символов
- Стойкие пароли (например, Office 2010-2016) можно восстановить только словарной атакой
- По статистике, успешность словарных атак ~50%



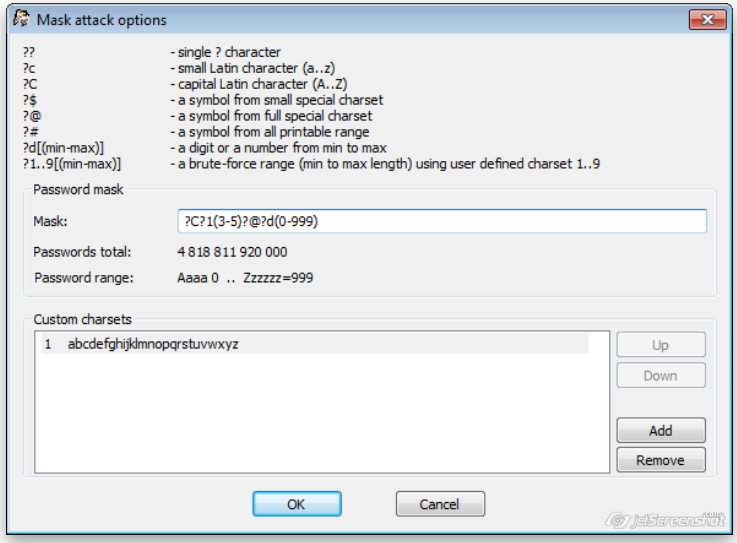
Атака по словарю

- **Подход к решению задачи:**
  - Используйте готовые словари, включая словари утечек паролей
  - Предварительные атаки с заранее сконфигурированными мутациями
  - Прямой перебор паролей в последнюю очередь
- **Наши рекомендации:**
  - Для каждого случая составляйте отдельный словарь
    Используйте **Proactive System Password Recovery**
  - Не тратьте слишком много времени на атаки по стандартным словарям общеупотребимых слов.
    Небольшой целенаправленный словарь сработает быстрее и более качественно.
  - Используйте слова как из английского языка, так и из родного языка пользователя
  - Не увлекайтесь мутациями. Доверьтесь здравому смыслу.



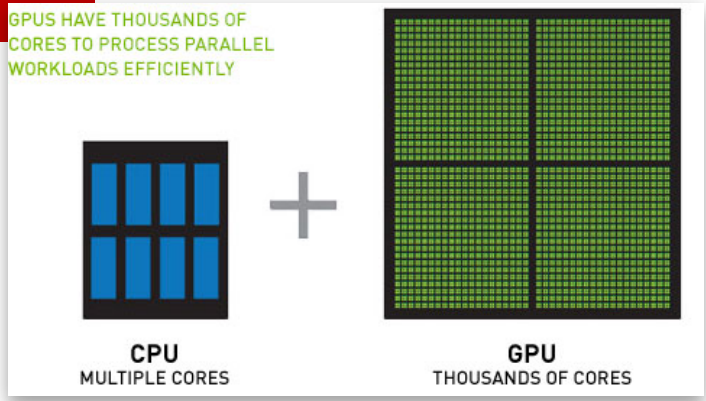
Продвинутые атаки

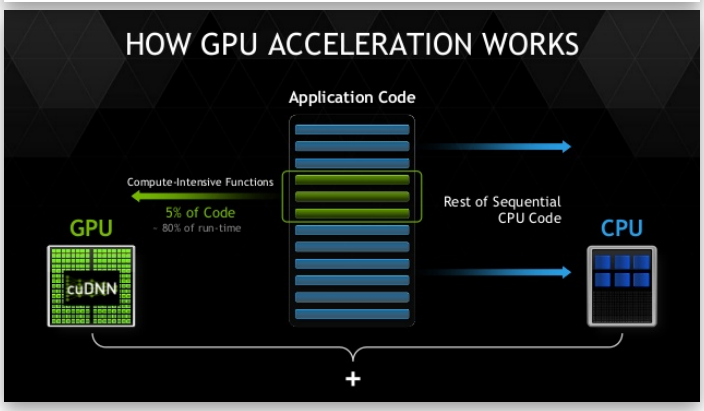
- Заметили закономерность в паролях пользователя?
- **Пароль соответствует требованиям политики безопасности?**
    - **Используйте шаблон для создания атаки**
- Существуют общие правила для мутаций
- Даты, «хакерский» жаргон l33t и другие
- Зеркалирование, вращение, дуплицирование, реверсирование, обрезка, изменение регистра: порядка 40 видов мутаций



