На правах рукописи

Аникевич Елена Александровна

МЕТОД ФОРМИРОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ОТКРЫТОГО КОЛЛЕКТИВНОГО КЛЮЧА ДЛЯ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРЕДПРИЯТИЯ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2010

Работа выполнена в Федеральном государственном образовательном учреждении высшего профессионального образования «Петербургский государственный университет путей сообщения» на кафедре «Информатика и информационная безопасность».

Научный руководитель: доктор технических наук, доцент
Еремеев Михаил Алексеевич

Официальные оппоненты: доктор технических наук, профессор
Яковлев Виктор Алексеевич

кандидат технических наук
Петренко Сергей Анатольевич

Ведущая организация: филиал ОАО «Научно-исследовательский и проектно-конструкторский институт информатизации, автоматизации и связи на железнодорожном транспорте» (г. Санкт-Петербург).

Защита состоится « 18 » марта 2010 года в 15 часов 00 мин. на заседании диссертационного совета Д 218.008.06 при Петербургском государственном университете путей сообщения по адресу: 190031, г. Санкт-Петербург, пр. Московский, д. 9 (ауд. 2-113).

С диссертацией можно ознакомиться в научно-технической библиотеке Петербургского государственного университета путей сообщения.

Автореферат разослан «16» 02 2010 г.

Ученый секретарь
диссертационного совета
кандидат технических наук, профессор Кудряшов В.А.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В современных условиях увеличение количества информации, обрабатываемой, передаваемой и хранимой в автоматизированных системах управления предприятий и организаций, привело к повышению актуальности задач:

обеспечения конфиденциальности, целостности, неотрицания авторства электронного документа;

создания защищённого электронного документооборота;

обеспечения высокой скорости обработки и подписания электронного документа.

В настоящее время основу обеспечения безопасности электронного документооборота составляют системы электронной цифровой подписи (ЭЦП). Наиболее широко применяемым видом ЭЦП является индивидуальная подпись. Современные системы электронного документооборота позволяют обрабатывать и подписывать документ одновременно только одним пользователем, что увеличивает время обработки и подписания документа, если его должны подписать несколько пользователей. Следовательно, размер ЭЦП увеличивается пропорционально числу пользователей, подписывающих электронный документ в несколько раз. При этом процедура проверки подлинности подписи подразумевает проверку подписей всех подписавших.

Кроме того, вариант "один документ – одна подпись" является не единственным, требуемым на практике. В частности, вопросы передачи документов от имени некоторого коллегиального органа или от имени совокупности субъектов делают актуальным вопрос разработки систем ЭЦП на основе понятия коллективного открытого ключа. Идея ЭЦП на основе открытого коллективного ключа состоит в том, чтобы построить протокол формирования и проверки подписи таким образом, что ЭЦП обычного размера будет подтверждать подлинность некоторого заданного электронного документа, подписанного каждым пользователем из некоторого заданного множества пользователей.

В области теории и практики разработки ЭЦП, как в нашей стране, так и за рубежом, издано большое количество трудов. Из их числа следует отметить работы ЭльГамаля Т., Шнорра К., Рабина М., Коблица Н., Ростовцева А. Г., Черемушкина А. В., Молдовяна Н. А., Еремеева М. А., Маховенко Е. Б. и др.

Создание метода формирования и проверки ЭЦП на основе коллективного открытого ключа даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер ЭЦП не увеличивается, что позволяет сократить объем избыточной информации, необходимой для аутентификации электронных документов и упростить протокол поддержки такой ЭЦП. Время на подписание документа остается прежним, как и при стандартной процедуре подписи, а время проверки подлинности ЭЦП уменьшается.

Таким образом, выявлена **проблемная ситуация,** определяемая как противоречие между необходимостью обеспечения подлинности и сохранения целостности информации в автоматизированной системе предприятия при коллективной обработке электронных документов и несоответствием существующих методов, алгоритмов и средств организации защищенного документооборота современным требованиям защищенности, функциональности и оперативности.

Разрешение данной проблемной ситуации требует создания метода формирования и проверки электронной цифровой подписи на основе коллективного открытого ключа.

Объектом исследования является система защищённого электронного документооборота в автоматизированной системе управления (АСУ) предприятия, а **предметом** – методы создания и проверки электронной цифровой подписи при организации электронного документооборота.

