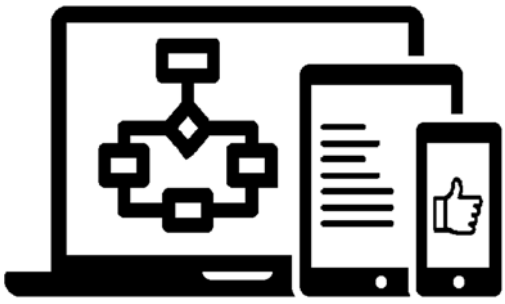
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Программное обеспечение информационных технологий»

ОПЕРАЦИОННЫЕ СИСТЕМЫ

Методические рекомендации к лабораторным работам для студентов направления подготовки 01.03.04 «Прикладная математика» дневной формы обучения

Часть 2



Могилев 2023

УДК 004.7
ББК 32.973.26
О60

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Программное обеспечение информационных технологий» «28» марта 2023 г., протокол № 9

Составитель ст. преподаватель Е. А. Зайченко

Рецензент Ю. С. Романович

Изложены рекомендации к выполнению лабораторных работ для студентов направления подготовки 01.03.04 «Прикладная математика» дневной формы обучения по дисциплине «Операционные системы». Приведен перечень необходимой литературы.

Учебное издание

ОПЕРАЦИОННЫЕ СИСТЕМЫ

Часть 2

Ответственный за выпуск	В. В. Кутузов
Корректор	Т. А. Рыжикова
Компьютерная верстка	Н. П. Полевничая

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 21 экз. Заказ №

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, г. Могилев.

Содержание

11 Лабораторная работа № 11. Изучение основных возможностей Windows PowerShell 4
12 Лабораторная работа № 12. Разработка сценариев Windows PowerShell 5
13 Лабораторная работа № 13. Установка виртуальной машины. Работа с файловыми системами и дисками 7
14 Лабораторная работа № 14. Изучение методов шифрования ОС Windows данных на дисках 8
15 Лабораторная работа № 15. Изучение средств защиты ОС Windows 9
16 Лабораторная работа № 16. Изучение методов аудита ОС Windows 13
Список литературы 14

Часть 2

10 Лабораторная работа № 11. Изучение основных возможностей Windows PowerShell

Цель работы: получить навыкие работы с командной оболочкой Windows PowerShell.

Теоретические сведения

1 Работа в среде командной оболочки Microsoft PowerShell [1, с. 9–16].
2 Командлеты PowerShell [1, с. 19–26].

Практическое задание

Изучив справку по командлетам Get-Process и Get-Service, а также возможности конвейера, фильтрации и сортировки, выполните задание, согласно варианту.

1 Получите список пяти процессов, которые наиболее активно используют процессорное время. Выводить имя процесса, объем процессорного времени и идентификатор процесса (ID).

2 Получите список 10 процессов, которые наиболее активно используют файл подкачки. Выведите имя процесса, идентификатор процесса (ID) и объем виртуальной памяти, используемой процессом.

3 Получите список служб (сервисов), установленных в системе, которые находятся в рабочем состоянии.

4 Получите список служб (сервисов), установленных в системе, которые находятся в рабочем состоянии, отсортировав их по свойству displayName.

5 Получите список пяти процессов, имеющих наименьший объем выгружаемой памяти. Выведите имя процесса, идентификатор процесса (ID) и объем выгружаемой памяти (PM).

6 Получите список процессов, отсортировав их по возрастанию количества открытых дескрипторов. Выведите только имя процесса и свойство Handles.

7 Получите список 15 процессов, имеющих наибольший объем невыгружаемой памяти. Выведите имя процесса, идентификатор процесса (ID) и объем выгружаемой памяти (NPM).

8 Получите список служб (сервисов), установленных в системе, которые остановлены.

9 Получите список процессов, использовавших процессорное время менее 1 с, отсортировав их возрастанию ID.

10 Выведите список служб (сервисов), запущенных в системе, чтобы сначала были работающие сервисы, а затем остановленные.

Контрольные вопросы

1 В чем отличие Windows PowerShell от традиционного интерфейса командной строки?

2 Что такое командлет?

3 Приведите примеры использования алиасов.

12 Лабораторная работа № 12. Разработка сценариев Windows PowerShell

Цель работы: получить навыки разработки сценариев Windows PowerShell.

Теоретические сведения

1 Работа с устройствами и файловой системой в PowerShell [1, с. 20–23].

