СТ РК 1073-2007

Средства криптографической защиты информации

Общие технические требования

**Комитет по техническому регулированию и метрологии Министерства индустрии и торговли
Республики Казахстан
(Госстандарт)**

Содержание

1 Область применения

Настоящий стандарт распространяется на средства криптографической защиты информации отечественного и зарубежного производства и устанавливает общие технические требования к ним.

Стандарт пригоден для целей подтверждения соответствия.

Настоящий стандарт не распространяется на средства криптографической защиты информации, являющиеся государственными шифровальными средствами Республики Казахстан.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ 28147-89 Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ 34.310-2004 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

3 Термины и определения

В настоящем стандарте применяются следующие термины с соответствующими определениями:

3.1 Алгоритм криптографического преобразования: Набор конечного числа простых и однозначно определенных правил, зависящих от изменяемого параметра (ключа) и задающих последовательность выполнения операций для решения задачи криптографического преобразования.

3.2 Асимметричный алгоритм криптографического преобразования: Алгоритм криптографического преобразования, в котором прямое и обратное преобразования используют открытый и секретный ключи, взаимосвязанные таким образом, что вычислительно сложно определить секретный ключ из открытого ключа.

3.3 Аутентификация: Установление подлинности одного или нескольких аспектов информационного взаимодействия: сеанса связи, его времени, связывающихся сторон, передаваемых сообщений, источника данных, времени создания данных, содержания данных.

3.4 Государственные шифровальные средства: средства криптографической защиты информации, предназначенные в качестве основной меры защиты для сохранения конфиденциальности сведений, составляющих государственные секреты Республики Казахстан.

3.5 Имитовставка: Строка бит фиксированной длины, полученная по определенному правилу из данных и ключа, добавленная к данным для обеспечения имитозащиты.

3.6 Имитозащита: Защита системы связи от навязывания ложных сообщений.

3.7 Ключ: Конкретное секретное или открытое (если специально указано) состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

3.8 Криптографическая стойкость средства криптографической защиты информации: вычислительная сложность метода (алгоритма) вскрытия криптографической защиты, наилучшего для данного средства криптографической защиты информации.

3.9 Криптографическое преобразование: Преобразование данных при помощи шифрования, выработки (проверки) имитовставки или формирования (проверки) электронной цифровой подписи.

3.10 Предварительное шифрование: Шифрование, технически реализованное отдельно от передачи зашифрованных данных по каналам связи.

3.11 Симметричный алгоритм криптографического преобразования: Алгоритм криптографического преобразования, в котором прямое и обратное преобразования используют один и тот же ключ или два ключа, каждый из которых легко вычисляется из другого.

3.12 Средство криптографической защиты информации; СКЗИ: Средство, реализующее алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами.

3.13 Схема электронной цифровой подписи: Алгоритм криптографического преобразования, осуществляющий формирование электронной цифровой подписи, и соответствующий ему алгоритм криптографического преобразования, осуществляющий ее проверку.

4 Общие положения

4.1 СКЗИ предназначены для:

а) сохранения конфиденциальности данных при помощи шифра;

б) аутентификации, в том числе контроля целостности данных, при помощи имитовставки и (или) ЭЦП;

в) генерации, формирования, распределения и (или) управления ключами.

4.2 СКЗИ, соответствующие требованиям настоящего стандарта, рассматриваются как технологически завершенные (работоспособные) аппаратные, программные или аппаратно-программные средства.

4.3 В зависимости от криптографической стойкости для СКЗИ устанавливаются 4 уровня безопасности:

4.3.1 СКЗИ первого уровня безопасности предназначены для защиты информации, ущерб от разглашения, навязывания, или несанкционированного изменения которой в объеме, защищенном с использованием одного и того же ключа (одних и тех же ключей), не превышает 100 минимальных расчетных показателей;

4.3.2 СКЗИ второго уровня безопасности предназначены для защиты информации, ущерб от изменения которой в объеме, защищенном с использованием одного и того же ключа (одних и тех же ключей), не превышает 10 000 минимальных расчетных показателей;

4.3.3 СКЗИ третьего уровня безопасности предназначены для защиты информации, ущерб от изменения которой в объеме, защищенном с использованием одного и того же ключа (одних и тех же ключей), не превышает 1 000 000 минимальных расчетных показателей;

4.3.4 СКЗИ четвертого уровня безопасности предназначены для защиты информации, ущерб от изменения которой в объеме, защищенном с использованием одного и того же ключа (одних и тех же ключей), не превышает 100 000 000 минимальных расчетных показателей.

