СТ РК 1073 в новой редакции
Предложения и замечания заинтересованных сторон

Главные вопросы:

- Роль и место СТ РК 1073 в РК?
- Зачем новый стандарт?
- Что плохого от использования «чужих» решений?

Проблемы деятельности по СКЗИ

Следствия от проблем

Хронология разработки и принятия СТ РК 1073

Основные тезисы СТ РК 1073-2007

Основные численные характеристики алгоритмов криптографического преобразования

Оценка стойкости алгоритмов криптографического преобразования через призму вычислительной трудоёмкости взлома

Соответствует реалиям прошлых десятилетий

Установление ступенчатых уровней безопасности исходя из размера возможного ущерба

Безопасность СКЗИ от «криптографических» угроз

Роль и место СТ РК 1073-2007

Постановление Правительства Республики Казахстан от 20 декабря 2016 года №832

Приказ МЦРИАП от 1 июня 2020 года №224/НҚ и приказ МИР от 28 декабря 2015 года № 1261

Постановление Правительства Республики Казахстан от 24 июня 2022 года № 429

СТ РК 1073 обязателен

Анализ НПА и стандартов

О разрешениях и уведомлениях

- Лицензия на разработку и разрешение реализацию СКЗИ
- Для получения лицензии требуется сдать **несложный** экзамен и тест
- Лицензии являются **неотчуждаемыми** и **не имеет сроков годности**

О техническом регулировании

- **Жизненный цикл**: процессы проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации СКЗИ
- Сертификация с привлечением независимых ОПС, срок сертификата – не более трех лет, различные схемы сертификации: сертификация каждого экземпляра, сертификация типа, анализ производства

СТ РК 1073

- **Не устанавливает требования к жизненному циклу СКЗИ, а также история происхождения не имеет значения**
- Не учитывает «**некриптографические**» угрозы: НДВ (аппаратные, программные), ТКУИ и т.д.
- Криптографические требования являются «**неполными**»: срок действия ключа, пространственная сложность, режимы работы алгоритмов, объем критической информации.

Изменения в новой редакции СТ РК 1073

Криптографические требования

- Оценивать стойкость через баланс «Time-Memory-Data»
- Привести перечень атак на алгоритмы
- Пересмотреть численные показатели безопасности

Некриптографические требования

- НДВ на уровне аппаратной и программной составляющей
- Технические каналы утечки информации

Жизненный цикл СКЗИ

- Определить понятие «отечественное СКЗИ»
- Определить требования к жизненному циклу СКЗИ
- Обеспечить «коллективную взаимозависимую ответственность»