2 Работа с объектами в PowerShell [1, с. 23–34].

3 Сценарии [1, с. 34–44].

Практическое задание

Разработайте сценарии PowerShell. Номера задач для каждого варианта представлены в таблице 12.1.

Таблица 12.1 – Варианты заданий

Вариант	Номер задачи
1	1, 6
2	2, 7
3	3, 8
4	4, 9
5	5, 10
6	1, 10
7	2, 9
8	3, 8
9	4, 7
10	5, 6

1 Проверьте, существует ли системный журнал событий, если нет, выведите на экран красным цветом сообщение об ошибке. В текстовый файл перепишите из журнала события, которые имеют тип EntryType «Error», черным цветом, а события, которые имеют тип «Information» зеленым.

2 Проверьте, существует ли системный журнал событий, если да, выведите на экран зеленым цветом сообщение. В текстовый файл перепишите из журнала события, которые имеют тип EntryType «Warning», черным цветом, а события, которые имеют тип «Information», желтым.

3 Проверьте, существует ли журнал событий WindowsPowerShell. Сгруппируйте сообщения по коду ID сообщения, а затем отсортируйте последние 15 записей в системном журнале событий по коду ID в нисходящем порядке. Результат запишите в текстовый файл.

4 Найдите имя журнала событий WindowsPowerShell. Сгруппируйте сообщения журнала по источнику (Source) сообщения, а затем отсортируйте последние 15 записей в системном журнале событий по коду ID в нисходящем порядке. Результат запишите в текстовый файл.

5 Проверьте, существует ли системный журнал событий, если да, выведите на экран зеленым цветом сообщение. Сгруппируйте сообщения журнала по типу EntryType, а внутри группы отсортируйте в порядке убывания времени возникновения Time.

6 Создайте в папке, где имеются файлы с различными расширениями, отдельные подпапки, поместив в каждую папку однотипные файлы.

7 Создайте в папке, где имеются файлы с различными датами создания, отдельные подпапки, в названии должна быть дата (например, «Отчеты01-01-21»), переместив в каждую папку файлы с одинаковой датой.

8 Создайте в папке, где имеются файлы различного размера, отдельные подпапки, поместив в каждую папку файлы по размерам (например, папка «МеньшеГб» и «БольшеГб»).

9 Имеется папка, где находятся файлы с однотипными именами (например, «Отчет_Май», «Отчет_Июнь», «Заявка_Май», «Заявка_Сентябрь» и т. п.). Создайте папки по начальным именам файлов («Отчеты», «Заявки» и т. п.) и переместите туда имеющиеся файлы.

10 Создайте в папке, где имеются файлы с различными атрибутами, отдельные подпапки, в названии должно быть отражено название атрибута (например, «Скрытые», «Системные» и т.д.), переместив в каждую папку соответствующие файлы.

Контрольные вопросы

1 Какие типы операций могут сохраняться в системном журнале?

2 Какое расширение используется для скриптов PowerShell?

3 Какие права доступа должны быть заданы при создании сценария?

4 Каким образом можно акцентировать внимание пользователя на выводимых результатах выполнения скрипта?

13 Лабораторная работа № 13. Установка виртуальной машины. Работа с файловыми системами и дисками

Цель работы: получение практических навыков выполнения операций с дисками, а также самостоятельной работы с информацией о соответствующих командах ОС.

Теоретические сведения

1 Виртуализация. Множественные прикладные среды [1, с. 345–352].
2 Файловые системы [2, с. 424–443].

Практическое задание

1 Установить виртуальную машину. Установить в виртуальной машине операционную систему Windows 8/10. Виртуальная машина должна иметь название «FIO_OS». Пользователь ОС должен иметь имя «FIO». Установленная ОС должны позволять использовать:
– CDROM;
– USB-накопитель.
Свойства виртуальной машины привести в отчете.
2 С помощью оснастки «Управление дисками» определить характеристики установленных в системе физических и логических устройств, привести их в отчете.
3 С помощью оснастки «Управление дисками» создать на основном диске новый том, присвоив ему имя и метку, последовательность действий привести в отчете.
4 Изучить справку работе с утилитой DiskPart. Создать виртуальный диск (.vhd), отформатировать его под файловую систему NTFS, присвоить имя и метку (label). В отчете привести последовательность выполненных для этого команд.
5 Изучить справку по работе с утилитой fsinfo. С ее помощью определить размер кластеров всех имеющихся в системе дисков (C:, D:, CDROM), представить в отчете.
6 Выбрать файл для исследований, с помощью утилиты fsinfo определить количество экстентов, занимаемых этим файлом.
7 С помощью справки Windows изучить виды дисковых пространств и их характеристики.
8 Назначить квоту диска, созданного в п. 3, для имеющегося в системе пользователя. Привести скриншот записи квот и скриншот команды fsutil quota query.

