УДК 681.322;003.26

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

ЙОНА Л.Г., ЙОНА Е.О., ТЕРЕШКО В.С.

Одесская национальная академия связи им. А.С. Попова
Одесский национальный экономический университет

CRYPTOGRAPHY SECURITY OF ELECTRONIC DOCUMENT CIRCULATION

IONA L.G., IONA E.O., TERESHKO V.S.

Odessa National Academy of Telecommunications n.a. A.S. Popov
Odessa National Economic University

Аннотация. *В данной статье рассмотрены криптографические методы защиты документооборота, приведена классификация криптографических алгоритмов по назначению и аргументирована необходимость имплементации международных стандартов электронной цифровой подписи в Украине.*

Abstract. *This article describes the methods of cryptographic protection of documents, shows the classification of cryptographic algorithms and argues the need the need to implement international standards for electronic signature in Ukraine.*

ВВЕДЕНИЕ

При обмене электронными документами по телекоммуникационным каналам существенно снижаются затраты на обработку и хранение документов, ускоряется их поиск. Однако злоумышленники могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, а также частным лицам, которые используют электронный документооборот. Это ставит перед нами вопрос о защите информации, содержащейся в документе, установлении подлинности автора и самого документа.

Защиту информации, содержащуюся в сообщениях, передающуюся по телекоммуникационным каналам, можно осуществить тремя способами:

- созданием надежного канала связи;
- криптографическими методами (шифрованием и аутентификацией);
- стеганографическими методами (скрытием факта передачи информации).

Очевидно, что именно криптографические методы оптимальны для предоставления защиты современному документообороту.

В задачи криптографической защиты информации входит обеспечение:

- конфиденциальности, т. е. защиты от утечки информации (решается шифрованием);
- доступности, т. е. информация должна быть доступна только тому пользователю, для которого она предназначена (решается шифрованием);
- целостности, т. е. информация должна быть защищена от несанкционированной модификации (решается электронной цифровой подписью);
- аутентификации, т. е. подтверждением подлинности (решается электронной цифровой подписью и сертификатом);
- неопровергаемости, то есть невозможности отказаться от совершенного действия (решается электронной цифровой подписью и сертификатом).

АНАЛИЗ ПОСЛЕДНИХ ИССЛЕДОВАНИЙ И ПУБЛИКАЦИЙ

Проблемам исследования криптографических методов защиты документооборота посвящены труды многих отечественных и зарубежных ученных, таких как Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф., Задирака В.К., Кудин А.Н., Людвиченко В.О. и др. [1–5] Однако вопросам усовершенствования законодательной базы Украины в сфере ЭЦП и имплементации международного законода-

тельства в части обеспечения безопасности применения ЭЦП уделено недостаточно внимания, что обуславливает необходимость дальнейших исследований в данном направлении.

Целью статьи является анализ существующих криптографических методов защиты документооборота, классификация криптографических алгоритмов, а также аргументация необходимости имплементации международных стандартов электронной цифровой подписи в Украине.

ОСНОВНОЙ МАТЕРИАЛ ИССЛЕДОВАНИЯ

В современном мире цифровых технологий вопрос актуальности применения криптографических методов защиты информации не вызывает сомнения. Криптографические методы защиты можно разделить на два класса:

- симметричные криптосистемы;
- асимметричные криптосистемы.

Криптосистема объединяет в себе пару алгоритмов шифрования (алгоритм зашифрования и алгоритм расшифровки), в которых криптографические преобразования осуществляются при помощи ключа шифрования.

Ключ шифрования – это правило, по которому осуществляется преобразования открытого текста в зашифрованный и наоборот.

Симметричные криптосистемы характеризуются тем, что и для зашифровки сообщения и для его расшифровки используется один и тот же ключ шифрования. В этом случае ключ шифрования необходимо держать в секрете и отправителю, и получателю сообщения. Поэтому часто возникает проблема распределения ключей между пользователями системы.

Асимметричные криптосистемы характеризуются тем, что для криптографического преобразования используется два ключа (первый ключ – открытый, то есть несекретный и второй ключ – секретный). Поэтому асимметричные криптосистемы еще называют двуключевыми системами или системами с открытым ключом.

