**Отчет по лабораторной работе №2**

**По дисциплине «Информационная безопасность»**

**Тема:** **Работа с программой вскрытия паролей AZPR**

Студент: Агниев Сергей Владимирович

Преподаватель Оганесян Левон Левонович

Краснодар 2025

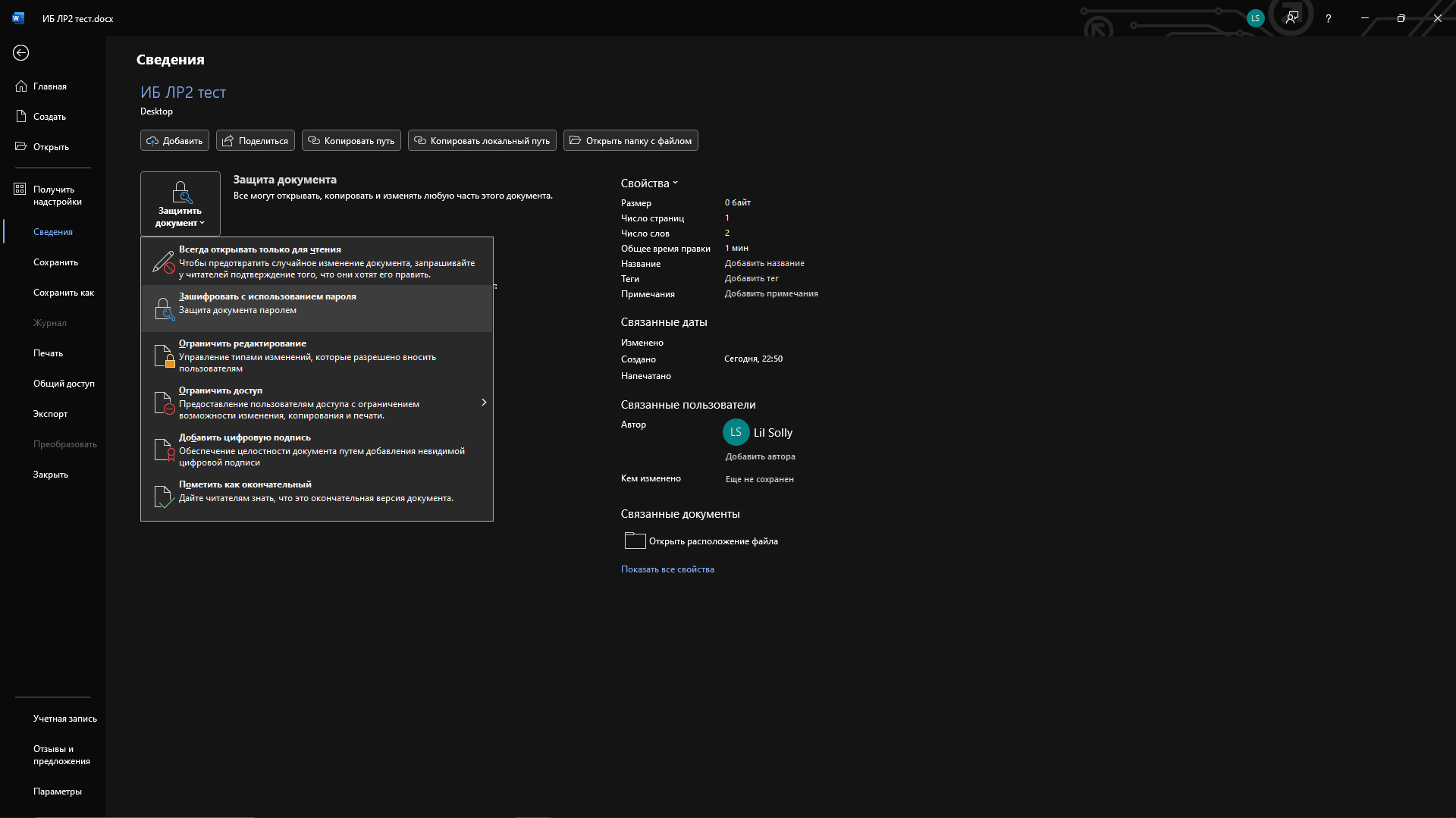
