УДК 681.3

ПРОБЛЕМЫ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

© 2018 В. Д. Камакин, И. Я. Львович

Воронежский институт высоких технологий (г. Воронеж, Россия)

В статье обсуждается проблема защиты электронных документов. Приведена схема распределения ключей для электронной цифровой подписи.

Ключевые слова: защита информации, электронный документ, электронная цифровая подпись.

Рассмотрим особенности построения систем, использующих для защиты электронной цифровой подписи (ЭЦП), открытые и закрытые ключи. Следует обеспечить, чтобы была доступность открытого ключа для всех возможных адресатов корреспондента. Личная подпись заверяет информацию, подлежащую для передачи. На разделяемом ресурсе можно сохранять подобный ключ [1].

Разумеется, что численность пользователей в таких системах может быть весьма большая. Прежде всего, каждый из них (рис. 1) должен обладать секретным ключом и надежным образом его сохранять. Помимо этого, необходимо чтобы был доступ по отношению к открытым ключам других адресатов.

Определённая система оказывает влияние на физическое представление ключей. В ней поддерживается использование ЭЦП.

Во многих случаях ключ размещается в файле. В подобном файле может содержаться данные о пользователях – которые применяют ключ, о сроке действия ключа, некоторый комплект данных, требуемых для работы определённой системы [2].

Когда мы знаем, кто владеет ключом, тогда можно установить автора писем.

В ряде случаев в программных продуктах мы на выходе можем увидеть на экране мониторе, например:

1: "Подпись файла message.doc верна (Автор: Иванов Петр Иванович)"

Если рассматривать построение ЭЦП с точки зрения математической формализации, то можно опираться на формулу: 292: S = f (h(M), Ks), где текст сообщения – это M, в качестве секретным ключа выступает Ks , h(M) – это функция хэширования.

Тогда рассматривается хэш сообщения, а не оно само для того, чтобы сформировать ЭЦП.

Подпись может заверить любой текст, в том числе и с графическими вставками [2, 3].

Для того, чтобы расчитывать сообщения в алгоритмах вычислений ЭЦП задают определенную длину (к примеру, в российском алгоритме ЭЦП ГОСТ Р 34.10-94 указан размер, равный в 32 байта).

Из сообщения любой длины хэш-функция определяет вычисление цифровой последовательности с необходимым размером (например, 32 байта).

Сама функция должна соответствовать конкретным требованиям [4, 5].

Хэш сообщения должен однозначным образом связан с исходным сообщением и была его модификация для при любого изменения. Также любое сообщения M нельзя допустить возможности по подбору такого сообщения M', при оценке хеша, для которого h(M) = h(M'). Значение трудоемкости по удачному вычислению сообщения M' по известному сообщению M и его хэшу h(M), связанного с условием h(M') = h(M), должно быть эквивалентно трудоемкости, связанном с прямым перебором сообщений [6, 7].

В противном случае злоумышленник мог бы сделать подмену сообщений, при верной их подписи.

При этом хэш будет одинаковым по многим сообщениям, так как множество возможных сообщений будет значительно большим, чем множество возможных хэш-значений.

Согласно закону No 63-ФЗ (ред. от 28.06.2014) «Об электронной подписи» от 06.04.2011, ЭП считается информация в электронном формате, присоединённая к

Камакин Виктор Дмитриевич – Воронежский институт высоких технологий, студент kamakttt156@yandex.ru.

Львович Игорь Яковлевич – Воронежский институт высоких технологий, д. т. н., профессор, office@vivt.ru.

другой информации в электронном формате (подписываемой информации) либо другим образом связанная с данной информацией и используемая, чтобы определить лицо, подписывающее информацию.

Рисунок 1. Распределение ключей ЭЦП.

Механизм ЭП функционирует, применяя 2 криптографических ключа – открытый и закрытый, генерируемые автором (отправителем) сообщения.

Закрытым (секретным) ключом ЭП считается последовательность символов, которая предназначена для вырабатывания ЭП и известна исключительно правомочному лицу, то есть владельцу. Этот ключ он использует, чтобы создавать свою подпись под документом.

Открытым (публичным) ключом ЭП принято считать общедоступную последовательность символов, которая предназначена, чтобы проверять электронную подпись отправителя. Открытым ключом можно только проверить существующую ЭП, однако нельзя поставить подпись вместо отправителя [8].

Асимметричными алгоритмами применительно к ЭП предполагается вычисление при её создании так именуемой хэш-функции (хэш-кода), другими словами последовательности нулей и единиц всё время одинаковой длины (согласно закону РФ «Об электронной подписи» она задается равной 256).

Несмотря на то, что длина хэш-кода любого документа произвольного размера, с первого взгляда, большой не представляется, аналогичные хэш-коды у различных документов могут встречаться с меньшей вероятностью, нежели вероятность совпадения отпечатков пальцев у разных людей.

Затем полученный хэш-код «закрывается» при помощи секретного ключа лица, которое подписывает документ, и ЭП документа как следствие описанного выше процесса присоединяется к исходному тексту [9, 10].

Таким образом, оформленный документ и будет считаться документом, подписанным ЭП.

На рисунке 2 показана схема процедуры передачи электронной подписи.

