Сейтбекова Г.О., Бернияз А.Қ.,Сағынат И.А. студент
Алматинский технологическийқ университет, Қазақстан

Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП)— реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе, а также обеспечивает неотказуемость подписавшегося.[1]

Алгоритмы ЭЦП делятся на два больших класса: обычные цифровые подписи и цифровые подписи с восстановлением документа. Обычные цифровые подписи необходимо пристыковывать к подписываемому документу. К этому классу относятся, например, алгоритмы, основанные на эллиптических кривых. Цифровые подписи с восстановлением документа содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и тело документа. К этому классу относится один из самых популярных алгоритмов — RSA.

В развитых странах мира, электронно-цифровая подпись широко используется в хозяйственном обороте. Алгоритм применения ЭЦП состоит из ряда операций:

- генерируется пара ключей: открытых и закрытых;
- открытый ключ передается заинтересованной стороне (получателю документов, подписанных стороной, сгенерировавшей ключи);
- отправитель сообщения шифрует его своим закрытым ключом и передает получателю по каналам связи;
- получатель дешифрует сообщение открытым ключом отправителя.

Суть в том, что создать зашифрованное сообщение, при расшифровке которого открытым ключом получается исходный текст, может только обладатель закрытого ключа, т. е. отправитель сообщения. Использовать для этого открытый ключ невозможно. Электронная подпись предназначена для идентификации лица, подписавшего электронный документ и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

Использование электронной подписи позволяет осуществить:

- контроль целостности передаваемого документа: при любом случайном или преднамеренном изменении документа подпись станет недействительной, потому что вычислена она на основании исходного состояния документа и соответствует лишь ему;
- защиту от изменений (подделки) документа: гарантия выявления подделки при контроле целостности делает подделывание нецелесообразным в большинстве случаев;

- невозможность отказа от авторства. Так как создать корректную подпись можно, лишь зная закрытый ключ, а он должен быть известен только владельцу, то владелец не может отказаться от своей подписи под документом.

Электронно-цифровая подпись применяется для подтверждения авторства и неизменности информации (того или иного электронного документа). В системе электронных торгов поставщик, подавший ценовое предложение или заявку на конкурс, обязуется осуществить поставку товара или осуществить услуги на условиях, указанных в его предложении. Будучи подписанным ЭЦП, данное предложение обретает юридическую значимость и влечет за собой ответственность в соответствии с законодательством. Таким образом, заказчик в системе электронных торгов имеет дело с реальными предложениями, исполнение которых гарантировано законодательством.

Цифровая подпись обеспечивает:

1. Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.
2. Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной.
3. Невозможность отказа от авторства. Так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом.
4. Предприятиям и коммерческим организациям сдачу финансовой отчетности в государственные учреждения в электронном виде;
5. Организацию юридически значимого электронного документооборота.

Возможны следующие угрозы цифровой подписи:

- Злоумышленник может попытаться подделать подпись для выбранного им документа.
- Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:Документ представляет собой осмысленный текст; Текст документа оформлен по установленной форме.
- Документы редко оформляют в виде Plain Text — файла, чаще всего в формате DOC или HTML.

В заключений, электронный документ - это зафиксированная на электронном носителе информация, которая записывается, сохраняется, передается и представляется в приемлемой для человека форме с помощью технологий, поддерживаемых ЭВМ, и которая содержит реквизиты, позволяющие ее идентифицировать. На сегодняшний день это одна из актуальных тем, поскольку практически ни одно дело не обходится без компьютерного обеспечения. Электронный документ имеет свой жизненный цикл, функции, особенности, признаки и требования которые отличаются от бумажного документа. Электронные документы имеют свою физическую и логическую структуру, не совпадающую с нашими традиционными представлениями о документе. Эта структура

зависит от способа размещения данных на машинных носителях, а также от программных и технических средств.

Система электронной цифровой подписи базируется на методах криптографической защиты данных. Учитывая бурное развитие вычислительных мощностей современных компьютерных систем и математических методов криптоанализа, практическая схема цифровой подписи должна гарантировать достаточный уровень защиты на годы вперед.

Список литературы

1. http://www.km.ru/referats/D8C33C845AFC4C99A669713B2FC4B68C

2. .Малофеев С.О применении электронной цифровой подписи в электронном документообороте / С. Малофеев // Секретарское дело. - 2009. - № 7. - С. 24-28.

3. .Бородакий Ю.В. Информационные технологии: методы, процессы, системы / Ю.В. Бородакий, Ю.Г. Лободинский. - М.: Радио и Связь, 2004. - С. 455.

4. .Бобылева М.П. Эффективный документооборот: от традиционного к электронном. / М.П. Бобылева // М.: Изд-во МЭИ, 2004. - С. 172.