Контрольные вопросы

1 В чем отличие понятий «физическое» и «логическое» форматирование диска?
2 Дайте определение кластера файловой системы.
3 Дайте определение понятия «том».

4 Какие средства можно использовать для создания нового логического диска?

5 Как можно присвоить логическому диску метку (имя)?

6 Какой размер кластера может использоваться в файловой системе NTFS?

7 Что такое отрезок (экстент) в файловой системе NTFS?

8 Перечислите основные системные файлы NTFS и поясните их назначение.

9 Что такое виртуальный диск? Как его создать?

10 Какие действия необходимо выполнить, чтобы привести виртуальный диск в рабочее состояние?

11 Что такое пул носителей?

12 Как на производительность дискового пространства влияет параметр «устойчивость»?

13 Для каких целей используются квоты диска?

14 Лабораторная работа № 14. Изучение методов шифрования ОС Windows данных на дисках

Цель работы: изучить методы шифрования ОС Windows данных на дисках.

Теоретические сведения

1 Безопасность ОС Windows [2, с. 926–930].

2 Шифрующая файловая система EFS [1, с. 198–202].

Практическое задание

1 Запустите ОС Windows версий 7/8/10 на виртуальной машине.

2 Выберите папку для шифрования. Папка должна называться по фамилии студента. Выполните шифрование файлов в выбранной папке. Сохраните сертификат в отдельном файле, чтобы иметь в дальнейшем возможность дешифрации файла при любых условиях. Убедитесь, что после этого был создан сертификат пользователя, запустив оснастку certmgr.msc от имени пользователя (раздел Личное). Просмотрите и добавьте в отчет основные параметры сертификата открытого ключа пользователя (срок действия, используемые алгоритмы).

3 Выполните шифрование и расшифрование файлов с помощью команды cipher группы файлов с использованием шаблона имени или расширения файлов.

4 Создайте на виртуальной машине новый раздел диска, отформатированный под NTFS. Скопируйте на новый раздел папку с файлами. Установите защиту созданного раздела с помощью BitLocker. Архивацию ключа восстановления выполните в файл, который должен находиться не на шифруемом диске.

5 Убедитесь, что доступ к диску без пароля невозможен.

6 С помощью утилиты manage-bde.exe получите сведения о имеющихся томах системы, их состоянии, перенаправив информацию в файл.

7 Выполните отключение BitLocker с помощью утилиты manage-bde.exe, убедитесь, что информация на диске доступна.

Контрольные вопросы

1 Каким образом реализуется шифрование файлов в NTFS?
2 Каким образом шифруются файлы в файловой системе EFS?
3 Что такое FEK, DDF, DDR?
4 Какие алгоритмы шифрования используются в EFS?
5 Каким образом реализуется шифрование дисков?
6 В чем отличие шифрование с помощью cipher и manage-bde?
7 Позволяет ли шифрование файлов обеспечить их защиту при передаче по сети?
8 Что произойдет с защифрованным файлом при копировании на флеш-память с файловой системой FAT32?

15 Лабораторная работа № 15. Изучение средств защиты ОС Windows

Цель работы: изучить средств защиты, права и разрешения ОС Windows.

Теоретические сведения

1 Управление доступом к ресурсам [2, с. 669–677].
2 Назначение разрешений для файлов [1, с. 187–190].
3 Назначение разрешений для папок [1, с. 190–193].

Практическое задание

1 Запустите ОС Windows версий 7/8/10 на виртуальной машине. Войдите в систему под учетной записью администратора.
2 Создайте учетную запись нового пользователя User1 в оснастке «Управление компьютером» (compmgmt.msc).
Обязательно введите пароль при создании пользователя!
При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу «Group1» и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске C: папку Lab10. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).
3 С помощью команды runas запустите сеанс командной строки (cmd.exe) от имени вновь созданного пользователя.
При вводе пароля пользователя он не отображается!
Командой whoami посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя. Дайте пояснения информации, содержащейся в полученных SID.
4 Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, каким пользователям в системе присвоены

SID, соответствующие шаблону S-1-5-21-*-*-100* (используйте ключ реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList).

