Основные принципы получения доступа к защищенным документам при помощи решений Elcomsoft

Типы паролей

- **Пароль не используется для шифрования документа**
  - Обычно восстанавливаются моментально, либо возможно изменение/удаление
- **Слабое шифрование**
  - Возможно гарантированное восстановление, либо расшифровка документа за приемлемое время
- **Сильное шифрование**
  - Пароль невозможно найти путем быстрых вычислений

Комплексный подход

Используем человеческий фактор

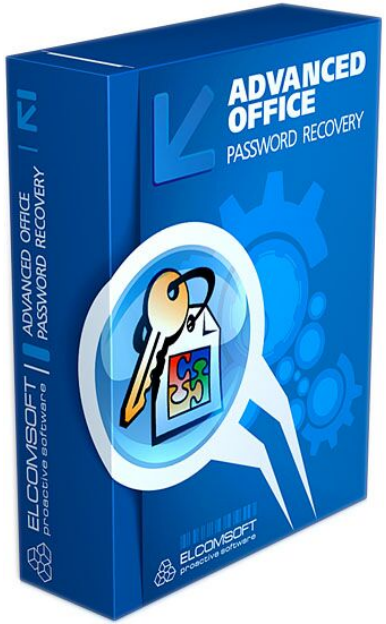
- Персональные данные
- Все документы подозреваемого, включая незащищенные, переписка, мессенджеры, социальные сети
- Найти все слабые пароли
- В первую очередь искать сильные пароли к хранилищам паролей (1Password, LastPass, KeePass)
- Проанализировать все конфискованные устройства: телефоны, планшеты и т.п.
- Собрать все данные подозреваемого, сохраненные в облачных хранилищах

Персональные данные

Часто в качестве паролей используют:

- Номера телефонов
- Свое собственное имя или фамилию
- Имена жены, детей, родственников, друзей и знакомых
- Номера автомобилей, паспортов, других документов
- Год рождения
- Клички животных

Слабые пароли



Advanced Office Password Recovery

- Старые документы Word (2.0 – 95)
- Старые документы Excel (4.0 – 95)
- Французские версии MS Office до Office 2000
- Старые версии MS Money
- Стойкие пароли, найденные в ходе предварительной атаки

Продукты Elcomsoft для расшифровки документов

Слабые пароли

Elcomsoft Internet Password Breaker

- Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail, Thunderbird
- Internet Explorer, Edge, Google Chrome, Mozilla Firefox, Yandex browser, Opera
- Автоматическое и мгновенное восстановление всех паролей
- Формирование отчета
- **Формирование словаря**

Слабые пароли

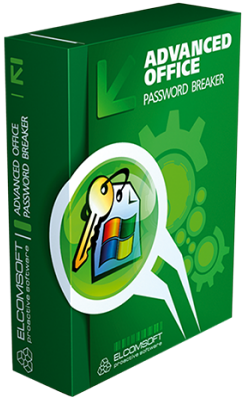
Другие утилиты

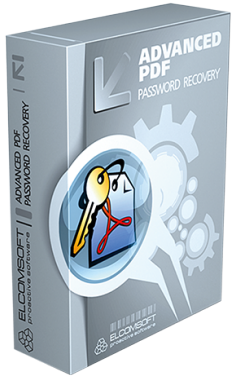
- Advanced ACT! Password Recovery
- Advanced IM Password Recovery
- Advanced Intuit Password Recovery
- Advanced Lotus Password Recovery
- Advanced Mailbox Password Recovery
- Advanced Sage Password Recovery
- Advanced WP Office Password Recovery
- Advanced SQL Password Recovery
- Proactive System Password Recovery

Слабое шифрование

Advanced Office Password Breaker
Advanced PDF Password Recovery

- Поддержка Word, Excel, PDF с шифрованием 40 bit RC4
- Вычисление ключа шифрования документа за несколько минут с использованием патентованной технологии Thunder Tables ®
- Минус: не находится пароль к документу





Сильное шифрование: атаки

1. Словари с часто используемыми словами
2. Словарь, созданный на основе данных пользователя
3. Словари с мутациями
4. Маски на основе выявленных закономерностей
5. Прямой перебор

