УДК 004.056.5

СТРУКТУРА ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Кудряшева А.Р., студентка 1 курса ФАЗРиПП
Научный руководитель – Бунина Н.Э., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *электронная подпись, бизнес-технологии, криптография, открытый ключ, хеширование, алгоритм, хеш, шифрование, цифровая подпись.*

В данной статье рассматриваются особенности цифровой подписи, ее структура и основные принципы, позволяющие предупредить фальсификацию юридических сделок, подделку подписей и замену пунктов в содержании юридических документов.

Цифровая подпись в электронном документе является аналогом традиционной подписи, но предполагает большую защиту от подделки подписи в документах и предназначена для решения проблемы фальсификации личности в электронных ресурсах. Цифровые подписи могут являться дополнительной гарантией подлинности электронного документа, его статуса, так же являются дополнительным гарантом сделки или сообщения. Во множестве стран, в том числе и в России, актуально использование такого вида подписи. При этом электронная цифровая подпись имеет такую же юридическую силу, как и более распространенная традиционная форма подписи.

В основе цифровой подписи лежит криптография с открытым ключом или ассиметричная криптография. Используя открытый ключ алгоритма, можно сгенерировать два ключа, связанных математически друг с другом. Закрытый ключ используется, чтобы зашифровать хеш.

Причина шифрования хеша, а не всей информации в документе в том, что хэш-функцией является преобразование произвольного ввода в значение закреплённой длины, которое обычно имеет меньший объём. Хеширование является более быстрым и удобным способом, поэтому экономит время.

Таким образом, цифровая подпись представляет собой зашифрованный хеш и дополняющую информацию (алгоритм хеширования).

Для создания цифровой подписи программа для подписания создаёт данные, которые хешируются, а затем будут подписаны.

Хеширование — преобразование информации, в результате которого получается отображение, называемое хешем — уникальная короткая символьная строка, которая присуща только входящей электронной информации.

Хеш имеет уникальное значение для электронных данных. Любое изменение данных, правка или удаление одной символьной единицы, приводит к другому значению. Это позволяет проверить монолитность данных с помощью открытого ключа подписавшего для расшифровки хеша. Если расшифрованный хеш совпадает со вторым вычисленным хешем тех же данных, это доказывает, что данные не были изменены с момента подписания. Если хеш не совпадает, данные либо были изменены в некотором роде (нарушена целостность) или подпись создана с использованием закрытого ключа, что представленные подписи не соответствует открытому ключу (нарушение аутентификации).

Цифровая подпись может использоваться с любым видом данных - будь они зашифрованы или нет - для уверенности получателя в личности отправителя и в стабильности и ненарушенности исходного сообщения.

6 апреля 2011 года вступил в силу Федеральный закон № 63-ФЗ. Полномочия электронной подписи были существенно расширены. Документы, подписанные квалифицированной электронной подписью, являются юридически равнозначными документам на бумажном носителе, подписанным собственноручно. В удостоверяющем центре можно получить квалифицированный сертификат ключа проверки электронной подписи, соответствующий требованиям Приказа ФСБ России №795 от 27.12.2011 г.

Простая электронная подпись - подтверждает факт формирования подписи лицом посредством кодов, паролей и иных средств защиты. Используется для оформления электронных сообщений, направляемых в органы государственной власти или должностным лицам.

Усиленная неквалифицированная электронная подпись - подтверждает факт формирования подписи определенным лицом и неизменность документа с момента подписания. Разрешена к использованию при оформлении документов, не требующих обязательного наличия печати. Подпись создается с помощью криптографических средств, при этом допускается использование сертификата неаккредитованного удостоверяющего центра.

Усиленная квалифицированная электронная подпись - квалифицированная подпись создается с помощью подтвержденных ФСБ криптографических средств и имеет сертификат от аккредитованного удо-

стоверяющего центра, выступающего гарантом подлинности подписи. Электронный документ, подписанный КЭП, во всех случаях приравнивается законодательством к бумажному документу с собственноручной подписью. Квалифицированная подпись признается действительной до тех пор, пока решением суда не установлено иное.

Развитие бизнес-технологий дало множество преимуществ руководителям крупных компаний. Но частыми стали случаи фальсификации документации, замены юридических лиц и подделки подписи руководителей. А заключение нотариально подтвержденной сделки с бумажным документооборотом занимает очень много времени. Один из методов решения такой проблемы является использование электронной цифровой подписи.

Таким образом, подводя итог, можно сказать - несмотря на то, что цифровая подпись требует вложения в нее денежных средств и некоторых специальных знаний для ее использования, она, несомненно, более преимущественна, чем традиционная подпись. Основным преимуществом использования ЭЦП следует обозначить экономию времени её пользователя, защиту от фальсификации и изменения документов, а следовательно и надежность обеспечиваемых ею сделок.

На данный момент сфера использования ЭЦП не достаточно широка и требует новых введений и доработок, но тем не менее, данное достижение технического прогресса имеет достаточно высокий оборот. Электронная подпись способна решить множество задач, стоящих перед ее пользователями. Я считаю, электронная подпись - это инструмент современного информационного общества.

Библиографический список:

1. Просто об электронной подписи [Электронный ресурс]. – URL: https://ecm-journal.ru/e-sign
2. Бунина, Н.Э. Анализ видов электронной коммерции / Н.Э. Бунина, Ю.А. Падиарова // Современное образование: плюсы, минусы и перспективы. Материалы VIII международной научно-практической конференции.- Саратов: Саратовский государственный технический университет. - 2017. - С. 32-35.
3. Бунина, Н.Э. Системы электронных платежей / Н.Э. Бунина, В.А. Аршинова // Инновационный и научный потенциал XXI века. Материалы I международной научно-практической конференции. - Саратов: Саратовский государственный технический университет, 2017. - С. 23-27.
4. Солнцева, О. В. Интерактивные методы изучения информационных систем в экономике / О. В. Солнцева, Н. Э. Бунина, О. А. Заживнова // Инноваци-

онные технологии в высшем профессиональном образовании. Материалы научно-методической конференции профессорско-преподавательского состава академии. – Ульяновск: УГСХА им. П.А. Столыпина, 2013. - С. 168-172.
5. Бунина, Н.Э. Актуальные проблемы информационного обеспечения регионального АПК / Н.Э. Бунина // Информационные системы и технологии в АПК. Материалы международной научно-практической конференции. – Ульяновск: УГСХА, 2002. - С.36-38.
6. Бунина, Н.Э. Применение метода проектов в высшей школе / Н.Э. Бунина, О.В. Солнцева, О.А. Заживнова //Инструменты и механизмы современного инновационного развития. Материалы международной научно-практической конференции. - 2016. - С. 124-127.
7. Информационные технологии в науке и образовании : лабораторный практикум для аспирантов / О.В.Солнцева, Н.Э.Бунина, О.А.Заживнова, М.А.Видеркер. - Ульяновск: УГСХА им. П.А.Столыпина, 2015. - 64 с.

THE STRUCTURE OF THE ELECTRONIC DIGITAL SIGNATURE

Kudryasheva A.R.

Keywords: *electronic signature, business technologies, cryptography, public key, hashing, algorithm, hash, encryption, digital signature.*

This article discusses the features of digital signature, its structure and basic principles to prevent the falsification of legal transactions, forgery of signatures and the replacement of items in the content of legal documents.