Целью исследования является повышение оперативности обработки информации в защищённом электронном документообороте предприятия. Для достижения поставленной цели решалась **научная задача** построения схем электронной цифровой подписи на основе коллективного открытого ключа.

Достижение поставленной цели и решение научной задачи потребовало решения следующих частных **задач исследований**:

1. Проведения анализа современных методов и средств защиты систем электронного документооборота.

2. Осуществления выбора системы электронной цифровой подписи как основного механизма обеспечения оперативного защищённого электронного документооборота.

3. Разработки метода формирования и проверки электронной цифровой подписи на основе открытого коллективного ключа (ЭЦП ОКК).

4. Разработки алгоритма выбора параметров ЭЦП ОКК.

5. Разработки методики организации защищённого документооборота предприятия.

6. Разработки программного комплекса по реализации ЭЦП ОКК и рекомендации по её внедрению в систему защищённого электронного документооборота (СЭД).

Основные положения, выносимые на защиту:

1. Метод формирования и проверки ЭЦП ОКК, использующий эллиптическую криптографию.

2. Алгоритм выбора параметров ЭЦП ОКК, отличающийся высокой оперативностью обработки информации.

3. Методика организации защищённого документооборота в АСУ предприятия и рекомендации по программно-аппаратной реализации ЭЦП ОКК.

Методы выполнения исследований. Для решения задач диссертационного исследования в работе применялись методы системного анализа, теории множеств, теории чисел и алгебраической геометрии. В ходе разработки предлагаемого метода и проверки его работоспособности проводились вычислительные эксперименты.

Достоверность полученных результатов диссертационной работы определяется корректным использованием математического аппарата теории чисел, совпадением теоретических результатов по использованию вычислительных задач высокой сложности с результатами вычислительных экспериментов, апробированием результатов на научных конференциях.

Научная новизна работы состоит в обосновании и разработке метода формирования и проверки ЭЦП ОКК на основе криптографических конструкций с использованием эллиптических кривых, позволяющего повысить оперативность совместной обработки электронных документов при сохранении требуемого уровня защищенности.

Практическая значимость работы состоит в разработке программного комплекса ЭЦП ОКК и возможности его реализации в существующих и перспективных СЭД, что позволит повысить оперативность обработки электронных документов.

Реализация и внедрение результатов исследований.

Основные результаты диссертации реализованы в Санкт-Петербургском филиале ФГУП «ЗащитаИнфоТранс» и в учебном процессе ФГОУ ВПО «Петербургского государственного университета путей сообщения».

Апробация. Основные результаты работы прошли апробацию докладами на II Международной научно-практической конференции «Актуальные проблемы развития железнодорожного транспорта» (Самара, 2005), 62-й научно-технической конференции «Неделя науки – 2002» (Санкт-Петербург, ПГУПС, 2002), 11-й, 12-й и 14-й международных научно-практических конференциях «Инфотранс-2006», «Инфотранс-2007» и «Инфотранс-2009», на научных семинарах кафедры информатики и информационной безопасности ПГУПС.

Публикации. Материалы диссертации опубликованы в 13 работах, в том числе: 11 статьях и докладах на научно-технических и научно-практических конференциях, из них одна в издании, рекомендованном ВАК Минобрнауки России, 2 отчетах НИР.

Структура и объем диссертации.

Диссертационная работа состоит из введения, четырех разделов основного содержания с выводами по каждому разделу, заключения, списка литературы, включающего 80 наименований. Материалы диссертации изложены на 153 страницах, включающих 20 иллюстраций и 16 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы, определяется цель диссертационной работы. Сформулированы основные научные результаты исследований, выносимые на защиту. Приведены сведения по апробациям и публикациям по теме исследований. Приводится краткая аннотация содержания диссертации по разделам.

В первой главе отмечается значимость внедрения защищенного электронного документооборота в структуру автоматизированных систем управления предприятием. Проводится анализ современных систем электронного документооборота (ЭД) и выявляются их недостатки с позиций обеспечения информационной безопасности.

Показано, что внедрение защищенного ЭД позволяет обеспечить: подлинность информации, автоматизацию работы с документами, систематизацию хранения информации, уменьшение количества бумажных документов, облегчение работы пользователей.

Однако, существующие системы ЭД, в большинстве своем, имеют следующие недостатки:

отсутствие юридически значимой ЭЦП;

низкая функциональность схем ЭЦП;

отсутствие возможности совместной работы с документами;

отсутствие управления потоками работ;

отсутствие поддержки различных типов данных.

