Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056:621.395.6

Дроздов
Михаил Михайлович

Система мобильной ЭЦП

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
(указать отрасль наук)
по специальности Методы и системы защиты информации, информационная безопасность
(шифр и название специальности согласно учебному плану)

_____
(подпись магистранта)

Научный руководитель
Новиков Владимир Иванович
(фамилия, имя, отчество)
кондидат техн. наук, доцент
(ученая степень, ученое звание)

_____
(подпись научного руководителя)

Минск 2016

ВВЕДЕНИЕ

Благодаря бурному развитию сферы информационных технологий, в нашу жизнь вошли и стали уже привычными технологии, без которых современный мир уже и трудно себе представить. Одной из таких технологий, которая, которая совершает функции безопасности в сети, является электронная цифровая подпись (ЭЦП). Ее применение в качестве средства для идентификации и подтверждения юридической значимости документов становится стандартом цифрового мира.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для удостоверения источника данных и защиты данного электронного документа от подделки. Электронная цифровая подпись представляет собой последовательность символов, полученную в результате криптографического преобразования электронных данных. ЭЦП добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки. ЭЦП используется в качестве аналога собственноручной подписи.

Благодаря цифровым подписям, многие документы – паспорта, избирательные бюллетени, завещания, договора аренды – теперь могут существовать в электронной форме, а любая бумажная версия будет в этом случае только копией электронного оригинала.

С развитием мобильной связи открылась возможность развития технологий мобильной ЭЦП. Главным преимуществом таких технологий является простота использования и мобильность. Если раньше ЭЦП пользователя хранилась на компьютере, переносном устройстве, или была записана на удостоверении личности, то теперь ЭЦП пользователя помещается в его мобильное устройство, SIM-карту или смарт-карту. Мобильная ЭЦП позволяет получать электронные услуги и сервисы со своего мобильного устройства без непосредственного контакта с поставщиками, и при этом можно быть уверенным в конфиденциальности сделки и в том, что данный поставщик является подлинным.

Актуальность развития системы мобильной ЭЦП обусловлена широким использованием мобильной связи, развитием электронного документооборота и необходимости в эффективных средствах защиты информации.

Система мобильной ЭЦП может применяться в информационных системах Республики Беларусь, в которых необходимо использование криптографической защиты информации ограниченного распространения, кроме государственных секретов. Наиболее целесообразным является использование системы мобильной ЭЦП в банковских системах, системах мобильной связи в качестве SIM-карт.

Новизна разработанного устройства заключается в наличии реализации сертифицированных в Республике Беларусь криптографических алгоритмов, гибкости применения и высокой масштабируемости решения.

В данной диссертационной работе представлено исследование и разработка системы мобильной ЭЦП.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует главе Главе 4 «аппаратная и программная реализация системы мобильной ЭЦП» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 – 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Цель и задачи исследования

Цель диссертационной работы создание системы мобильной ЭЦП ограниченного распространения.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Проанализировать современные стандарты и методики в области в области анализа систем мобильной ЭЦП.
2. Разработать модуль криптографической защиты информации для систем мобильной ЭЦП.
3. Провести апробацию предложенной методики.

Личный вклад соискателя

Все основные результаты, выводы получены соискателем самостоятельно. Разработка модуля криптографической защиты информации для систем мобильной ЭЦП также разработана самостоятельно.

Апробация результатов диссертации

Основные положения и результаты диссертации обсуждались на 51-й научной конференции аспирантов, магистрантов и студентов (Минск 2015).

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 1 работа, в том числе 1 статьи в сборниках материалов конференций.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Первая глава «Введение в мобильную ЭЦП» состоит из двух основных частей.

В первой части «Мобильная ЭЦП» дается краткое объяснение мобильной ЭЦП и описываются основные качества службы мобильной ЭЦП, которая учувствует в процессе ее создания.

Вторая часть «Нормативная база» разделена на три раздела. В первом разделе «Уровень стандартизации и унификации» указываются основные стандарты алгоритмов, составов, структур и способов организации данных для выполнения криптографических преобразований компонентов системы мобильной ЭЦП. Во втором разделе «Описание стандартов смарт-карт» подробно описывается стандарты применимые для смарт-карт. В третье разделе «Оценка информационной безопасности смарт-карты» автор рассматривает стандарты для оценки информационной безопасности для смарт-карт.

Во **второй главе** «Система мобильной ЭЦП» автор описывает систему мобильной ЭЦП. Показана среда создания мобильной ЭЦП и показан алгоритм создания подписи. Так же сформулированы рекомендации для мобильной ЭЦП.

Третья глава «Требования к безопасности системы создания мобильно ЭЦП» поделена на 4 основных части в которых указаны основные функции безопасности, которые должны быть переданы для обеспечения безопасности объектов системы создания мобильной ЭЦП.

В первой части «Общие требования к безопасности MSCS» определены основные требования безопасности для компонентов системы создания мобильной подписи. Вторая часть «Общие требования безопасности MSCA» описывает основные требования безопасности для компонентов приложения создания мобильной подписи. В третьей части «Общие требования безопасности MSSP» автор описывает основные требования безопасности для провайдера услуг мобильной подписи. В четвертой части «Требования к безопасности для MSCD» указаны требования по безопасности для устройства создания мобильной подписи.

Четвертая глава «Аппаратная и программная реализация системы мобильной ЭЦП» разделена на 27 основных разделов.

В четвертой главе автор описывает состав разработанного устройства, его используемые интерфейсы, криптографические операции, рассмотрена общая характеристика устройства. Дается объяснение выбранной архитектуры микросхемы, технологии платформы разработки, обосновывается выбор платформы и технологии. Так же автор рассмотрел вопросы персонализации разрабатываемого устройства, управления ключами. Автором был произведен анализ угроз безопасности функционирования системы и Криптоанализ при

сбоях оборудования. Представлен принцип разработки приложений для систем мобильной ЭЦП, выбор средств разработки. Представлена работа устройства, описание работы программных приложений, набор задач, решаемый устройством. В конце главы автор сделал анализ результатов работы.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работы были проанализированы современные стандарты и методики в области в области анализа систем мобильной ЭЦП, и был разработан модуль криптографической защиты информации для систем мобильной ЭЦП.

Систем мобильной ЭЦП может быть применено для защиты объектов информатизации, обрабатывающих информацию ограниченного распространения.

Разработанный модуль криптографической защиты информации для систем мобильной ЭЦП выполняет криптографические операции шифрования, выработки и проверки ЭЦП, управления криптографическими ключами в соответствии со стандартами Республики Беларусь, с целью обеспечения конфиденциальности, подлинности и целостности информации ограниченного распространения. Также данный модуль предназначен для:

- персонифицированного средства аутентификации пользователя в информационных системах;
- защищенного хранилища критичных данных (личных криптографических ключей, прочих персональных данных, требующих защиту от несанкционированного доступа);
- средства генерации криптографических ключей;
- генератора случайных чисел.

Разработанный модуль обеспечивает конкурентоспособность в отношении аналогичных устройств Республики Беларусь, Украины, Казахстана, Узбекистана и Российской Федерации.

Из всего написанного ранее можно сделать вывод, что система мобильной ЭЦП — очень полезное нововведение в информационных системах Республики Беларусь, в которых необходимо использование криптографической защиты информации ограниченного распространения, обладающее следующими преимуществами:

- возможность защиты документов от несанкционированного чтения и изменения
- сокращение бумажного документооборота благодаря переводу части внутренних документов в электронный вид

– возможность определять юридический статус документа по электронной подписи (устанавливать авторство документа).