



## Криптографические методы и средства обеспечения информационной безопасности инфокоммуникаций.

- 1 Наука, занимающаяся проблемой защиты информации путем ее преобразования, – это ...
- 2 Наука о методах защиты информации с помощью шифров – это ...
- 3 Конечное множество используемых для кодирования информации знаков – это ...
- 4 Процесс преобразования информации в данные является ...
- 5 Процесс преобразования открытых данных в зашифрованные при помощи шифра называется ...
- 6 Результат шифрования открытого сообщения называется ...
- 7 Криптографическое преобразование может быть ...
- 8 Конкретное значение некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из семейства, – это ...
- 9 Неверно, что при кодировании информации может использоваться ...
- 10 Различают ... системы шифрования
- 11 Системы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ, называются ... системами шифрования
- 12 Если  $x$  – исходное сообщение,  $K$  – ключ,  $f$  – функция шифрования,  $F$  – функция дешифрования, то принцип действия симметричных шифров описывается выражением ...
- 13 Одним из простых симметричных шифров является ...
- 14 Неверно, что к простым шифрам относят ...
- 15 Стойкостью шифра называют ...



- 16 По Шеннону, шифр считается абсолютно стойким (идеальным), если любые знания, извлеченные из шифрограммы, ...
- 17 Метод шифрования, основанный на наложении на открытый текст случайной числовой последовательности, используемой для шифрования и расшифровывания данных, – это ...
- 18 Наиболее распространенным способом наложения гамма-последовательностей является ...
- 19 Неверно, что одним из параметров блочного шифра является ...
- 20 В асимметричных системах шифрования ...
- 21 Если  $x$  – исходное сообщение,  $A$  – шифрограмма,  $K1$  – секретный ключ, то выражение  $A = f(K1, x)$  описывает процесс ...
- 22 Если  $x$  – исходное сообщение,  $A$  – шифрограмма,  $K1$  – секретный ключ,  $K2$  – открытый ключ,  $f$  – функция шифрования,  $F$  – функция дешифрования, то асимметричное шифрование-дешифрование описывается выражением ...
- 23 Одним из достоинств асимметричных алгоритмов шифрования является ...
- 24 Функция, которую легко рассчитать, но обратное восстановление которой требует непропорционально больших усилий, называется ...
- 25 Неверно, что к алгоритмам вычисления хеш-функций относится алгоритм ...
- 26 Функция, вычисляющая контрольное число блока методом циклического сложения значений содержимого блока, называется ...
- 27 Операция сложения, при которой бит переполнения добавляется к младшему разряду результата сложения, называется ...
- 28 Неверно, что к возможностям электронной подписи по ГОСТ Р 34.10-2001 относится ...
- 29 Присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения, называется ...
- 30 Сокращение PKI означает «...»
- 31 Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают средства ...





- 32 Выделяют ... политики безопасности
- 33 В число принципов управления персоналом входит ...
- 34 В состав комплексной политики безопасности включается ...
- 35 Неверно, что ... политика является видом частной политики безопасности
- 36 Комплексная политика безопасности строится на основе анализа ...
- 37 Целевые политики безопасности направлены на ...
- 38 Комплексная политика безопасности содержит раздел «...»
- 39 Одним из видов частных политик безопасности является ... политика
- 40 Программные политики безопасности направлены на ...
- 41 Комплексная политика безопасности содержит раздел «...»
- 42 Одним из видов частных политик безопасности является ... политика
- 43 Платформенные политики безопасности направлены на ...
- 44 Комплексная политика безопасности содержит раздел «...»
- 45 Неверно, что частная политика безопасности (ПБ) содержит раздел «...»

