ПРОТОКОЛЫ И СРЕДСТВА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

УДК 681.3. 06

СТОЙКОСТЬ ОСНОВНЫХ СТАНДАРТОВ ЭЦП ОТ АТАК НА СВЯЗАННЫХ КЛЮЧАХ И «ПОЛНОЕ РАСКРЫТИЕ»

М.Ф. БОНДАРЕНКО, Ю.И. ГОРБЕНКО

Приводятся результаты сравнительного анализу криптографической стойкости ЭЦП ISO/IEC 15946-2 (EC-DSA, EC-GDSA, EC-KCDSA), ГОСТ Р 34.10-2001 и ДСТУ 4145-2002 от атак на связанных ключах и «полное раскрытие».

The results of comparative analysis of cryptographic security of EDS ISO/IEC 15946-2 (ESDSA, ESGDSA, ESKCDSA), State Standard of R 34.10-2001 and State Standard of Ukraine 4145-2002 against attacks on linked keys and «complete opening» are provided.

В условиях существующей неопределенности присутствует риск разработки и внедрения ненадежных элементов системы электронной цифровой подписи (ЭЦП) и инфраструктуры открытых ключей (ИОК) в целом. На наш взгляд, в Украине недостаточно полно учитывается практический опыт технологически развитых государств относительно применения ИОК. Работа по гармонизации международных стандартов, поддерживающих инфраструктуру открытых ключей, также осуществляется медленно. Остаются открытыми вопросы согласования национальной системы ЭЦП с международными инфраструктурами технологически развитых государств. Существуют проблемные вопросы в части доказательства безопасности, соответствующих уровней гарантий безопасности и стойкости криптографических преобразований. Особое внимание на международном уровне отводится проблемам стандартизации и отображению реализованных Политик. Приняты и уже нашли широкое применение базовые стандарты на системы электронной цифровой подписи [1-8].

На сегодня разработан и используется ряд стандартов (электронной) цифровой подписи [12-15]. Некоторые из них хорошо исследованы и прошли проверку временем относительно вопросов криптографической стойкости, в них обеспечиваются приемлемые скорости, они приняты в качестве международных или региональных стандартов.

Украина при создании национального стандарта пошла по пути использования преобразований в группе точек эллиптической кривой. В результате разработан и принят национальный стандарт ДСТУ 4145-2002 [11]. В отличие от Российской Федерации в своей разработке Украина пошла дальше, выбрав в качестве прототипа новый алгоритм, а не совершенствуя известный [12]. Как показывают исследования и практика, это было прогрессивным решением, которое позволило получить одну из лучших цифровых подписей по критерию стойкости против известных атак. Целью доклада является оценка и сравнения стандартов ЭЦП, применяемых на практике.

1. СТОЙКОСТЬ ЭЦП В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКОЙ КРИВОЙ ОТ АТАКИ ТИПА «ПОЛНОЕ РАСКРЫТИЕ»

Считается, что быстрейшими алгоритмами проведения атаки типа «полное раскрытие» случайных и не слабых кривых над полями $F(p)$, $F(2^m)$ и $F(p^m)$ на сегодняшний день являются методы Полларда со сложностью $O(\sqrt{\pi n/4}/r)$, где r – количество процессоров, применяемых в процессе криптоанализа.

Рассмотрим подробнее математический аппарат осуществления криптоаналитической атаки с применением методов Полларда, реализующих атаку типа полное раскрытие [8]. Основной задачей атаки является определение личного ключа соответствующего пользователя (объекта, субъекта).

Известны также уравнения, связывающие личный и открытый ключи:

$$Q = kG(\mathrm{mod}\, f(x), p), \qquad (1)$$

где $k = d$, или $k = -d$, или $k = d^{-1}$; d – личный ключ; G – значение базовой точки порядка n; $f(x)$ – примитивный полином над полем F_{p^m}.

