УДК 004.021

РАЗРАБОТКА АЛГОРИТМА КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ ДЛЯ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА БЕЗ ИСПОЛЬЗОВАНИЯ СЕРТИФИКАЦИОННЫХ ЦЕНТРОВ

Макшеев И.Д
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный Исследовательский Университет ИТМО»)
Санкт-Петербург
Научный руководитель – доцент факультета безопасности информационных технологий Таранов С.В.
(Федеральное государственное автономное образовательное учреждение высшего образования «Национальный Исследовательский Университет ИТМО»)
Санкт-Петербург

В настоящей работе представлено решение использования алгоритма коллективной цифровой подписи для системы электронного документооборота без использования сертификационных центров.

Введение. Электронная цифровая подпись (ЭЦП) — это современный и удобный инструмент для взаимодействия внутри компании, контрагентами и государственными органами. Сегодня ЭЦП необходима для ведения бизнеса.

Наличие легитимных электронных подписей в системе позволяет отказаться от бумажных носителей. В связке с системами юридически значимого документооборота это позволяет построить полностью безбумажный внутренний и внешний документооборот.

На практике потребность в протоколах коллективной электронной цифровой подписи (КЭЦП) имеет место при разработке документации для крупных проектов, требующих привлечения достаточно большого числа специалистов различного профиля. Каждый из них готовит отдельный раздел документации. При этом отдельные разделы проектной документации или вся их совокупность должны быть подписаны всеми разработчиками. Для сокращения размера совокупной цифровой подписи и снижения вычислительной сложности проверки подлинности ЭЦП могут быть применены протоколы КЭЦП.

КЭЦП обладает важным для практического применения свойством внутренней целостности, которое состоит в том, что по коллективной подписи вычислительно невозможно вычислить подпись, относящуюся к другой совокупности подписантов. Целостность означает, что подпись едина и неделима: либо все подписанты подписали электронный документ, либо никто из них не подписывал этот документ. Размер такой подписи равен размеру одной обычной (индивидуальной) ЭЦП.

Основная часть. В рамках данной работы, предлагается разработать алгоритм КЭЦП, в котором, при формирование подписи каждый подписант генерирует свой разовый личный секретный ключ, и вычисляет свой разовый открытый ключ. Все разовые открытые ключи рассылаются каждому участнику протокола, после чего по ним вычисляется разовый коллективный открытый ключ, который маскирует все личные секретные ключи подписантов. При формировании коллективной подписи к электронному документу произвольного размера документ представляется значением хэш-функции.

Открытый ключ может быть взят в качестве первого элемента КЭЦП. Вторым элементом КЭЦП является число, представляющее собой сумму долей, вычисляемых каждым подписантом индивидуально. Число зависит от значения открытого ключа, значения хэш-функции, значения личного секретного ключа подписанта и его разового секретного ключа. Если кто-либо из подписантов, участвовавших в формировании параметра рандомизации, не предоставит правильно вычисленную долю подписи, то нахождение правильного значения второго элемента КЭЦП вычислительно нереализуемо.

Если все доли вычислены правильно. Они рассылаются всем подписантам и любой из них может вычислить по всем долям их значение, представляющее собой второй элемент КЭЦП. Полученное корректным способом значение КЭЦП может быть использовано для доказательства того, что каждый из заданного множества подписантов действительно подписал электронный документ.

Выводы. В конечной разработке предложенный алгоритм коллективной цифровой подписи будет внедрен в разрабатываемую систему электронного документооборота. С помощью тестирования конечного продукта будет изучена эффективность использования предложенной реализации.

Макшеев И.Д. (автор) _____

Таранов С.В. (научный руководитель) _____