УДК 656.2.08

ОСОБЕННОСТИ СИСТЕМЫ ПРИМЕНЕНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В ОРГАНИЗАЦИЯХ С ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СТРУКТУРОЙ

С.П. КАЛЮТЧИК

Белорусская железная дорога
Ленина, 17, Минск, 220030, Беларусь

Поступила в редакцию 17 июля 2008

Рассматриваются принципы развертывания и функционирования системы применения электронной цифровой подписи с учетом требований законодательных и нормативных актов Республики Беларусь в условиях крупной организации (корпорации), имеющей территориально распределенную структуру с централизованным управлением на примере Белорусской железной дороги. Описываются основы организационно-технических и технологических методов, позволяющих реализовать принцип юридической достоверности элементов системы применения электронной цифровой подписи в условиях специфики функционирования организации с территориально распределенной структурой.

Ключевые слова: электронная цифровая подпись, генерация ключа.

Введение

Республика Беларусь является одним из первых государств на постсоветском пространстве, которое успешно разработало законодательную и нормативную методическую базу для работы с электронной цифровой подписью (ЭЦП), являющейся, в соответствии с действующим законодательством, неотъемлемой частью электронного документа [1].

В этой связи можно констатировать рост числа информационных систем, в которых применяются средства электронной цифровой подписи. При этом все чаще ЭЦП, наряду с иными средствами информационной безопасности, рассматривается не как чистое средство защиты информации (криптозащита), а как элемент той или иной технологической системы [2].

Вместе с тем, при внедрении средств ЭЦП в уже имеющиеся организационные, технические и технологические процессы, существует риск недостаточного учета всех необходимых организационно-правовых элементов системы применения электронной цифровой подписи, что в случае возникновения коллизии может свести на нет смысл использования ЭЦП по ее прямому назначению.

Как зарубежный, так и отечественный опыт применения средств криптозащиты показывает, что с практической точки зрения значимость имеет не столько сама ЭЦП, сколько система применения ЭЦП, включающая в себя комплекс технических, технологических и организационно-правовых объектов, в совокупности образующих средство создания, передачи, применения и хранения электронных документов или иных информационных массивов (сообщений), получивших посредством ЭЦП юридически значимый статус.

Система применения ЭЦП в территориально распределенной системе. Ключевые элементы. Особенности

Рассмотрим ключевые аспекты формирования элементов ведомственной (корпоративной) системы применения ЭЦП. Действующей нормативной и правовой базой [1] определены понятия основных элементов системы применения ЭЦП: личный (закрытый) ключ подписи, открытый (публичный) ключ проверки подписи, удостоверяющий и регистрационный центры, средства электронной цифровой подписи. Субъектами, критичными для организационно-правовой структуры системы применения ЭЦП, являются: владелец личного и открытого ключа проверки подписи; пользователь личного и открытого ключа проверки подписи.

Руководящий документ Республики Беларусь "Банковские технологии. Технология электронной цифровой подписи. Термины и определения" определяет владельца личного ключа подписи как конкретное физическое или юридическое лицо, осуществившее выработку этого ключа и соответствующего ему открытого ключа проверки подписи путем применения средств ЭЦП, а также осуществляющее его хранение и использование. Наряду с этим указанный нормативный акт обязывает владельца личного ключа подписи в своих интересах хранить личный ключ в тайне и обеспечивать его защиту от случайного уничтожения или модификации [3].

Соответственно, владельцем открытого ключа проверки подписи является физическое или юридическое лицо, являющееся владельцем личного ключа подписи, соответствующего данному открытому ключу проверки подписи [4], а пользователем открытого ключа проверки подписи — лицо, которому владельцем личного ключа подписи, уполномоченным им лицом или удостоверяющим центром предоставлена карточка или сертификат открытого ключа проверки подписи для проверки ЭЦП [5].

Мировая практика использования электронной цифровой подписи предполагает, что в качестве пользователя и владельца личного ключа выступает физическое лицо, применяющее ЭЦП в своих интересах. В таком случае физическое лицо, являющееся владельцем личного ключа, обладает правом собственности на него со всеми вытекающими последствиями. В варианте же ведомственной системы применения ЭЦП владельцем личного ключа подписи будет являться организация (юридическое лицо). Конкретный работник этой организации будет уполномочен соответствующим руководителем единолично использовать личный ключ электронной цифровой подписи для исполнения возложенных на него должностных (служебных) обязанностей. Правом собственности на личный ключ подписи будет обладать организация, в которой работает владелец личного ключа, так как он предоставлен конкретному работнику исключительно в ведомственных интересах. Конкретный работник в данном случае является не владельцем, а пользователем личного ключа.

В соответствии со ст. 13 Закона Республики Беларусь "Об электронном документе" владелец личного ключа осуществляет выработку этого ключа и соответствующего ему открытого ключа проверки подписи путем применения средств ЭЦП. И, если в случае владельца личного ключа — физического лица чаще всего применяется метод личной генерации ключей владельцем (рис. 1), то в варианте владельца личного ключа — юридического лица (организации, имеющей территориально распределенную структуру) такой подход нецелесообразен либо невозможен по ряду причин.