Криптосистемы с открытым ключом можно использовать как для шифрования, так и для аутентификации сообщений с применением электронной цифровой подписи (ЭЦП).

В асимметричных криптосистемах для зашифровки сообщения используется один (открытый) ключ, а для расшифровки сообщения – второй (секретный) ключ, известный только получателю сообщения.

В случае аутентификации с применением ЭЦП также используется два ключа, но для постановки подписи под документом отправителем используется секретный ключ, а для проверки подписи получателем – открытый ключ.

Электронная цифровая подпись – это реквизит электронного документа, предназначенный для защиты от подделки путем идентификации владельца сертификата ключа подписи. ЭЦП привязывает автора к документу и защищает документ от подделок.

ЭЦП по своему существу представляет собой относительно небольшой блок информации (хэш), который получается из электронного документа путем криптографического преобразования (с использованием секретного ключа) и передается вместе с подписываемым текстом. Так как подписываемые документы обычно достаточно большого объема, в схемах ЭЦП зачастую подпись ставится не на сам документ, а на его хэш (результат сжатия документа). Для вычисления хэша используются стандартные криптографические хэш-функции, которые позволяют при проверке подписи выявить изменения в документе. При этом хэш-функции не являются частью алгоритма ЭЦП, поэтому в схеме может быть использована любая надежная хэш-функция.

В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Каждая электронная цифровая подпись содержит следующую информацию:

– дату подписи;
– срок окончания действия ключа данной подписи;
– информацию о лице, подписавшем файл (Ф.И.О., должность, краткое наименование фирмы);
– идентификатор подписавшего (имя открытого ключа);

– собственно цифровую подпись.

Наличие в асимметричной криптосистеме открытого ключа накладывает некоторые ограничения для выбора подходящей пары “открытый-секретный” ключ. В частности, для обеспечения необходимой криптостойкости (стойкости к взлому) системы, длина ключей в асимметричных системах значительно возрастает по сравнению с симметричными системами. Так, в системах с открытым ключом, длина ключа в 512 бит соответствует длине ключа в 64 бита для симметричных криптосистем. Симметричная криптосистема с длиной ключа в 128 бит, обеспечивает такую же криптостойкость, что и криптосистема с открытым ключом, имеющим длину 2304 бита [1].

Для генерации пары ключей (секретного и открытого) в алгоритмах ЭЦП, как и в асимметричных системах шифрования, используются разные математические схемы, основанные на применении однонаправленных функций. Эти схемы разделяются на две группы. В основе такого разделения лежат известные сложные вычислительные задачи:

– задача факторизации (разложения на множители) больших целых чисел;

– задача дискретного логарифмирования.

Генерация пары ключей основана на генерации больших простых чисел, а процедуры криптопреобразований достаточно громоздки. Все это уменьшает быстродействие асимметричных криптосистем.

С развитием технологий оценки соотношения быстродействия симметричных и асимметричных систем все время меняются, но быстродействие симметричных криптосистем всегда выше. Поэтому на практике чаще применяются комбинированные (гибридные) системы, которые позволяют сочетать преимущество асимметричных криптосистем (высокая безопасность, так как нет необходимости ни передавать секретный ключ, ни подтверждать его подлинность) с достоинством симметричных криптосистем (высокая скорость работы).

Таким образом, симметричные системы применяются для шифрования текстов произвольного объема, а асимметричные криптосистемы обычно используются для шифрования ключей, распределения ключей и аутентификации с помощью ЭЦП.

Специфика асимметричных криптосистем определила их основные задачи:

– распределение ключей;
– направленное шифрование;
– электронная цифровая подпись.

Защита юридической значимости платежных документов является важным условием для справедливого разрешения споров и определения виновных в нанесенном ущербе в электронной платежной системе (ЭПС). Только юридическая защищенность создает доверие к ЭПС у ее участников и повышает их дисциплинированность при совершении расчетов. Это является еще одним аргументом в пользу того, что для ЭПС более приоритетными являются криптографические методы обеспечения подлинности и целостности платежных документов, то есть ЭЦП, а не методы обеспечения конфиденциальности.

Для юридически значимого использования ЭЦП более чем между двумя субъектами права открытые ключи ЭЦП должны сертифицироваться. На практике это означает, что к ЭЦП добавляется еще электронный сертификат ее открытого ключа, подтверждающий его принадлежность.