Показано, что при выборе той или иной модели электронного документооборота необходимо руководствоваться следующими критериями:

полнота соответствия системы ЭД необходимому (или типовому) набору функций;

затраты на внедрение системы в существующую автоматизированную систему управления предприятия и её последующее сопровождение;

расширяемость (масштабируемость) системы;

наличие механизмов обеспечения информационной безопасности.

В общем виде сформулированы подходы к устранению недостатков существующих систем ЭД:

внедрение юридически значимой ЭЦП по схемам ГОСТ и альтернативным схемам;

расширение функциональности схем ЭЦП;

обеспечение разграничения прав доступа;

полная поддержка жизненного цикла электронного документа;

внедрение возможностей совместной работы с документами и управление потоками работ;

повышение удобства работы пользователя.

Определены цель проведения диссертационного исследования и частные задачи исследования.

Во второй главе выполнена постановка научной задачи исследования в следующем виде.

Дано:

N – количество пользователей СЗЭД;

S – структура АСУ предприятия, использующего СЗЭД;

Λ – множество алгоритмов криптографического преобразования;

$K_{\text{инф}}$ – категория защищаемой информации;

Ограничения и допущения:

– имитостойкость информации $I \geq I_{\text{зад}}$;

– производительность СЗЭД $P \geq P_{\text{зад}}$;

– стоимость создания СЗЭД $C \leq C_{\text{зад}}$;

– принадлежность характеристик используемой вычислительной техники области допустимых значений $V \in \{V_{\text{д}}\}$.

Найти: $M=\{N, S, A, K_{инф}\}$ – модель системы защищенного электронного документооборота, удовлетворяющую следующему выражению:

$$M^* = \arg\min_{M\in\Omega_M}\left\{T\left(M=\{N,S,A,K_{инф}\}\right) \Big/ \left(P(M)\ge P_{зад}(M)\right), \left(C(M)\le C_{зад}(M)\right)\right\},$$

где Ω_M – множество моделей СЭЭД, T – время выполнения обработки информации в СЭЭД от момента создания и подписания документа до момента проверки подписи.

При разработке метода формирования и проверки ЭЦП ОКК предложено использовать групповой закон сложения точек эллиптической кривой (ЭК) $E(GF_p)$ вида $y^2 = x^3 + ax + b \pmod p$, где GF_p – конечное поле с характеристикой $p\neq 2$ и $p\neq 3$, x, y – координаты точек ЭК, a, b – коэффициенты уравнения ЭК. Групповой закон сложения точек $P_1 \oplus P_2 = (x_3, -y_3)$ для случая двух различных точек $P_1=(x_1,y_1)$ и $P_2=(x_2,y_2)$ имеет следующий вид: $x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_2 - x_1 \pmod p$, $y_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3) - y_1 \pmod p$, при $P_1=P_2=(x_1,y_1)$: $x_3 = \frac{(3x_1^2+a)^2}{4(x_1^3+ax_1+b)} - 2x_1 \pmod p$ и $y_3 = \frac{(3x_1^3+a)}{2y_1}(x_1-x_2) - y_1 \pmod p$. Для кривых с ненулевым инвариантом над полем GF_2^n используются следующие выражения сложения точек: $\begin{cases} x_3 = \lambda^2 + \lambda - a - x_1 - x_2 \\ y_3 = -(\lambda+1)x_3 - \nu \end{cases}$, где для случая $P_1\neq P_2$: $\lambda = \frac{y_2-y_1}{x_2-x_1}$, $\nu = \frac{y_1x_2-y_2x_1}{x_2-x_1}$, а при $P_1=P_2$: $\lambda = \frac{3x_1^2+2x_1a}{2y_1+x_1}$, $\nu = \frac{3x_1^3+2x_1^2-2y_1^2-y_1x_1}{2y_1+x_1}$. Обращение точки имеет вид $P_3=(x_3, -y_3-x_3)$. Аналогично для кривых с ненулевым инвариантом j над полем GF_3^n: $\begin{cases} x_3 = \lambda^2 - a - x_1 - x_2 \\ y_3 = -x_3\lambda - \nu \end{cases}$, где для $P_1\neq P_2$: $\lambda = \frac{y_2-y_1}{x_2-x_1}$, $\nu = \frac{y_1x_2-y_2x_1}{x_2-x_1}$, а при $P_1=P_2$: $\lambda = \frac{3x_1^2+2x_1a}{2y_1}$ и $\nu = \frac{3x_1^3+2x_1^2-2y_1^2}{2y_1}$.

