Лабораторная работа

«Создание зашифрованного архива с использованием программы BCArchive»

Программа BCArchive разработана для сжатия группы файлов или папок в зашифрованный архив (т.е. в единый сжатый файл).

Программа позволяет пользователю:

- Создать сжатый и зашифрованный архив, защищенный паролем.
- Создать сжатый и зашифрованный архив, зашифрованный публичным ключом другого пользователя.
- Добавить несколько паролей к существующему архиву.
- Добавить несколько публичных ключей к существующему архиву, чтобы несколько пользователей могли расшифровать архив.
- Создать новую пару ключей публичный/секретный в формате PKCS-12/X.509, а также добавить в свою базу данных существующие ключи для последующего использования.
- Зашифровать и сжать данные в самораспаковывающийся исполняемый файл. Пользователь, знающий пароль, может запустить файл даже если на его компьютере не установлена программа BCArchive и получить данные.

BCArchive использует следующие алгоритмы шифрования, стандарты и спецификации:

- Симметричные алгоритмы: Blowfish, Blowfish -448, Twofish, GOST, Rijndael (AES), IDEA, Triple-DES, Serpent и CAST5.
- Хэш Алгоритмы: SHA-1, SHA-256, MD5 и RIPEMD-160.
- Асимметричные алгоритмы(публичного и секретного ключа): RSA, ElGamal / Diffie-Hellman.
- Спецификации для публичного и секретного ключа: PKCS #12, X.509.
- PKCS #5 (рекомендации по реализации шифрования, основанного на паролях).
- Спецификации RFC 2440 для сессионных ключей, зашифрованных симметричными алгоритмами или алгоритмами публичного ключа.

Задание:

- Установить BCArchive;
- .Создать зашифрованный архив;
- Добавить в архив файлы;
- Создать самораспаковывающейся архив;
- Оформить отчет о проделанной работе.

Инструкция по выполнению работы:

