

несанкционированного доступа к информации. КомпьютерПресс №3'2008. 8. Межгосударственный стандарт ГОСТ 34.310-95. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997. 9. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. Київ. Державний комітет України з питань технічного регулювання та споживчої політики. 2003. 10. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Государственный комитет СССР по стандартам. Москва. 1989. 11. Межгосударственный стандарт ГОСТ 34.311-95. Информационная технология. Криптографическая защита информации. Функция хеширования. Межгосударственный совет по стандартизации, метрологии и сертификации. Минск. Госстандарт Украины, с дополнениями, 1997. 12. В. Глухов, Н. Заіченко, Б. Оліярник. Шифропроцесор для бортових інформаційно-керуючих систем. Наукові нотатки. Міжвузівський збірник (за напрямком «Інженерна механіка»), випуск 19 (січень 2007). Луцький державний технічний університет, Луцьк. 2007. С.33-43. 13. В. С. Глухов, К. С. Євтушенко, Н. В. Заіченко, Б. О. Оліярник "Криптографічні засоби спеціалізованої бортової ЕОМ для бронетехніки" 7 с. Вісник Хмельницького національного університету №2, 2007. Технічні науки. Том 2. с.29-33. Хмельницький, 2007. 14. IEEE Std 1363-2000 IEEE Standard Specifications for Public-Key Cryptography Sponsor Microprocessor and Microcomputer Standards Committee of the IEEE Computer Society. Approved 30 January 2000. 9. В. С. Глухов, Н. В. Заіченко, Б. О. Оліярник, А. Б. Бондарук. Особливості проектування обчислювальних модулів для бортових інформаційно-керуючих систем бронетанкової техніки. "Механіка та машинобудування" // Науково-технічний журнал – Харків: НТУ «ХПІ», 2006. - №1, -311 с. С.238-244. 10. Глухов В. С., Заіченко Н. В., Иванов В. І., Оліярник Б. О., Тупиця А. В. Обчислювальні модулі для бортових інформаційно-керуючих систем бронетанкової техніки. "Механіка та машинобудування". Науково-технічний журнал №1'2000. Харківський державний політехнічний університет, Відділення механіки та машинобудування Академії наук Вищої школи України. Харків, 2000. 17. ДСТУ ISO/IEC 7498-1:2004. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. Частина 1. Базова модель (ISO/IEC 7498-1:1994, IDT). 18. Автомобильная навигационная система POCKET GPS PRO MOSCOW. <http://www.sysnavigation.ru/articles/1818/> 19. Электронная картографическая навигационная информационная система SAVENAV-3. <http://www.ntutc.ru/kartografia.htm> 20. В.С. Глухов. Система команд криптографічного процесора " // Вісник Національного університету "Львівська політехніка" № 523 «Комп'ютерні системи та мережі». Львів. Видавництво Національного університету «Львівська політехніка». 2004. С.42 – 50. 21. А. О. Мельник, Т. А. Коркішко. Система підтримки виконання алгоритмів криптографічного захисту інформації на основі програмованого процесора та криптографічних акселераторів // Вісник Державного університету "Львівська політехніка" № 385 «Комп'ютерні системи та мережі». Львів. Видавництво Державного університету «Львівська політехніка». 2000. С. 77 – 80. 22. В. Б. Аронов, В. С. Глухов, Я. К. Деревенко, Н. В. Заіченко, С. Ф. Федуняк. Одноплатный арифметический процессор, подключаемый к магистрали ГОСТ 26765.51-86, и средства обеспечения его серийного производства // "1-ая научно-техническая конференция НПО "Фазотрон". Тезисы докладов. Москва, 19-21 сентября 1989 г. 23. В. С. Глухов, Н. В. Заіченко. Арифметический спецвычислитель с кэш-памятью команд. "Тезисы докладов 29-ой научно-технической конференции НПО "Антей". Москва, 1990 г

УДК 004.056.5:004.057.2(045)

КРИПТОГРАФИЧЕСКИЕ ОСНОВАНИЯ РАЗРАБОТКИ СТАНДАРТА СТ РК 1073-2007

Альжан Абдрахманов, Дана Байбатчаева
КНБ Республики Казахстан

Аннотация: Рассматривается концепция построения стандарта СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования", общие требования к средствам криптографической защиты информации (СКЗИ), основания выбора допустимых диапазонов значений основных параметров криптографических алгоритмов, дополнительные меры безопасности.

