Protecting documents with electronic digital signatures
Cherkasov D.[1], Ivanov V.[2] (Russian Federation)

Защита документов при помощи электронной цифровой подписи
Черкасов Д. Ю.[1], Иванов В. В.[2] (Российская Федерация)

[1]Черкасов Денис Юрьевич / Cherkasov Denis – студент;
[2]Иванов Вадим Вадимович / Ivanov Vadim – студент,
кафедра компьютерной и информационной безопасности,
Институт кибернетики
Московский институт радиотехники электроники и автоматики,
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования
Московский технологический университет, г. Москва

Аннотация: *статья посвящена анализу проблемы защиты документов при помощи электронной цифровой подписи. Рассматриваются виды и алгоритмы ЭЦП, а также её функции и области применения.*
Abstract: *this article analyzes the problems of protection of the documents using digital signatures. We consider the types and algorithms of digital signature as well as its functions and application areas.*

Ключевые слова: *электронная цифровая подпись (ЭЦП), защита документа, криптография, закрытый ключ, открытый ключ, ключевая пара, сертификат открытого ключа.*
Keywords: *electronic digital signature (EDS), document protection, cryptography, private key, public key, key pair, a public key certificate.*

Электронной подписью (ЭП), или электронной цифровой подписью (ЭЦП), называется реквизит электронного документа, представляющий собой программно-криптографическое (то есть зашифрованное определённым образом) средство - число, полученное в процессе изменения электронного документа как цифровой последовательности с помощью закрытого ключа автора. Такая цифровая обработка информации позволяет: а) зафиксировать отсутствие искажения или изменения информации электронного документа с момента подписания (критерий целостности); б) проверить подлинность подписи конкретного владельца, обладающего «сертификатом ключа подписи» (критерий авторства); в) подтвердить подписание электронного документа, если он прошел успешную проверку (критерий неотказуемости).

Все вопросы, касающиеся ЭЦП, регулирует Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи». Этот закон определяет три вида электронных подписей: простую электронную подпись, усиленную неквалифицированную электронную подпись и усиленную квалифицированную электронную подпись [2].

Электронная подпись ставится с теми же целями, что и обычная ручная подпись под бумажными документами, для определения лица, подписавшего документ в случаях, предусмотренных законом - предназначается для определения лица, подписавшего электронный документ, и является аналогом собственноручной подписи в случаях, предусмотренных законом. ЭЦП применяется в гражданско-правовых сделках, государственных и муниципальных услугах, при совершении целого спектра юридически значимых действий. В так называемой «электронной» экономике она обеспечивает качественный контроль над целостностью передаваемого электронного платёжного документа. Если произойдет случайное или умышленное изменение документа ЭЦП автоматически станет недействительной, поскольку она вычисляется по специальному алгоритму, «привязанному» к исходному состоянию документа, и соответствует только ему. ЭЦП обеспечивает гарантию того, что при осуществлении проверки целостности будут выявлены различные подделки, следовательно, подделывание документов в большинстве случаев на практике заранее становится нецелесообразным.

Также электронная подпись означает невозможность отказаться от авторства данного документа, то есть формирует доказательства подтверждения авторства. Благодаря своим свойствам ЭЦП может использоваться в различных сферах электронного документального и денежного обращения: например, в области таможенного декларирования, при электронных регистрациях сделок с недвижимостью, для банковских платёжных систем, электронной коммерции, управления госзаказами, для обязательных налоговых (фискальных), бюджетных, статистических отчётностей, в расчётных и трейдинговых системах, в глобальных системах межбанковских рынков обмена валют и т.д.

Существуют различные способы построения цифровой подписи: это так называемое симметричное шифрование (наличие в системе третьего лица - арбитра, пользующегося доверием обеих сторон; авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру), а также асимметричное шифрование, групповая подпись, неоспоримая подпись, доверенная подпись.

Общая схема образования цифровой подписи – это три взаимосвязанных процесса: во-первых, генерация «ключевой пары» (из нескольких возможных вариантов «закрытых ключей» выбирается один

«закрытый ключ» в виде последовательности цифр определённой длины, а затем сопоставляется соответствующий ему «открытый ключ»); во-вторых, формирование самой подписи (она вычисляется с помощью «закрытого ключа»); в-третьих, проверку (или верификацию) подписи (для данного документа и данной подписи при помощи «открытого ключа», который доступен любому, определяется действительность подписи). Важно, что данный процесс требует выполнения двух условий: а) верификация подписи открытым ключом, соответствующим закрытому ключу, использованному при подписании; б) без закрытого ключа должно быть, в принципе, сложно создать законную цифровую подпись. По закону информация о принадлежности открытого ключа определённому пользователю должна быть документально оформлена соответствующим ответственным органом. Такой документ называется сертификатом открытого ключа ЭЦП.

Электронная цифровая подпись - современный инструмент, позволяющий быстро, независимо от времени суток либо от расстояния заключить юридически полноценную сделку, а также в случае необходимости решить разнообразные споры, в том числе и в судебном порядке [1]. ЭЦП в условиях развития компьютерных систем и методов криптоанализа продолжает совершенствоваться, чтобы гарантировать необходимый уровень защиты своим пользователям.

Литература

1. *Бобылёва М. П.* Эффективный документооборот: от традиционного к электронному. М.: Изд-во МЭИ, 2004. 172 с.

2. *Семилетов С. И.* Электронный документ как продукт технологического процесса документирования информации и объект правового регулирования // Государство и право, 2003. № 1. 101 с.