Лабораторная работа №2

Изучение программных средств защиты от несанкционированного доступа и разграничения прав пользователей

Содержание задания

1. Запустить программы просмотра и редактирования реестра Windows regedit.exe и regedt32.exe (с помощью команды «Выполнить» главного меню). Ознакомиться со структурой реестра, включить в отчет краткие сведения о содержании основных разделов реестра (HKEY_CURRENT_USER и HKEY_LOCAL_MACHINE). Включить в отчет сведения о различиях в функциональных возможностях изученных программ редактирования реестра. Включить в электронную версию отчета копии экранных форм, иллюстрирующих использование редакторов реестра.

Примечание: в операционную систему Windows XP Professional включен один редактор реестра, который можно запустить с помощью любого из указанных выше имен.

2. Скопировать в произвольную папку на диске рабочей станции файл rt.zip из указанного преподавателем сетевого диска.
3. Извлечь файлы из скопированного в пункте 2 архива.
4. Запустить программу restrick.exe, позволяющую ограничить возможности пользователей ОС Windows. Включить в отчет сведения о назначении и основных функциях программы. С помощью редактора реестра найти и отразить в отчете разделы реестра Windows, хранящие информацию о выбранной политике безопасности. Включить в отчет ответ на вопрос, какое ограничение на работу пользователя должно быть обязательно установлено, чтобы обеспечить минимальную эффективность рассмотренных и аналогичных средств. Включить в электронную версию отчета копии экранных форм, используемых при работе с программой restrick.exe. Завершить работу с программой restrick.exe.
5. Заблокировать работу с используемой рабочей станцией на период временного отсутствия пользователя. Разблокировать работу рабочей станции. Включить в отчет сведения о порядке защиты рабочей станции на период временного отсутствия пользователя и о других функциях операционной системы, доступных при этом наряду с блокировкой.
6. Открыть (или создать) произвольный документ в текстовом процессоре Word. Изучить порядок использования паролей для защиты документов в Microsoft Word и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Word.
7. Открыть (или создать) произвольную таблицу Excel. Изучить порядок использования паролей для защиты документов в табличном процессоре Microsoft Excel и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с Excel.
8. Скопировать в произвольную папку на локальном жестком диске файл whisper.zip из указанного преподавателем сетевого диска.
9. Запустить программу Setup для установки программы Whisper 32 (непосредственно из архива, скопированного в пункте 8, без его распаковки).

10. Запустить программу whisper.exe, предназначенную для создания и ведения базы данных паролей пользователя. Изучить назначение и основные функции программы и включить в отчет соответствующие сведения. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта. Завершить работу с программой whisper.exe.
11. Ознакомиться (на примере папок, созданных в папке c:\ Documents and Settings \ *Имя пользователя* \ Документы и в папке c:\ Documents and Settings \ All Users \ Документы) с порядком разграничения доступа к ресурсам в защищенных версиях операционной системы Windows (с помощью контекстного меню объекта и элементов управления соответствующих диалоговых окон). Если команда «Общий доступ и безопасность» недоступна (при работе в ОС Windows XP Professional), то выключить режим «Использовать простой общий доступ к файлам» на вкладке «Вид» окна свойств папки. Включить в отчет сведения об особенностях управления доступом к папкам и файлам в этих ОС. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.
12. Ознакомиться (с помощью Панели управления Windows и редактора реестра) с порядком разграничения доступа к принтерам и разделам реестра. Включить в электронную версию отчета копии экранных форм, использованных при выполнении данного пункта.
13. Ознакомиться (с помощью функции Панели управления Администрирование | Управление компьютером) с порядком создания и изменения учетных записей пользователей и групп в защищенных версиях операционной системы Windows. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
14. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Локальные политики | Назначение прав пользователя) с порядком назначения прав пользователям и группам. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
15. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика паролей) с порядком определения параметров безопасности для парольной аутентификации. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
16. Ознакомиться (с помощью функции Панели управления Администрирование | Локальная политика безопасности | Политики учетных записей | Политика блокировки учетных записей) с порядком определения параметров безопасности для политики блокировки учетных записей. Включить в отчет соответствующие сведения. Включить в электронную версию отчета копии соответствующих экранных форм.
17. Включить в отчет ответы на контрольные вопросы, номера которых выбираются в соответствии с номером варианта.
18. Включить в отчет титульный лист и сохранить файл с электронной версией отчета в произвольной папке на локальном жестком диске.

19. После проверки отчета преподавателем удалить файл с электронной версией отчета и файл программы Restrick, удалить программу Whisper 32 с помощью Панели управления Windows, удалить файлы архивов rt.zip и whisper.zip.
20. Завершить работу с ОС Windows.