Аппаратное ускорение

- Современные видеокарты справляются с выводом 3D видео 60 кадров в секунду
- Их вычислительная мощь превышает способности центрального процессора
  - **Быстрые вычисления**
  - **Ежегодный прирост производительности больше, чем у CPU**
  - **Intel i7: производительность за последний год увеличилась на 15%**
  - **NVIDIA GeForce: рост производительности за год на 70% (устройства одной серии)**
- **Используйте вычислительные ресурсы видеокарт для аппаратного ускорения перебора**
- Фактический прирост производительности в сравнении с 4-ядерным Intel i7:
  - 50x ускорение с одной видеокартой
  - 200x ускорение с 4 видеокартами
  - Поддержка неограниченного числа вычислительных модулей



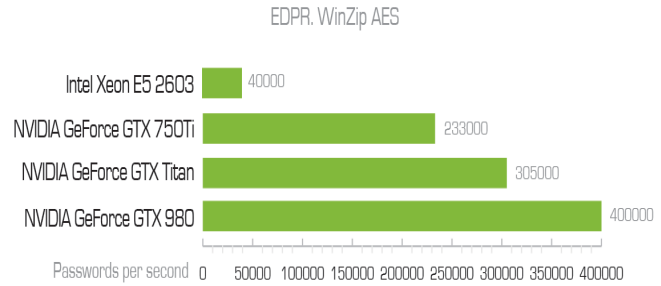


Аппаратное ускорение

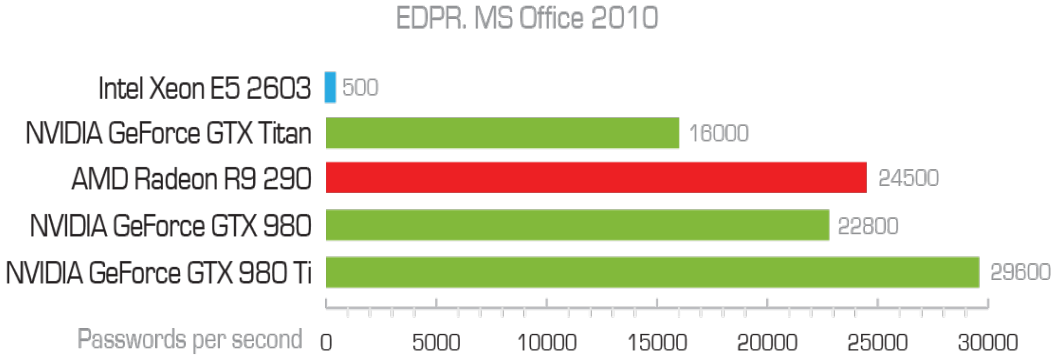
- **Подход к решению задачи:**
  - Обязательно используйте аппаратное ускорение
  - Устанавливайте максимальное число ускорителей
  - Экономия бюджетных средств: используйте существующий парк видеокарт (в продуктах Элкомсофт - асинхронная поддержка с одновременной работой карт AMD и NVIDIA)
- **Наши рекомендации:**
  - GPU (а не CPU) – лучшее вложение средств
  - Докупайте дополнительные видеокарты. Добавляйте, а не заменяйте: совместное использование даст максимальный прирост производительности при минимальных вложениях