Постановка на электронный документ ЭЦП (даже вместе с сертификатом открытого ключа) не делает документ конфиденциальным, т.е. не защищает от несанкционированного просмотра в случае перехвата. Как уже писалось выше, ЭЦП гарантирует лишь авторство документа и его целостность, но не конфиденциальность.

Для гарантирования конфиденциальности электронные документы с добавленной ЭЦП и сертификатом открытого ключа при передаче телекоммуникационными каналами могут дополнительно шифроваться симметричным ключом.

Необходимо уточнить, что выше рассматриваются криптографические схемы универсального назначения. Кроме таких схем в криптографии имеются два направления исследований, разрабатываемых специально для банковских приложений. К ним относятся так называемые банковские криптографические протоколы и криптографическое обеспечение банковских карточек. В современном понимании банковская карточка – это интеллектуальная карточка с соответствующим цифровым со-

держимым, криптографическая часть которого может включать в себя как специфические для банков компоненты, так и криптоалгоритмы шифрования, аутентификации и т.п.

Появившиеся позже криптосистемы на эллиптических кривых (ЭК) наследуют протоколы асимметричных криптосистем (Эль-Гамаля) и дают выигрыш в криптостойкости, основанной на сложности дискретного логарифмирования. Криптосистема на ЭК с длиной ключа в 160 бит сравнима по безопасности с криптосистемами RSA и Эль-Гамаля с размерами ключа 1024 бита. Причем, этот выигрыш прогрессирует с увеличением длины ключа [3].

Необходимо заметить, что развитие квантовой криптографии может привести к тому, что все современные криптографические методы защиты информации окажутся бессильными против вычислительной мощности квантовых компьютеров, но пока они справляются со своей задачей. Основным вопросом защиты документооборота остается выбор надежного криптоалгоритма и ключа шифрования.

Учитывая все вышесказанное, можно классифицировать криптографические алгоритмы по назначению (рис. 1) [2, 3, 4].

ВЫВОДЫ

Несмотря на то, что на рис. 1 представлены далеко не все имеющиеся криптографические алгоритмы, данная на нем схема демонстрирует, что они отличаются по назначению и не имеют общей терминологии. Из всех приведенных алгоритмов, только 4 являются стандартами Украины [5]. Кроме того, украинский стандарт сертификата ЭЦП отличается от европейского [4].

Нужно также отметить, что “вставка” принятых в Украине стандартов криптографических алгоритмов в западное программное обеспечение является сложной, практически неразрешимой задачей.

Большинство операционных систем и браузеров используют встроенный асимметричный алгоритм защиты данных RSA. Даже то, что теоретически доказана подверженность алгоритма ЭЦП RSA мультипликативной атаке (возможности создания подписи без знания секретного ключа), не останавливает Европейские страны от использования именно этого алгоритма для аутентификации с помощью ЭЦП. Кроме того, в Евросоюзе законодательная база предусматривает формирование единой базы таможенных деклараций. Вся система строится на распознании электронной подписи, цифровых сертификатов, которые несовместимы с украинскими.

Подводя итог вышеперечисленному, можно сделать вывод о необходимости дальнейшего развития и усовершенствования законодательной базы Украины в сфере ЭЦП и имплементации международного законодательства в части обеспечения безопасности применения ЭЦП.

ЛИТЕРАТУРА

1 Романец Ю.В., Защита информации в компьютерных системах и сетях/ Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин Под ред. В.Ф. Шаньгина. – М.: Радио и связь. – 328 с.

2 Задірака В.К., Комп’ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / Задірака В.К., Кудін А.М., Людвиченко В.О., Олексюк О.С. Київ – Тернопіль: Підручники і посібники, 2007. – 272 с.

3 Бессалов А.В., Криптосистемы на эллиптических кривых: учеб. пособ. / А.В. Бессалов, А.Б.Телиженко. – К.: ІВЦ Видавництво “Політехніка”, 2004. – 224 с.

4 Материалы сайта [Электронный ресурс] http://www.cryptopro.ru/cryptopro/documentation/digcert.htm

5 Вимоги до структури об’єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами) / Мін'юст України, Держспецзв'язку України; Наказ, Вимоги від 20.08.2012 № 1236/5/453 — Редакція від 07.06.2013.