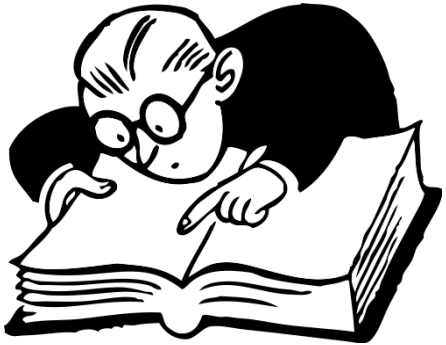
- Слабые пароли
- Персональные данные
- Пароли из мобильных устройств
- Пароли из облачных сервисов
- Пароли из 1Password, KeePass, LastPass
- Другие слова, которые могут быть использованы

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**

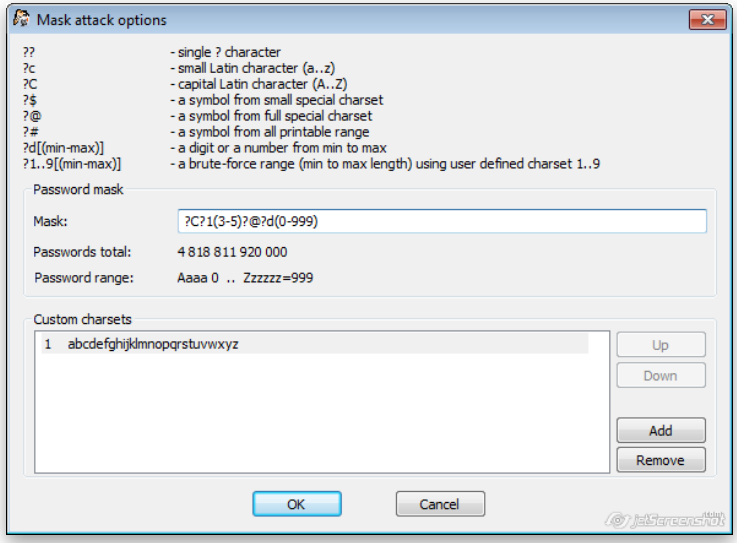
Атака по словарю

- **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%



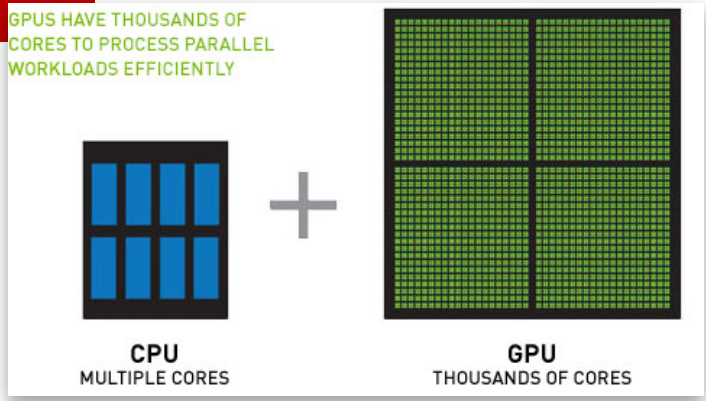
Продвинутые атаки

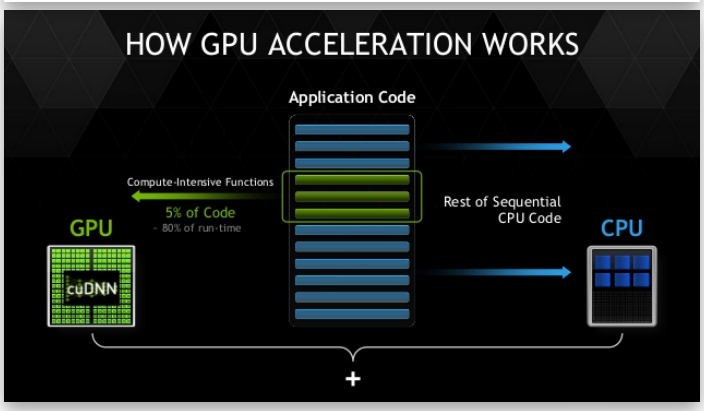
- Заметили закономерность в паролях пользователя?
- **Пароль соответствует требованиям политики безопасности?**
    - **Используйте шаблон для создания атаки**
- Существуют общие правила для мутаций
- Даты, «хакерский» жаргон l33t и другие
- Зеркалирование, вращение, дуплицирование, реверсирование, обрезка,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



