1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский Политехнический Университет Петра Великого
3. —
4. Институт кибербезопасности и защиты информации

**ЛАБОРАТОРНАЯ РАБОТА № 2**

1. «СЕРВИСЫ MS WINDOWS»
2. по дисциплине «Безопасность современных информационных технологий»
3. Выполнил
4. студент гр. 4851003/00002 Вологдин М.В.

<*подпись*>

1. Преподаватель Дахнович А.Д.

<*подпись*>

1. Санкт-Петербург
2. 2022
3. **Цель работы**

Получить навыки работы с сервисами Windows.

Написать программу, работающую в качестве сервиса (службы) Windows (версии 7–10). Программа должна осуществлять резервное копирование данных из указанной директории.

1. **Ход работы**

1)Настройка работы сервиса aBackupService

Сначала реализуем функции, управляющие сервисом. Функция \_tmain является точкой входа, она осуществляет инициализацию необходимых параметров(например, таблицу сервиса), далее соединяет основной поток процесса службы с диспетчером управления службами, в результате чего поток становится потоком диспетчера управления службами для вызывающего процесса. Основной исполняемой функцией сервиса является функция ServiceMain. Кроме того, в зависимости от аргументов командной строки программа может выполнить установку, старт, остановку и удаление сервиса по имени сервиса и пути его исполняемого файла.

Сервису присвоено название “aBackupService”, исполняемый файл – C:\Users\volog\source\repos\bsit\Release\bsit.exe

С помощью команды bsit install устанавливаем сервис, на рисунках 1(до) и 2(после) можно увидеть, что в списках служб появилась установленная нами новая служба “aBackupService”.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 1 – Список служб до установки

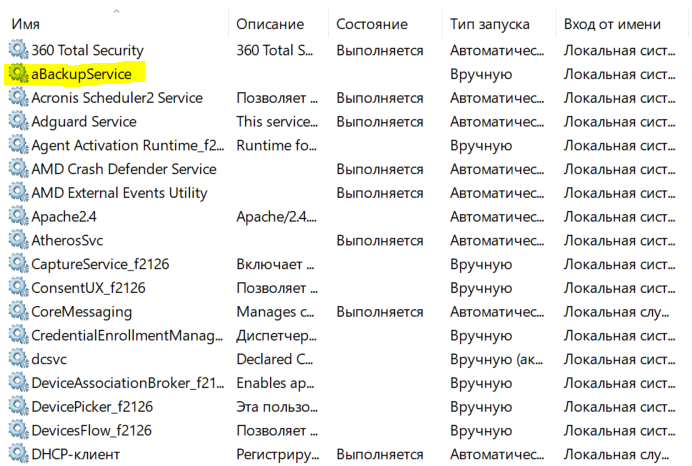


Рисунок 2 – Список служб после установки

Далее с помощью команды bsit start запускаем сервис: начинает выполняться алгоритм, который описан в ранее упомянутой функции ServiceMain.

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 3 – Состояние сервиса после запуска

С помощью функции bsit stop выполняем остановку сервиса, итоговый результат будет аналогичен результату с рисунка 2.

И последней управляющей функцией является bsit remove, которая удаляет сервис из списка служб, итоговая картина аналогична рисунку 1.

2)Основным алгоритмом сервиса является создание резервной копии некоторой директории. Для регулировки работы используется конфигурационный файл, который содержит в себе:

-Имя директории, из которой выполняется резервное копирование;

-Имя файла-архива и директории, в которой он должен находиться;

-Маски/имена файлов, помещаемых в резервную копию.

Для реализации архивации была выбрана библиотека libzip, которая прекрасно подходит для архивации вложенных папок.

Основной алгоритм работы архивации:

1. Из конфигурационного файла считываются входные данные
2. С помощью рекурсивной функции находятся и сохраняются все файлы, которые лежат внутри исходной директории. Далее все файлы проходят проверку на соответствие маскам, сохраняются только подходящие.
3. Создаётся/открывается архив по нужному адресу
4. Далее файлы добавляются в архив с учётом вложенности папок, с флагом перезаписи, чтобы внести все изменения
5. После этого происходит проверка актуальности всех имеющихся файлов в архиве: файлы, неподходящие под маски удаляются из архива.
6. Архив закрывается
7. Переход к шагу 1

Стоит заметить, что действие происходит циклично, в первой итерации архив создаётся, далее он просто открывается.