Бенчмарки

- **Фактическая производительность**
  - Office 2010: 500 п/сек (CPU) vs. 22800 (GPU)
  - WinZip AES: 40,000 vs. 400,000

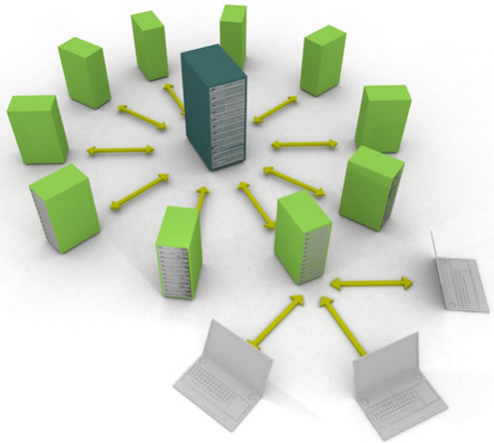


Intel Xeon E5 2603 vs.
NVIDIA GeForce GTX 980



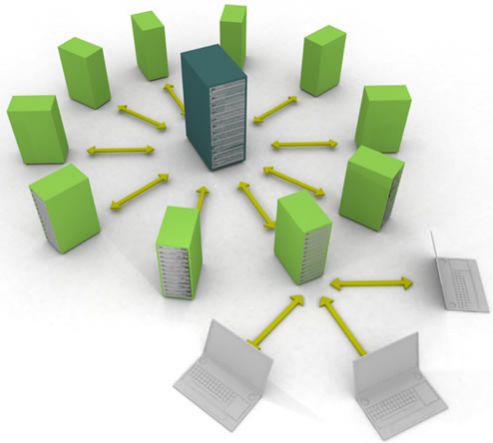
Распределённые вычисления

- **Во многих случаях одного компьютера недостаточно**
- Атаки с использованием распределённых вычислительных ресурсов
- Несколько компьютеров (укомплектованных видеоускорителями) работают над задачей одновременно
- Фактический прирост производительности зависит от конкретной системы



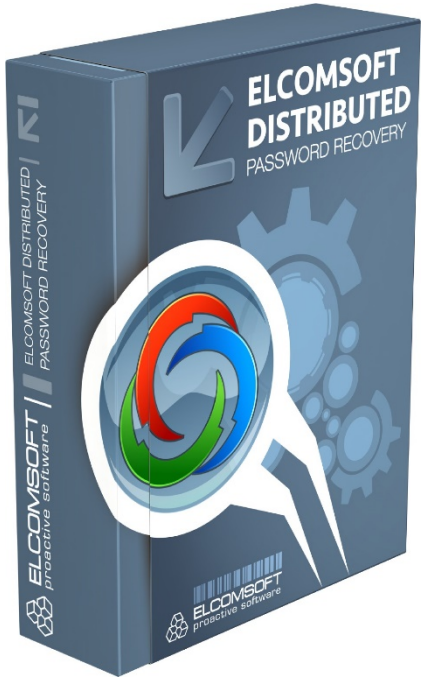
Распределённые вычисления

- **Подход к решению задачи:**
  - Используйте распределённые атаки
  - Масштабируемость без накладных расходов:
    10,000 компьютеров сработают ровно в 10,000 раз быстрее вне зависимости от пропускной способности сети
  - Подключайте дополнительные компьютеры через LAN и через Internet
- **Наши рекомендации:**
  - Единственный компьютер с видеокартой работает быстрее 50-ти компьютеров без видеокарт
  - Кластер компьютеров с видеокартами обеспечивает производительность порядка нескольких терафлоп



Elcomsoft Distributed Password Recovery

- Ускорение с использованием GPU на картах AMD и NVIDIA
- Распределённые вычисления с линейным масштабированием без накладных расходов
- Поддержка до 32 ядер CPU и до 8 GPU (видеокарт) на каждом компьютере
- Поддержка огромного числа форматов файлов