Взаимозависимая ответственность участников деятельности

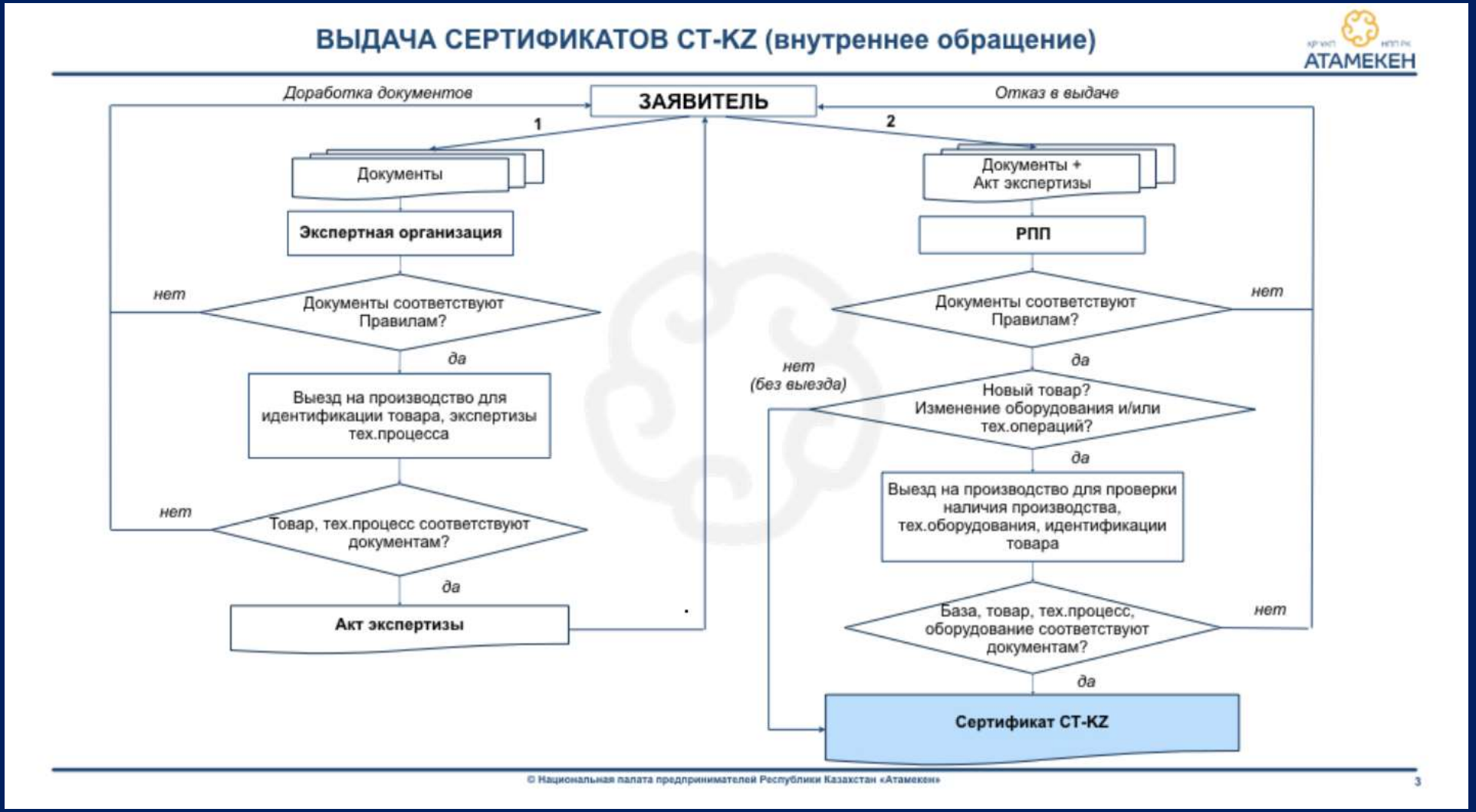
Предложения и замечания сторон

Жизненный цикл	• **УБРАТЬ!!!** • **Все через СТ-KZ!!!**
Криптографические требования	• **Атаки УБРАТЬ!!!** • **Численные показатели свойств безопасности на ОБСУЖДЕНИЕ**
Некриптографические требования	• **ТКУИ УБРАТЬ!!!** • **НДВ УБРАТЬ!!!** • **Обязательность УБРАТЬ!!!**

Предложения и замечания сторон

3. Определение отечественного СКЗИ в пункте 3.14 и требования к отечественным СКЗИ в пунктах 5.6, 5.7 и 6.4 Проекта являются попыткой создания альтернативной системы определения происхождения СКЗИ вместо сертификатов происхождения товаров "СТ-KZ" и индустриальных сертификатов, что противоречит законодательству Республики Казахстан в этой области. Кроме того, требование разработки и производства отечественных СКЗИ "*без участия иностранных субъектов научной, научно-производственной и производственной деятельности*" являются невыполнимыми в полном объеме, в частности, из-за отсутствия отечественных электронных микросхем и других электронных компонентов, средств разработки аппаратного и программного обеспечения. Отказ же от классических (иностранных) алгоритмов криптографического преобразования, криптографических режимов и протоколов в погоне за "отечественностью" может негативно повлиять на криптографическую стойкость СКЗИ.

СТ - KZ


ВЫДАЧА СЕРТИФИКАТОВ СТ-KZ (внутреннее обращение)
АТАМЕКЕН
ЗАЯВИТЕЛЬ
Доработка документов
Отказ в выдаче
1
2
Документы
Экспертная организация
нет
Документы соответствуют Правилам?
да
Выезд на производство для идентификации товара, экспертизы тех.процесса
нет
Товар, тех.процесс соответствуют документам?
да
Акт экспертизы
Документы + Акт экспертизы
РПП
нет
Документы соответствуют Правилам?
да
нет (без выезда)
Новый товар? Изменение оборудования и/или тех.операций?
да
Выезд на производство для проверки наличия производства, тех.оборудования, идентификации товара
нет
База, товар, тех.процесс, оборудование соответствуют документам?
да
Сертификат СТ-KZ
© Национальная палата предпринимателей Республики Казахстан «Атамекен»
3