6 Материалы сайта [Электронный ресурс] http://zakon.rada.gov.ua.

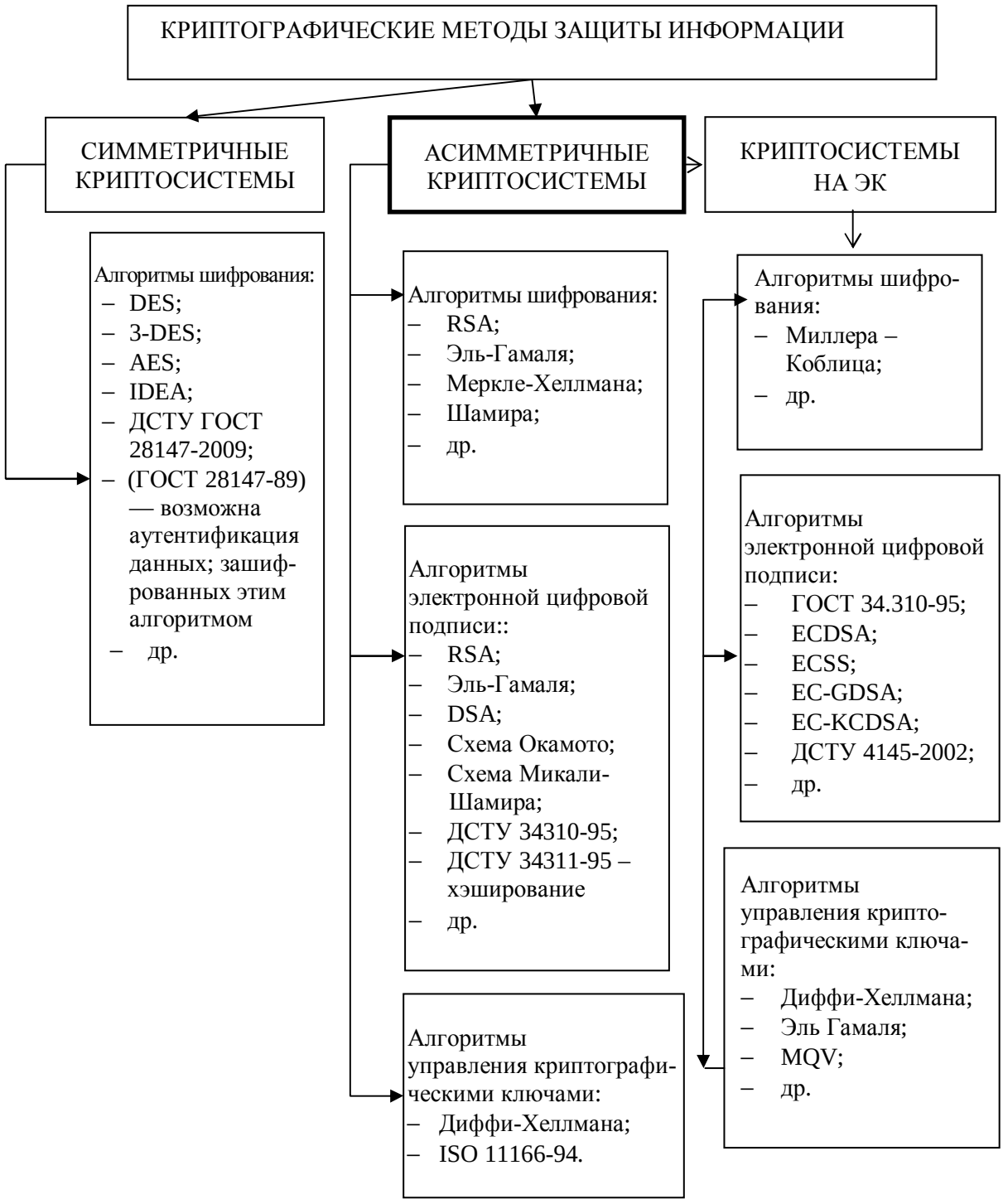

Рисунок 1 – Классификация криптографических алгоритмов по назначению