3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 004.056.5:004.057.2(045)

КРИПТОГРАФИЧЕСКИЕ ОСНОВАНИЯ РАЗРАБОТКИ СТАНДАРТА СТ РК 1073-2002

Альжан Абдрахманов, Дана Байбатчаева
Комитет национальной безопасности республики Казахстан

Аннотация: **Рассматривается концепция построения стандарта СТ РК 1073-2002 "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 1073-2002 "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, сертификация.**

I Введение

В последние годы, когда обеспечение защищенности информации перестало быть задачей только национальной безопасности, все более пристальное внимание уделяется информационной безопасности в коммерческой сфере. Процесс информатизации общества способствует появлению на рынке информационных услуг и технологий различных программных продуктов и средств обработки информации, вследствие чего возникает острая необходимость проведения сертификации коммерческих средств криптографической защиты информации (СКЗИ).

К 2002 году в Казахстане в области стандартизации коммерческих СКЗИ сложилась ситуация, характеризуемая следующими противоречивыми факторами:

– действующими стандартами являлись ГОСТ 28147-89 и, в качестве межгосударственных, ГОСТ 34.310-95 и ГОСТ 34.311-95;

– не были регламентированы многие криптографические аспекты, в частности, асимметричное шифрование, генерация и распределение ключей;

– де-факто на рынке присутствовали СКЗИ, реализующие, в основном, иностранные стандарты и алгоритмы DES, TripleDES, AES, DSA, SHA-1;

– значительное количество разработанных в Казахстане СКЗИ, даже реализующих указанные выше стандарты, являлись криптографически нестойкими, в частности, из-за некорректной реализации управления ключами.

В результате было невозможно проводить объективную оценку стойкости СКЗИ в рамках механизма сертификации.

Выходом из создавшейся ситуации стала разработка Комитетом национальной безопасности Республики Казахстан и принятие Госстандартом Республики Казахстан стандарта СТ РК 1073-2002 "Средства криптографической защиты информации. Общие технические требования".

Концептуальными основаниями разработки стандарта явились:

1. рассмотрение СКЗИ как комплексных технологически завершенных средств защиты информации, а не как отдельных элементов системы, реализующих некие криптографические алгоритмы;

2. введение четырех уровней безопасности СКЗИ, увязывание их с возможным ущербом от разглашения, навязывания или несанкционированного изменения защищаемой информации, а также с вычислительной сложностью известных алгоритмов вскрытия криптографической защиты (не менее 2^{48}, 2^{96}, 2^{128} и 2^{192} операций для 1, 2, 3 и 4 уровней соответственно, см. таблицу 1);

3. определение 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;

4. отказ от стандартизации (определения) собственно криптографических алгоритмов, ориентация на возможность сертификации СКЗИ, реализующих практически любые криптографические алгоритмы.

Исходя из основных принципов безопасности эксплуатации криптосетей, в стандарте были сформулированы следующие общие требования к СКЗИ всех уровней:

Таблица 1 – Сводная таблица СТ РК 1073-2002

Пункт	Требование	1 уровень	2 уровень	3 уровень	4 уровень
3.1	Технологическая завершенность, работоспособность СКЗИ	+	+	+	+
3.3.y	Ущерб от НСД к защищаемой информации, не более МРП	100	10 000	1 млн.	100 млн.
3.4	Вычислительная сложность алгоритма вскрытия, не менее	2^48	2^96	2^128	2^192
4.1.1 4.y.6	Генератор ключей	случайные события	случайные события	физический шум	физический шум
4.1.2	Криптозащита ключей, распределяемых по незащищенному каналу	+	+	+	+
4.1.3	Единственность алгоритма для каждого ключа	+	+	+	+
4.1.4	Защита от несанкционированного изменения СКЗИ	+	+	+	+
4.2.1	Полное описание алгоритмов в нормативной и техдокументации	+	+	+	+
4.2.3	Соответствие СКЗИ нормативной и технической документации	+	+	+	+
4.2.4	Полнота эксплуатационной документации	+	+	+	+
4.y.1	Длина ключа симметричных алгоритмов, не менее бит	56	112	168	256
4.y.2	Длина ключа асимметричных алгоритмов, не менее бит	384	1536	3072	8192
4.y.3	Длина ключа асимметричных алгоритмов на эллиптических. кривых, бит	112	224	336	512
4.y.4	Длина хэш-кода, не менее бит	112	160	256	320
4.y.5	Длина ЭЦП, не менее бит	112	160	256	512
4.y.6	Вероятность 1 для бита ключа, отклонение от 0,5 не более	0.01 (псевдо-случайный.)	0.001 (псевдо-случайный.)	0.001 (случайный)	0.0001 (случайный)
4.y.7	Выявление искаженных ключей, с вероятностью не менее		0.9999 (случайные искажения)	0.999999 (имитовставка, ЭЦП)	0.999999999 (имитовставка, ЭЦП)
4.y.8	Выявление искаженных зашифрованных данных, с вероятностью не менее		0.9999 (случайные искажения)	0.999999 (имитовставка, ЭЦП)	0.999999999 (имитовставка, ЭЦП)
4.y.9	Информирование о режиме работы		режим шифрования	+ нештатные ситуации	+ предотвраще-ние транзита
4.y.10	Криптозащита ключей на этапе распределения и управления			+ (или орг. меры)	+ (иерархи-ческая)

