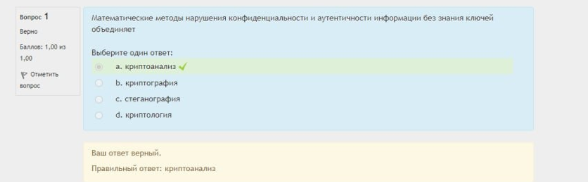
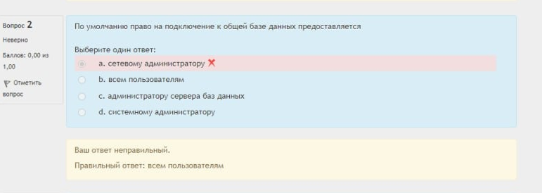
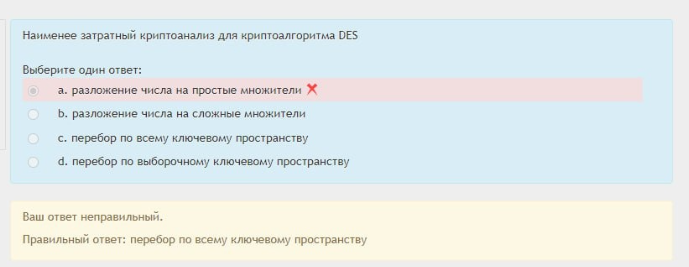
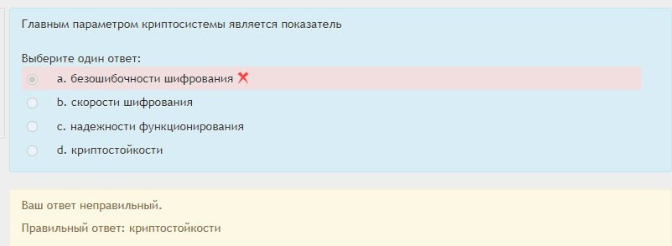
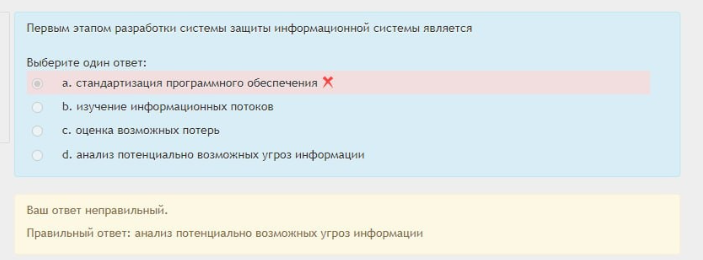
Математические методы нарушения конфиденциальности и аутентичности информации без знания ключей

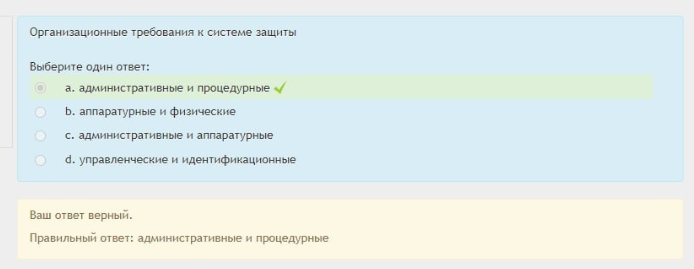
По умолчанию право на подключение к общей базе данных предоставляется  


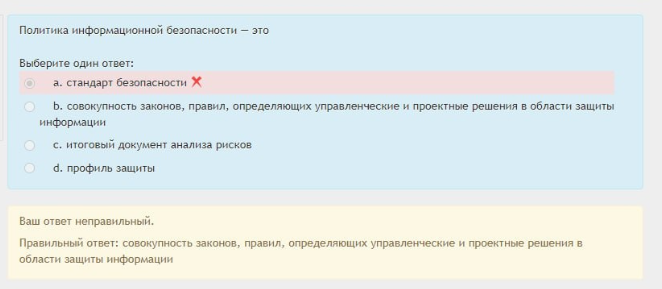
Наименее затратный криптоанализ для криптоалгоритма DES  


