Темы для курсового проекта

1. Разработка программы аутентификации пользователей с помощью паролей и с дополнительными средствами администрирования

Указание для темы 1: программа разрабатывается на основе программы для лабораторной работы 1 с включением дополнительных функций в режиме администратора (задание максимального и минимального сроков действия пароля для всех пользователей, ведение списка уже использованных паролей каждого пользователя задаваемой администратором максимальной длины, аудит удачных и неудачных попыток входа в программу и выхода из нее с фиксацией времени события, его результата – успех или неудача – и имени учетной записи пользователя в специальном файле, аудит изменений в файле учетных записей – добавления нового пользователя, установки и снятия блокировки или ограничений на используемые пароли – с фиксацией времени события и его типа).

2. Разработка программы аутентификации пользователей на основе модели «рукопожатия».
3. Разработка программы аутентификации пользователей по их «росписи» мышью.
4. Разработка программы аутентификации пользователей по их клавиатурному почерку.
5. Разработка программы аутентификации пользователей на основе их реакции на события.

Общее указание для тем 2-5: программа должна обладать функциями, аналогичными функциям программы для лабораторной работы 1.

6. Разработка программы протоколирования в специальном файле событий, связанных с доступом других приложений к выбираемым информационным ресурсам (папкам, принтерам, разделам реестра).
7. Программная реализация криптоалгоритма ГОСТ 28147-89 (ГОСТ Р 34.12-2015 «Магма»).
8. Программная реализация криптоалгоритма ГОСТ Р 34.12-2015 «Кузнечик».
9. Программная реализация криптоалгоритма DES.
10. Программная реализация криптоалгоритма 3-DES.
11. Программная реализация криптоалгоритма DESX.
12. Программная реализация криптоалгоритма IDEA.
13. Программная реализация криптоалгоритма SAFER+.
14. Программная реализация криптоалгоритма Blowfish.
15. Программная реализация криптоалгоритма Twofish.
16. Программная реализация криптоалгоритма RC2.
17. Программная реализация криптоалгоритма RC4.
18. Программная реализация криптоалгоритма RC6.
19. Программная реализация криптоалгоритма AES.

Общее указание для тем 7-19: программа должна шифровать/расшифровывать как выбираемые файлы любого типа, так и вводимые текстовые сообщения на ключе, выводимом из парольной фразы с регулируемой пользователем минимальной длиной и сложностью. Для блочных шифров должна быть возможность выбора режима шифрования.

20. Программная реализация протокола SSL.
21. Программная реализация трехфазного протокола Microsoft.
22. Программная реализация протокола MS-CHAP.
23. Программная реализация протокола Диффи-Хеллмана.
24. Программная реализация протокола S/Key.

Для КП по темам 20-24 необходима разработка программы, создающей защищенный сеанс связи между двумя приложениями на основе указанного протокола.

25. Разработка программы получения списка пользователей, имеющих право доступа к выбираемому информационному ресурсу (файлу, папке, принтеру, разделу реестра), с указанием имеющихся у них прав доступа.
26. Разработка программы получения списка информационных ресурсов (файлов, папок, разделов реестра) к которым имеет доступ на чтение (запись) задаваемый пользователь (группа).

27. Разработка программы получения списка папок, к которым имеют право на чтение (запись) все пользователи системы.
28. Разработка программы выявления легко подбираемых паролей пользователей (совпадающих с паролями из специального словаря и (или) не удовлетворяющих задаваемым требованиям сложности и минимальной длины).

Для КП по темам 25-28 возможна разработка программ для ОС Windows или Linux.

29. Разработка программы скрытия и извлечения информации в графических файлах.
30. Разработка программы скрытия и извлечения информации в звуковых файлах.
31. Разработка программы скрытия и извлечения информации в видеофайлах.
32. Разработка программы скрытия и извлечения информации в текстовых файлах.

Общее указание для тем 29-32: программа должна позволять выбирать файл-контейнер, выбирать файл-сообщение произвольного типа или вводить текст скрываемого сообщения, контролировать возможность скрытия сообщения в контейнере (сравнением их длин, например), шифровать/расшифровывать внедряемое/извлекаемое сообщение.

33. Программная реализация криптоалгоритма RSA.
34. Программная реализация криптоалгоритма ElGamal.
35. Программная реализация криптоалгоритма на основе эллиптических кривых.

Общее указание для тем 33-35: программа должна шифровать/расшифровывать короткие сообщения на случайных асимметрических ключах выбираемой пользователем длины с возможностью сохранения пары ключей (закрытый ключ должен при этом шифроваться на ключе, выводимом из специальной парольной фразы).

36. Программная реализация вычисления и проверки электронной подписи по алгоритму RSA.
37. Программная реализация вычисления и проверки электронной подписи по алгоритму ElGamal.
38. Программная реализация вычисления и проверки электронной подписи по алгоритму ГОСТ Р 34.10-2012.

Общее указание для тем 36-38: программа должна подписывать и проверять выбираемые произвольные файлы на случайной паре ключей с возможностью ее сохранения (закрытый ключ должен при этом шифроваться на ключе, выводимом из специальной парольной фразы).

39. Программная реализация функции хеширования ГОСТ Р 34.11-2012.
40. Программная реализация функции хеширования SHA1.
41. Программная реализация функции хеширования SHA512.
42. Программная реализация функции хеширования RIPEMD.
43. Программная реализация функции хеширования MD4.
44. Программная реализация функции хеширования MD5.
45. Программная реализация функции хеширования MD6.

Общее указание для тем 39-45: программа должна хешировать как выбираемые произвольные файлы, так и вводимые текстовые сообщения с возможностью сохранения в файле полученного хеш-значения. Должна быть возможность вычисления, сохранения и проверки контрольного хеш-значения, зависящего от хешируемых данных и секретного ключа, выводимого из парольной фразы с регулируемой минимальной длиной и сложностью.