ПРОГРАММНОЕ СРЕДСТВО ПОД ОПЕРАЦИОННУЮ СИСТЕМУ ANDROID ДЛЯ РАБОТЫ С МОБИЛЬНОЙ ЦИФРОВОЙ ПОДПИСЬЮ

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

Никель О. С.

Шелест А. В. – магистр техники и технологии

Каждый день количество данных, передаваемых пользователями в сети Интернет, неуклонно растет. Среди данных могут оказаться секретные сведения компании или государственной организации, поэтому чрезвычайно важно обеспечить защиту данных.

При помощи современных компьютерных и сетевых технологий проводятся различные бизнес-расчёты, совершаются многомиллионные сделки во многих странах, осуществляется финансовый и юридический электронный документооборот. И для обеспечения безопасности данных необходимо решить задачи аутентификации информации. При этом важным элементом является ***электронная цифровая подпись*** (ЭЦП) – последовательность символов, являющаяся реквизитом электронного документа – и её достоверность. Она представляет собой эффективное средство защиты информации от модификации и переносит свойства реальной подписи под документом в сферу электронного документооборота. Существует несколько схем построения цифровой подписи. Они основываются либо на алгоритмах симметричного шифрования, либо на алгоритмах ассиметричного шифрования [1]. Ввиду распространения мобильных технологий, широкое распространение получила ***мобильная электронная цифровая подпись*** (ЭЦП-М) – технология, которая позволяет использовать мобильный телефон в качестве надежного средства идентификации при получении электронных сервисов.

Хранение личного ключа мобильной ЭЦП на SIM-карте делает процедуру подписи электронных документов удобной и простой: пользователь не ограничен доступом к компьютеру, документ может быть подписан в любое время и в любом месте. Необходимые для этого условия – наличие SIM-карты с поддержкой функции ЭЦП и устройства с функцией отправки и получения SMS. Процесс подписания электронного документа (рисунок 1) представляет собой отправку специальных зашифрованных сообщений – бинарных SMS – и подтверждение путем ввода PIN-кода.

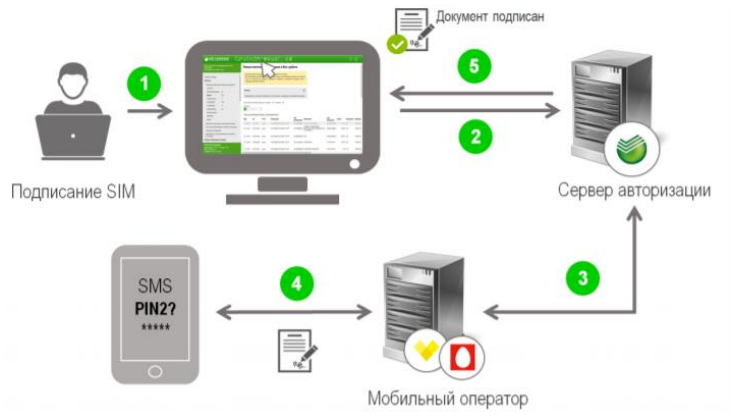

Рисунок 1 – Подписание документа ЭЦП пользователя

Предложенное в дипломном проектировании решение позволяет отказаться от использования бинарных сообщений, ускорив процесс передачи данных, а также ускорив отказ от потенциально опасной технологии с точки зрения информационной безопасности. Несомненным плюсом данного программного приложения, также является возможность ускорить документооборот внутри различных организаций и между ними. Документ, подписанный при помощи технологии электронной цифровой подписи защищен от модификации по пути от отправителя к получателю, что гарантирует неизменность этого документа.

Список использованных источников:

1.Тенденции развития и проблемы современной криптографии / Научное сообщество студентов XXI столетия. Технические науки: сб. ст. по мат. LXVI междунар. студ. науч.-практ. конф. № 6(65); А.Г. Малолеткина.

2.Национальный центр электронных услуг [Электронный ресурс]. – Режим доступа: https://nces.by/pki/kak-poluchit-ecp/ -- Дата доступа 10.04.2019