**Цель работы:**

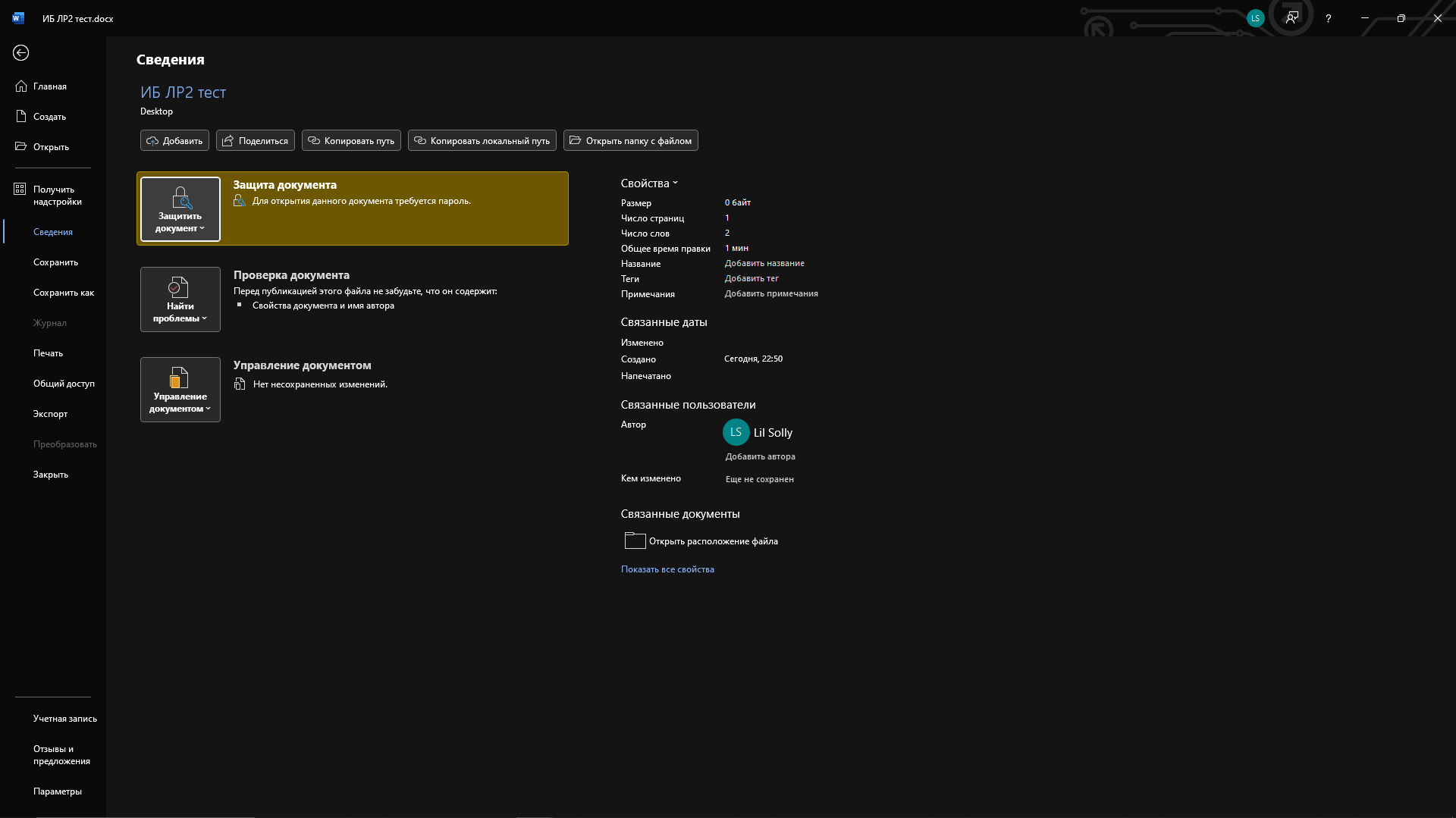
изучить возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery

**Ход работы:**

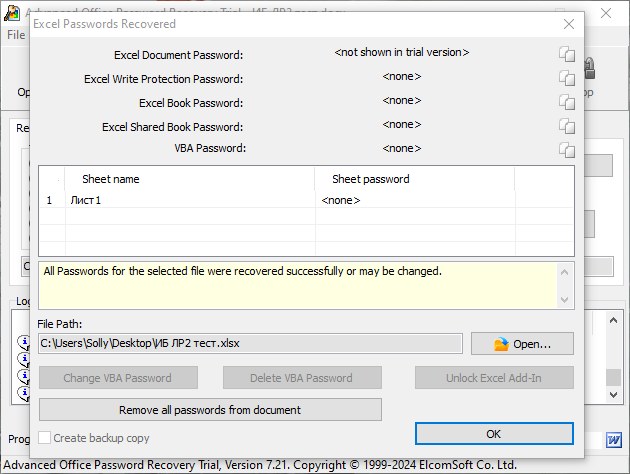
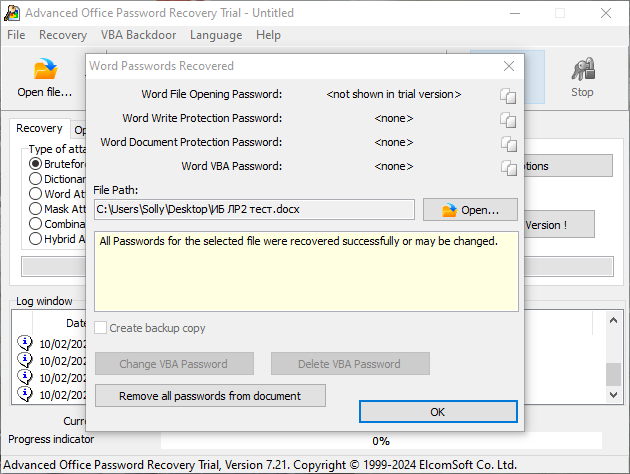
**Задание 1. Восстановление пароля в документах MS**