Методы Полларда были предложены для вычисления дискретного логарифма в (Z/nZ). Идея заключается в том, что для любого конечного набора W и его отображения $F: W \to W$, последовательность $(w_k)_{k \in N_0}$ формируется по правилу $w_0 \in W$, $w_{k+1} = F(w_k)$, где $k \in N_0$ и в конечном итоге является замкнутым. Т.е. существуют целые числа $\lambda \geq 1$ и $\mu \geq 0$, такие, что $w_0, ..., w_{\mu+\lambda-1}$ являются попарно определенными, и $w_k = w_{k+\lambda}$, $k \geq \mu$. Допуская, что $w_0 \in W$ – попарно определенные, и $w_k = w_{k+\lambda}$, $k \geq \mu$, а также, что $w_0 \in W$ выбирается случайно (относительно равномерного распределения) и F – случайное отображение, ожидаемые значения для μ и λ находятся близко к $\sqrt{\pi |W|}/8 = 0.626...\sqrt{|W|}$. Для вычисления дискретного логарифма $d = \log_G Q$.

В работе [8] проведен анализ классической формулы определения сложности криптоанализа в группе точек эллиптической кривой, показано, что математическое ожидание сложности крипто-

анализа, как ожидаемое число элементов, выбранных для повторения, будет равняться:

$$E(X) \approx \sum_{k=0}^{\infty} e^{-x^2/(2n)} = \int_0^{\infty} e^{-x^2/(2n)} dx = \sqrt{\pi n/2}\,. \qquad (2)$$

Для формулы (2) необходима реализация, которая может сохранять все вычисленные значения. Т.е. ресурсы памяти для выполнения атаки должны представлять порядка $\sqrt{\pi n/2}$ элементов памяти, где каждый элемент памяти равняется количеству байт, необходимых для хранения одной точки.

В случае необходимости вычисления вероятности коллизии $P(n,k)$ при изменяемых (n,k), с учетом того, что n и k, как правило, недостаточно велики, рекомендуется использовать несколько модифицированную формулу (2) в следующем виде:

$$P(n,k) = 1 - \frac{n}{n}\cdot\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)\ldots\left(\frac{n-(k-1)}{n}\right) = 1 - \prod_{i=1}^{k-1}\left(1-\frac{i}{n}\right). \qquad (3)$$

В нашем случае $k << n$, поэтому $x \equiv k/n << 1$.

После простых преобразований получаем:

$$I^2 - I + 2n\ln(1-P_k) = 0. \qquad (4)$$

Проведем анализ уравнения (4).

1. Точное значение сложности с учетом приближения получим, решив уравнение второй степени (4).

2. Учитывая, что $I^2 >> I$, можно воспользоваться приближением:

$$I^2 \approx -2n\ln(1-P_k) \text{ или } I_{\rho} \approx \sqrt{-2n\ln(1-P_k)}\,. \qquad (5)$$

3. В случае $P_k = 0{,}99$ получим оценку:

$$I_{0,99} \approx \sqrt{-2n\ln 10^{-2}} = \sqrt{4\ln 10 n} \approx 3{,}03\sqrt{n}\,. \qquad (6)$$

Проведем также оценки на основе метода λ-Полларда с учетом вероятности коллизии.

$$I^2 - I + n\ln(1-P_k) = 0\,. \qquad (7)$$

Уравняв (7) и (4), видим, что в (7) вместо $2n$ присутствует параметр n. Решение уравнения (7) дает точный результат относительно I.

В табл. 1 приведенны значения сложности криптоанализа методами ρ- и λ-Полларда, полученные с использованием формул (4) и (7), в зависимости от значения n.

2. ОСНОВНЫЕ МЕТОДЫ ОЦЕНКИ СТОЙКОСТИ ЭЦП В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ ОТ АТАК НА СВЯЗАННЫХ КЛЮЧАХ

Помимо существующих атак относительно криптографических преобразований в группе точек эллиптических кривых, в том числе ЭЦП, существуют атаки на связанных ключах. При чем попытки реализовать атаки могут быть выполнены средством связывания как долгосрочных ключей, так и краткосрочных. Целью исследований в этом направлении является определение и сравнение стойкости разных стандартизированных ЭЦП против атак на связанных ключах. При этом особый интерес вызывает сравнение трех конкурирующих стандартов – FIPS 186 – 2 (ECDSA, X – 9.62) – стандартов США, ДСТУ 4145-2002 – национального стандарта, а также стандарта Российской Федерации ГОСТ Р 34.10-2001.