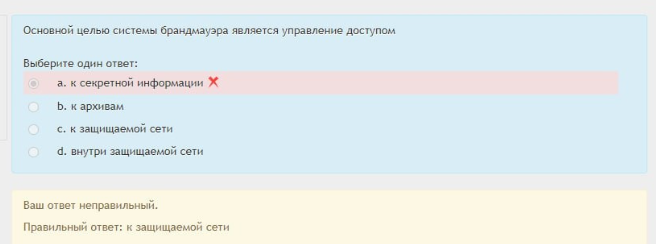
Главным параметром криптосистемы является показатель  


Первым этапом разработки системы защиты информационной системы является

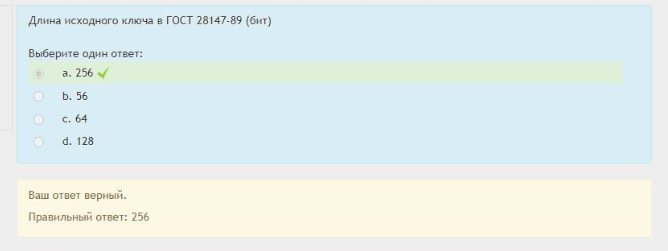


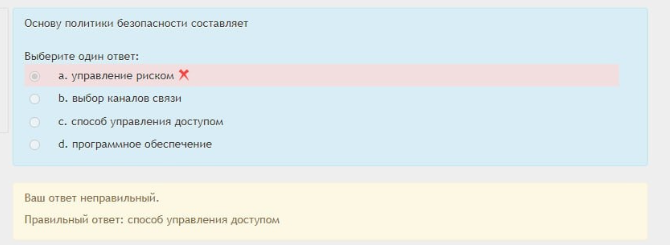
Организационные требования к системе защиты  


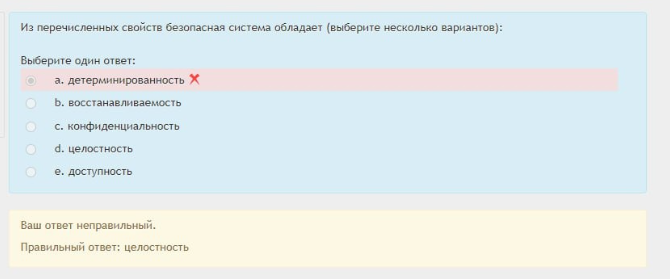
Политика информационной безопасности – это  


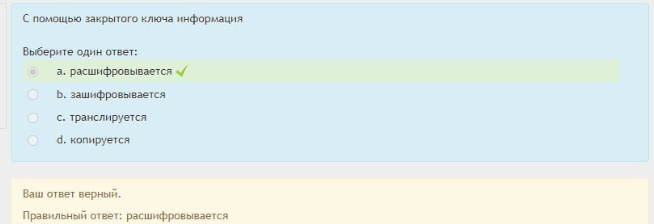
Основной целью системы брандмауэра является управление доступом  


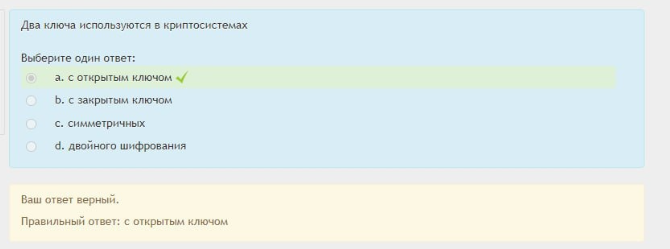
Длина исходного ключа в ГОСТ 28147-89 (бит)