Предложения и замечания сторон

4. Пункт 4.5 Проекта содержит перечень из 15 криптографических атак, к которым и к комбинациям которых должны быть устойчивы СКЗИ. Считаем целесообразным этот пункт удалить, так как изложенные в нем требования носят декларативный характер. Так, для глубокого научного исследования криптостойкости только одного алгоритма криптографического преобразования только к одной атаке может потребоваться от месяца до года работы. То есть на проведение предварительных и/или сертификационных исследований СКЗИ только в части криптостойкости к указанным атакам может уйти около 10-15 человеко-лет. Если исследовать хотя бы парные комбинации атак, то их 14*15/2 = 105 комбинаций, то это потребует около 100 человеко-лет. При этом, проведение одним криптографом исследования криптостойкости к конкретной атаке, как правило, не закрывает вопрос. Другой исследователь теоретически может предложить более эффективный вариант той же криптографической атаки. Кроме того, указанный перечень

3

криптографических атак не является исчерпывающим, и с учетом особенностей конкретного алгоритма криптографического преобразования могут быть со временем найдены другие более эффективные атаки. Сами авторы Проекта признают это в том же пункте 4.5: "*указанный перечень криптографических атак может дополняться разработчиком и (или) органом по подтверждению соответствия ...*".

4.5 СКЗИ должны быть устойчивы к следующим видам и типам криптграческих атак, а также их комбинациям:

дифференциальный анализ и его разновидности;
линейный анализ;
метод «встреча посередине»;
криптографический анализ на основе связанных ключей;
алгебраический анализ и XSL-атаки;
сдвиговые атаки;
интегральный анализ;
атаки, основанные на решении базовой задачи асимметричного алгоритмов криптографического преобразования;
анализ статистических свойств шифрующей гаммы;
аналитические атаки на поточные криптографические алгоритмы;
корреляционные атаки на поточные криптографические алгоритмы;
атака «человек посередине»;
атака на чтение назад;
атака на перекрытии шифрующей гаммы;
атака, основанная на повторах передаваемых сообщений.

Указанный перечень криптографических атак может дополняться разработчиком и (или) органом по подтверждению соответствия в ходе проведения соответствующих испытаний иными видами и типами атак, являющимися более эффективными, адаптированными и (или) оптимизированными по отношению к конкретному СКЗИ.

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 2^{50}, 2^{80}, 2^{120} или 2^{160} соответственно.

Предложения и замечания сторон

12. Проверка требования отсутствия недекларированных возможностей из пунктов 9.3.9, 9.4.12, 9.5.14 и 9.6.14 Проекта в общем случае является невыполнимой задачей не только для сертификационных органов, но и для самих разработчиков СКЗИ. Так, отсутствие в Казахстане производства микроэлектронных компонентов и, особенно, процессоров и других интегральных схем, делает невозможной исчерпывающую проверку этого требования для аппаратных и аппаратно-программных средств. Аналогичная ситуация и для программного обеспечения, исполнимый код которого является результатом работы импортных компиляторов и отладчиков.

9.4.12° В СКЗИ должны отсутствовать недекларированные возможности, создающие угрозу безопасности защищаемой, в том числе ключевой, информации.¶

Предложения и замечания сторон

9.4.13 Требования к СКЗИ по защите от утечки информации по техническим каналам должны быть определены разработчиком и (или) приобретателем в соответствии с национальными, государственными и межгосударственными стандартами или другими нормативными документами по стандартизации, действующими или применяемыми в Республике Казахстан в установленном порядке.¶

13. Требование по защите от утечки информации по техническим каналам в пунктах 9.3.10, 9.4.13, 9.5.15 и 9.6.15 Проекта носит декларативный характер и не содержит конкретных технических требований, перекладывая ответственность за их определение на разработчика и (или) приобретателя. Это также противоречит существующей практике, когда заявитель (разработчик, производитель, реализатор) представляет СКЗИ на сертификацию еще до реализации товара, то есть тогда, когда будущий пользователь (приобретатель) и внешние условия эксплуатации еще не определены.

СТ РК 1694-2007 «Средства защиты телефонных аппаратов от утечки информации за счет акустоэлектрических преобразований и высокочастотного навязывания. Общие технические требования».¶

СТ РК 1697-2007 «Защита информации. Средства защиты технических средств от утечки информации по цепям электропитания. Общие технические требования».¶

СТ РК 1698-2007 «Защита информации. Защита информации от технических разведок и от ее утечки по техническим каналам на объекте средств вычислительной техники. Методы защиты».¶

СТ РК 1700-2007 «Техническая защита информации в служебных помещениях. Общие технические требования».¶

СТ РК 1701-2007 «Техническая защита информации в средствах вычислительной техники, автоматизированных информационных системах и сетях от утечки посредством побочных электромагнитных излучений и наводок. Общие технические требования».¶

СТ РК 3085-2017 «Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний».¶