Особенностью (электронной) цифровой подписи как криптографического преобразования является то, что асимметричная пара ключей генерируется каждым владельцем лично в составе личного и открытого ключей. Это означает, что владелец такой пары ключей может генерировать ее, используя специальные средства, в том числе такие, что создаются нарушителем для мошенничества. Будем также считать, что ЭЦП осуществляется с использованием криптографических преобразований в группе точек эллиптической кривой.

Задача исследований заключается в следующем. Рассматриваются ЭЦП в группе точек ЭК, что представленные в ISO/IEC 15946-2 (EC-DSA, EC-GDSA, EC-KCDSA), ГОСТ Р 34.10-2001 и ДСТУ 4145-2002. Необходимо определить защищенность этих ЭЦП от селективной подделки на основе атак на связанных ключах, например, личных ключей сеанса k_1 и k_2. При рассмотрении ограничимся связанными ключами (k_1, k_2), при знании одного из которых другой может быть определен не выше чем с полиномиальной сложностью. Кроме того, необходимо определить условия и возможности обеспечения защиты от такой угрозы. В соответствии с указанным выше условиями также будем рассматривать защищенность от атак, для случаев, когда связываются долгосрочные ключи для трех видов ЭЦП – (EC-DSA, EC-GDSA, EC-KCDSA), ГОСТ Р 34.10-2001 и ДСТУ 4145-2002. Общим же критерием оценки защищенности ЭЦП от атак на связанных ключах является защищенность как от атак на связанных ключах сеанса, так и на долгосрочных ключах.

Таблица 1

Сложность решения дискретного логарифмического уравнения в группе точек ЕК с вероятностью $P = 0{,}99$

Метод \ n	2^{160}	2^{192}	2^{224}	2^{256}	2^{384}	2^{512}	2^{571}	2^{1021}
ρ-Полларда	$3{,}03\cdot 2^{80}$	$3{,}03\cdot 2^{96}$	$3{,}03\cdot 2^{112}$	$3{,}03\cdot 2^{128}$	$3{,}03\cdot 2^{192}$	$3{,}03\cdot 2^{256}$	$4{,}27\cdot 2^{285}$	$4{,}27\cdot 2^{510}$
λ-Полларда	$4{,}28\cdot 2^{80}$	$4{,}28\cdot 2^{96}$	$4{,}28\cdot 2^{112}$	$4{,}28\cdot 2^{128}$	$4{,}28\cdot 2^{192}$	$4{,}28\cdot 2^{256}$	$6{,}03\cdot 2^{285}$	$6{,}03\cdot 2^{510}$

Так как ключи k_1 и k_2 являются связанными для ЭЦП EC-DSA, например, $k_1 + k_2 = n$, где n – порядок базовой точки G, тогда $r_2 = r_1$ и у разных сообщений M_i и M_j первые составляющие подписи r_1 и r_2 являются одинаковыми. Отсюда следует, что если личный долгосрочный ключ сформировать согласно правилу:

$$d_a = -\frac{h_1 + h_2}{r_1} (\mathrm{mod}\, n), \qquad (8)$$

где h_1 и h_2 это хеш – значение для сообщений M_i и M_j, тогда для сообщений M_i и M_j будут сформированы одинаковые ЭЦП, т.е. $r_2 = r_1$ и $s_1 = s_2$.

Анализ возможных последствий для ЭЦП EC-DSA позволяет сделать такие выводы.

1. Угроза может быть реализована только для двух заведомо заданных M_i и M_j сообщений путем связывания ключей сеанса, т.е. k_1 и k_2.

2. Поскольку сообщения M_i и M_j известны и $r_1 = r_2$ являются открытыми ключами, то нарушитель может выработать для своего сообщения M_v такой же ЭЦП.

3. Из анализа EC-DSA необходимо также сделать вывод, что при известных h_1 и h_2, т.е. сообщениях M_i и M_j, а также всегда доступных $r_1 = r_2$ и n, нарушитель всегда может определить личный ключ.

4. Если эти сообщения обрабатываются в системе, то возникает угроза и для самого нарушителя, поскольку его личный ключ d_a при выполнении «обманных» действий также компрометируется. Показано также, что ЭЦП ECDSA является незащищенной и от атаки на связанных долгосрочных ключах.