4.4 СКЗИ не могут быть признаны соответствующими первому, второму, третьему или четвертому уровню безопасности, если вычислительная

сложность существующих алгоритмов вскрытия криптографической защиты, обеспечиваемой ими, составляет менее 250, 280, 2^{120} или 2^{160} соответственно.

5 Общие технические требования

Средства криптографической защиты информации должны соответствовать требованиям настоящего стандарта и технической документации, утвержденной в установленном порядке.

5.1 Общие требования к СКЗИ

5.1.1 Генерируемые СКЗИ ключи (кроме открытых ключей) должны представлять собой последовательности случайных чисел, формируемые с помощью физических генераторов шума (например, тепловых, диодных, радиационных, импульсных), либо последовательности псевдослучайных чисел, формируемые с использованием случайных событий (например, системных параметров ЭВМ, движений мыши, нажатий клавиатуры, состояния таймера).

5.1.2 СКЗИ, использующие распределение ключей по незащищенным каналам связи, должны обеспечивать криптографическую защиту ключей в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также навязывания ложных ключей.

5.1.3 Любой используемый СКЗИ ключ должен применяться только одним алгоритмом криптографического преобразования, например, только для шифрования или только для формирования электронной цифровой подписи.

5.1.4 Должна обеспечиваться защита от несанкционированного изменения СКЗИ, в том числе от модификации или подмены их элементов и модулей, с целью исключения влияния на криптографическую стойкость СКЗИ.

5.2 Требования к технической документации СКЗИ

5.2.1 Техническая документация (конструкторская, технологическая и программная документация, в зависимости от вида СКЗИ) должна содержать полное описание реализованных в СКЗИ алгоритмов криптографических преобразований, генерации, формирования, распределения и управления ключами.

5.2.2 Если в СКЗИ реализованы алгоритмы криптографических преобразований, определенные государственными и межгосударственными стандартами или другими нормативными документами по стандартизации, действующими или применяемыми в Республике Казахстан в установленном порядке, то в технической документации вместо их полного описания допускается делать ссылки на данные документы.

5.2.3 СКЗИ должны реализовывать алгоритмы криптографических преобразований в точном соответствии с их описанием, приведенным в технической документации.

5.2.4 В каждый комплект СКЗИ должна входить эксплуатационная документация, которая полно и адекватно описывает все возможные режимы их использования и содержит перечень всех организационных и технических мер, необходимых для обеспечения безопасности обрабатываемой информации, включая порядок и частоту смены ключей, порядок технического обслуживания СКЗИ и действия, которые необходимо предпринять для устранения ошибок оператора и других нештатных ситуаций, возможных во время эксплуатации, а также их последствий.

5.3 Требования к СКЗИ первого уровня безопасности

5.3.1 Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 60 бит.

5.3.2 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 120 бит.

5.3.3 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 500 бит.

5.3.4 Длина вычисляемого СКЗИ хэш-кода должна быть не менее 120 бит.

5.3.5 Длина формируемой СКЗИ ЭЦП должна быть не менее 120 бит.

5.3.6 Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,50 ± 0,03).

5.4 Требования к СКЗИ второго уровня безопасности

5.4.1 Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 100 бит.

5.4.2 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 160 бит.

5.4.3 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 1500 бит.

5.4.4 Длина вычисляемого СКЗИ хэш-кода должна быть не менее 160 бит.

5.4.5 Длина формируемой СКЗИ ЭЦП должна быть не менее 200 бит.

5.4.6 Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,50 ± 0,01).

5.4.7 СКЗИ должны реализовывать процедуры вычисления и проверки контрольной информации о ключах в целях предотвращения использования случайно искаженных на этапе распределения и загрузки ключей с вероятностью не менее 0,9999.