Был зашифрован один тестовый документ. Для зашифовывания необходимо перейти во вкладку «Сведения» и нажать на кнопку «Защита документа», после чего выбрать нужную функцию. Пароль у файлов был 4-значный.





Далее эти два зашифрованных файла были взломаны с помощью AOPR.



**Задание 2**

**1. Выполните поиск в сети Internet специализированных программных средств для создания, а также для восстановления паролей**

**2. Подготовьте сообщение по данной теме**

**1. Программы для создания паролей**

Создание надежного пароля — важный шаг в обеспечении безопасности. Надежный пароль должен быть длинным, содержать буквы (в верхнем и нижнем регистре), цифры и специальные символы. Для создания таких паролей используются следующие программы:

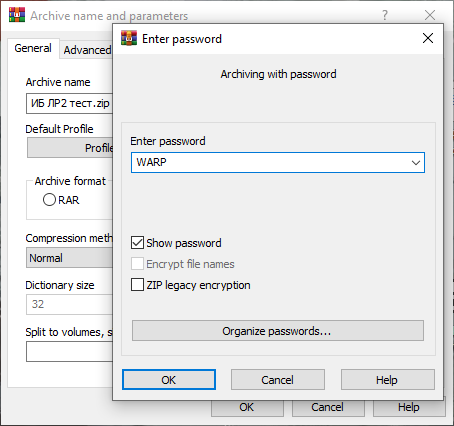
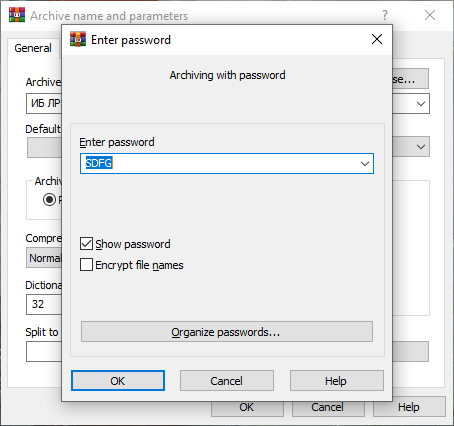
* **KeePass**  
  KeePass — это бесплатное программное обеспечение с открытым исходным кодом для управления паролями. Оно позволяет генерировать сложные пароли и хранить их в зашифрованной базе данных.  
  Особенности:
  + Генерация паролей с настраиваемыми параметрами.
  + Хранение паролей в зашифрованном виде.
  + Поддержка плагинов для расширения функциональности.
* **LastPass**  
  LastPass — это популярный менеджер паролей, который также включает функцию генерации паролей.  
  Особенности:
  + Интеграция с браузерами и мобильными устройствами.
  + Автоматическая генерация сложных паролей.
  + Синхронизация данных между устройствами.
* **Dashlane**  
  Dashlane — еще один менеджер паролей, который предлагает инструменты для создания и хранения паролей.  
  Особенности:
  + Генерация паролей с учетом требований к безопасности.
  + Возможность автоматической смены паролей на сайтах.
  + Хранение зашифрованных данных в облаке.

Если пароль утерян или забыт, существуют специализированные программы, которые помогают его восстановить. Эти программы используют различные методы, такие как перебор (brute force), атака по словарю или анализ хэшей.

* **John the Ripper**  
  John the Ripper — это мощная программа для восстановления паролей, которая поддерживает множество алгоритмов шифрования.  
  Особенности:
  + Поддержка различных операционных систем (Windows, Linux, macOS).
  + Возможность использования словарей и масок для перебора.
  + Высокая скорость работы благодаря оптимизации.
* **Hashcat**  
  Hashcat — это программа для восстановления паролей, которая использует GPU для ускорения процесса перебора.  
  Особенности:
  + Поддержка множества алгоритмов хэширования.
  + Возможность работы с видеокартами NVIDIA и AMD.
  + Высокая производительность.
* **Ophcrack**  
  Ophcrack — это программа для восстановления паролей, которая использует радужные таблицы для взлома хэшей.  
  Особенности:
  + Бесплатная и простая в использовании.
  + Поддержка Windows и Linux.
  + Возможность восстановления паролей за короткое время.