Аппаратное ускорение

- Современные видеокарты справляются с выводом 3D видео 60 кадров в секунду
- Их вычислительная мощность 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



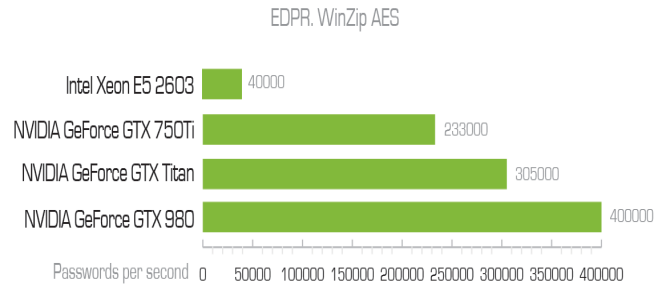


Аппаратное ускорение

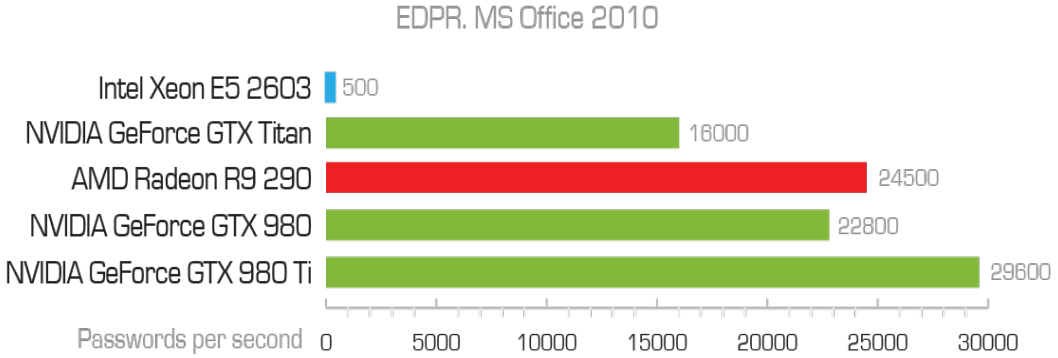
- **Подход к решению задачи:**
  - Обязательно используйте аппаратное ускорение
  - Устанавливайте максимальное число ускорителей
  - Экономия бюджетных средств: используйте существующий парк видеокарт (в продуктах Элкомсофт - асинхронная поддержка с одновременной работой карт AMD и NVIDIA)
- **Наши 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