Продовження Таблиці 1.

4.у.11	Процедуры гарантированного удаления ключей			+ (если есть)	+

– использование для генерации ключей физических генераторов шума или датчиков случайных событий;
– криптографическая защита ключей, распределяемых по незащищенному каналу;
– использование ключа только одним криптографическим алгоритмом;
– защита от несанкционированного изменения СКЗИ;
– полное описание алгоритмов в нормативной и технической документации;
– соответствие СКЗИ нормативной и технической документации;
– полнота эксплуатационной документации.

II Криптографические основания выбора параметров

Рассмотрим более подробно основные параметры криптографических алгоритмов, непосредственно влияющие на оценку их стойкости сверху, а также криптографические основания выбора допустимых диапазонов.

1. Длина ключа симметричных алгоритмов (не менее 56, 112, 168, 256 бит для 1, 2, 3, 4 уровней соответственно) ограничивается исходя из вычислительной сложности атаки тотального опробования ключей и 10 – 20% уменьшением экспоненты вычислительной сложности иных атак на общепризнанно качественные симметричные алгоритмы. Например, для алгоритма DES при длине ключа 56 бит, при максимальной и средней вычислительной сложности тотального опробования 2^{56} и 2^{55} соответственно, сложность различных алгоритмов его дифференциального и линейного криптографического анализа составляет порядка $2^{48} – 2^{50}$, то есть DES соответствует 1 уровню безопасности. Для сравнения: TripleDES – 2 уровень, ГОСТ 28147-89 – 4 уровень, AES – 2 – 4 уровни в зависимости от параметров.

2. Длина ключа асимметричных алгоритмов (не менее 384, 1536, 3072, 8192 бит для 1, 2, 3, 4 уровней соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной сложности алгоритмов разложения числа на множители в кольце целых чисел Z и дискретного логарифмирования в кольце вычетов Z_n, которая составляет для универсальных в применении алгоритмов примерно $L_n(1/3; 1,8)$ или более, где

$$L_n(\alpha, c) = \exp\{c * (\ln n)^{\alpha} * (\ln \ln n)^{1-\alpha}\},$$

для числовых колец. Для иллюстрации: RSA-512,-1024 соответствуют 1 уровню, RSA-2048 – 2 уровню.

3. Длина ключа асимметричных алгоритмов на эллиптических кривых (не менее 112, 224, 336, 512 бит) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной сложности $O(\sqrt{q})$ алгоритма Полларда дискретного логарифмирования на эллиптической кривой, где q – мощность группы точек кривой. Данная оценка была выбрана как лучшая (наименьшая) из известных в международной практике алгоритмов дискретного логарифмирования на эллиптических кривых и наиболее применимая к большинству видов кривых. Для иллюстрации: EC DSA-160 соответствует 1 уровню, ГОСТ Р 34.10-2001 – 2 уровню.

4. Длина хэш-кода (не менее 112, 160, 256, 320 бит для 1, 2, 3, 4 уровней соответственно) ограничивается исходя из сбалансированности со стойкостью симметричных алгоритмов и вычислительной сложности $O(\sqrt{2^m})$ атаки Ювеля (эффект "день рождения"), где m – длина хэш-кода. Для 2 уровня было существенным образом учтено наличие в те годы максимум 160-битовых базовых хэш-функций и целесообразность повышения их уровня по сравнению с 1 уровнем широко распространенных 128-битовых хэш-функций. Для 3 и 4 уровней была учтена возможность удвоения длины хэш-кода агрегированием типа MDC-2 хэш-функций, удовлетворяющих 1 и 2 уровням соответственно. При этом, сложность атаки Ювеля на хэш-функции, удовлетворяющие 2 и 4 уровням, составляет около 2^{80} и 2^{160} соответственно. Данные оценки ниже заявленного порога для вычислительной сложности алгоритмов вскрытия криптографической защиты этих уровней – 2^{96} и 2^{192} соответственно. Однако здесь явного противоречия нет, так как атака Ювеля не является в полной мере атакой только по выходным данным. Для иллюстрации: MD4, MD5, RIPEMD соответствуют 1 уровню, RIPEMD-160, SHA-1 – 2 уровню, ГОСТ 34.311-95 – 3 уровню, SHA-2 – 4 уровню.