Приведенные групповые законы сложения точек на ЭК используются в качестве функций криптографического преобразования. Если P и G – элементы циклической подгруппы A кривой $E(GF_q)$ и G – примитивный элемент (генератор) этой подгруппы, то, при $P=n*G$, где n – случайное число (ключ), поиск числа n по двум заданным элементам

подгруппы P и G при $n \to \infty$ является вычислительно сложной задачей с точки зрения теории сложности алгоритмов.

В кольце целых чисел наиболее трудоемкой операций является инверсия. В целях исключения данной операции осуществлен переход из аффинных координат в проективные, что обеспечило повышение скорости вычислений на 30–40 %.

Разработан обобщенный метод формирования и проверки ЭЦП ОКК, схема взаимосвязей этапов которого представлена на рис. 1.

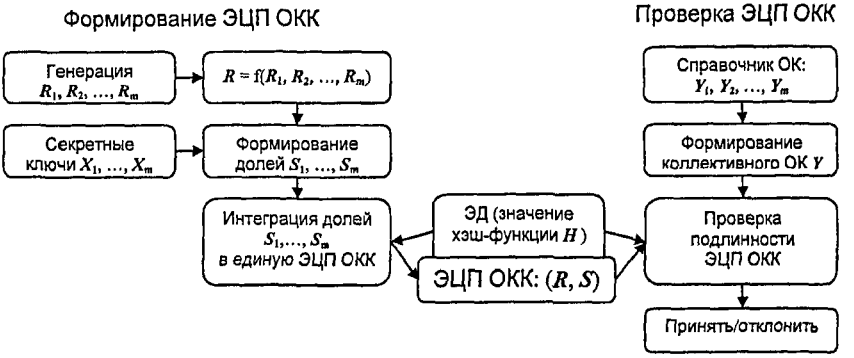

Рисунок 1 – Схема взаимосвязей этапов метода формирования и проверки ЭЦП ОКК

Метод состоит из трёх этапов:

I этап – формирование ЭЦП ОКК, заключается в выполнении следующих шагов:

1. Создание первой части ЭЦП ОКК R на основе генерации индивидуальных параметров подписи R_i и применение функции, отображающей их в коллективный параметр подписи R.

2. Создание секретных ключей и формирование долей второй части подписи S_i.

3. Интеграция в единую ЭЦП ОКК S.

II этап – собственно создание ЭЦП ОКК, состоящей из двух частей (R, S), хэш-функции и отправка ЭЦП ОКК соответствующим пользователям автоматизированной системы управления.

III этап – проверка ЭЦП ОКК:

1. По справочнику открытых ключей выбираются индивидуальные открытые ключи пользователей Y_i, участвовавших в создании и подписании документа.

2. На основе выбранных индивидуальных открытых ключей

пользователей формируется открытый коллективный ключ Y.

3. Осуществляется проверка подлинности ЭЦП ОКК, а затем принимается решение: принять или отклонить ЭЦП ОКК.

Сравнение характеристик обычной и ЭЦП ОКК для m пользователей показывает (табл. 1), что сложность генерации подписи является одинаковой, а сложность проверки ЭЦП ОКК в m раз меньше.

Таблица 1. Сравнение характеристик ЭЦП и ЭЦП ОКК.

Характеристика	Обычная ЭЦП	ЭЦП ОКК
Сложность генерации подписи (количество преобразований)	m	m
Сложность проверки подписи (количество преобразований)	$2m$	2
Функциональность	средняя	высокая

Исследована реализуемость ЭЦП ОКК на основе известных алгоритмов ЭЦП (таблица 2), показана возможность разработки ЭЦП ОКК на основе отечественных стандартов и схемы Шнорра.

Таблица 2. Реализуемость ЭЦП ОКК.

Алгоритм ЭЦП	Возможность реализации ЭЦП ОКК
ГОСТ Р 34.10-94	+
ГОСТ Р 34.10-2001	+
DSA (стандарт США 1991 г.)	–
EDSA (стандарт США 1999 г.)	–
Эль-Гамаля	–
Шнорра	+

На основе стандарта ЭЦП РФ ГОСТ Р 34.10-2001 разработана схема формирования и проверки ЭЦП ОКК. Она соответствует обобщенному методу формирования ЭЦП ОКК и заключается в последовательном выполнении следующих этапов и шагов.