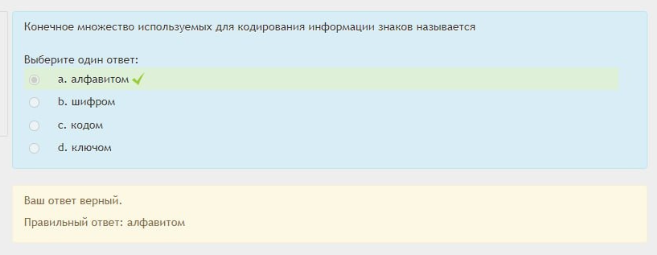


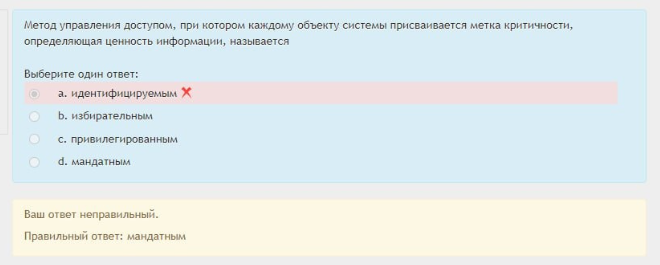
Основу политики безопасности составляет  


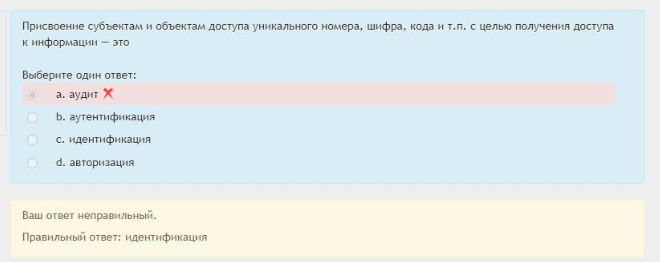
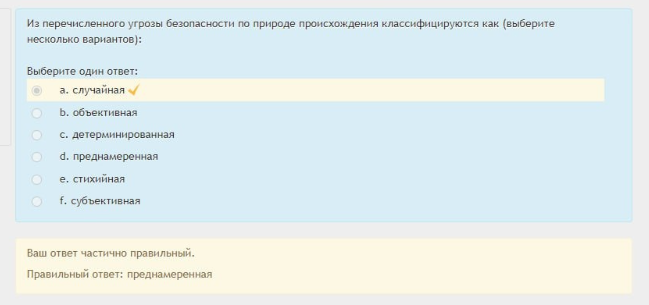
Из перечисленных свойств безопасная система обладает   


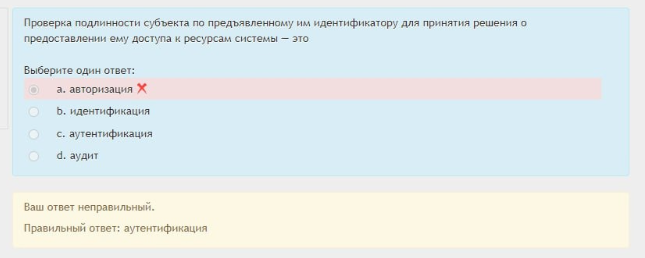
С помощью закрытого ключа информация  


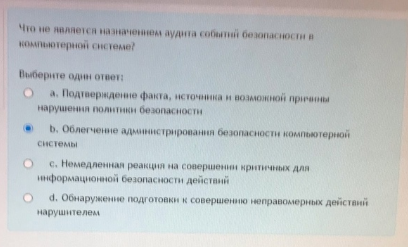
Два ключа используются в криптосистемах  


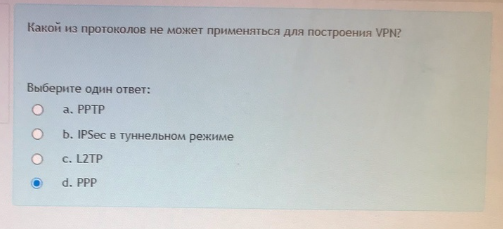
Конечное множество используемых для кодирования информации знаков называется  


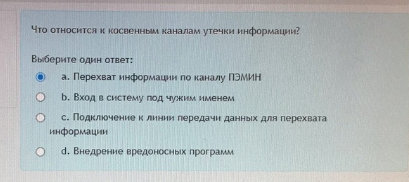
Метод управления доступом, при котором каждому объекту системы присваивается метка критичности, определяющая ценность информации, называется  


Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации – это  
  
Из перечисленного угрозы безопасности по природе происхождения классифицируются как  


Проверка подлинности субъекта по предъявленному им идентификатору для принятия о предоставлении ему доступа к ресурсам системы – это  
 

Что не является назначением аудита событий безопасности в компьютерной системе  


Какой из протоколов не может применяться для построения VPN  


Что относится к косвенным каналам утечки информации  


В чем разница между протоколами AH и ESP в IPSec  