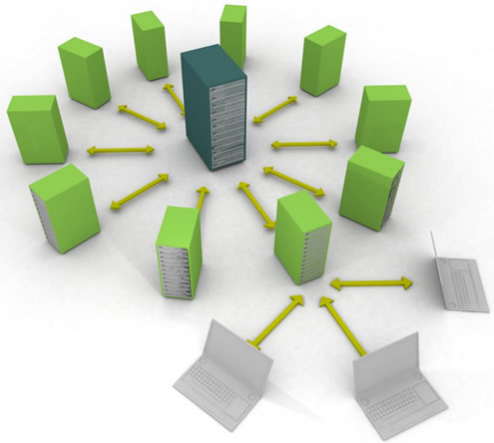


Intel Xeon E5 2603 vs.
NVIDIA GeForce GTX 980



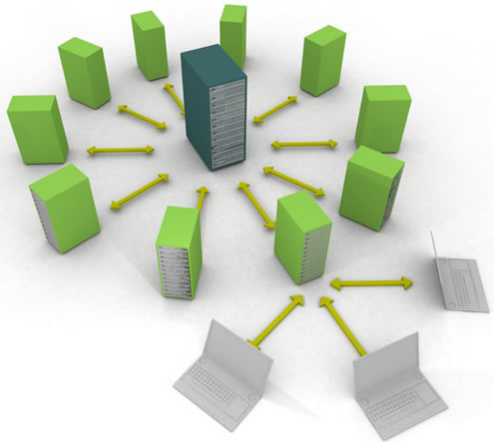
Распределённые вычисления

- **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



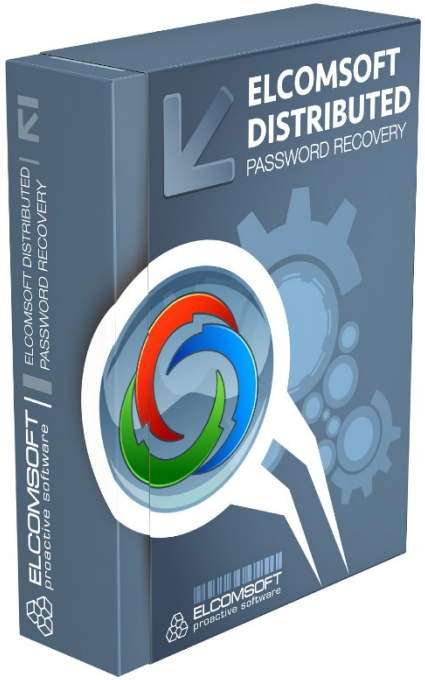
Распределённые вычисления

- **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

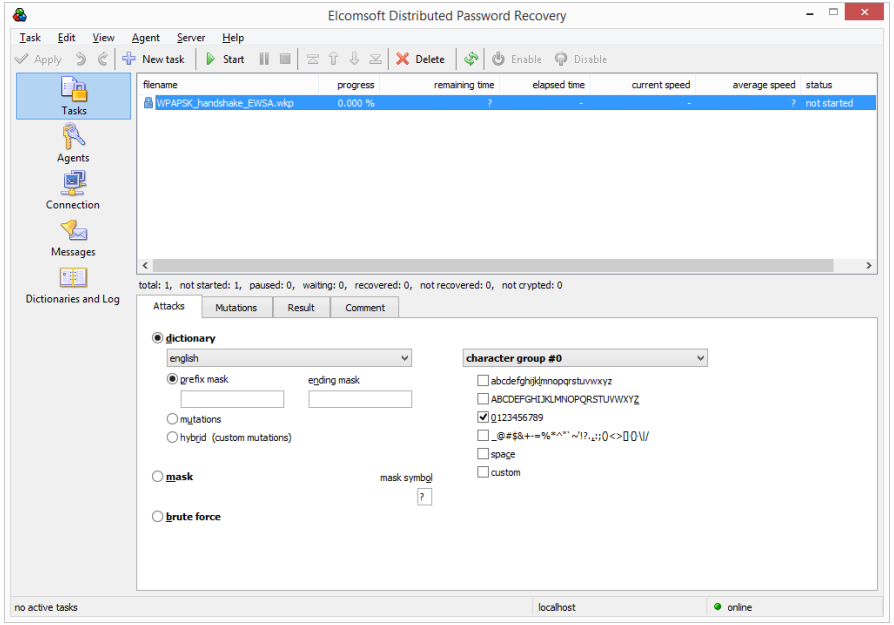


Elcomsoft Distributed Password Recovery

- 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

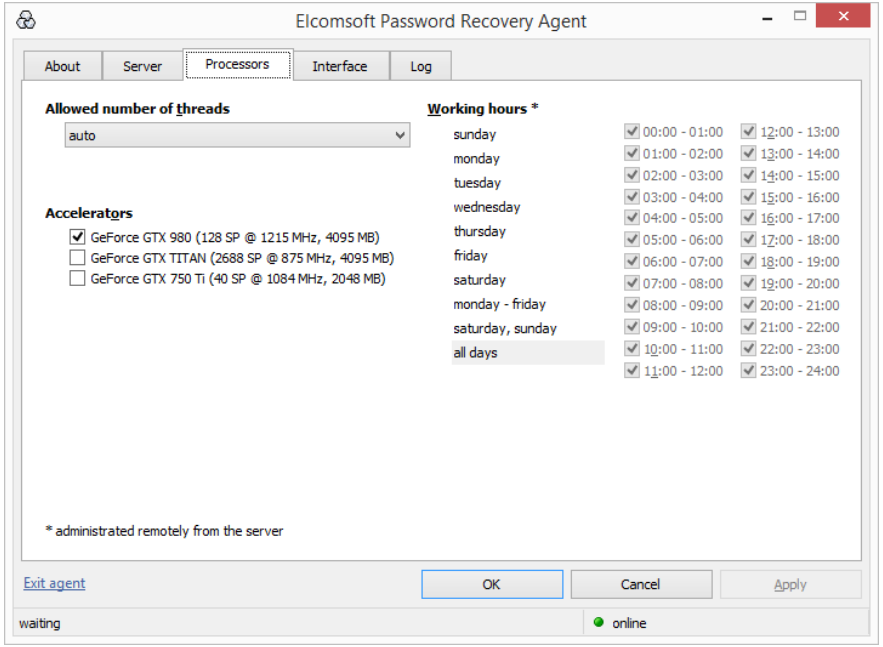
Elcomsoft Distributed Password Recovery

- 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

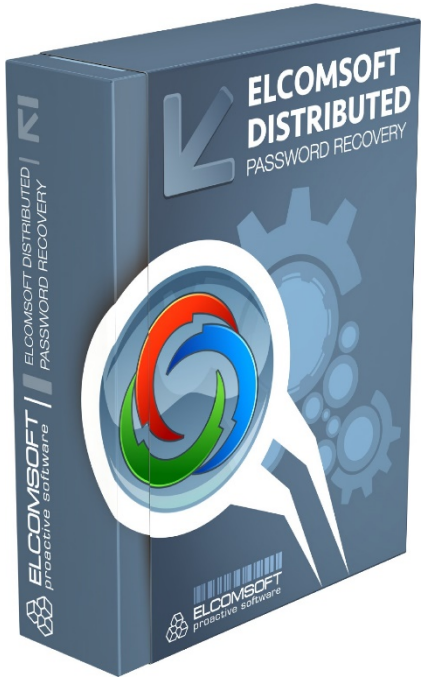
