ЗАЩИЩЕННАЯ СХЕМА ДОВЕРЕННОЙ ЦИФРОВОЙ ПОДПИСИ С ПОЛНОМОЧИЯМИ В СИСТЕМАХ ДИСТАНЦИОННОГО ОБУЧЕНИЯ

Р.В. Еленевич

Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, raman.yelianevich@gmail.com

Abstract. The main aspects of information security that relate to online education systems are authentication, non-repudiation, integrity and confidentiality. Cryptography is the main method to provide information security properties mentioned previously. In this paper we focus on providing authentication, non-repudiation and integrity properties in online education using digital signature as the most reliable technique.

Традиционные протоколы ЭЦП были предложены довольно давно, но зачастую их свойств оказывается недостаточно для решения современных проблем в дистанционном обучении. Важную группу составляют схемы доверенной цифровой подписи [1, 2]: частичное делегирование, делегирование с полномочиями, частичное делегирование с полномочиями, коллективное делегирование и другие. Доверенная цифровая подпись может быть применена для систем дистанционного обучения, в электронной коммерции, распределенных системах и в электронном документообороте. Была исследована и реализована защищенная схема доверенной цифровой подписи с полномочиями на основе алгоритма цифровой подписи Эль-Гамаль.

На рисунке 1 приведена схема, поясняющая принципы работы защищенной доверенной цифровой подписи с полномочиями в системе дистанционного обучения:

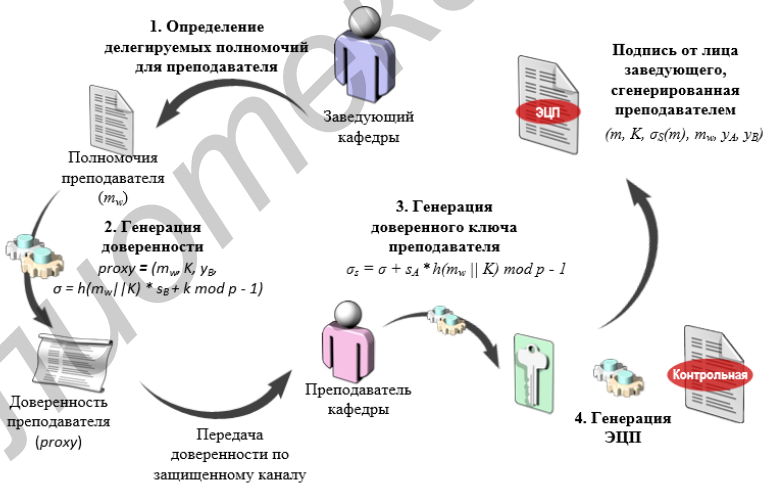

Рисунок 1 – Принципы работы защищенной доверенной цифровой подписи с полномочиями

Одним из главных шагов алгоритма доверенной цифровой подписи является генерация личного ключа доверенной стороны Преподавателя на основе ключевой информации доверителя Заведующего и делегируемых полномочий, определенных на стороне доверителя [1, 3]:

$$\sigma = h(m_w||K) * s_B + k \bmod p - 1,$$

где h - алгоритм криптографического хеширования, m_w – информация о полномочиях, s_B – личный ключ доверителя, k – сгенерированное случайное число, p – большое простое число.

После генерации секретного значения и передачи его по защищенному каналу происходит вычисление подстановочного секретного ключа доверенной стороны Преподавателя, который и определяет свойства защищенной схемы доверенной цифровой подписи с полномочиями:

$$\sigma_s = \sigma + s_A * h(m_w||K)\ mod\ p - 1,$$

где s_A – секретный ключ доверенной стороны Преподавателя.

После получения доверенной стороной конечного подстановочного секретного ключа может быть сгенерированна защищенная доверенная цифровая подпись с полномочиями. Электронная цифровая подпись имеет структуру $(m_p, s_{\sigma_p}(m_p), K, m_w)$, где m_p – передаваемое сообщение, $s_{\sigma_p}(m_p)$ – электронная цифровая подпись сообщения.

При получении сообщения с защищенной доверенной цифровой подписью проверяющая сторона выполняет проверку электронной цифровой подписи в два шага. На первом этапе вычисляет значение открытого ключа на основе открытой ключевой информации доверителя Заведующего кафедры и доверенной стороны Преподавателя:

$$y_p = (y_A \cdot y_B)^{h(m_W||K)} \cdot K\ mod\ p,$$

где y_A – открытый ключ Преподавателя, y_B – открытый ключ Заведующего.

На втором этапе происходит проверка цифровой подписи по алгоритму Эль-Гамаль с использованием вычисленного открытого ключа y_p. В результате проверки доверенной цифровой подписи проверяющая сторона может убедиться в целостности переданного документа, однозначно идентифицировать доверителя и доверенную сторону.

На основе приведенных выше вычислений можно сделать следующие выводы о разработанной математической модели: преподаватель может сгенерировать подпись от лица заведующего кафедры, заведующий кафедры не может сгенерировать защищенную доверенную подпись от лица преподавателя, заведующий кафедры может наложить ограничения на перечень дисциплин и срок возможности применения цифровой подписи с использованием полномочий, результирующая электронная цифровая подпись однозначно идентифицирует доверителя и доверенную сторону. Эти свойства выделяют данную схему по сравнению с другими алгоритмами ЭЦП [4].

Таким образом, была разработана и реализована математическая модель защищенной доверенной цифровой подписи с полномочиями применительно к системам дистанционного обучения. Для реализации математической модели использовался язык программирования Java и криптографическая библиотека с открытым исходным кодом Bouncy Castle. Корректное функционирование было проверено с использованием модульных тестов.

Литература

1. Sattar, A. A practical proxy signature scheme / A. Sattar, Y. Sufian // IJDIWC – 2012. – P. 27 – 35. Mambo, M. Proxy Signatures: Delegation of the power to sign Foundation / M. Mambo, K. Usuda, and E. Okamoto // IEICE Trans. Fundamentals Volume E79-A, Number 9, Sep 9, - 1996. – P. 1338-1354.

2. Mambo, M. Proxy Signatures: Delegation of the power to sign Foundation / M. Mambo, K. Usuda, and E. Okamoto // IEICE Trans. Fundamentals Volume E79-A, Number 9, Sep 9, - 1996. – P. 1338-1354.

3. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms / T. ElGamal // IEEE Trans. On Information Theory, Vol. IT-31, No. 4 – 1985 - P 86-91.