Приведем некоторые результаты и выводы относительно защищенности алгоритма ЭЦП ГОСТ Р 34.10-2001 сначала рассмотрим атаки на связанных сеансовых ключах. Выберем, как и раньше, связанные ключи k_1, $k_2 = n - k_1$ и найдем ЭЦП для сообщений M_i и M_j. Таким образом, ГОСТ Р 34.10-2001 является стойким для атак на связанных ключах k_1 и k_2.

В то же время относительно ГОСТ Р 34.10-2001 существует атака на связанных долгосрочных личных ключах. Действительно, если

$$d_2 = n - d_1, k_1 = k_2 = k = const, n = q$$
$$\text{это } r_1 = r_2 = r \text{ и } s_1 = s_2.$$

Поэтому при указанных условиях

$$rd_1 + k,\ h_1 = rd_2 + kh_2 \text{ и } d_2 = q - d_1$$
$$\text{и } 2rd_1 = k(h_2 - h_1)$$

получаем, что

$$d_1 = k(h_2 - h_1)/(2r), \text{ а также } k = 2rd_1/(h_2 - h_1).$$

Т.е. поскольку составляющие сеанса k, r фиксированы, а h_2, h_1 можно вычислить, то и d_1 или k можно всегда вычислить.

Рассмотренное выше позволяет сделать вывод о криптографической слабости стандарта Российской федерации ГОСТ Р 34.10-2001, что объясняется незащищенностью от атаки на связанных долгосрочных ключах.

Проведем также анализ защищенности стандарта ЭЦП ДСТУ 4145-2002 от атаки на связанных ключах сеанса k_1 и $k_2 = n - k_1$. Рассмотрим возможности создания коллизий подписей для M_i и M_j на связанных ключах k_1 и $k_2 = n - k_1$. Результаты приведены в табл. 2.

Таблица 2

Анализ защищенности ЭЦП ДСТУ 4145-2002 от атаки на связанных ключах сеанса

Для сообщения M_i	Для сообщения M_j
1. $k_1 \in [1, n-1]$ 2. $f_{k_1} = \pi(k_1 G) =$ $= \pi(x_{R_1}, y_{R_1}) = x_{R_1}$ 3. Формируется предподпись $(k_1, f_{k_1}) = (k_1, x_{R_1})$. 4. Вычисляется $h_1 = H(M_i)$. 5. Вычисляется элемент основного поля $y_1 = h_1 x_{R_1} = r_1$. 6. Вычисляется $s_1 = (k_1 + dr_1) \bmod n$.	1. $k_2 = (n - k_1) \in [1, n-1]$ 2. $f_{k_2} = \pi((n - k_1)G) =$ $= \pi(nG - k_1 G) =$ $= \pi(x_{R_1}, -y_{R_1}) = x_{R_1}$ 3. Формируется предподпись $(k_2, f_{k_2}) = (k_2, x_{R_1})$. 4. Вычисляется $h_2 = H(M_j)$. 5. Вычисляется элемент основного поля $y_2 = h_2 x_{R_1} = r_2$. 6. Вычисляется $s_2 = (k_2 + dr_2) \bmod n$.

Проведем анализ результатов, полученных в 5 строке таблицы. В этом случае $r_1 \neq r_2$, но r_1 и h_1 являются известными, поэтому:

$$x_{R_1} = \frac{y_1}{h_1}, \qquad (9)$$

$$y_2 = r_2 = h_2 \frac{y_1}{h_1} = y_1 \frac{h_2}{h_1} = r_1 \frac{h_2}{h_1}, \qquad (10)$$

Из этого следует, что знание r_1 и h_1 позволяет найти x_{R_1}.

Таким образом, хотя $r_1 \neq r_2$, но компоненты r_1, r_2 связаны между собой и вычислительно легко находятся при известных M_i и M_j.

Дальше рассмотрим условия, при которых $S_1 = S_2$.

В результате имеем

$$(k_1 + dr_1) \bmod n = (k_2 + dr_2) \bmod n$$

или

$$d = \frac{2k_1}{r_1\left(-1 + h_2/h_1\right)} \bmod n = \frac{2k_1 h_1}{r_1(-h_1 + h_2)} \bmod n. \qquad (11)$$

В целом относительно ЭЦП согласно ДСТУ 4145-2002 можно сделать вывод, что этот алгоритм ЭЦП защищен от атаки на связанных ключах сеанса. Хотя и имеет потенциальную слабость, связанную с тем, что r_1, r_2 связаны между собой, а $S_1 = S_2$.