5.4.8 При предварительном шифровании СКЗИ должны реализовывать процедуры вычисления и проверки контрольной информации о шифруемых

данных в целях выявления случайно искаженных зашифрованных данных с вероятностью не менее 0,9999.

5.4.9 СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования.

5.5 Требования к СКЗИ третьего уровня безопасности

5.5.1 Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 150 бит.

5.5.2 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 250 бит.

5.5.3 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 4000 бит.

5.5.4 Длина вычисляемого СКЗИ хэш-кода должна быть не менее 250 бит.

5.5.5 Длина формируемой СКЗИ ЭЦП должна быть не менее 300 бит.

5.5.6 Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,500 ± 0,003), при этом ключи должны быть последовательностями случайных чисел и формироваться с помощью физических генераторов шума.

5.5.7 СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭЦП для ключей в целях предотвращения использования случайно или умышленно искаженных на этапе распределения и загрузки ключей с вероятностью не менее 0,999999.

5.5.8 При предварительном шифровании СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭЦП для шифруемых данных в целях выявления случайно или умышленно искаженных зашифрованных данных с вероятностью не менее 0,999999.

5.5.9 СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования и других нештатных ситуациях.

5.5.10 СКЗИ должны обеспечивать иерархическую криптографическую защиту ключей на этапе их распределения и управления в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также навязывания ложных ключей, или эксплуатационная документация СКЗИ должна содержать организационные и технические меры по обеспечению защиты от данных угроз.

5.5.11 Реализуемые СКЗИ штатные процедуры удаления (уничтожения) ключей должны гарантировать невозможность их восстановления.

5.6 Требования к СКЗИ четвертого уровня безопасности

5.6.1 Длина ключа реализуемых СКЗИ симметричных алгоритмов криптографического преобразования должна быть не менее 200 бит.

5.6.2 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования должна быть не менее 400 бит.

5.6.3 Длина ключа реализуемых СКЗИ асимметричных алгоритмов криптографического преобразования, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле, должна быть не менее 8000 бит.

5.6.4 Длина вычисляемого СКЗИ хэш-кода должна быть не менее 400 бит.

5.6.5 Длина формируемой СКЗИ ЭЦП должна быть не менее 400 бит.

5.6.6 Реализуемый СКЗИ принцип генерации и формирования ключей должен обеспечивать принятие каждым битом ключа единичного значения с вероятностью из интервала (0,500 ± 0,001), при этом ключи должны быть последовательностями случайных чисел и формироваться с помощью физических генераторов шума.

5.6.7 СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭЦП для ключей в целях предотвращения использования случайно или умышленно искаженных на этапе распределения и загрузки ключей, с вероятностью не менее 0,999999999.

5.6.8 СКЗИ должны реализовывать процедуры формирования и проверки имитовставок или ЭЦП для шифруемых данных в целях выявления случайно или умышленно искаженных зашифрованных данных с вероятностью не менее 0,999999999.

5.6.9 СКЗИ должны информировать оператора об установлении, сбросе, а также о невозможности установления режима шифрования и других нештатных ситуациях, предотвращать транзит через себя открытых данных в область хранения, распределения и последующей обработки зашифрованных данных.

5.6.10 СКЗИ должны обеспечивать иерархическую криптографическую защиту ключей на этапе их распределения и управления в целях предотвращения разглашения и несанкционированного изменения этих ключей (кроме разглашения открытых ключей), а также от навязывания ложных ключей.

5.6.11 Реализуемые СКЗИ штатные процедуры удаления (уничтожения) ключей должны гарантировать невозможность их восстановления. Если СКЗИ не реализуют указанных процедур, то эти процедуры гарантированного удаления (уничтожения) ключей (кроме открытых ключей) должны быть реализованы техническими средствами, поставляемыми в комплекте с СКЗИ.

УДК 681.3 **МКС 35.040**
КПВЭД 30.02.16

Ключевые слова: защита информации, криптография, шифрование, аутентификация, электронная цифровая подпись, хэш-код, уровень безопасности, подтверждение соответствия