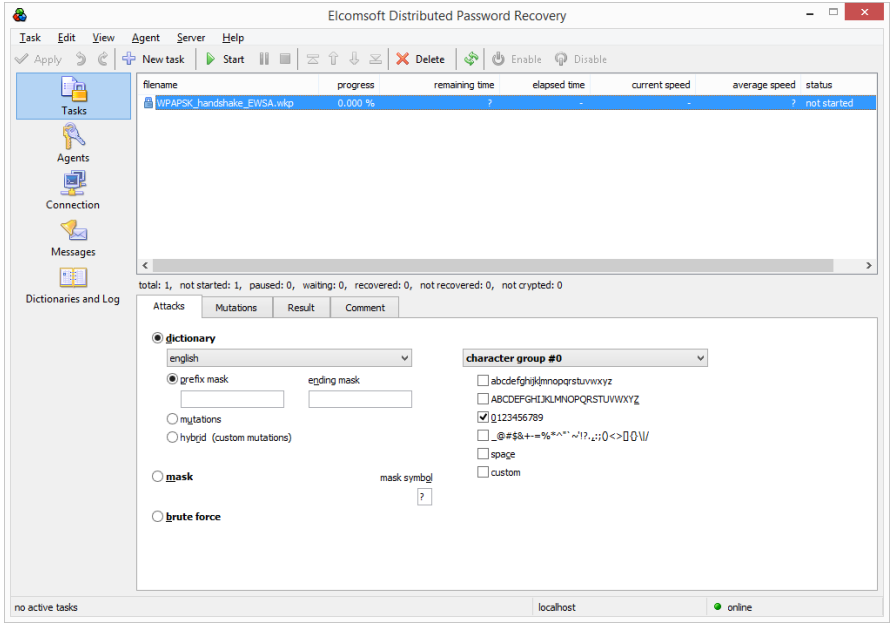


Elcomsoft Distributed Password Recovery

- Архивы ZIP, RAR
- Офисные приложения Microsoft Office 97 - 2016
- Open Office, Hangul Office
- PGP и OpenKey, IKE, TrueCrypt, BitLocker
- Системные пароли (учётных записей, keychain и т.п.):
  - Windows, UNIX, Mac OS X
- Lotus Notes, Oracle, The Bat!, Mozilla, FireFox, ThunderBird
- Резервные копии BlackBerry (BB OS 6.0 – 7.1)
- Apple iWork ‘09, 2013-2014

