УДК 004.056

ЭЛЕКТРОННО-ЦИФРОВАЯ ПОДПИСЬ КАК СПОСОБ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ И НАДЕЖНОСТИ В ЦИФРОВОМ МИРЕ

Мороз М.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Бруй Н.М. – магистр техн. наук, ст. преподаватель кафедры ПИКС

Аннотация. Обоснована важность электронно-цифровой подписи в современном информационном пространстве, особенно в контексте развития цифровых технологий. Выделена структура и принципы работы электронной цифровой подписи, включая роль сертификатов, открытых и закрытых ключей, их использования для удостоверения информации и проверки подлинности документов.

Ключевые слова: электронная цифровая подпись, защита документа, открытый ключ, закрытый ключ, сертификат электронной подписи

Введение. С развитием цифровых технологий и распространением интернета возникают новые вызовы в области безопасности информации. В Беларуси, где цифровизация и автоматизация процессов активно развиваются, защита данных от несанкционированного доступа и подделки становится особенно важной. Сегодня многие организации перешли на современные методы обработки и обмена документами без использования бумаги. Это значительно сокращает время, необходимое для оформления сделок и передачи документов, а также совершенствует и удешевляет процесс их подготовки, передачи, учета и хранения. Для компаний это становится важным инструментом, позволяющим наладить эффективное внутреннее и внешнее взаимодействие через цифровой документооборот. В то же время, переход на электронный документооборот поднимает вопрос об авторстве и надежности документов. Важно обеспечить защиту документов от изменений и однозначно идентифицировать отправителя сообщения. В этом контексте электронная цифровая подпись становится наиболее удобным и эффективным средством защиты электронных документов и подтверждения их подлинности, несмотря на отличие от рукописной подписи внешним видом.

Основная часть. Электронная-цифровая подпись – последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности [1].

Электронная цифровая подпись предназначена для:

– удостоверения информации, составляющей общую часть электронного документа;

– подтверждения целостности и подлинности электронного документа;

Удостоверение информации, составляющей общую часть электронного документа, осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием личных ключей лиц, подписывающих электронный документ.

Подтверждение целостности и подлинности электронного документа осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием открытых ключей лиц, подписавших электронный документ. Электронная цифровая подпись является аналогом собственноручной подписи. Электронная цифровая подпись может применяться как аналог оттиска печати или штампа.

Совокупность процедур, методов, программных, программно-технических и технических средств, относящихся к практическому применению электронной цифровой подписи, образует технологию электронной цифровой подписи. Требования к технологии электронной цифровой подписи устанавливаются техническими нормативными правовыми актами.

Электронная цифровая подпись, как правило, состоит из трех компонентов: сертификата, открытого ключа и закрытого ключа. Сертификат электронной подписи подтверждает принадлежность открытого ключа (ключа проверки) владельцу сертификата. Такие сертификаты выдаются удостоверяющими центрами или их авторизованными представителями, а владелец сертификата ЭЦП – физическое лицо, на имя которого выдан сертификат.

Система электронной цифровой подписи использует асимметричный метод шифрования, который включает два различных ключа: закрытый и открытый. Закрытый ключ ЭЦП используется для подписи и шифрования информации, а открытый ключ – для проверки подписи и расшифрования данных. Владелец сертификата должен обеспечивать строгую конфиденциальность своего закрытого ключа.

Открытый ключ, связанный с закрытым ключом, распространяется среди пользователей системы для проверки подлинности подписей и документов. Этот ключ не может использоваться для расшифрования информации, что позволяет его безопасно распространять.

При получении документа с электронной цифровой подписью пользователь, имея открытый ключ, выполняет проверку подписи. Этот процесс позволяет убедиться в подлинности документа и отсутствии изменений. В случае обнаружения ошибок система оповещает об этом электронным сообщением.

Электронный обмен документами обеспечивает равные возможности для всех участников, независимо от их местоположения. Новые технологии сокращают расстояния между участниками и упрощают взаимодействие.

Заключение. Современные технологии позволяют организациям эффективно управлять документооборотом и обеспечивать безопасность передачи информации. Электронно-цифровая подпись играет ключевую роль в этом процессе, обеспечивая аутентичность, целостность и конфиденциальность данных. Внедрение и использование ЭЦП помогает организациям улучшить эффективность своей работы, сократить временные и финансовые затраты, а также повысить доверие к электронным документам. Все это делает электронно-цифровую подпись неотъемлемым элементом современной цифровой инфраструктуры и важным инструментом для обеспечения безопасности информации в условиях цифровой трансформации.

Список литературы

1. *Об электронном документе и электронной цифровой подписи. Основные термины [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3961&p0=H10900113. Дата доступа 15.02.2024.*

UDC 004.056

ELECTRONIC DIGITAL SIGNATURE AS MEANS OF ENSURING SECURITY AND RELIABILITY IN THE DIGITAL

Moroz M.S.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Brui N.M. – master of technical sciences, senior lecture of the department of ICSD

Annotation. The importance of electronic digital signature in the modern information space, particularly in the context of digital technology development, has been justified. The structure and principles of electronic digital signature operation have been outlined, including the role of certificates, public and private keys, and their utilization for authentication of information and verification of document authenticity.

Keywords: electronic digital signature, document protection, public key, private key, electronic signature certificate.