Лабораторная работа №1

Разработка программы разграничения полномочий пользователей на основе парольной аутентификации c использованием встроенных криптопровайдеров.

**Содержание задания**

1. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя.
2. В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):
3. смена пароля администратора (при правильном вводе старого пароля);
4. просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли, минимальная длина пароля, срок действия пароля) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу;
5. добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины);
6. блокирование возможности работы пользователя с заданным именем;
7. включение или отключение ограничений на выбираемые пользователем пароли (в соответствии с индивидуальным заданием, определяемым номером варианта);
8. завершение работы с программой.
9. Для каждого пользователя должны устанавливаться минимальная длина пароля(по умолчанию – 0, т.е. пароль может быть не установлен) и срок действия пароля в месяцах(значение 0 означает бессрочный пароль).
10. В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть заблокированы.
11. После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘\*’.
12. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой.
13. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.
14. При первоначальном вводе пароля (обязательном при первом входе администратора или пользователя с зарегистрированным ранее администратором именем) и при дальнейшей замене пароля программа должна просить пользователя подтвердить введенный пароль путем его повторного ввода.
15. Если выбранный пользователем пароль не соответствует требуемым ограничениям (при установке соответствующего параметра учетной записи пользователя), то программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность ввода другого пароля, завершения работы с программой (при первом входе данного пользователя) или отказа от смены пароля.
16. Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой, а также включении или отключении ограничений на выбираемые пароли должна сохраняться в специальном файле или базе данных(предпочтительнее). При первом запуске программы, в случае файла, он должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль.
17. Файл или база данных с учетными данными зарегистрированных пользователей должен быть защищен криптографическими средствами от несанкционированного доступа.
18. При запуске программы файл с учетными данными должен расшифровываться во временный файл (или в файл в оперативной памяти), который после завершения работы программы должен быть снова зашифрован для отражения возможных изменений в учетных записях пользователей. «Старое» содержимое файла учетных записей при этом стирается.
19. Пароль в файл(базу данных) записывается в виде хэш-кода. При вводе пароля идет сравнение хэш-кода введенного пароля с хэш-кодом пароля, сохраненного в файле.
20. После ввода парольной фразы при запуске программы, генерации ключа расшифрования и расшифрования файла с учетными данными зарегистрированных пользователей правильность введенной парольной фразы определяется по наличию в расшифрованном файле учетной записи администратора программы.
21. При вводе неправильной парольной фразы или отказе от ее ввода работа программы должна завершаться с выдачей соответствующего сообщения.
22. Временный файл на диске с расшифрованными учетными данными после завершения работы программы удаляется.
23. Варианты использования алгоритмов шифрования и хеширования выбираются в соответствии с выданным преподавателем заданием.
24. Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния.
25. Для реализации указанных в пунктах 2-3 функций в программе должны использоваться специальные диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию.
26. Отчет по лабораторной работе должен содержать листинги программы с подробными комментариями, скрин-шоты экранов, описание структуры файла или базы данных с пользовательской информацией, подробное описание функций, связанных с хэшированием и шифрованием, описание мест хранения зашифрованных данных, в т.ч. в момент их шифрования(расшифрования).

# Индивидуальные варианты заданий (ограничения на выбираемые пароли)

1. Наличие строчных и прописных букв, а также знаков арифметических операций.
2. Наличие латинских букв, символов кириллицы и знаков арифметических операций.
3. Наличие букв, цифр и знаков арифметических операций.
4. Наличие букв, знаков препинания и знаков арифметических операций.
5. Наличие цифр, знаков препинания и знаков арифметических операций.
6. Отсутствие повторяющихся символов.
7. Чередование букв, цифр и снова букв.
8. Чередование букв, знаков препинания и снова букв.
9. Чередование цифр, букв и снова цифр.
10. Отсутствие подряд расположенных одинаковых символов.
11. Чередование цифр, знаков препинания и снова цифр.
12. Чередование цифр, знаков арифметических операций и снова цифр.
13. Несовпадение с именем пользователя.
14. Несовпадение с именем пользователя, записанным в обратном порядке.
15. Наличие строчных и прописных букв, цифр и знаков препинания.
16. Наличие строчных и прописных букв, цифр и знаков арифметических операций.
17. Несовпадение с датой в одном из форматов: дд/мм/гг, дд-мм-гг, дд.мм.гг.
18. Наличие строчных и прописных букв.
19. Наличие букв и цифр.
20. Наличие букв и знаков препинания.
21. Наличие цифр и знаков препинания.
22. Наличие букв и знаков арифметических операций.
23. Наличие цифр и знаков арифметических операций.
24. Наличие латинских букв и символов кириллицы.
25. Наличие букв, цифр и знаков препинания.
26. Наличие латинских букв, символов кириллицы и цифр.
27. Наличие латинских букв, символов кириллицы и знаков препинания.
28. Наличие строчных и прописных букв, а также цифр.
29. Наличие строчных и прописных букв, а также знаков препинания.

# Индивидуальные варианты заданий на использование криптографических методов

|  |  |  |  |
| --- | --- | --- | --- |
| № | Используемый режим шифрования алгоритма DES для шифрования файла | Добавление к ключу случайного значения | Используемый алгоритм хеширования пароля |
|  | 3 | 4 | 5 |
| 1 | ECB | Да | MD4 |
| 2 | CBC | Нет | MD5 |
| 3 | CFB | Да | SHA |
| 4 | OFB | Нет | MD4 |
| 5 | ECB | Да | MD5 |
| 6 | CBC | Нет | SHA |
| 7 | CFB | Да | MD4 |
| 8 | OFB | Нет | MD5 |
| 9 | ECB | Да | SHA |
| 10 | CBC | Нет | MD4 |
| 11 | CFB | Да | MD5 |
| 12 | OFB | Нет | SHA |
| 13 | ECB | Да | MD4 |
| 14 | CBC | Нет | MD5 |
| 15 | CFB | Да | SHA |
| 16 | OFB | Нет | MD4 |
| 17 | ECB | Да | MD5 |
| 18 | CBC | Нет | SHA |
| 19 | CFB | Да | MD4 |
| 20 | OFB | Нет | MD5 |
| 21 | ECB | Да | SHA |
| 22 | CBC | Нет | MD4 |
| 23 | CFB | Да | MD5 |
| 24 | OFB | Нет | SHA |

У ЮЗЕРА ДОБАВИТЬ ВЫХОД.   
У АДМИНА НЕ РЕФРЕШИТСЯ СУЧКА