I этап – Генерация ключей.

1. Генерация секретных ключей пользователей $d_i < P$.

2. Формирование индивидуальных открытых ключей пользователей $Q_i = d_i * P$, где P – точка ЭК, являющаяся генератором аддитивной циклической группы точек, и коллективного открытого ключа:

$$Q = Q_1 + Q_2 + \ldots + Q_m .$$

II этап – Формирование ЭЦП ОКК.

1. Вычисление значения хэш-функции H от подписываемого ЭД и вычисление вспомогательной переменной $e = H \bmod q$.

2. Генерация каждым пользователем значений k_i и вычисление точек ЭК $C_i = k_i * P$.

3. Сложение точек ЭК каждого пользователя $C = C_1 + C_2 + \ldots + C_m$ и вычисление первой части ЭЦП ОКК через координату x точки C ЭК: $R = x_C \bmod q$.

4. Формирование долей ЭЦП каждого пользователя $S_i = (Rd_i + k_i e) \bmod q$ и вычисление второй части ЭЦП ОКК

$$S = (S_1 + S_2 + \ldots + S_m) \bmod q .$$

5. Формирование ЭЦП ОКК в виде пары значений (R, S).

III этап – Проверка ЭЦП ОКК.

1. Определение точки ЭК с помощью значений ЭЦП ОКК (R, S), вспомогательной переменной e, коллективного открытого ключа проверочного уравнения следующего вида:

$$C' = ((Se^{-1}) \bmod q) * P + ((q-R)e^{-1} \bmod q) * Q .$$

2. Вычисление значения параметра R' по координате x точки C':

$$R' = x_{C'} \bmod q .$$

3. Проверка условия: если $R' = R$, то подпись верна.

Третья глава диссертационной работы посвящена разработке алгоритма выбора параметров ЭЦП ОКК.

В качестве показателя стойкости к криптоанализу ЭЦП ОКК на основе применения группового закона сложения точек на ЭК предлагается использовать асимптотическую оценку сложности алгоритма вскрытия в терминах O – символики. На основе исследования алгоритмов криптоанализа показано, что стойкость ЭЦП ОКК существенно зависит от порядка группы, определяется как сложность наилучшего алгоритма по определению индекса и оценивается значением $O\left(\sqrt{\zeta_p}\right)$, где ζ_p – наибольший простой множитель порядка группы точек кривой.

Показано, что параметрами, от которых зависит безопасность систем ЭЦП в целом и ЭЦП ОКК в частности, на основе ЭК, являются:

- вид конечного поля;
- характеристика поля и (или) его расширения;
- уравнение ЭК;
- порядок циклической подгруппы точек ЭК;
- генератор подгруппы точек ЭК.

Выявлен ряд свойств кривых, при которых существенно уменьшается стойкость, в частности нецелесообразно использовать кривые с инвариантом j=0. Найдены случаи, когда стойкость преобразования на ЭК уменьшается до сложности нахождения дискретного логарифма в мультипликативном поле.

Поскольку основным параметром, определяющим стойкость, является величина порядка группы на кривой, был разработан алгоритм выбора параметров ЭЦП ОКК, основанный на выборе параметров ЭК с требуемым порядком группы:

1. В соответствии с исходными данными из неравенства $q+1-2\sqrt{q} \le \#E(GF_q) \le q+1+2\sqrt{q}$ определяется характеристика p конечного поля GF_p^n или кольца Z_p и степень расширения поля n.

2. Выбирается уравнение ЭК в соответствии с характеристикой p.

3. Случайным образом генерируются коэффициенты a, b уравнения ЭК. Перейти к шагу 4 при p=2 или p=3, и к шагу 5 в ином случае.