Summary: Constructing conception of the standard ST RK 1073-2007 "Means of cryptographic information protection. General technical requirements", general requirements for MCIP, reasons of the selection of

allowable ranges of basic parameter values of cryptographic algorithms, additional security measures are considered.

Ключевые слова: Защита информации, криптография, шифрование, имитозащита, аутентификация, электронная цифровая подпись, уровень безопасности, подтверждение соответствия.

I Введение

С конца прошлого века в Казахстане, как и во всем современном мире, активно создаются и развиваются информационные системы различного масштаба и назначения, идет процесс глобальной информатизации всех сфер жизни общества. В результате этого стали чрезвычайно востребованы средства криптографической защиты информации (СКЗИ), предназначенные для защиты несекретных служебных и коммерческих сведений, а также сведений ограниченного распространения. Одновременно с этим, для защиты покупателей и пользователей СКЗИ в Казахстане стала развиваться система сертификации этих средств.

На первом этапе сложилась неоднозначная ситуация, характеризующаяся следующими противоречивыми факторами.

1. Действующими криптографическими стандартами являлись только советский стандарт ГОСТ 28147-89, а также межгосударственные стандарты ГОСТ 34.310-95 и ГОСТ 34.311-95.

2. Не были регламентированы многие криптографические аспекты, в частности, асимметричное шифрование, генерация и распределение ключей.

3. Де-факто на рынке присутствовали СКЗИ, реализующие, в основном, иностранные стандарты и алгоритмы DES, TripleDES, AES, DSA, SHA-1 и другие.

4. Значительное количество разработанных в Казахстане СКЗИ, даже реализующих указанные выше действующие и иностранные стандарты, являлись криптографически нестойкими, в частности, из-за некорректной реализации генерации и управления ключами.

5. На практике сертификацию СКЗИ проводили неоправданно большое количество аккредитованных в Госстандарте органов, многие из которых подменяли понятия и проводили исследования на соответствие СКЗИ иным, а не криптографическим стандартам.

В результате всего этого было невозможно проводить объективную оценку качества (криптографической стойкости) СКЗИ в рамках существующей на тот момент системы сертификации.

Создавшееся положение было исправлено Комитетом национальной безопасности путем разработки и утверждения в Госстандарте Республики Казахстан государственного стандарта СТ РК 1073-2002 "Средства криптографической защиты информации. Общие технические требования" [1], аккредитации в Госстандарте Республиканского государственного предприятия "Казспецпредприятие" Комитета национальной безопасности на проведение исследований на соответствие этому стандарту, фактического ограничения Госстандартом количества аккредитованных органов, проводящих такие исследования.

В основание разработки этого стандарта были положены следующие концептуальные подходы [2].

1. В ходе сертификационных исследований следует рассматривать СКЗИ как комплексные технологически завершенные средства защиты информации.

2. Определение в стандарте четырех уровней безопасности СКЗИ, увязанных с возможным ущербом от разглашения, навязывания или несанкционированного изменения защищаемой информации, а также с вычислительной сложностью алгоритмов вскрытия криптографической защиты (не менее 248, 296, 2128 и 2192 операций для 1, 2, 3 и 4 уровней безопасности соответственно). При этом ущерб выражается в минимальных расчетных показателях (МРП), введенных законодательством Республики Казахстан (1 мрп в различные годы соответствовал 5-10 евро).

3. Определение в стандарте основных криптографических терминов, соответствующих терминам, используемым в широко распространенных иностранных и международных стандартах.

4. Определение в стандарте общих требований, предъявляемых ко всем СКЗИ, независимо от уровня безопасности (например, полное описание реализованных алгоритмов в нормативной и технической документации, полнота эксплуатационной документации, контроль несанкционированного изменения СКЗИ, использование для генерации ключей физических генераторов шума или датчиков случайных событий).