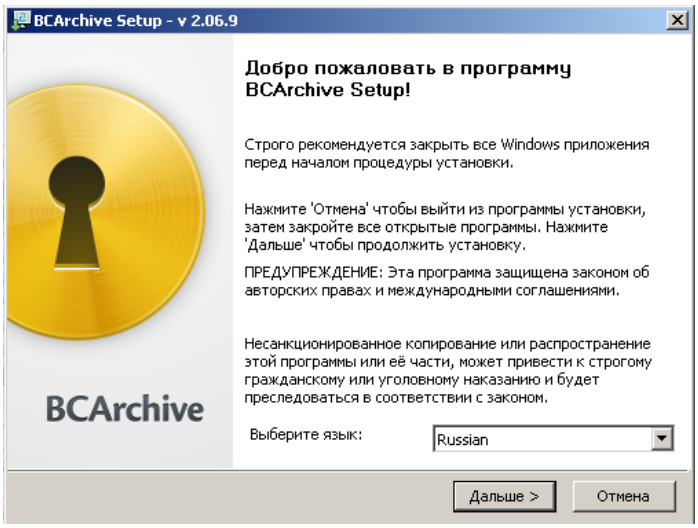

Рисунок 1 – Окно установки программы. Выбираем нужный язык

Рисунок 2 – Принимаем лицензионное соглашение

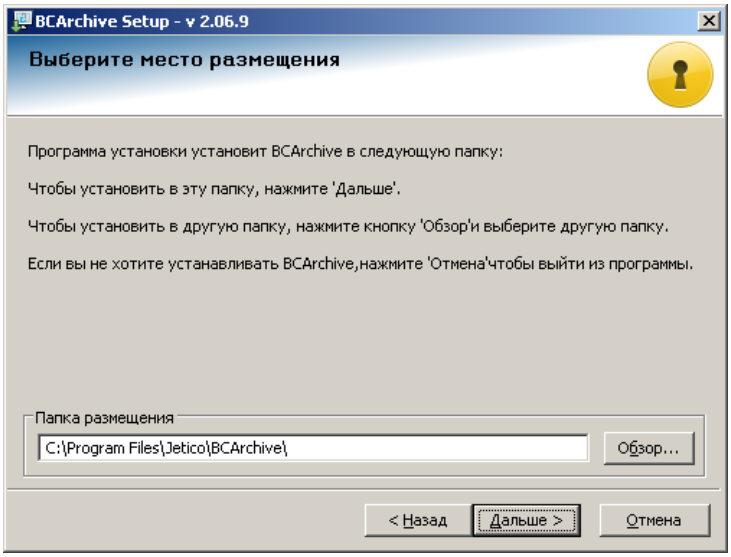

Рисунок 3 – Выбираем место размещения

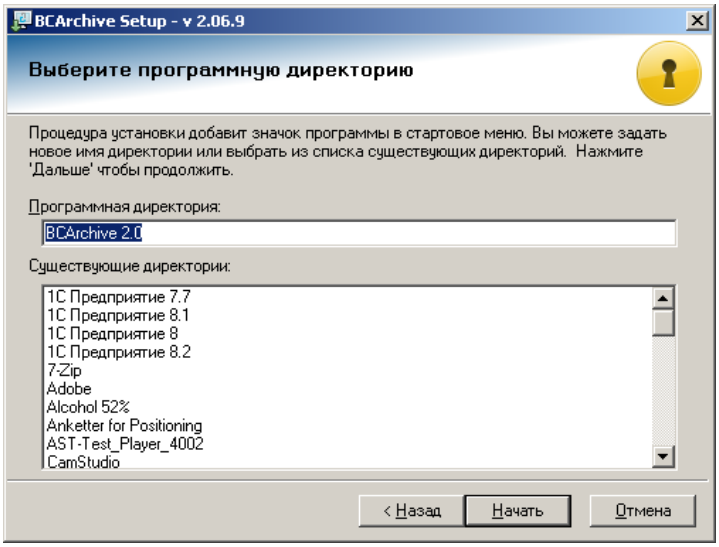

Рисунок 4 – Выбираем программную директорию

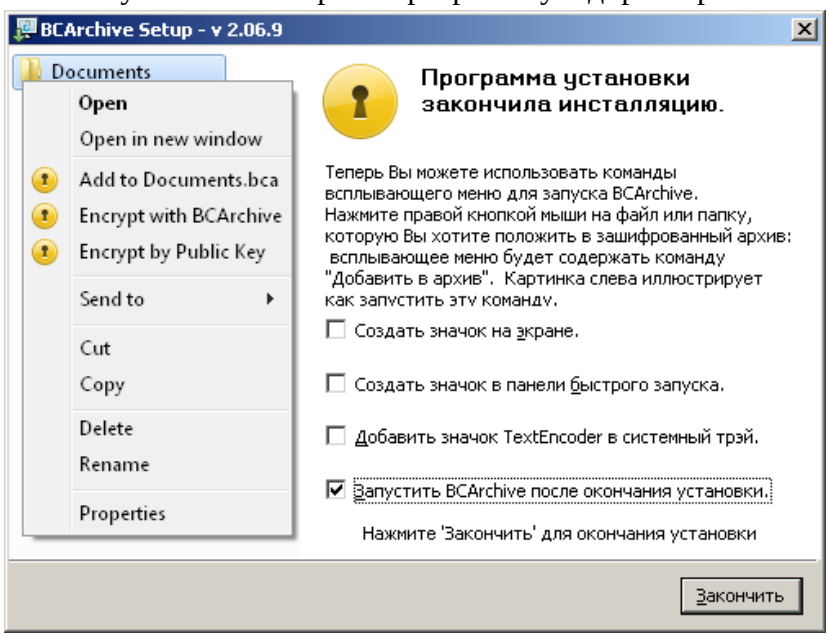

Рисунок 5 – Завершающее окно установки

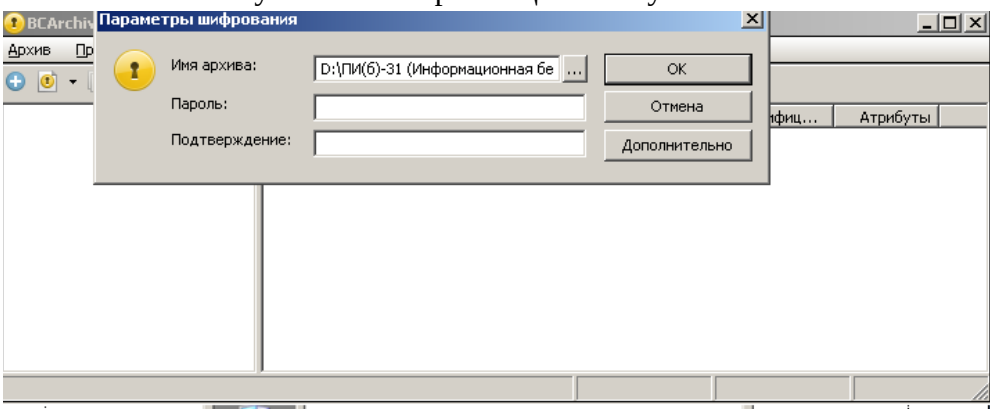