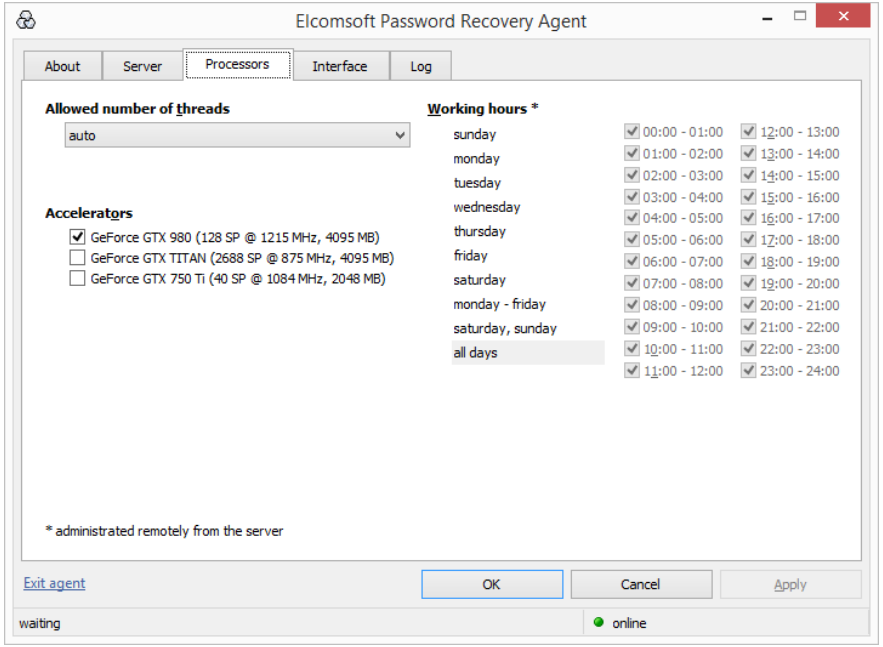
Elcomsoft Distributed Password Recovery

- Работа через LAN и/или Интернет
- Управление через консоль
- Минимальные требования к пропускной способности сети
- Агенты работают как системные службы
- Официальные сертификаты соответствия



Elcomsoft Distributed Password Recovery

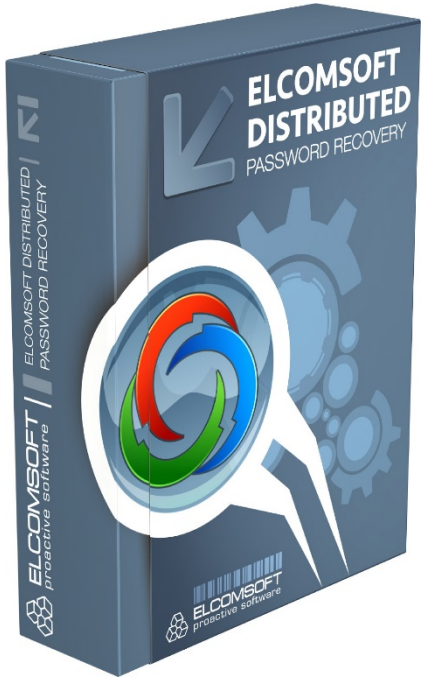
- Удалённая установка и управление клиентами
- Гибкое управление задачами
- Контроль утилизации процессорного времени
- Расширяемость через плагины
- Найденные пароли автоматически сохраняются и используются в последующих задачах



Elcomsoft Distributed Password Recovery

Заключение

- Распределённое восстановление с аппаратным ускорением
- Оптимизирован для использования 24x7
- Самый мощный и продвинутый продукт ElcomSoft



Elcomsoft Advanced Office Password Recovery

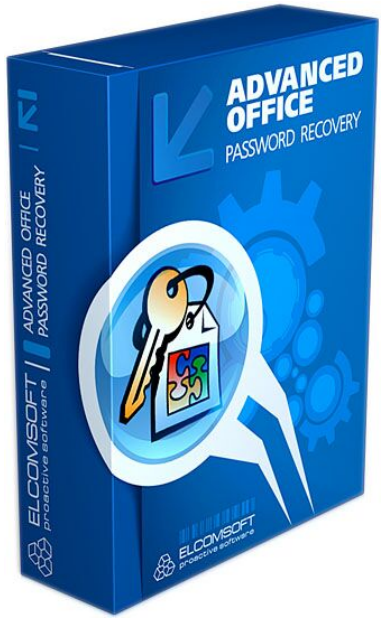
- Microsoft Office 2.0 - 2016
- OpenOffice и OpenDocument
- Hangul Office
- Apple iWork 2009, 2013/2014
- Adobe PDF

Elcomsoft Advanced Office Password Recovery

Microsoft Office 2.0 - 2016

- Word, Excel, Access
- Outlook
- Project, PowerPoint, OneNote
- Money, Visio

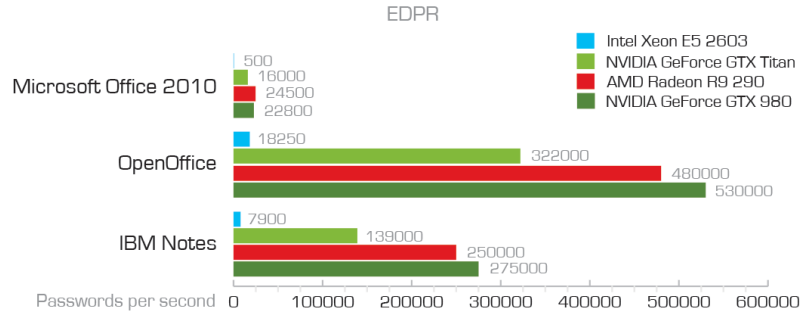
- **Восстановление пароля на открытие**
- **Снятие ограничений**