5. Определение в стандарте дополнительных организационных и технических требований, предъявляемых к СКЗИ, в зависимости от уровня безопасности (например, информирование о режиме работы СКЗИ, защита ключей на этапе распределения и управления, гарантированное удаление ключей).

6. Определение в стандарте основных параметров криптографических алгоритмов и допустимых диапазонов их значений для потенциального достижения криптографической стойкости, соответствующей уровню безопасности и сбалансированной со стойкостью алгоритмов другого типа, с учетом реально существующих криптографических алгоритмов (например, длина ключа симметричных алгоритмов – не менее 56, 112, 168 и 256 битов для 1, 2, 3 и 4 уровней безопасности соответственно).

7. Отказ от определения в стандарте конкретных криптографических алгоритмов и, как следствие, возможность сертификации СКЗИ, реализующих криптографические алгоритмы практически любого вида.

Проведение сертификации целого ряда отечественных и импортных СКЗИ различного типа на соответствие требованиям стандарта СТ РК 1073-2002, широкое внедрение сертифицированных СКЗИ, в том числе в рамках Закона Республики Казахстан от 7 января 2003 года "Об электронном документе и электронной цифровой подписи", изменение популярности и распространения некоторых стандартов и алгоритмов, в частности, принятие в качестве межгосударственного стандарта ГОСТ 34.310-2004, апробация СТ РК 1073-2002 на международных научных конференциях подтвердили правильность указанных выше концептуальных подходов и саму идею разработки стандарта "Средства криптографической защиты информации. Общие технические требования".

В 2007 году на плановой основе Комитетом национальной безопасности Республики Казахстан была разработана новая редакция этого стандарта – государственный стандарт СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" [3], который вводится в действие с 1 января 2009 года. Сохраняя концепцию предыдущей редакции новый стандарт учитывает современные теоретические и практические достижения в криптографии, опыт сертификационных исследований, имеет более выраженную ориентацию на криптографические алгоритмы, стандартизованные в странах СНГ.

Наиболее сильные изменения коснулись вычислительной сложности алгоритмов вскрытия криптографической защиты, увязанных с уровнями безопасности СКЗИ (не менее 250, 280, 2120 и 2160 операций для 1, 2, 3 и 4 уровней безопасности соответственно, см. таблицу 1), что повлекло некоторые изменения допустимых диапазонов значений основных параметров криптографических алгоритмов.

II Криптографические основания выбора параметров СКЗИ

Рассмотрим более подробно параметры криптографических алгоритмов и другие параметры СКЗИ, которые определены в стандарте и непосредственно влияют на верхнюю оценку стойкости СКЗИ, а также рассмотрим криптографические основания выбора допустимых диапазонов значений этих параметров.

1. Длина ключа симметричных алгоритмов (не менее 60, 100, 150 и 200 бит для 1, 2, 3 и 4 уровней безопасности, соответственно) ограничивается исходя из вычислительной сложности атаки тотального опробования ключей и 10 – 20% уменьшением экспоненты вычислительной сложности иных атак (по сравнению с указанной атакой) на общепризнанные качественные симметричные алгоритмы. Например, DES не соответствует требованиям стандарта; TripleDES, AES-128 соответствуют 2 уровню; AES-192 – 3 уровню; ГОСТ 28147-89, AES-256 – 4 уровню.

2. Длина ключа асимметричных алгоритмов (не менее 120, 160, 250 и 400 бит для 1, 2, 3 и 4 уровней безопасности, соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов, вычислительной сложности $O(\sqrt{q})$ р-алгоритма Полларда дискретного логарифмирования в произвольной конечной циклической группе порядка q , а также с учетом параметров реально существующих алгоритмов. Например, DSA, EC DSA (160-битовый секретный ключ, являющийся элементом циклической группы) соответствуют 2 уровню (из-за другого параметра общая оценка DSA все же будет ниже дана); ГОСТ 34.310-2004 (255/256-битовый секретный ключ) – 3 уровню [4, 5].

