1. Процесс управления доступом субъектов к ресурсам системы – это …

2. Процесс контроля (мониторинга) доступа субъектов к ресурсам системы – это …

3. Аутентификация на основе знания и на основе обладания, в соответствии с Руководством NCSC-TG-017, обозначается «…»

4. Аутентификация на основе знания и на основе биометрических характеристик, в соответствии с Руководством NCSC-TG-017, обозначается «…»

5. Аутентификация на основе обладания и на основе биометрических характеристик, в соответствии с Руководством NCSC-TG-017, обозначается «…»

6. Аутентификация на основе знания, обладания и на основе биометрических характеристик, в соответствии с Руководством NCSC-TG-017, обозначается «…»

7. В качестве «четвертого» фактора аутентификации предлагается рассматривать … процедуры аутентификации

8. В качестве метода защиты от атаки с использованием аппаратного сниффера клавиатуры используется …

9. В качестве метода защиты от атаки «трассировка памяти» используют …

10. Для защиты от атаки методом воспроизведения используют …

11. Для защиты от атаки «троянский конь» применяют …

12. Для защиты от атаки «подбор пароля» используется …

13. В локальном устройстве, в котором осуществляется аутентификация с помощью PIN-кода, ввод аутентифицирующей информации производится …

14. Используя только заглавные буквы латинского алфавита, можно сгенерировать … десятизначных паролей (повторения символов допускаются)

15. Неверно, что … относится к статическим биометрическим характеристикам

16. Неверно, что … относится к динамическим биометрическим характеристикам

17. Более просты в использовании биометрические системы …

18. Пороговая величина – это …

19. «Негативная аутентификация» – это …

20. Для противодействия атаке «подделка отличительной черты» используется …

21. Для противодействия атаке «воспроизведение поведения пользователя» используется …

22. При применении метода «запрос – ответ» в качестве исходной информации для аутентификации используется …

23. При применении метода «только ответ» в качестве исходной информации для аутентификации берется значение …

24. Наибольшее число шагов предполагает такой метод OTP-аутентификации, как …

25. Особенностью системы S/Key (схема Лэмпорта) является …

26. В системе HOTP используется такой из методов OTP-аутентификации, как …

27. «Примесью» в схеме S/Key называется … генерации значений хэш-функции

28. Путем введения PIN-кода в аутентификационный токен может быть нейтрализована такая атака, как …

29. Порядок формирования и проверки электронной цифровой подписи регламентирует …

30. Порядок симметричного криптопреобразования регламентирует …

31. Цифровая подпись органа сертификации удостоверяет …

32. При хранении закрытых ключей внутри локального хранилища операционной системы использовать их для начальной аутентификации …

33. Рекомендуемая длина личного ключа пользователя при использовании асимметричного алгоритма на настоящий момент – не менее …

34. Факторизация ключа – это …

35. При использовании интеллектуальных устройств аутентификации пользователь обязан …

36. Механизм Single Sign-On …

37. «Ticket» в протоколе Kerberos – это …

38. В протоколе Kerberos в качестве мастер-ключей пользователей используются …

39. При использовании протокола Kerberos рабочая станция …

40. В протоколе Kerberos используется … аутентификация

41. Для противодействия восстановлению и/или модификации закрытых данных используется …

42. Системные часы всех участвующих в обмене данными компьютеров …

43. Протокол CHAP обеспечивает защиту от использования чужих паролей за счет …

44. Протокол TACACS+ позволяет обмениваться аутентификационными сообщениями …

45. Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью …

46. При авторизации по протоколу TACACS + сообщение REQUEST содержит …

47. Транзакции между клиентом и сервером RADIUS идентифицируются с помощью …

48. При использовании протокола EAPOL в случае кратковременного отключения рабочей станции …

49. При использовании протокола TLS Handshake Protocol атакующая сторона …

50. При использовании протокола SSH компрессия данных …

51. Ассоциация безопасности является …

52. При проверке аутентичности сообщения стороны, участвующие в информационном обмене, …

53. Заголовок AH … исходный пакет

54. Туннельный режим протокола IPSec обеспечивает защиту данных на участке «…»

55. ESP-заголовки в туннельном и транспортном режимах …

56. Многоуровневая ролевая модель доступа, как правило, включает в себя …