5. Длина ЭЦП (не менее 112, 160, 256, 512 бит для 1, 2, 3, 4 уровней соответственно) ограничивается, исходя из сбалансированности со стойкостью симметричных алгоритмов, хэш-функций и вычислительной сложности алгоритмов дискретного логарифмирования и атаки Ювеля. Для иллюстрации: ГОСТ 34.310-95, ГОСТ Р 34.10-2001, DSA соответствуют 3 уровню, RSA-512,-1024,-2048 – 4 уровню.

Требование равновероятности бита ключа (отклонения вероятности принятия каждым битом ключа единичного значения от 0,5 не более 0,01, 0,001, 0,001, 0,0001 для 1, 2, 3, 4 уровней соответственно), а также требование использования для 3 и 4 уровней только физических генераторов шума, дающих случайную, а не псевдослучайную последовательность, сформулированы исходя из их взаимной сбалансированности, возможности эксплуатации на основе проведенного статистического анализа работы целого ряда датчиков случайных и псевдослучайных чисел.

Требование полноты эксплуатационной, нормативной и технической документации сформулировано с целью установления соответствия заявляемых и реализуемых СКЗИ криптографических алгоритмов, а также для проверки восстановления корректной работы средства после смоделированных нештатных ситуаций при проведении сертификации СКЗИ.

Кроме того, для старших уровней стандарт предусматривает следующие дополнительные меры безопасности:

1. выявление искаженных на этапе распределения и загрузки ключей (с вероятностью не менее 0,9999, 0,999999, 0,999999999 для 2, 3 и 4 уровня соответственно); для иллюстрации: CRC-16, CRC-32 соответствуют 2 уровню, режим выработки имитовставки ГОСТ 28147-89 – 4 уровню;
2. выявление искаженных зашифрованных данных (с вероятностью не менее 0,9999, 0,999999, 0,999999999 для 2, 3 и 4 уровня соответственно); аналогично предыдущему: CRC-16, CRC-32 соответствуют 2 уровню, режим выработки имитовставки ГОСТ 28147-89 – 4 уровню;
3. информирование о режиме работы СКЗИ (об установлении, сбросе и невозможности установления режима шифрования; а также о других нештатных ситуациях; а также предотвращать транзит через себя открытых данных для 2, 3 и 4 уровня соответственно);
4. защита ключей на этапе распределения и управления (организационными и техническими мерами и иерархическая криптографическая защита для 3 и 4 уровня соответственно);
5. процедуры гарантированного удаления ключей (с помощью штатных процедур и, в случае отсутствия таковых, с помощью поставляемых в комплекте с СКЗИ технических средств для 3 и 4 уровня соответственно).

Ш Заключение

В Республике Казахстан сертификацию коммерческих СКЗИ на соответствие требованиям стандарта СТ РК 1073-2202 проводит аккредитованный орган Республиканское государственное предприятие “Казспецпредприятие”. К настоящему времени сертифицировано четыре средства: программное средство шифрования файловых сообщений (4 уровень), аппаратно-программное средство генерации ключей (4 уровень), программное средство, реализующее функции удостоверяющего центра в рамках инфраструктуры открытых ключей (2 уровень), и аппаратно-программное средство шифрования данных и формирования и проверки электронной цифровой подписи (2 уровень).

Таким образом, стандарт СТ РК 1073-2002 является достаточно сбалансированным, криптографически обоснованным, ориентированным на реальное применение в ходе сертификационных исследований. Как разработчики данного стандарта, полагаем, что по мере развития различных направлений криптографии, разработки новых СКЗИ, криптографических алгоритмов и подходов к их анализу в стандарт СТ РК 1073-2002 будут вноситься соответствующие изменения.