Проведем также анализ уровня защищенности для случая, когда связанными являются долгосрочные ключи. Результаты анализа сведены в табл. 3.

Таблица 3

Анализ защищенности ЭЦП ДСТУ 4145-2002 от атаки на связанных личных ключах (долгосрочных)

Для сообщения M_i	Для сообщения M_j
1. $k_1 = k \in [1, n-1]$ 2. $f_{k_1} = \pi(kG) =$ $= \pi(x_{R_1} y_{R_1}) = x_R$ 3. Формируется предподпись $(k, f_{k_1}) = (k, x_R)$. 4. Вычисляется $h_1 = H(M_i)$ 5. Вычисляется элемент основного поля $y_1 = h_1 x_R = r_1$ 6. Вычисляется $s_1 = (k + dr_1) \bmod n$	1. $k_2 = k \in [1, n-1]$ 2. $f_{k_2} = \pi(kG) =$ $= \pi(x_R, y_R) = x_R$ 3. Формируется предподпись $(k, f_{k_2}) = (k, x_R)$. 4. Вычисляется $h_2 = H(M_j)$ 5. Вычисляется элемент основного поля $y_2 = h_2 x_R = r_2$ 6. Вычисляется $s_2 = (k + (n-d) r_2) \bmod n =$ $= (k - dr_2) \bmod n$

Поведем анализ результатов, полученных в 4 и 5 строчках. В этом случае $r_1 \neq r_2$, но r_1 и h_1 являются известными. Дальше при условии $S_1 = S_2$ получим

$$s_1 = (k + dr_1) \bmod n = s_2 = (k + (n-d) r_2) \bmod n = (k - dr_2) \bmod n,$$

или $d(r_1 + r_2) \equiv 0 (\bmod n) = dx_R (h_1 + h_2) (\bmod n) = vn$.

Из приведенного выражения находим, что:

$$d = vn / (x_R (h_1 + h_2)) \ (\bmod n) = 0 / (x_R (h_1 + h_2)), \quad (12)$$

т.е. личный ключ не нулевой.

Таким образом, для рассмотренной атаки на связанных долгосрочных ключах имеем что $r_1 \neq r_2$, т.е. эти составляющие подписи практически никогда не совпадут. Кроме того, уравнение (12) не имеет решения. Поэтому можно считать, что ЭЦП согласно ДСТУ 4145-2002 является защищенной от атаки на связанных ключах.

3. ОЦЕНКА ЗАЩИЩЕННОСТИ ЭЦП В ГРУППЕ ТОЧЕК ЭЛЛИПТИЧЕСКИХ КРИВЫХ ОТ АТАК НА РЕАЛИЗАЦИЮ

Известно, что на сегодня в той или другой мере в операционных системах нашли распространение и широко применяются программные средства реализации цифровых подписей [10]. По аналогии оценим защищенность ЭЦП ДСТУ 4145-2002 от атак на реализацию.

Ориентируясь на подход и результаты, полученные выше, рассмотрим также условия осуществления атаки на реализацию ЭЦП ДСТУ 4145-2002. Как и раньше, будем считать, что нарушитель может заставить средство ЭЦП выработать $k_1 = k_2 = k \in (1, n-1)$. Можно показать, что:

$$d = \frac{s_1 - s_2}{r_1 - r_2} (\bmod n), \quad (13)$$

$$k = s_1 - dr_1 (\bmod n). \quad (14)$$

Используя подход, примененный выше, для ЭЦП, определяемого в ГОСТ Р 34.10-2001, получим [9]:

$$d = \frac{s_1 h_2 - s_2 h_1}{r(h_2 - h_1)} (\bmod n), \quad (15)$$

$$k = \frac{s_1 - rd}{h_1} (\bmod n). \quad (16)$$

Т.е. и относительно ЭЦП ГОСТ Р 34.10-2001 есть атаки на программную реализацию ЭЦП или другую реализацию, когда нарушитель может заставить средство два раза формировать одно и то же значение k для двух различных сообщений. В результате такой атаки нарушитель может определить долгосрочный личный ключ d и соответственно сможет навязывать как ошибочные сообщения, так и искажать истинные.