4. Определяется порядок группы $\#E(GF_q)$ согласно выражению $\#E(GF_2)_k = 2^k + 1 - 2^{\frac{k}{2}+1}\cos\left(k\arctan\left(\pm\sqrt{7}\right)\right)$ для поля с p=2 при любом k для $\#E(GF_2)$=2 и $\#E(GF_2)$=4 соответственно, и согласно выражениям для поля с p=3: $\#E(GF_3)_k = 3^k + 1 - 2\cdot 3^{\frac{k}{2}}\cos\left(k\arctan\left(\pm\sqrt{11}\right)\right)$ для $\forall\ k$ при $\#E(GF_3)$=5 и $\#E(GF_3)$=3; $\#E(GF_3)_k = 3^k + 1 - 2\cdot 3^{\frac{k}{2}}\cos\left(k\arctan\left(\pm\sqrt{2}\right)\right)$ для $\forall\ k$ при $\#E(GF_3)$=6 и $\#E(GF_3)$=2; $\#E(GF_3)_k = 3^k + 1 - 2\cdot 3^{\frac{k}{2}}\cos\left(k\arctan\left(\pm 3^{-\frac{1}{2}}\right)\right)$ для $\forall\ k$ при $\#E(GF_3)$=7 и $\#E(GF_3)$=1; $\#E(GF_3)_k = \begin{cases} 3^k + 1 - 2\cdot(-3)^{\frac{k}{2}} \\ 3^k + 1 \end{cases}$ для $\#E(GF_3)$=4 при k – четном и k – нечетном соответственно. Перейти к шагу 6 алгоритма.

5. Определяется порядок группы $\#E(GF_p)$ согласно выражениям:
] $(p=2(mod\ 3) \cap p=5(mod\ 6) \cap a=0) \cup (p=3(mod\ 4) \cap b=0) \Rightarrow \#E(GF_p)=p+1$;

] $\Delta=0$ и $a,b\neq0$ $\Rightarrow$ при $\{p=2(mod\ 3) \cap (p\neq1(mod\ 4) \cup p=3(mod\ 4))\} \cup \{p=1(mod\ 3) \cap (p=1(mod\ 4) \cup p\neq3(mod\ 4)\} \Rightarrow \#E(GF_p)=p+1\pm1$, если b квадратический вычет или невычет;

] $\Delta=0$ и $a,b\neq0$ $\Rightarrow$ при $\{p=2(mod\ 3) \cap (p=1(mod\ 4) \cup p\neq3(mod\ 4))\} \cup \{p=1(mod\ 3) \cap (p\neq1(mod\ 4) \cup p=3(mod\ 4)\} \Rightarrow \#E(GF_p)=p+1\pm1$, если b квадратический невычет или вычет;

] $a=0$, $p=1(mod\ 6)$ $\Rightarrow$ $\#E(GF_q)=p+1+r$, где $p=d^2-de+f^2$ в $Z[\omega]$, $\omega=\left(-1+\sqrt{-3}\right)/2$, $d=2\ (mod\ 3)$, $e=0\ (mod\ 3)$, $r=d+e$, $r=-d-e$, $r=2d-e$, $r=-2d+e$, $r=d-2e$, $r=-d+2e$, если b квадратический или кубический вычет или невычет;

] (b-кубический вычет)$\cap$(b-квадратический вычет) $\Rightarrow$ $\#E(GF_p)=6l$;

] (b-кубический вычет)$\cap$(b-квадратический невычет) $\Rightarrow$ $\#E(GF_p)=3l$;

] (b-кубический невычет)$\cap$(b-квадратический вычет) $\Rightarrow$ $\#E(GF_p)=2l$;

] (b-кубический невычет)$\cap$(b-квадратический невычет) $\Rightarrow$ $\#E(GF_p)=1(mod6)$;

] $b=0$, $p=1(mod\ 4)$, $-a$-квадратический вычет $\Rightarrow$ $\#E(GF_q)=p+1\pm2d$, $\#E(GF_q)=0\ (mod\ 4)$, где $p=d^2+e^2$ в $Z[i]$, d - нечетное;

] $b=0$, $p=1(mod\ 4)$, $-a$-квадратический невычет $\Rightarrow$ $\#E(GF_q)=p+1\pm2e$, $\#E(GF_q)=2\ (mod\ 4)$, где $p=d^2+e^2$ в $Z[i]$;

Если коэффициент a (при $p=2(mod\ 6)$) или b (при $p=3(mod\ 4)$ кривой равны 0, то порядок группы $\#E(GF_q)=p+1$.

6. Проверяется невыполнимость условия делимости полученного порядка группы согласно выражению $\#E(GF_{p^n}) \left| \left(p^{n^i}-1 \right) \right.$, где $i=1, 2,..., k$ (если свойство делимости выполняется, тогда вернуться к шагу 3 алгоритма выбора параметров ЭЦП ОКК).