Рисунок 6 – Создаем архив и придумываем для него пароль

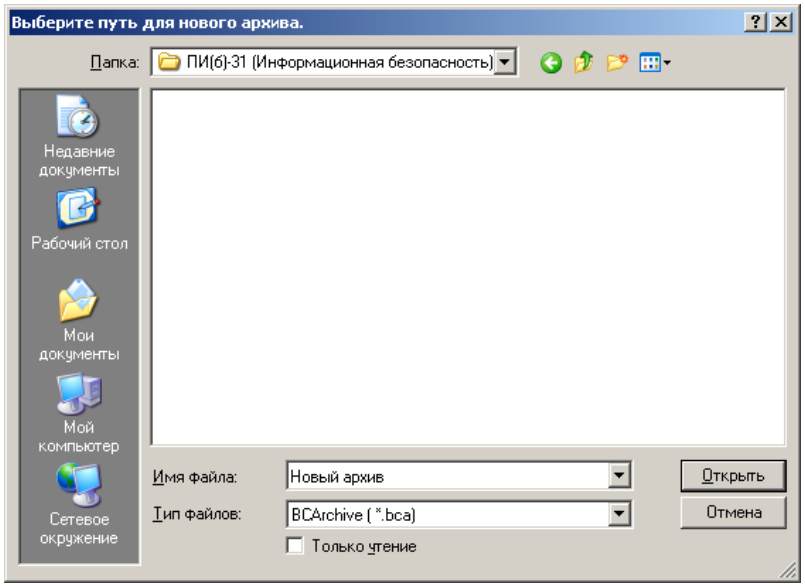

Рисунок 7 – Выбираем расположение архива

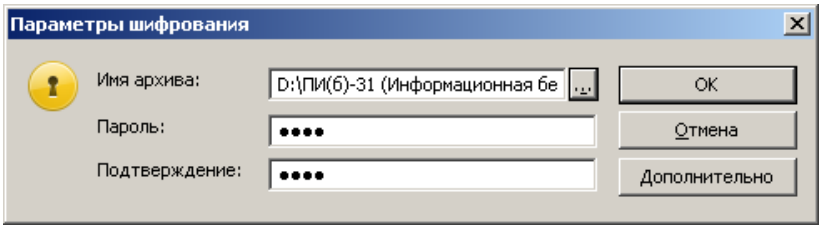

Рисунок 8 – Создаем пароль для архива

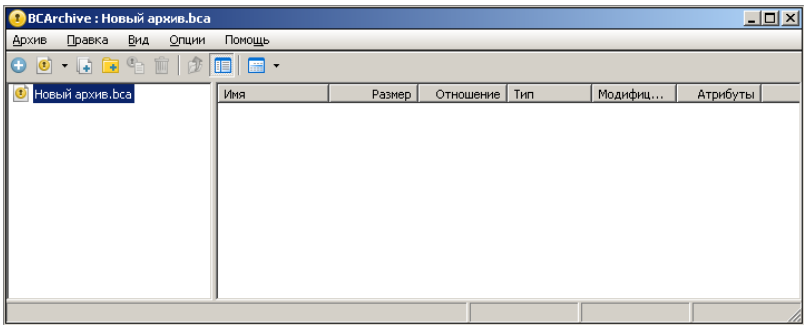

Рисунок 9 – Открываем архив

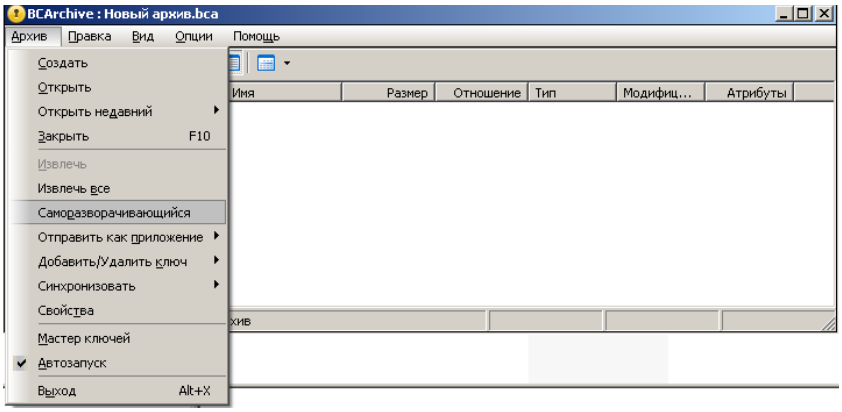

Рисунок 10 – Для открытия архива на компьютере, на котором не установлена программа, создаем самораспаковывающейся архив.