- Удалённая установка и управление клиентами
- Гибкое управление задачами
- Контроль утилизации процессорного времени
- Расширяемость через плагины
- Найденные пароли автоматически сохраняются и используются в последующих задачах



Elcomsoft Distributed Password Recovery

Заключение

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



Облачные вычисления

Облачные вычисления

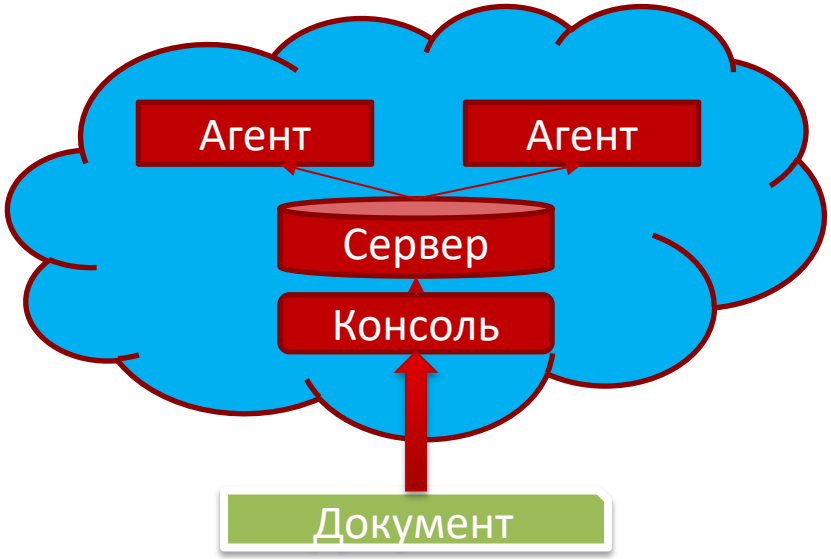
- Обычно запускаются «по требованию» – ниже цена
- Очень просто развернуть и администрировать
- ~~Железо~~
- ~~Обслуживание~~
- ~~Электричество, кондиционеры и т.п.~~
- ~~Апгрейды~~
- Цена одной брутфорс атаки не зависит от количества купленных машин!