Результатом выбора параметров ЭЦП ОКК является уравнение ЭК с порядком группы, удовлетворяющим требуемой стойкости и скорости преобразования.

Применение данного алгоритма позволяет осуществлять поиск уравнения ЭК для создания ЭЦП ОКК с требуемым уровнем стойкости за конечное число шагов со сложностью $O(\log^5 p)$.

Четвертая глава посвящена разработке методики организации защищённого документооборота в АСУ предприятия и обоснованию практических рекомендаций по программно-аппаратной реализации ЭЦП ОКК.

Методика организации защищенного электронного документооборота заключается в выполнении следующих взаимоувязанных действий.

1. Создание удостоверяющего центра в структуре АСУ предприятия для придания легитимности и юридической значимости защищенного электронного документооборота.

2. Определение порядка подключения пользователя к АСУ и допуска пользователя к осуществлению электронного документооборота.

3. Разработка требований, предъявляемых к электронному документу.

4. Разработка требований и организация процессов электронного документооборота в АСУ предприятия (формирование, отправка, доставка, проверка подлинности, подтверждение получения, отзыв, учёт, хранение электронных документов).

5. Определение правил использования ЭЦП и ЭЦП ОКК в электронном документообороте.

6. Разработка требований и определение порядка создания криптографических ключей, выдачи электронных цифровых сертификатов, действий при компрометации ключей.

7. Определение обязательств владельцев цифровых сертификатов.

8. Разработка правил действий при разрешении конфликтных ситуаций и споров, возникших в связи с осуществлением электронного документооборота в АСУ предприятия.

Составной частью предложенной методики является разработанный программный комплекс, в котором реализован метод формирования и проверки ЭЦП ОКК и алгоритм выбора параметров ЭЦП ОКК. Его возможности включают формирование ЭЦП и ЭЦП ОКК, проверку ЭЦП и ЭЦП ОКК, генерацию ключей подписи и проверки, генерацию эллиптической кривой, параметры которой удовлетворяют всем требованиям стандарта на ЭЦП. Время формирования одной подписи и ее проверки не превышает 0,2 секунды. Время генерации параметров ЭЦП ОКК составляет несколько минут.

Назначение программного комплекса – обеспечение целостности и авторства хранимой и обрабатываемой информации в системе защищенного электронного документооборота предприятия на основе применения систем ЭЦП ОКК.

Проведено исследование безопасности ЭЦП ОКК в сравнении с системами ЭЦП подобного и других видов. Показано, что выигрыш в

показателе безопасности при использовании аддитивной группы точек эллиптических в сравнении с использованием мультипликативной группы кольца целых чисел зависит от длины ключа и может достигать нескольких порядков при равной длине ключа. Например, стойкость ЭЦП ОКК на основе ЭК с длиной ключа 200 бит соответствует стойкости ЭЦП на основе сложности решения задачи дискретного логарифмирования в мультипликативной группе кольца целых чисел или сложности разложения больших чисел на простые сомножители с длинной ключа порядка 500 бит. Преимущество использования ЭК при создании ЭЦП ОКК подтверждается также результатами исследования скорости криптографического преобразования.

В заключении сформулированы основные результаты работы, определены возможные области их применения. Сделан вывод о степени выполнения поставленных задач и достижении цели исследований.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. В ходе проведенного анализа существующих систем электронного документооборота выявлены их основные недостатки и обоснована целесообразность применения электронной цифровой подписи на основе открытого коллективного ключа в системах защищенного электронного документооборота предприятия.

2. Разработан метод формирования и проверки ЭЦП ОКК, использующий эллиптическую криптографию. Метод формирования и проверки ЭЦП ОКК даёт возможность обработки и подписания документа одновременно несколькими пользователями. При этом размер ЭЦП не увеличивается. Время на подписание документа остается прежним, как и при стандартной процедуре подписи, а время проверки подлинности ЭЦП уменьшается в m-раз пропорционально количеству пользователей, участвующих в создании и подписании документа.

3. Разработан алгоритм выбора параметров ЭЦП ОКК, основанный на выборе ЭК, эффективных как по показателю криптостойкости, так и по показателю скорости выполнения криптографического преобразования. Применение данного алгоритма позволит повысить оперативность обработки информации при формировании и проверке электронной цифровой подписи.