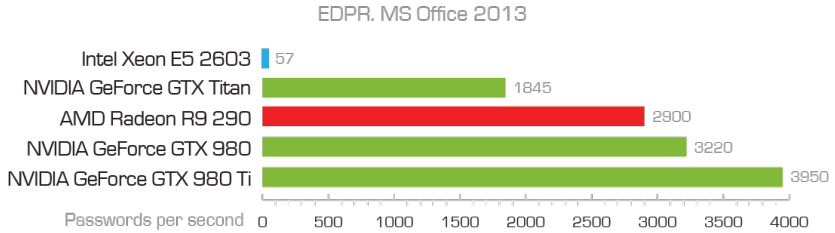


Elcomsoft Advanced Office Password Recovery

Аппаратное ускорение

- AMD и NVIDIA
- Единственная видеокарта в 70 раз быстрее 4-ядерного CPU
- Поддержка до 4 видеокарт
- Пароли к документам Office 2010-2016 могут быть восстановлены исключительно с использованием аппаратного ускорения





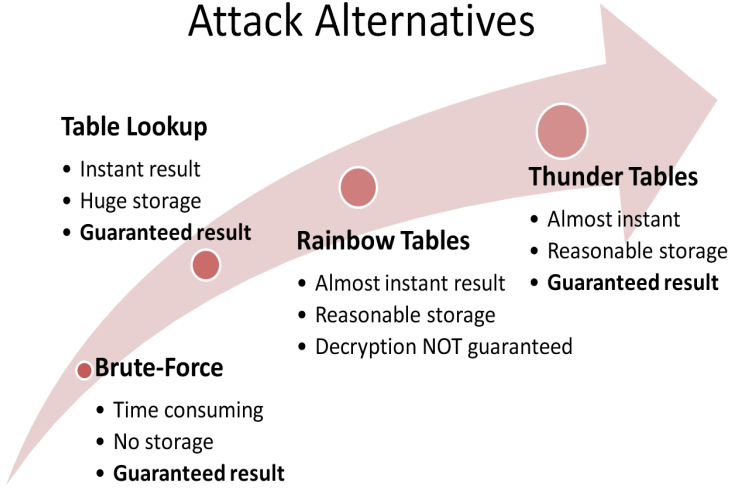
Thunder Tables ®

Конец 40-битного шифрования

- Гарантированное восстановление в считанные секунды для документов Office и PDF с 40-битным шифрованием
- Использование патентованной технологии **Thunder Tables ®**

Доступно в продуктах:

- Elcomsoft Advanced Office Password Recovery
- Elcomsoft PDF Password Recovery



Некоторые пароли слабее прочих

Моментальное восстановление

- Sage, ACT!, Lotus, WordPerfect, SQL, Intuit
- Многие программы мгновенного обмена сообщениями
- Пароли от Email
- Наши продукты для моментального восстановления паролей:
  - Advanced Sage Password Recovery
  - Mailbox Password Recovery
  - Advanced Lotus Password Recovery
  - Advanced Intuit Password Recovery
  - Advanced Mailbox Password Recovery
  - …и несколько других

Компьютерно-техническая экспертиза
Breaking Passwords and Overcoming Encryption

(c) ООО «Элкомсофт» 2016
Владимир Каталов, CEO

Facebook: ElcomSoft
Twitter: @elcomsoft