5 Командой whoami определите перечень текущих привилегий пользователя User1. Попробуйте изменить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» раздела Локальные политики -> Назначение прав пользователя. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. Попробуйте изменить системное время командой time.

6 Убедитесь, что привилегия «Завершение работы системы» (SeShutdownPrivilege) предоставлена пользователю User1 . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой shutdown –s. Добавьте ему привилегию «Принудительное удаленное завершение» (SeRemoteShutdownPrivilege).

Приготовьтесь отменить команду завершения!

Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой shutdown –a).

7 Просмотрите разрешения пользователям и группам на папку c:\ Lab10. Используйте графический интерфейс:

а) разрешите пользователю User1 запись в папку Lab10, но запретите запись для группы Group1. Попробуйте записать файлы или папки в Lab10 от имени пользователя User1. Объясните результат. Посмотрите эффективные (действующие) разрешения пользователя User1 к папке Lab10 в окне свойств папки;

б) используя стандартное окно свойств папки, задайте для пользователя User1 такие права доступа к папке, чтобы он мог записывать информацию в папку Lab10, но не мог просматривать ее содержимое. Проверьте, что папка Lab10 является теперь для пользователя User1 «слепой», запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки;

в) для вложенной папки Lab10\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка Lab10\Docs перестала быть «слепой» (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл);

г) снимите запрет на чтение папки Lab10 для пользователя User1;

д) запретите пользователю все права на доступ к папке Lab10 и разрешите полный доступ к вложенной папке Lab10\Docs. Убедитесь в доступности папки Lab10\Docs для пользователя. Удалите у пользователя User1 привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке Lab10\Docs. Объясните результат.

8 Создайте для папки Lab10 SACL, позволяющий протоколировать отказы и успехи доступа к этой папке со стороны пользователя User1 (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита

включен). Запретите пользователю User1 запись в папку Lab10. Попробуйте от имени пользователя User1 просмотреть содержимое папки, скопировать в нее файлы. Убедитесь, что записи аудита были размещены в журнале безопасности (eventvwr.msc).

9 Создайте пользователя по имени User2. Создайте каталоги «Public» и «Private». В каждый из этих каталогов скопируйте исполняемый файл (с расширением .exe, .bat или .cmd) и текстовый файл.

Напишите командный файл, в котором с помощью команд разграничьте доступ к созданным каталогам и файлам в соответствии со своим вариантом (рисунок 15.1). В отчете приведите код файла и результат его работы.

Вариант1			
Субъекты	**Объекты**		
	Каталог **Public**	Каталог **Private**	Текстовый файл в «**Private**»
Администратор	Полный доступ	Чтение	Нет доступа
User1	Чтение	Изменить, кроме удаления	Изменить
User2	Изменить	Нет доступа	Нет доступа
Вариант 2			
Субъекты	**Объекты**		
	Каталог **Public**	Каталог **Private**	Исполняемый файл в «**Private**»
Администратор	Полный доступ	Чтение и выполнение	Изменить
User1	Изменить	Чтение	Выполнение
User2	Чтение и выполнение	Изменить	Нет доступа
Вариант 3			
Субъекты	**Объекты**		
	Каталог **Public**	Каталог **Private**	**Текстовый файл в «Private»**
Администратор	Полный доступ	Список содержимого	Нет доступа
User1	Чтение	Изменить, кроме удаления	Изменить
User2	Изменить	Нет доступа	Нет доступа
Вариант 4			
Субъекты	**Объекты**		
	Каталог **Public**	Каталог **Private**	**Текстовый файл в «Private»**
Администратор	Изменить	Чтение и выполнение	Нет доступа
User1	Чтение	Изменить	Запрет удаления
User2	Полный доступ, кроме смены владельца	Запись	Нет доступа
Вариант 5			
Субъекты	**Объекты**		
	Каталог **Public**	Каталог **Private**	**Исполняемый файл в «Private»**
Администраторг	Полный доступ	Список содержимого	Выполнение
User1	Чтение	Чтение и удаление	Выполнение, запрет удаления
User2	Изменить, кроме удаления	Запись	Нет доступа