**Задание 3. Создайте 2 архива, содержащие по 3 файла. Установите пароль на каждый архив**

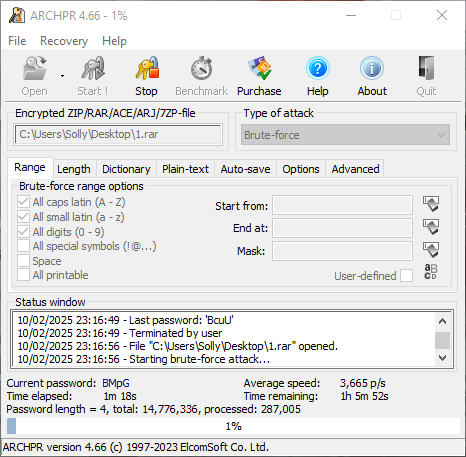
Были созданы два архива: RAR-архив и ZIP-архив.



**Задание 4. Вскрытие пароля архива**

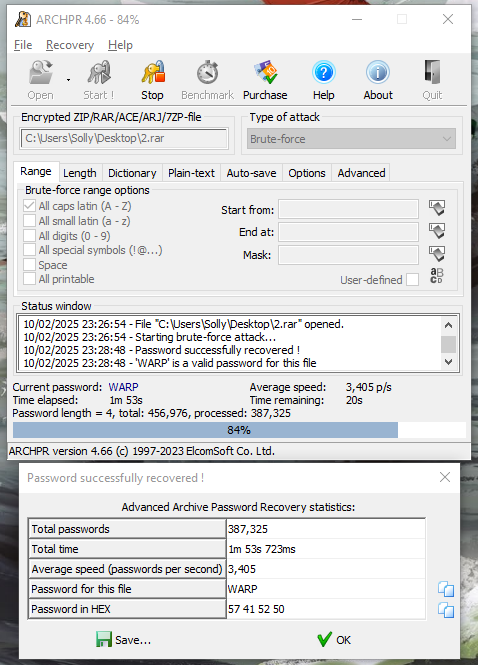
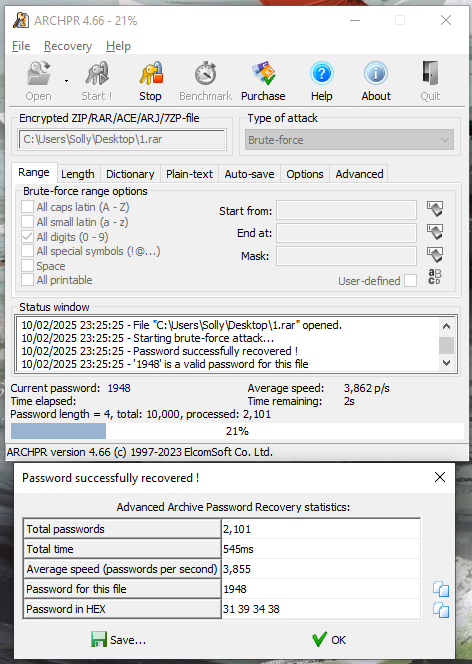
**Проведение атаки перебором (bruteforce attack)**

Пронаблюдав алгоритм перебора становится очевидно, что перебираются все комбинации символов в порядке A-Z, a-z, 0-9. Из этого можно сделать вывод, что программа будет перебирать выбранный для первого архива пароль «1948» около часа.



Оставшиеся 4 архива с паролями «WARP», «SgRv», «s1G5», «asdf» будут найдены за примерно 20-25 минут, 20 минут, 40 минут и 30 минут соответственно, если делать грубую оценку по положению первого символа пароля в ряду A-Z, a-z, 0-9.

При этом при подборе пароля только по цифрам для первого архива поиск занимает всего полсекунды. Для второго архива с паролем, состоящем из букв английского алфавита верхнего регистра, время поиска составило почти 2 минуты.



**Проведение атаки по словарю (dictionary attack)**

С использованием атаки по словарю пароль «god» был отгадан за 21 секунду. Скорость отгадывания обуславливается тем, что первая буква слова («G») – седьмая в алфавите и к ней программа перешла достаточно быстро, т.к. слова в используемом словаре также расположены в алфавитном порядке.

Далее для сравнения был использован метод прямого перебора по буквам нижнего регистра английского алфавита. Результат – 1 секунда.