1. **Тестирование**

Изображение выглядит как текст

Автоматически созданное описание

Рисунок 4 – Пример конфигурационного файла

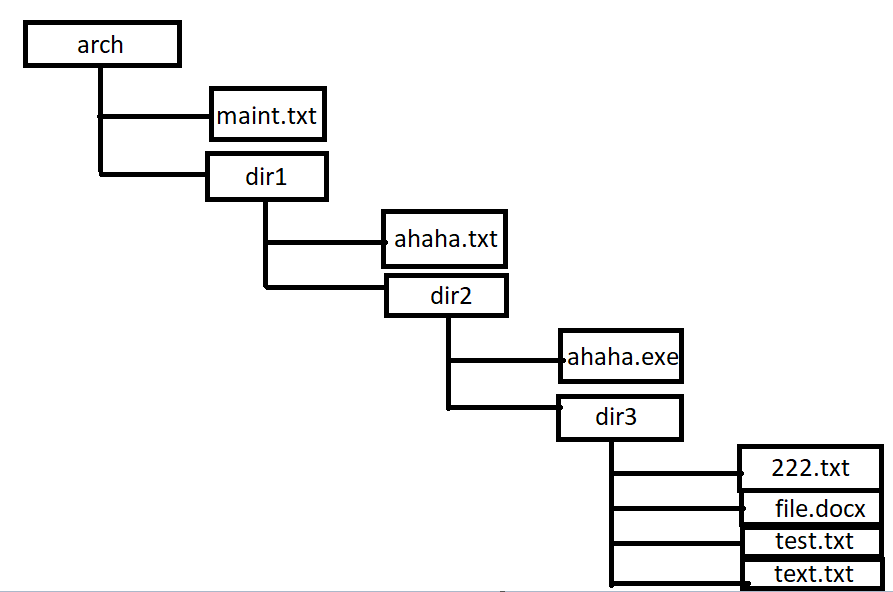


Рисунок 5 – Исходная иерархия архивируемой директории

Под действием масок ????.\* и \*.doc\* архивируются файлы file.docx, text.txt и test.txt.

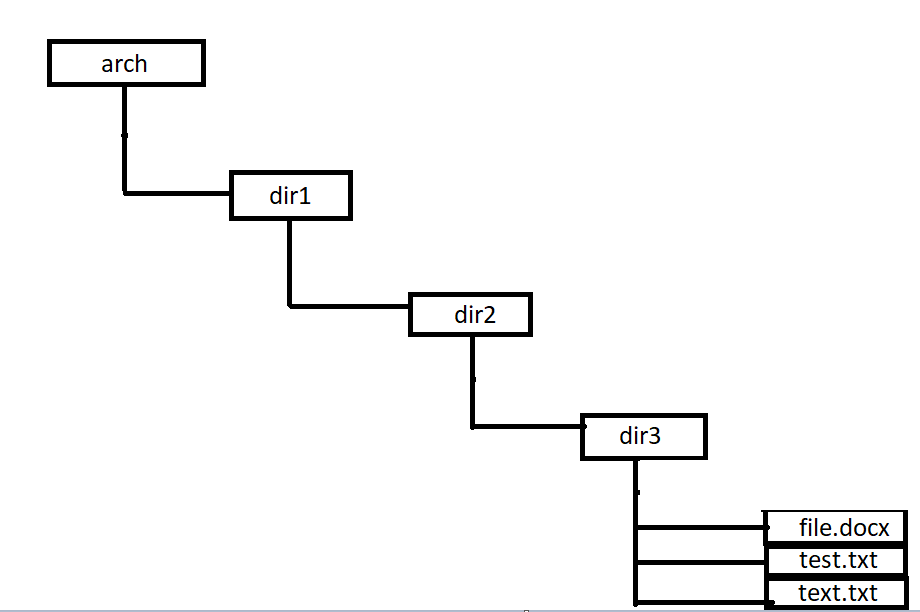


Рисунок 6 – Итоговая иерархия полученного архива

1. **Контрольные вопросы**

**Какие операции выполняются при установке сервиса в систему?**

Сначала необходимо зарегистрировать сервис в системе, для этого вызывается Windows-функция CreateService.

Регистрируя сервис через эту функцию программа посылает SCM сообщение о том, где будет находиться данный сервис.

Затем SCM создает в реестре раздел для сервиса по адресу HKLM\SYSTEM\CurrentControl-Set\Services

Зарегистрировав сервис, программа установки или управляющее приложение может запустить его через функцию StartService.

**Что такое SCP и зачем необходимо его реализовывать?**

Программы управления сервисами (service control programs, SCP) — стандартные Windows-приложения, использующие SCM-функции управления сервисами CreateService, OpenService, StartService, Controfiervice, QueryServiceStatus и DeleteService. Для вызова SCM-функций SCP сначала должна установить канал связи с SCM через функцию OpenSCManager.

## Какие возможности по управлению сервисами НЕ предоставляет оснастка "Службы"?

В оснастке службы есть не все возможности по управлению сервисами. Так, например, для того чтобы сервис появился в самой оснастке его в любом случае необходимо установить из консоли. Далее, в конце работы там также не будет функции удаления сервиса и эту команду придётся совершать из командной строки.

1. **Выводы**

В ходе выполнения лабораторной работы были получены навыки работы с сервисами Windows. Была написана программа, работающая в качестве сервиса, выполняющего резервное копирование директории. Также были получены навыки установки библиотек с помощью vcpackage, и разработан алгоритм архивации с помощью библиотеки libzip.