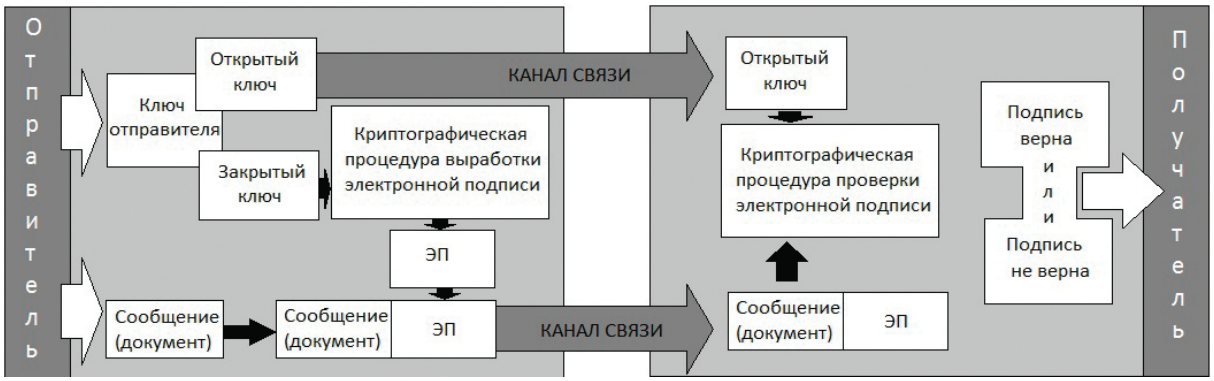

Рисунок 2. Постановка и проверка ЭП под электронным документом.

Получатель сообщения по такой подписи может удостовериться, что сообщение отправлено именно автором, а не кем-то другим.

Помимо этого, таким образом, подписанный документ изменить уже невозможно.

Проверка ЭП под электронным документом с целью установления его достоверности осуществляется при помощи открытого ключа, парного закрытому, который может свободно распространяться и обязан быть доступен любому из участни-

ков информационного обмена с обладателем закрытого ключа.

Когда коды совпали, то подпись верна, а значит документ считается подлинным.

И когда в процессе создания ЭП действительно применялся секретный ключ того лица, которое должно было подписать электронный документ, и в процессе его пересылки содержимое документа преднамеренно либо случайно (к примеру, по причине помех в канале связи) не менялось, то документ является подлинным и считается действительным.

Все рутинные операции по генерации и проверке ЭП производятся автоматически специальными криптографическими средствами – подсистемой ЭП.

Средства создания ЭП могут быть различными. Их правомочность устанавливается законодательно.

Отправитель, кроме подшивки в документ своей ЭП, может свое сообщение ещё и полностью зашифровать.

Соответственно, шифрование всего отправляемого документа и ЭП под ним отправитель сообщения может применять совместно.

Вначале документ можно подписать при помощи своего секретного ключа, а затем при помощи открытого ключа получателя его зашифровать. Подпись при этом заверяет личность отправителя, а шифрованием письмо защищается от чужого просмотра.

ЛИТЕРАТУРА

1. Львович, И. Я. Основы информатики / И. Я. Львович, Ю. П. Преображенский, В. В. Ермолова. – Воронеж, Издательство: Воронежский институт высоких технологий (Воронеж). – 2014. – 339 с.

2. Преображенский, Ю. П. Проблемы кодирования информации в каналах связи / Ю. П. Преображенский // Современные инновации в науке и технике; Отв. ред. А. А. Горохов. – 2018. – С. 180-182.

3. Преображенский, Ю. П. О видах информационных систем в организации / Ю. П. Преображенский // Современные инновации в науке и технике; Отв. ред. А. А. Горохов. – 2018. – С. 131-134.

4. Преображенский, Ю. П. Применение программных средств для повышения защищенности компьютерных систем / Ю. П. Преображенский // Современные инновации в науке и технике; Отв. ред. А. А. Горохов.. – 2018. – С. 76-78.

5. Преображенский, Ю. П. Проблемы управления в производственных организациях / Ю. П. Преображенский // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления; Под ред. Ю. В. Вертаковой. – 2018. – С. 208-211.

6. Питолин, А. В. Исследование возможностей использования стеганографических способов защиты информации / А. В. Питолин, Ю. П. Преображенский, О. Н. Чопоров // Моделирование, оптимизация и информационные технологии. – 2018. – Т. 6. – № 2 (21). – С. 336-353.

7. Преображенский, Ю. П. О возможности защиты информации на предприятиях / Ю. П. Преображенский // Современные материалы, техника и технология; Отв. ред. А. А. Горохов. – 2017. – С. 294-298.

8. Преображенский, Ю. П. Предложения по оптимизации систем защиты информации / Ю. П. Преображенский // Современные материалы, техника и технология; Отв. ред. А. А. Горохов. – 2017. – С. 298-302.

9. Воронов, А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

10. Львович, И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. – Т. 14. – № 3. – С. 469-470.

THE PROBLEMS OF PROTECTION OF ELECTRONIC DOCUMENTS

© 2018 V. D. Kamakin, I. Ya. Lvovich

Voronezh Institute of High Technologies (Voronezh, Russia)

The problems of using different approaches to protect electronic documents are discussed. The scheme of distribution of keys for electronic digital signature is given.

Key words: information security, electronic document, electronic digital signature.