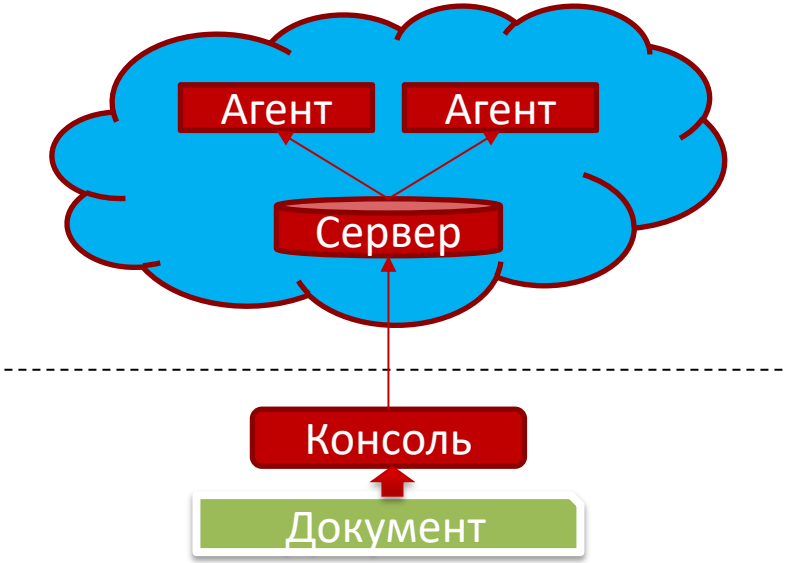
# паролей	Скорость	# машин	Время	Цена
P	S	N	T = P/S/~~N~~	P = P1*~~N~~/T

Перебор паролей будет быстрее на большем количестве VM при фиксированной цене

Облачные вычисления: безопасность

Все компоненты в облаке

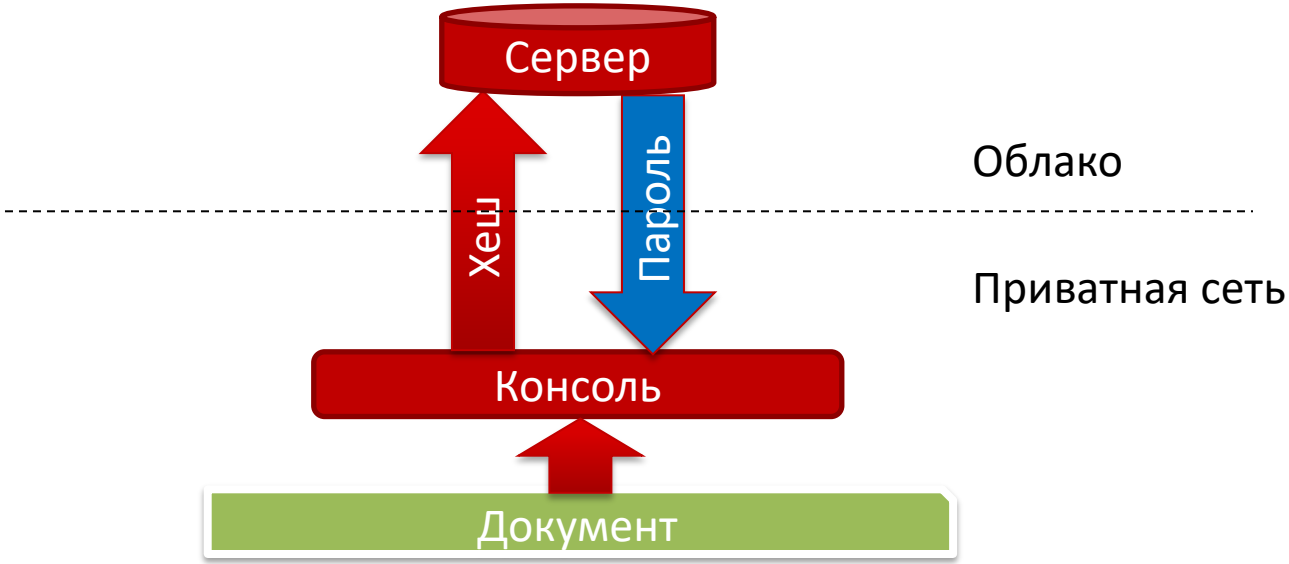




Private LAN

Облачные вычисления: безопасность

- В облако передается только пароль и его хеш
- Владельцы облака видят только пароль, но не документ



Облачные сервисы: Amazon

Виртуальные машины P2 (Tesla K80) были представлены в сентябре 2016,цены за Windows Server ”по требованию”.

Имя	# CPU	# GPU	Цена
p2.xlarge	4	1	$1.084/hour
p2.8xlarge	32	8	$8.672/hour
p2.16xlarge	64	16	$17.344/hour

Стоимость перебора 20000000 паролей (6 символов, A-Z, 0-9)

Формат	Скорость на 1 K80	Время (ч)	Цена
MS Word 2007	44 000	12	$13
MS Word 2013	2 300	241	$261