УДК 004.056.5(075.8)

ИСПОЛЬЗОВАНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Романова Марина Александровна, к.ф.-м.н., доцент
Полесский государственный университет
Romanova Marina, PhD
Polessky State University, kazubomarina@yandex.ru

Аннотация. В связи с развитием электронного документооборота возникает необходимость защиты электронных документов цифровыми инструментами. Один из таких инструментов – электронная цифровая подпись (ЭЦП). В статье рассмотрены варианты использования ЭЦП, а также перспективы её развития.

Ключевые слова: электронная цифровая подпись, защита электронных документов, электронный документооборот, хэш-функция.

Не секрет, что количество информации в мире растет по закону экспоненты: по данным википедии – оно удваивается каждые 18 месяцев, по другим источникам – каждые два года. Постоянный рост количества документов и как следствие, затрат, связанных с их обработкой и обслуживанием, является важнейшим фактором перехода к электронному документообороту. Беларусь не исключение, поэтому последнее десятилетие у нас в стране наблюдается активная замена бумажных документов их электронным аналогом. Вполне возможно в ближайшие десять-двадцать лет ожи-

дать полного вытеснения бумажного документооборота электронным. Однако использование незащищенных каналов связи, в том числе Internet и Ethernet, для электронных документов значительно повышает риск несанкционированных действий с важной информацией. Защитных атрибутов, присущих бумажным документам — подписей, печатей, водяных знаков, специальной фактуры бумажной поверхности и т.п. — у электронных документов нет. Поэтому возникает потребность использования такого инструмента электронной защиты, который смог наделить электронные документы всеми необходимыми защитными атрибутами. Один из таких инструментов – электронная цифровая подпись (ЭЦП).

ЭЦП — реквизит электронного документа, получаемый благодаря криптографическому преобразованию информации с использованием особого ключа. Этот реквизит прилагается к документу, чтобы установить аутентичность: ЭЦП является доказательством факта подписания и подтверждает, что подпись поставил именно владелец сертификата ключа подписи.

Таким образом, механизм цифровой подписи (digital signature) заключается в присоединении к электронному документу цифрового атрибута в виде определенным образом полученной последовательности символов, которая зависит от некоторых секретных атрибутов лица, подписавшего документ (закрытого ключа). Кроме того, электронная цифровая подпись зависит также от содержания подписываемого документа. Следовательно, разные документы, подписанные с помощью одного и того же закрытого ключа будут иметь разные ЭЦП. В этом одно из основных отличий ЭЦП от обычной подписи, поставленной от руки.

Законы об ЭЦП сегодня имеют более 60 государств [0]. Около 10 лет назад к ним присоединилась Республика Беларусь.

Основные понятия и механизм функционирования ЭЦП

Согласно Закону Республики Беларусь «Об электронном документе и электронной цифровой подписи» от 28 декабря 2009 г.:

ЭЦП – это последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности, а также для иных целей, предусмотренных настоящим Законом и иными законодательными актами Республики Беларусь [0].

Согласно теории построение и проверка цифровой подписи происходит на базе криптографии с открытым ключом. Механизм ЭЦП работает, используя два криптографических ключа — закрытый и открытый, которые генерирует автор (отправитель) сообщения.

Закрытый (секретный) ключ ЭЦП (Secret Key) — это секретная последовательность символов, предназначенная для выработки ЭЦП и известная только правомочному лицу — владельцу. Он использует этот ключ для создания своей подписи под документом.

Открытый (публичный) ключ ЭЦП (Public Key) — это общедоступная последовательность символов, предназначенная для проверки электронной подписи отправителя. Открытый ключ позволяет только про-

верять существующую ЭЦП, но не позволяет «расписаться» вместо отправителя.

Как правило, подписывается не сам файл, а его хэш-образ. Последний вычисляется с помощью элементов ключа и так называемой хэш-функции. Данная функция для каждого файла-документа возвращает последовательность символов определенной длины. И хотя хэш-образ документа имеет фиксированный размер, одинаковые хэш-образы у различных документов могут встретиться с вероятностью меньшей, чем вероятность совпадения отпечатков пальцев у людей. После этого полученный хэш-образ «подписывается» секретным (закрытым) ключом и ЭЦП документа, как результат описанного процесса, добавляется к его исходному файлу.

Оформленный таким образом документ и есть документ, подписанный ЭЦП.

По подписи получатель сообщения может удостовериться, что сообщение отправил именно автор, а не кто-то другой. Кроме того, подписанный таким образом документ уже нет смысла изменять, так как подделать новую подпись к измененному документу вычислительно сложно.

Проверка ЭЦП под электронным документом для установления его подлинности выполняется с помощью открытого ключа, парного закрытому, который может распространяться свободно и должен быть доступен любому участнику информационного обмена с владельцем закрытого ключа.

Если коды совпали — подпись верна, а документ подлинный. И если при создании ЭЦП действительно использовался секретный ключ того человека, который должен был подписать электронный документ, и при его пересылке содержимое документа не менялось преднамеренно или случайно (например, из-за помех в канале связи), то документ считается подлинным и является действительным.