4. Разработан программный комплекс ЭЦП ОКК для применения в составе методики организации защищённого электронного документооборота в АСУ предприятия, который позволяет повысить

оперативность и защищённость коллективной обработки информации. В частности время обработки электронных документов при их согласовании и совместном принятии решений уменьшается на 50–60%.

5. Разработанный подход к созданию ЭЦП ОКК не только обеспечивает значительное упрощение процесса аутентификации коллективных документов и повышает оперативность процедуры проверки ЭЦП, но и придает внутреннюю целостность аутентифицирующей информации. Предполагаемые области дальнейшего применения коллективной подписи: разработка крупных проектов, системы коллективного управления, системы управления государственными и силовыми структурами, финансы и бизнес.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ РАБОТЫ

(публикации в изданиях, рекомендованных ВАК Минобрнауки России, выделены курсивом)

1. Аникевич Е.А., Еремеев М.А., Сергиенко П.В. Совершенствование системы защищенного электронного документооборота на основе новых схем электронной цифровой подписи // Проблемы информационной безопасности. Компьютерные системы. – Вып. 2. – СПб. : СПбГТУ, 2009. – С. 21–31.

2. Аникевич Е.А., Еремеев М.А., Корниенко А.А. Высокоскоростные алгоритмы и протоколы криптографической защиты информационных ресурсов железнодорожного транспорта // Известия Петербургского университета путей сообщения. – Вып. 2. – СПб. : ПГУПС, 2004. – С. 85–88.

3. Аникевич Е.А., Маркевич М.Ю. Особенности защиты документооборота в вузе // Материалы II Международной научно-практической конференции «Актуальные проблемы развития железнодорожного транспорта». Самара, 7 – 8 декабря 2005г. – Самара : СамГАПС, 2005. – С. 343–344.

4. Аникевич Е.А., Еремеев М.А., Маркевич М.Ю., Корниенко А.А., Сергиенко П. В. Организация системы и программный комплекс защищенного документооборота предприятия на основе электронной цифровой подписи // Известия Петербургского университета путей сообщения. – Вып. 1 (6). – СПб. : ПГУПС, 2006. – С. 21–29.

5. Аникевич Е.А., Костянко Н.Ф. Использование при создании электронной документации средств текстового процессора WORD //

Сборник программы и тезисов 62-й научно-технической конференции «Неделя науки – 2002». Ч. 2. – СПб. : ПГУПС, 2002. – С. 257–258.

6. Аникевич Е.А., Костянко Н.Ф. Возможности текстового процессора WORD при разработке электронных документов // Сборник программы и тезисов 62-й научно-технической конференции «Неделя науки – 2002». Ч. 2. – СПб. : ПГУПС, 2002. – С. 258–259.

7. Аникевич Е.А. Структурный подход к организации процесса сбора данных // Межвузовский сборник трудов молодых учёных, аспирантов и докторантов. Железнодорожный транспорт: проблемы и решения. – Вып. № 6. – СПб. : ПГУПС, 2002. – С. 92–93.

8. Аникевич Е.А., Еремеев М.А. Разработка систем электронной цифровой подписи документов на основе свойств эллиптических кривых // Материалы докладов одиннадцатой международной научно-практической конференции «Инфотранс-2006». – Санкт-Петербург, 2006. – С. 293–294.

9. Аникевич Е.А., Еремеев М.А., Молдовян Н.А. Принципы создания коллективной электронной цифровой подписи для систем защищенного электронного документооборота ОАО «РЖД» // Материалы докладов двенадцатой международной научно-практической конференции «Инфотранс-2007», Санкт-Петербург, 2007. – С. 41.

10. Аникевич Е.А., Еремеев М.А., Сергиенко П.В. Предложения по реализации коллективной электронной цифровой подписи сообщений в системе защищенного электронного документооборота предприятия // Материалы докладов четырнадцатой международной научно-практической конференции «Инфотранс-2009», Санкт-Петербург, 2009. – С. 27–28.

11. Аникевич Е.А. Практическая реализация схем стандартной и коллективной электронной цифровой подписи // Известия Петербургского университета путей сообщения. Вып. 3 (20). – СПб. : ПГУПС, 2009. – С. 169–176.

Подписано к печати	11. 02. 2010 г.	Печ.л. – 1,0
Печать - ризография.	Бумага для множит. апп.	Формат 60x84 1\16
Тираж 100 экз.	Заказ № 130.	
СР ПГУПС	190031, С-Петербург, Московский пр. 9	