

## Приложение 1

### Перечень категорий товаров (продукции), являющихся шифровальными (криптографическими) средствами или содержащих в своем составе шифровальные (криптографические) средства, технические и криптографические характеристики которых подлежат нотификации

1. Товары, содержащие шифровальные (криптографические) средства, имеющие любую из следующих составляющих:

симметричный криптографический алгоритм, использующий криптографический ключ длиной, не превышающей 56 бит; или

асимметричный криптографический алгоритм, основанный на любом из следующих методов:

а) на разложении на множители целых чисел, размер которых не превышает 512 бит;

б) на вычислении дискретных логарифмов в мультипликативной группе конечного поля размера, не превышающего 512 бит; или

в) на дискретном логарифме в группе, отличного от поименованного в вышеприведенном подпункте "б" размера, не превышающего 112 бит.

*Примечание.*

1. Биты четности не включаются в длину ключа.

2. Термин "криптография" не относится к фиксированным методам сжатия или кодирования данных.

2. Товары, содержащие шифровальные (криптографические) средства, обладающие ограниченными функциями:

а) аутентификацией, включающей в себя все аспекты контроля доступа, где нет шифрования файлов или текстов, за исключением шифрования, которое непосредственно связано с защитой паролей, персональных идентификационных номеров или подобных данных для защиты от несанкционированного доступа;

б) электронной цифровой подписи.

*Примечание. Функции аутентификации и электронной цифровой подписи включают в себя связанную с ними функцию распределения ключей.*

3. Шифровальные (криптографические) средства, являющиеся компонентами программных операционных систем, криптографические возможности которых не могут быть изменены пользователями, которые разработаны для установки пользователем самостоятельно без дальнейшей существенной поддержки поставщиком и техническая документация (описание алгоритмов криптографических преобразований, протоколы взаимодействия, описание интерфейсов и т.д.) на которые является доступной.

4. Персональные смарт-карты (интеллектуальные карты):

а) криптографические возможности которых ограничены использованием в оборудовании или системах, указанных в пунктах 5 – 8 настоящего перечня; или

б) для широкого общедоступного применения, криптографические возможности которых недоступны пользователю и которые в результате специальной разработки имеют ограниченные возможности защиты хранящейся на них персональной информации.

*Примечание. Если интеллектуальная карта может выполнять несколько функций, то контрольный статус каждой из функций определяется отдельно.*

5. Приемная аппаратура для радиовещания, коммерческого телевидения или аналогичной коммерческой аппаратуры для вещания на ограниченную аудиторию без шифрования цифрового сигнала, кроме случаев использования шифрования исключительно для управления видео- или аудиоканалами и отправки счетов или возврата информации, связанной с программой, провайдером вещания.

6. Оборудование, криптографические возможности которого недоступны пользователю, специально разработанное и ограниченное для применения любым из следующего:

а) программное обеспечение исполнено в защищенном от копирования виде;

б) доступом к любому из следующего:

- защищенному от копирования содержимому, хранящемуся только на доступном для чтения носителе информации;

- информации, хранящейся в зашифрованной форме на носителях, когда эти носители информации предлагаются на продажу населению в идентичных наборах;  
в) контролем копирования аудио- и видеоинформации, защищенной авторскими правами.

7. Шифровальное (криптографическое) оборудование, специально разработанное и ограниченное применением для банковских или финансовых операций.

*Примечание. Финансовые операции включают сборы и оплату за транспортные услуги и кредитование.*

8. Портативные или мобильные радиоэлектронные средства гражданского назначения (например, для использования в коммерческих гражданских системах сотовой радиосвязи), которые не способны к сквозному шифрованию (т.е. от абонента до абонента).

9. Беспроводное радиоэлектронное оборудование, осуществляющее шифрование информации только в радиоканале с максимальной дальностью беспроводного действия без усиления и ретрансляции менее 400 м в соответствии с техническими условиями производителя.

10. Шифровальные (криптографические) средства, используемые для защиты технологических каналов информационно-телекоммуникационных систем и сетей связи.

11. Товары, у которых криптографическая функция заблокирована производителем.