3. Длина ключа асимметричных алгоритмов, криптографическая стойкость которых основана на вычислительной сложности задачи разложения составного числа на множители или задачи дискретного логарифмирования в конечном поле (не менее 500, 1500, 4000 и 8000 бит для 1, 2, 3 и 4 уровней безопасности, соответственно), ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной сложности не более $L_p [1/3, 1,923]$ общего решения задачи дискретного логарифмирования в

Таблица 1 – Основные параметры стандарта СТ РК 1073-2007

Пункт	Требование	1 уровень	2 уровень	3 уровень	4 уровень
4.2	Технологическая завершенность, работоспособность СКЗИ	+	+	+	+
4.3.у	Ущерб от НСД к защищаемой информации, не более мрп	100	10 000	1 млн.	100 млн.
4.4	Вычислительная сложность алгоритма вскрытия, не менее	2^{50}	2^{80}	2^{120}	2^{160}
5.1.1 5.у.6	Генератор ключей	случайные события	случайные события	физический шум	физический шум

5.1.2	Криптозащита ключей, распределяемых по незащищенному каналу	+	+	+	+
5.1.3	Единственность алгоритма для каждого ключа	+	+	+	+
5.1.4	Защита от несанкционированного изменения СКЗИ	+	+	+	+
5.2.1	Полное описание алгоритмов в технической документации	+	+	+	+
5.2.3	Соответствие СКЗИ технической документации	+	+	+	+
5.2.4	Полнота эксплуатационной документации	+	+	+	+
5.y.1	Длина ключа симметричных алгоритмов, не менее бит	60	100	150	200
5.y.2	Длина ключа асимметричных алгоритмов, не менее бит	120	160	250	400
5.y.3	Длина ключа асимметричных алгоритмов в конечных полях, бит	500	1500	4000	8000
5.y.4	Длина хэш-кода, не менее бит	120	160	250	400
5.y.5	Длина ЭЦП, не менее бит	120	200	300	400
5.y.6	Отклонение от 0,5 вероятности (бит_ключа = 1), не более	0,03	0,01	0,003	0,001
5.y.7	Выявление искаженных ключей, с вероятностью не менее		0,9999	0,999999	0,99999999
5.y.8	Выявление искаженных зашифр. данных, с вероятностью не менее		0,9999	0,999999	0,99999999
5.y.9	Информирование о режиме работы		режим шифрования	+ нештатные ситуации	+ предотвращение транзита
5.y.10	Криптозащита ключей на этапе распределения и управления			+(или орг.меры)	+
5.y.11	Процедуры гарантированного удаления ключей			+(если есть)	+

конечном поле и $L2n [1/3, 1,587]$ – в конечном поле $GF(2n)$, а также вычислительной сложности не более $Ln[1/3, 1,526]$ разложения в ряде случаев целого числа n на множители, где $Lq[\alpha, c] = O((\exp((c + o(1)) * (\ln q)^\alpha (\ln \ln q)^{1-\alpha})))$. В частности, при $q \approx 2500, 21500, 24000$ и 28000 значение $Lq=p [1/3, 1,923]$ достигает 263,3, 2102,3, 2154,9 и 2206,4 соответственно, а значение $Lq=n [1/3, 1,526]$ достигает 250,2, 281,2, 2122,9 и 2163,8, что также удовлетворяет ограничениям на вычислительную сложность алгоритмов вскрытия криптографической защиты для 1, 2, 3 и 4 уровней безопасности соответственно. Например, DSA (512-1024 битовый открытый ключ, являющийся элементом конечного поля), RSA-512, RSA-1024 соответствуют 1 уровню; RSA-1536, RSA-2048 – 2 уровню; RSA-4096 – 3 уровню.