Так, для новой редакции стандарта, выход которой предусмотрен в 2007 году, прорабатывается увеличение величины возможного ущерба от разглашения, навязывания или несанкционированного изменения защищаемой информации, некоторое уменьшение вычислительной сложности алгоритмов вскрытия криптографической защиты (не менее 2^{40}, 2^{80}, 2^{120} и 2^{160} для 1, 2, 3, 4 уровней соответственно), соответствующая коррекция допустимых диапазонов значений параметров криптографических алгоритмов (например, длина ключа симметричных алгоритмов не менее 50, 100, 150 и 200 бит для 1, 2, 3, 4 уровней соответственно). Кроме того, планируется разработать методические указания по проведению сертификационных исследований.

*Литература: **1.** Средства криптографической защиты информации. Общие технические требования. СТ РК 1073-2002. – Астана: Госстандарт, 2002. – 32 с. **2.** ГОСТ 28147-89 Системы защиты информации. Защита криптографическая. Алгоритм криптографического преобразования. **3.** ГОСТ 34.310-95 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи на базе асимметрического криптографического алгоритма. **4.** ГОСТ 34.311-95 Информационная технология. Криптографическая защита информации. Функция хэширования. **5.** ГОСТ Р 34.10-2001 Информационная технология. Криптографическая защита информации.*

Процессы формирования и проверки электронной цифровой подписи на эллиптических кривых.. ***6.*** *A. Menezes, P. Oorschot, S. Vanstone "Handbook of Applied Cryptography", CRC Press, 1997, 780 с.*

УДК 681.3.06

ОЦЕНКА ВЕРОЯТНОСТИ ПЕРЕКРЫТИЯ ШИФРА В РЕЖИМЕ СЧЕТЧИКА

Юрий Горбенко, Денис Пономарев
Харьковский национальный университет радиоэлектроники

Аннотация: **Рассматривается и решается проблема расчета и обоснования срока действия ключей поточного шифра или блочного шифра, используемого в режиме гаммирования. Произведена оценка вероятностей перекрытия шифра с использованием наиболее распространенных длин ключа.**
Summary: **The problem of calculating and estimation key validity time of stream cipher and block symmetric cipher in a counter mode has been considered and solved. The probability of overlapping estimation has been made for the most common key lengths.**
Ключевые слова: **Информационная безопасность, вероятность перекрытия шифра, поточный шифр, режим счетчика.**

Введение

Алгоритмы шифрования играют жизненно важную роль при защите таких данных, как медицинская и финансовая информация, уникальные персональные идентификационные номера (PIN) и т. д. Однако в последнее время возникает необходимость проверки качества функционирования шифров в некоторых режимах. Даная работа имеет целью анализ наиболее распространенных в настоящее время блочно симметричных криптоалгоритмов и оценка перекрытия таких шифров в режиме счетчика.

I Вероятность перекрытия шифра

Пускай вероятность перекрытия шифра равна $P_{пш}$. Тогда, исходя из того, что вероятности перекрытия и вероятность обратного этому события составляют полную группу событий, получаем: $P_{пш}+P_{оп}=1$. Вероятность $P_{оп}$ можно выразить как

$$P_{оп} = n_{оп}/n_{\Sigma}. \quad (1)$$

Тут $n_{оп}$ – число размещений n сообщений на периоде L без перекрытия за n обращений, а n_{Σ} является общим числом гамм, сформированных для n сообщений. При каждом обращении к алгоритму формирования гаммы шифрующей существует L вариантов выбора. Поскольку все обращения являются случайными, то на n обращениях

$$n_{\Sigma} = \mathrm{L}^n. \quad (2)$$

За n обращений $n_{оп}$ можно описать, учтя, что при первом обращении существует $n_1=n$ вариантов выбора гамм. При втором и последующих обращениях соответственно имеется n–1, n–2 ... и т. д. вариантов выбора отрезков. Таким образом, всего можем выбрать:

$$n_{оп}=(n-1)! \quad (3)$$

Далее поскольку отрезки не перекрываются, то расстояния между ними будут $x_1, x_2, \ldots, x_n \geq 0$ и таких расстояний будет n. Значит, справедливым будет следующее выражение

$$\sum_{i=1}^{n} x_i + \sum_{i=1}^{n} l_i = L. \quad (4)$$

Из этого выражения следует, что число свободных для размещения позиций в периоде будет равно

$$\sum_{i=1}^{n} x_i = L - \sum_{i=1}^{n} l_i = L - Z, \quad (5)$$

где $Z=nl_M$ – произведение длин сообщений l_M на их число n.

Определить число разных расстановок $n-1$ перегородок между $L-Z$, т. е. число способов размещения n предметов по $L-Z$ ящикам [1, 2], можно по следующей формуле

$$C_{L-Z+r-1}^{r-1}. \quad (6)$$