

1. Для противодействия хакерским атакам ...
2. Информационные брокеры – это люди, которые ...
3. Принцип неопределенности обусловлен ...
4. Специализированные протоколы, предназначенные для организации защищенного взаимодействия через Интернет: ...
5. Аутентификация – это ...
6. Фишинг – это ...
7. Криптографическая защита – это защита информации ...
8. Public Key Infrastructure (Инфраструктура открытых ключей) предполагает, что ключи не зашифрованы и передаются в открытом виде по ... каналу
9. Электронная цифровая подпись (ЭЦП) ...
10. При рассмотрении конкретной компьютерной системы (КС) следует обратить внимание на используемые методы и способ реализации наиболее важных функций – ...
11. Сертификат открытого ключа – это ...
12. Репозиторий – это хранилище, содержащее ...
13. Конечными пользователями сертификатов выступает ...
14. Структура подчинения при иерархической модели доверительных отношений предполагает, что во главе стоит ...
15. Сетевая модель доверительных отношений строится как ...
16. Базовые ограничения – это ограничения ...
17. Ограничения по политике приложений могут ...
18. Чтобы зарегистрировать частный номер организации для привязки к нему сертификатов, необходимо подать заявку ...
19. Протокол SSL (Secure Socket Layer) – это ... протокол



20. Для протокола SSL используют аббревиатуру ...
21. Сетевой анализатор трафика, программа или программно-аппаратное устройство, которые используются для перехвата и последующего анализа сетевого трафика, предназначенного для других узлов, называют ...
22. Для успешного функционирования SSL
23. Как называется атака, когда злоумышленник прикидывается сервером для клиента и клиентом для сервера:
24. Субпротоколы SSL предназначены для ...
25. В обычных приложениях для шифрации применяется ... ключ
26. Аббревиатура кода аутентификации сообщения следующая: ...
27. Протокол SSL используется ...
28. Три основных свойства протокола SSL: ...