Контрольные вопросы

1. Какой из изученных в лабораторной работе редакторов реестра предоставляет функции по разграничению доступа к разделам реестра и как использовать эти функции?
2. Полномочия какого из пользователей ограничиваются с помощью программы restrick.exe?
3. В чем разница между функциями программы restrick.exe «Restrict “Run program” window» и «Restrict “Run” command»?
4. Как с помощью программы restrick.exe ограничить доступ пользователей к дисковым устройствам?
5. Как ограничить доступ пользователей к функциям Панели управления с помощью программы restrick.exe?
6. Доступ к каким функциям Панели управления может быть ограничен с помощью программы restrick.exe?
7. В чем недостаточность средств ограничения прав пользователей, предоставляемых программой restrick.exe?
8. Как может быть заблокирована рабочая станция на период временного отсутствия пользователя? Укажите несколько вариантов.
9. Какой из способов блокирования рабочей станции на период временного отсутствия пользователя является наиболее безопасным и почему?
10. Как устанавливается защита от чтения документов Microsoft Word и таблиц Microsoft Excel?
11. Как реализована (в чем выражается) защита документов Microsoft Office от чтения с помощью паролей?
12. Насколько надежна защита документов Microsoft Office от чтения с помощью паролей?
13. Как устанавливается защита от изменения документов Microsoft Word и таблиц Microsoft Excel?
14. Как реализована (в чем выражается) защита документов Microsoft Office от изменения с помощью паролей?
15. Насколько надежна защита документов Microsoft Office от изменения с помощью паролей?
16. Как создать новую базу данных паролей с помощью программы whisper.exe и защитить ее от несанкционированного доступа?
17. Как реализована (в чем выражается) защита базы данных паролей программы whisper.exe?
18. Как добавить новый пароль в базу данных программы whisper.exe?
19. Какая информация указывается при добавлении новой записи в базу данных программы whisper.exe?
20. Для чего в программе whisper.exe предназначена функция Generate?
21. Для чего предназначены элементы управления в окне автоматической генерации паролей программы whisper.exe?

22. Как скрыть отображаемые на экране пароли из базы данных программы whisper.exe, но при этом сохранить возможность их переноса в требуемую программу?
23. Какие права доступа к личным и разделяемым файлам и папкам устанавливаются операционной системой по умолчанию?
24. Кто может управлять разрешениями на доступ к ресурсу?
25. Какая информация содержится в дескрипторе безопасности объекта?
26. Какая модель разграничения доступа к объектам реализована в защищенных версиях операционной системы Windows?
27. В чем основные недостатки модели разграничения доступа к объектам, реализованной в защищенных версиях операционной системы Windows?
28. Какие специфические права доступа могут быть определены для принтера?
29. Какие специфические права доступа могут быть определены для раздела реестра?
30. Какие разрешения на доступ к принтеру установлены в системе и почему?
31. Какие установлены разрешения на доступ к разделу реестра HKEY_LOCAL_MACHINE и почему?
32. Какие установлены разрешения на доступ к разделам реестра HKEY_CURRENT_USER и HKEY_CURRENT_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies и почему?
33. Кто управляет разрешениями на доступ к принтерам и почему?
34. Кто управляет разрешениями на доступ к разделам реестра и почему?
35. Какие из объектов могут наследовать разрешения на доступ к ним и от кого?
36. Для чего предназначены параметры создаваемой учетной записи пользователя?
37. В чем разница между отключением и блокировкой учетной записи?
38. В чем целесообразность разбиения множества пользователей на группы?
39. Как назначаются права пользователям и группам в защищенных версиях операционной системы Windows?
40. Какие требования по сложности могут предъявляться к паролям в операционной системе Windows?
41. Для чего предназначены параметры парольной аутентификации, связанные с установкой минимального срока действия и неповторяемости паролей?
42. Какие параметры могут быть установлены для политики блокировки учетных записей?
43. Для чего предназначены параметры политики блокировки учетных записей?
44. В чем слабость парольной аутентификации?
45. Как может быть повышена надежность аутентификации с помощью паролей?
46. Какой может быть реакция системы на попытку подбора паролей?
47. Кому может быть разрешен доступ по чтению ко всей базе учетных записей пользователей и почему?
48. Кому может быть разрешен доступ по записи к базе учетных записей пользователей и почему?

Варианты для выбора номеров контрольных вопросов

№	Номера вопросов	№	Номера вопросов	№	Номера вопросов
1	1, 2, 9, 18, 32, 35	11	4, 13, 23, 29, 41, 48	21	1, 8, 16, 28, 38, 48
2	3, 10, 11, 19, 34, 36	12	16, 24, 28, 33, 38, 43	22	2, 17, 25, 27, 32, 35
3	4, 12, 20, 21, 37, 43	13	8, 15, 23, 27, 36, 37	23	3, 11, 13, 18, 36, 38
4	5, 13, 22, 27, 38, 44	14	7, 14, 20, 22, 34, 35	24	4, 14, 24, 30, 34, 44
5	6, 14, 23, 28, 39, 45	15	2, 12, 21, 31, 32, 44	25	5, 15, 20, 25, 35, 40
6	7, 15, 24, 29, 40, 46	16	3, 15, 20, 25, 39, 45	26	6, 16, 26, 31, 36, 42
7	8, 16, 25, 30, 41, 47	17	4, 9, 26, 27, 32, 47	27	7, 11,17, 27, 37, 47
8	17, 26, 31, 33, 42, 48	18	5, 10, 19, 22, 37, 46	28	8, 9, 18, 22, 38, 43
9	2, 10, 21, 27, 39, 46	19	6, 16, 26, 30, 40, 48	29	1, 10, 19, 33, 41, 45
10	3, 12, 22, 28, 40, 47	20	10, 11, 20, 32, 33, 43	30	2, 11, 17, 30, 37, 46