4. РЕЗУЛЬТАТЫ СРАВНИТЕЛЬНОГО АНАЛИЗА СТАНДАРТОВ ЭЦП ПО ИНТЕГРАЛЬНОМУ КРИТЕРИЮ

Важной задачей не имеющими на сегодня решения является сравнения разных цифровых подписей по некоторому множеству критериев и показателей. В процессе исследований также было обоснована необходимость и возможность применения метода анализа иерархий.

Предлагается осуществлять сравнения ЭЦП на основе использования безусловных и условных критериев. Результаты исследований ЭЦП позволили упорядочить по интегральному показателю.

1. EC-KCDSA – значение интегрального показателя 0.3259.
2. EC-GDSA – значение интегрального показателя 0.2256.
3. ДСТУ 4145-2002 – значение интегрального показателя 0.1346.
4. ГОСТ Р 34.10-2001 – значение интегрального показателя 0.1301.
5. EC-DSA – значение интегрального показателя 0.0924.
6. ECSS – значение интегрального показателя 0.0913.

Таким образом, ЭЦП согласно ISO/IEC 15946-2 (EC-KCDSA и EC-GDSA) по интегральному показателю имеют наибольшие преимущества, который объясняет необходимость их гармонизации в Украине.

Литература.

[1] Закон України «Про електронний документ та електронний документообіг» від 22.05.2003 №851-IV.

[2] Закон України «Про електронний цифровий підпис» від 22.05.2003 №852-IX.

[3] Директива 1999/93/ЕС Європейського парламенту та Ради від 13 грудня 1999 року про систему елек-

тронних цифрових підписів, що застосовуються в межах Співтовариства. «Інформаційні технології – взаємодія відкритих систем. Каталог: Основні положення сертифікації відкритого ключа та сертифікації атрибутів».

[4] ДСТУ ISO/IEC ISO/IEC 9594-8: 2006 «Інформаційні технології. Взаємодія відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів».

[5] *В. Гребнев, А. Скиба.* Направление правового регулирования вопросов использования ЭЦП // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні – № 6, 2003. – С. 6-10.

[6] *Д. Мялковский, А. Скиба.* Организационно-технические вопросы построения и функционирования национальной системы ЭЦП // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні – № 6, 2003. – С. 11–15.

[7] *І.Д. Горбенко, В.А. Демехін, Ю.І. Горбенко, О.В. Потій, В.В. Онопрієнко, С.С. Батюшко.* Стан та проблемні питания створення та розвитку національної інфраструктури відкритих ключів. Прикладна радіоелектроніка. – Том 5. 2006. – № 1. – С. 41-51.

[8] *Балагура Д.С., Горбенко Ю.И.* Методы оценки сложности криптоанализа для криптографических приложений в группе точек эллиптической кривой, учитывающие вероятность коллизий. Радиотехника. 2005. Вып. 142. – С.205-214.

[9] *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз існуючих ЕЦП від атак на зв'язаних ключах. Прикладная радиоэлектроника. Том 5. – 2006. №1. – С. 52-59.

[10] *Бондаренко М.Ф., Горбенко Ю.І., Батюшко С.С.* Аналіз захищеності існуючих ЕЦП від атак на реалізацію. Прикладная радиоэлектроника. – Том 5. 2006. № 1. – С. 59-62.

[11] ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка.

[12] ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры формирования и проверки электронной цифровой подписи. – М.: Госстандарт России, 2001. – 20 с.

[13] ДСТУ ISO/IEC 15946 – 3:2006. Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 1. Загальні положення (ISO/IEC 15946 – 3:2002, IDT).

[14] FIPS 186-2-2000. Digital signature standard. National Institute of standard and technology. – 2000.

[15] American National Standard X9.62-1999. Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm, 1999.

Поступила в редколлегию 2.09.2008

Бондаренко Михаил Федорович, доктор технических наук, профессор, ректор Харьковского национального университета радиоэлектроники.

Горбенко Юрий Иванович, кандидат технических наук, технический директор ЗАО «ИИТ», научный сотрудник НИЦ «Z» кафедры БИТ ХНУРЭ. Область научных интересов: защита информации в информационно-телекоммуникационных системах.