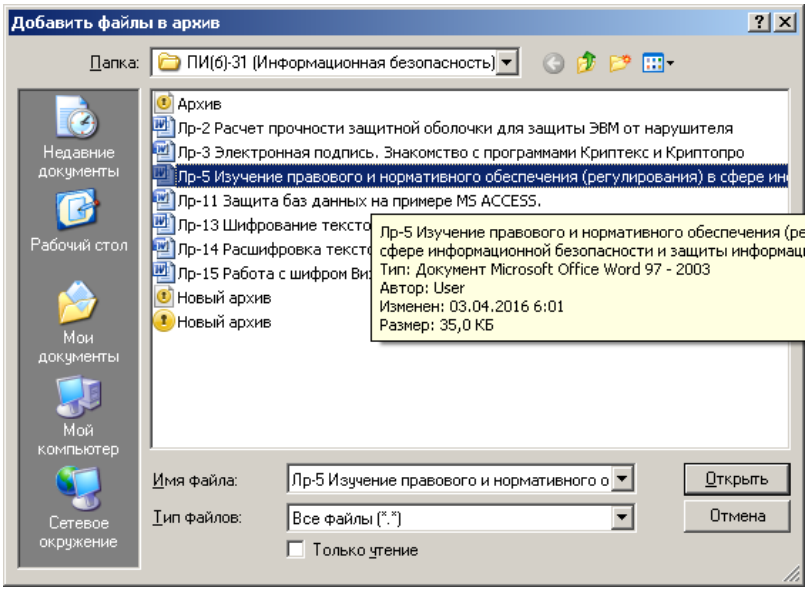

Рисунок 11 – В зашифрованный архив можно добавлять файлы, папки

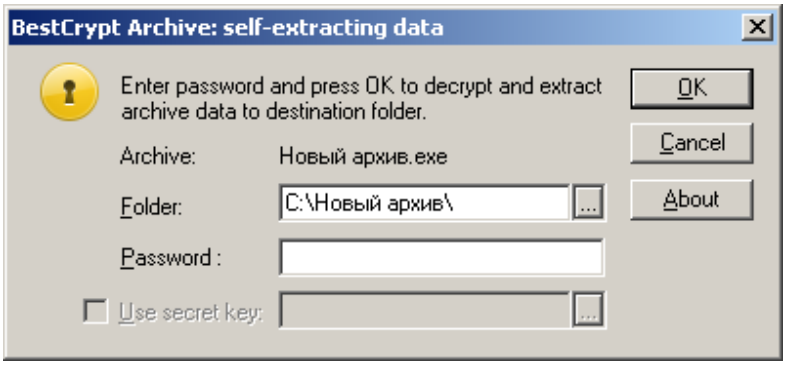

Рисунок 12 – Для того чтобы открыть самораспаковывающейся архив, вводим пароль

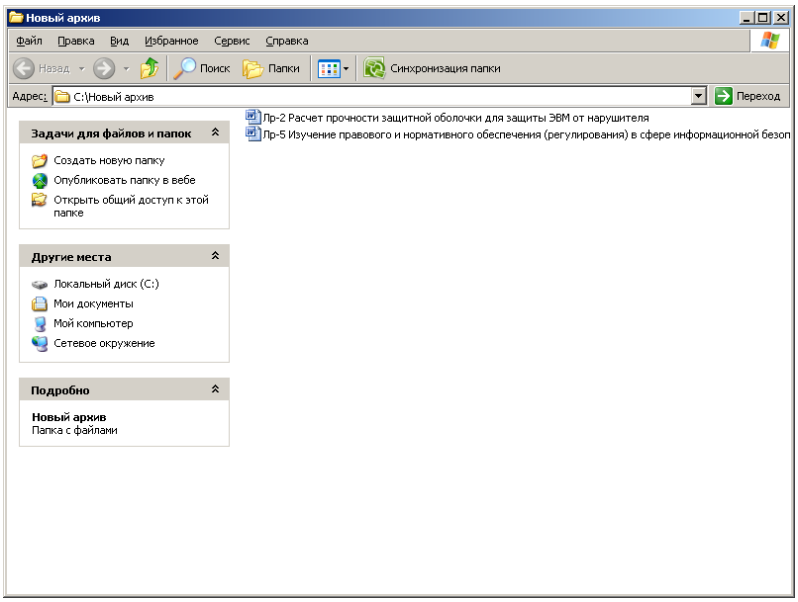

Рисунок 13 – Открытый архив.

Контрольные вопросы:

1. Назовите способы создания архивного файла.
2. Преимущества самораспаковывающегося архива
3. Какие типы шифрования используются в программе?
4. Назовите недостатки программы.