УДК 681.142

МЕХАНИЗМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Семёнов В.В., студент 1 курса экономического факультета.
Научный руководитель - Ильдутов Е.А., кандидат экономических наук, старший преподаватель
ФГБОУ ВПО «Ульяновская ГСХА им. П.А. Столыпина»

Ключевые слова: *документ, безопасность, подпись, алгоритм, функция, ключ, сообщение*

В статье описан механизм функционирования электронной цифровой подписи. Показаны алгоритмы формирования, цели, типы, а также способы проверки цифровой подписи.

Включение компьютеров во многие сферы деятельности человека привело к увеличению информации, хранящейся в электронном виде. Это действие было оправдано, ведь информацию в электронном виде очень просто хранить, копировать, передавать кому-либо. Но возникла новая проблема – подделка информации. Появление электронной цифровой подписи позволило существенно повысить уровень защиты данных в сети.

Электронная цифровая подпись – особый атрибут документа, удостоверяющий авторство определенного человека.

Цели электронной цифровой подписи:

- Защита участников обмена от ложной информации;
- Защита от несанкционированного изменения документа;
- Доказательство авторства документа [1].

Выделяется три основных типа электронной цифровой подписи:

1. Простая электронная цифровая подпись, в данном случае подпись создается без криптографических преобразований;

2. Усиленная электронная цифровая подпись, она получается при применении криптографического преобразования информации, с использованием закрытого ключа;

3. Квалифицированная электронная цифровая подпись, отличается от предыдущего типа тем, что для её создания используется сертифицированное программное обеспечение [2].

Характерными чертами электронной цифровой подписи являются:

- невозможность редактирования исходного документа с электронной цифровой подписью, так как после этого она становится недействительной;
- уникальность электронной цифровой подписи для каждого документа;
- идентификация лица, поставившего электронную цифровую подпись на документе;

- контроль целостности электронного документа [3].

Существует 2 алгоритма построения электронной цифровой подписи:

1. Симметричное шифрование на основе криптосистемы с использованием одного ключа, известного только обеим сторонам.

2. Асимметричное шифрование на основе криптосистемы с открытым ключом. Открытый ключ находится в открытом доступе в сети. Целью его использования является проверка авторства документа, целостности информации в нем и самой электронной подписи. Доступ к закрытому ключу имеет только владелец сертификата подписи, он необходим для генерации электронной подписи при использовании программного обеспечения [4].

Документ подписывается таким образом: сначала создается особая функция, похожая на контрольную сумму – хэш-функция, она идентифицирует содержание документа, далее автор электронного документа зашифровывает хеш-функцию при помощи закрытого ключа, известного только ему. Зашифрованная хеш-функция отсылается вместе с документом. Это послание может храниться на любом носителе или отсылаться по сети. Хеш-функция не сильно увеличивает вес сообщения [5].

Получатель сообщения с документом, подписанным электронной цифровой подписью, может проверить его на подлинность.

Проверка обычно осуществляется при помощи специального программного обеспечения, а также сравнением хеш-функций.

При получении сообщения получатель строит свою хеш-функцию, а далее расшифровывается присланная с документом хеш-функция. Далее идет их сравнение, в случае совпадения документ подлинный [6].

Таким образом, огромная сложность подделки и легкость передачи документа, имеющего электронную цифровую подпись, по сетевым каналам делают её идеальной заменой ручной подписи.

Библиографический список:

1. Википедия – свободная энциклопедия [Электронный ресурс].- Режим доступа: https://ru.wikipedia.org
2. Важное об электронном документообороте, бизнес процессах и взаимодействии. Система документооборота [Электронный ресурс].- Режим доступа: http://ecm-journal.ru
3. Герман, О.Н. Теоретико-числовые методы в криптографии/ О.Н. Герман. – Издательство: «Академия (Academia)», 2012. – 272 с.
4. Удостоверяющий центр ekey.ru [Электронный ресурс].- Режим доступа: http://www.ekey.ru

5. АЭТП - Ассоциация электронных торговых площадок [Электронный ресурс].- Режим доступа: http://aetp.ru
6. Введение в теоретико-числовые методы криптографии: учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. – СПб.: Лань, 2011. – 400 с.
7. Заживнова, О.А. Роль информационно-правового обеспечения на современном этапе / О.А. Заживнова, Е.В. Штурмина, Е.А. Ильдутов // Аграрная наука и образование на современном этапе развития: опыт, проблемы и пути их решения. Материалы IV Международной научно-практической конференции. – Ульяновск: ГСХА им. П.А. Столыпина, 2012. – Том 3. -С. 81-84.
8. Информационные системы и технологии в экономике: учебное пособие для специальностей экономического профиля/ В.В. Романов О.В. Солнцева, А.В. Севастьянова, О.А. Заживнова. - Ульяновск: УГСХА, 2010. - 134 с.

THE MECHANISM OF ELECTRONIC DIGITAL SIGNATURE

Semenov V.V.

Keywords: *document, safety, signature, algorithm, the function key message*

This article describes the operation of the entire mechanism of electronic digital signature. Showing forming algorithms, goals, types, and how to verify the digital signature.