Рисунок 15.1 – Варианты для разработки командного файла

Вариант 6			
Субъекты	Объекты		
	Каталог Public	Каталог Private	Исполняемый файл в «Private»
Администратор	Полный доступ	Чтение	Изменить
User1	Чтение и удаление	Список содержимого	Выполнение
User2	Изменить	Нет доступа	Нет доступа
Вариант 7			
Субъекты	Объекты		
	Каталог Public	Каталог Private	Текстовый файл в «Public»
Администратор	Список содержимого	Полный доступ	Нет доступа
User1	Изменить, кроме удаления	Чтение	Изменить
User2	Нет доступа	Изменить	Нет доступа
Вариант 8			
Субъекты	Объекты		
	Каталог Public	Каталог Private	Текстовый файл в «Private»
Администратор	Чтение и выполнение	Изменить	Нет доступа
User1	Изменить	Чтение	Изменить, запрет изменения дополнительных атрибутов
User2	Запись	Изменить, кроме удаления	Нет доступа
Вариант 9			
Субъекты	Объекты		
	Каталог Public	Каталог Private	Исполняемый файл в «Private»
Администратор	Список содержимого	Полный доступ	Выполнение
User1	Чтение и удаление	Чтение	Выполнение, запрет удаления
User2	Запись	Полный доступ	Нет доступа
Вариант 10			
Субъекты	Объекты		
	Каталог Public	Каталог Private	Исполняемый файл в «Private»
Администратор	Чтение	Полный доступ	Изменить
User1	Список содержимого	Чтение и удаление	Выполнение
User2	Нет доступа	Изменить	Нет доступа

Окончание рисунка 15.1

Контрольные вопросы

1 Каким образом реализуется защита файлов в NTFS?

2 Перечислите стандартные права доступа к файловым объектам, существующие в файловой системе NTFS.

3 Объясните принцип работы разрешения «Запись».

4 Перечислите элементы разрешений.

5 Кто может стать владельцем объекта?

6 Как отключить наследование разрешений?

7 Перечислите приоритеты применения разрешений при определении действующих разрешений на доступ к файловым объектам.

16 Лабораторная работа № 16. Изучение методов аудита ОС Windows

Цель работы: изучеть методы аудита ОС Windows.

Теоретические сведения

1 Управление доступом к ресурсам [2, с. 669–677].

2 Средства защиты информации в ОС [3, с. 165–178].

Практическое задание

1 Запустите ОС Windows версий 8/10 на виртуальной машине.

2 Войдите в систему с учетной записью администратора.

3 Активизируйте средствами политики безопасности аудит доступа к объекту (Успех и Отказ).

4 Создайте временную папку (ФИО студента) и текстовый файл внутри ее.

5 Выберите эту папку как объект аудита.

6 Настройте аудит доступа к папке для администратора и пользователя компьютера, ограничив пользователя в возможных действиях с папкой и файлом, чтобы в ряде случаев происходило событие Отказ.

7 Выполните ряд типовых действий с папкой и файлом от имени администратора и затем от имени пользователя.

8 Прочитайте журнал событий Безопасности и найдите в нем записи, в которых отражены Ваши действия с объектами как от имени администратора, так и от имени пользователя. Сделайте соответствующие выводы.

9 Результаты в виде экранов и текстов должны быть сохранены в файле отчета по лабораторной работе и представлены к защите.

10 Самостоятельно освойте настройку аудита для принтеров.

Контрольные вопросы

1 Какова роль аудита в обеспечении безопасности компьютерной системы?

2 Где и каким образом формируется информация о событиях аудита?

3 Какая информация может быть получена в результате аудита?

4 Какие типы аудита Вы знаете и для чего предназначен каждый из них?

5 Каким образом активизируется политика аудита?

6 Каким образом политика аудита применяется для выбранных объектов и пользователей?

7 В каких случаях целесообразно учитывать Успех, а когда целесообразно фиксировать Отказ?

8 Как пользоваться журналами безопасности?

9 Какие учетные записи дают право на настройку аудита и проверку результатов аудита?

10 Каким образом администратор может использовать информацию об аудите для повышения безопасности системы?

Список литературы

1 **Назаров, С. В.** Операционные системы. Практикум : учебное пособие / С. В. Назаров, Л. П. Гудыно, А. А. Кириченко. – Москва : КНОРУС, 2012. – 376 с.

2 **Таненбаум, Э.** Современные операционные системы/ Э. Таненбаум, Х. Бос. – Санкт-Петербург: Питер, 2015. – 1120 с.

3 Защита информации: учебное пособие / А. П. Жук [и др.]. – 3-е изд. – Москва : РИОР; ИНФРА-М, 2021. – 400 с.