4. Длина хэш-кода (не менее 120, 160, 250 и 400 бит для 1, 2, 3 и 4 уровней безопасности, соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов, вычислительной сложности $O(2^{m/2})$ атаки Юваля (эффект "день рождения"), где m – длина хэш-кода, а также с учетом параметров реально существующих алгоритмов. Например, MD4, MD5, RIPEMD соответствуют 1 уровню (из-за существования алгоритмов поиска коллизий вычислительной сложности ≈ 220 -230 оценка этих хэш-функций будет дана ниже); RIPEMD-160, SHA-1 – 2 уровню; ГОСТ 34.311-95 – 3 уровню; SHA-2 – 4 уровню.

5. Длина ЭЦП (не менее 120, 200, 300 и 400 бит для 1, 2, 3 и 4 уровней безопасности, соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной

сложности атаки Юваля. Например, DSA, EC DSA соответствуют 3 уровню; ГОСТ 34.310-2004, RSA-512, RSA-1024, RSA-2048, RSA-4096 – 4 уровню.

6. Вероятность принятия каждым битом ключа единичного значения (отклонение вероятности от 0,5 не более 0,03, 0,01, 0,003 и 0,001 для 1, 2, 3 и 4 уровней безопасности соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной сложности модифицированного метода тотального опробования ключей [6].

7. Вероятность выявления искаженных на этапе распределения и загрузки ключей (не менее 0,9999, 0,999999 и 0,99999999 для 2, 3 и 4 уровней безопасности соответственно, при этом для 3 и 4 уровней выявление как случайно, так и умышленно искаженных ключей) ограничивается с учетом параметров реально существующих алгоритмов вычисления контрольных сумм и имитовставок. Например, CRC-16, CRC-32 соответствуют 2 уровню; режим выработки имитовставки ГОСТ 28147-89 – 4 уровню.

8. Вероятность выявления искаженных зашифрованных данных (не менее 0,9999, 0,999999 и 0,99999999 для 2, 3 и 4 уровней безопасности соответственно, при этом для 3 и 4 уровней выявление как случайно, так и умышленно искаженных данных) ограничивается с учетом параметров реально существующих алгоритмов вычисления контрольных сумм и имитовставок. Аналогично предыдущему: CRC-16, CRC-32 соответствуют 2 уровню; режим выработки имитовставки ГОСТ 28147-89 – 4 уровню.

III Заключение

Таким образом, можно сделать вывод, что государственный стандарт Республики Казахстан СТ РК 1073-2007 "Средства криптографической защиты информации. Общие технические требования" является достаточно сбалансированным, криптографически обоснованным, ориентированным на реальное применение в ходе разработки и сертификационных исследований СКЗИ, регламентирующим криптографические, а также наиболее важные организационные и технические вопросы, возникающие при эксплуатации СКЗИ. Полагаем, что этот стандарт удовлетворяет современным потребностям в области сертификации СКЗИ и рекомендуется нами для широкого использования в странах СНГ в целях гармонизации действующей нормативной правовой базы.

Литература: 1. СТ РК 1073-2002. Средства криптографической защиты информации. Общие технические требования. – Астана: Госстандарт, 2002. – 32 с. 2. Абдрахманов А. Е., Байбатчаева Д. А. Криптографические основания разработки стандарта СТ РК 1073-2002 // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник. – К.: КПІ, ДСТСЗІ СБУ, 2004. – Вип. 9. – С. 121–125. 3. СТ РК 1073-2007. Средства криптографической защиты информации. Общие технические требования. – Астана: Госстандарт, 2008. – 30 с. 4. Бабаи А. В., Шанкин Г. П. Криптография / Под ред. В. П. Шерстюка, Э. А. Применко. – М.: СОЛОН-Р, 2002. – 512 с. 5. A. Menezes, P. Oorschot, S. Vanstone. Handbook of Applied Cryptography. – Boca Raton, New York, London, Tokyo: CRC Press, 1997. – 780 p. 6. Абдрахманов А. Е., Байбатчаева Д. А. К вопросу об использовании неравновероятности генератора ключей при вскрытии шифров методом тотального опробования // Математический журнал. – Алматы: Институт математики МО и Н РК, 2006. – Т. 6, № 3(21). – С. 14–17.