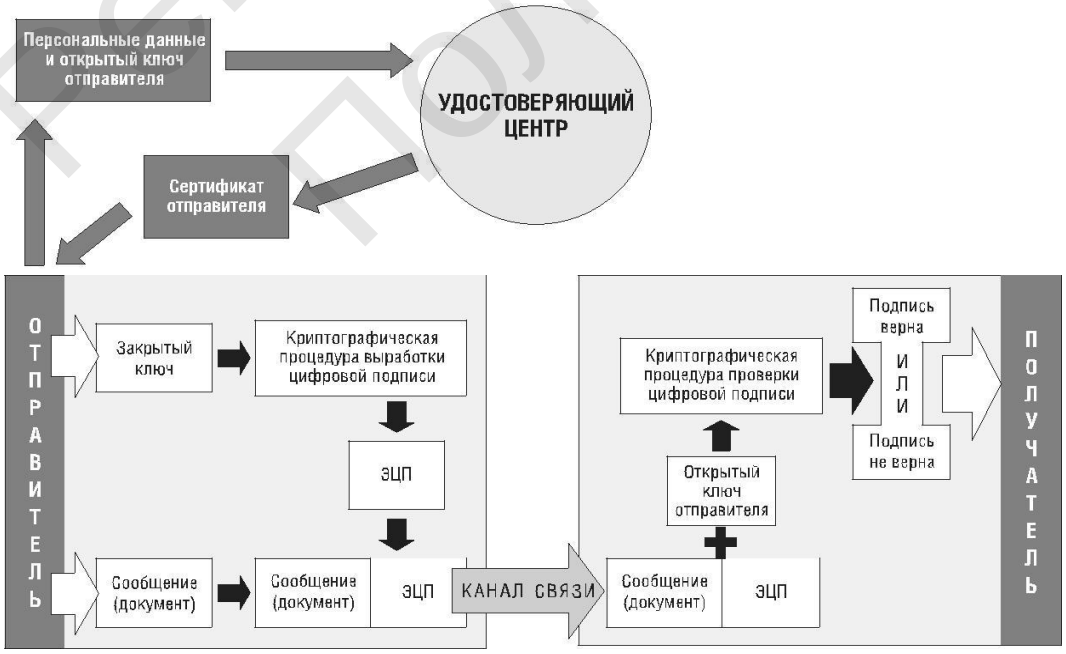

Рисунок – Схема работы системы ЭЦП

Все рутинные операции по генерации и проверке ЭЦП производятся автоматически специальными криптографическими средствами — системой ЭЦП, а пользователю остается только нажимать соответствующие экранные клавиши при помощи компьютерной мыши. Схема работы системы ЭЦП представлена на рисунке.

Выдачу ЭЦП осуществляют специальные удостоверяющие центры, отвечающие за управление криптографическими ключами пользователей. Для получения системы ЭЦП в нашей стране необходимо обратиться в специальное подразделение Национального центра электронных услуг, представительства которого имеются не только в столице, но и в областных и некоторых крупных белорусских городах, например, в Пинске.

Использование ЭЦП в Республике Беларусь

На сегодняшний день республиканский удостоверяющий центр ГосСУОК предлагает пользователям более 25 вариантов информационных систем, использующих сертификаты открытых ключей. Среди них система межведомственного электронного документооборота, автоматизированные информационные системы Министерства по налогам и сборам, информационная система электронного декларирования таможенных органов, информационная система электронной торговой площадки, информационная система государственных закупок, система дистанционного банковского обслуживания юридических лиц ОАО «БПС-Сбербанк», система Интернет-Банкинга ОАО «Белинвестбанк», сервис доставки электронных документов «mDoc» и другие. Сервис доставки электронных документов «mDoc» – это кроссбраузерное веб-решение, позволяющее взаимодействовать с абонентами системы межведомственного электронного документооборота государственных органов с использованием средств мобильной электронной цифровой подписи [2].

На сегодняшний день Национальный статистический комитет готов принять от предприятий и организаций более 85 различных форм централизованных государственных статистических наблюдений в электронном виде.

В сентябре 2018 года подписан Регламент использования электронной цифровой подписи врача в медицинских информационных системах для подписания электронных рецептов.

Перспективы использования ЭЦП в Республике Беларусь

Одним из перспективных направлений развития ЭЦП является выпуск и выдача гражданам республики ID-карт, с записанными на них электронными цифровыми подписями их владельцев. Такая ID-карта станет еще одним удостоверением личности и ею можно будет свободно пользоваться внутри страны, а паспорт понадобится только для поездок за границу.

ЭЦП широко используется во всем мире для получения различного вида услуг и заверения документов, не выходя из дома. Например, в Эстонии соответствующее законодательство действует с 2002 года, граждане этой страны старше 15 лет обязаны иметь ID-карту. Даже голосование на выборах происходит с использованием ID-паспортов — дистанционно, при

помощи специального считывающего устройства, которое подключается к компьютеру.

Поправками в действующее законодательство в Беларуси создаются условия для более широкого применения и использования ЭЦП и электронных документов. Количество выданных ключей электронной цифровой подписи постоянно увеличивается и составляет в стране более 260 тысяч[0].

Новым направлением использования ЭЦП будет являться ее применение для доступа к единому порталу электронных услуг и, как следствие, простой и эффективный способ получения государственных услуг и административных процедур в электронном виде.

Сегодня в Беларуси выстраиваются амбициозные планы по созданию передовой IT-страны, развитию цифровой экономики.

Список использованных источников

1. https://kodeksy-by.com/zakon_rb_ob_elektronnom_dokumente_i_elektronnoj_tsifrovoj_podpisi/1.htm

2. https://nces.by/service/mdoc/

3. https://www.belta.by/tech/view/ispolzovanie-elektronnoj-tsifrovoj-podpisi-rasshirjat-v-belarusi-v-2018-godu-280140-2017/

4. http://www.brandmanage.ru/flcs-108-5.html

5. Романова, М.А. Криптография и защита информации : уч.-мет. пос. / М.А.Романова. – Пинск : ПолесГУ, 2016. – 47 с.