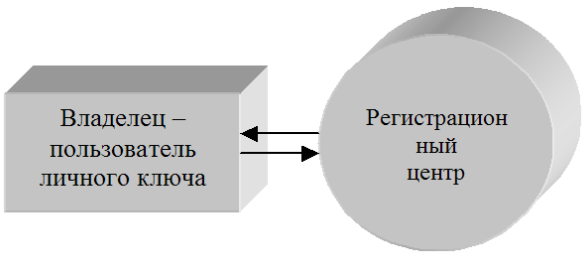

Рис. 1. Генерация ключа в варианте владелец-пользователь — физическое лицо

Одно из основных требований, предъявляемых к осуществлению процессов генерации и управления ключами — минимизация рисков информационной безопасности, в том числе внесения умышленных и неумышленных технологических ошибок, предоставления доступа третьим лицам к носителям закрытого ключа, служебным сведениям и т.п.

С этой точки зрения оптимальным является вариант централизованной генерации ключей, как обеспечивающий наибольшую степень контроля за критичными процессами и соблюдением соответствующих положений корпоративной политики информационной безопасности. При этом непосредственная генерация личных ключей осуществляется не персонифицированным программным средством ЭЦП, устанавливающимся на личном рабочем месте, а оборудованием регистрационного центра.

Очевидно, что в варианте корпоративной системы применения ЭЦП существование единого центра генерации (регистрационного центра) создает условия максимально полной реализации мер безопасности и контроля за ними, увеличивая степень надежности ЭЦП как таковой и всей системы применения ЭЦП в целом, что, в свою очередь, формирует ряд специфических условий.

Так, в варианте владелец-пользователь личного ключа, при личной генерации ключей владельцем в регистрационном центре практикуется механизм технологических связей, указанный на рис. 2.

Генерация ключей осуществляется регистрационным центром. Задача передачи адресату сертификата открытого ключа (вместе со значением открытого ключа) отправителя, а также верификации его владельца осуществляется удостоверяющим центром.

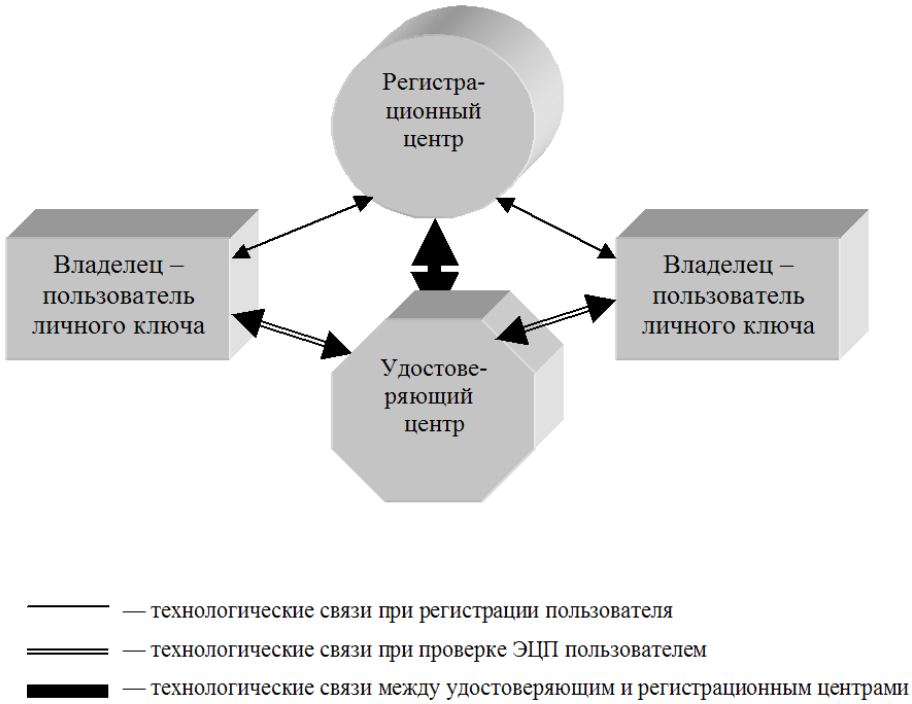

Рис. 2. Технологические связи системы применения ЭЦП
в варианте владелец-пользователь личного ключа

В варианте организации со сложной территориально распределенной структурой наличие единого элемента системы, осуществляющего генерацию ключей (головного регистрационного центра), также является оптимальным.

С учетом территориально распределенной структуры, для качественного процесса проверки ЭЦП (поступления на персонифицированные средства ЭЦП адресата открытого ключа отправителя письма) аутентификация отправителя с помощью сертификата и (или) передача адресату открытого ключа отправителя осуществляется аппаратно-программными средствами подчиненных регистрационных центров (рис. 3).

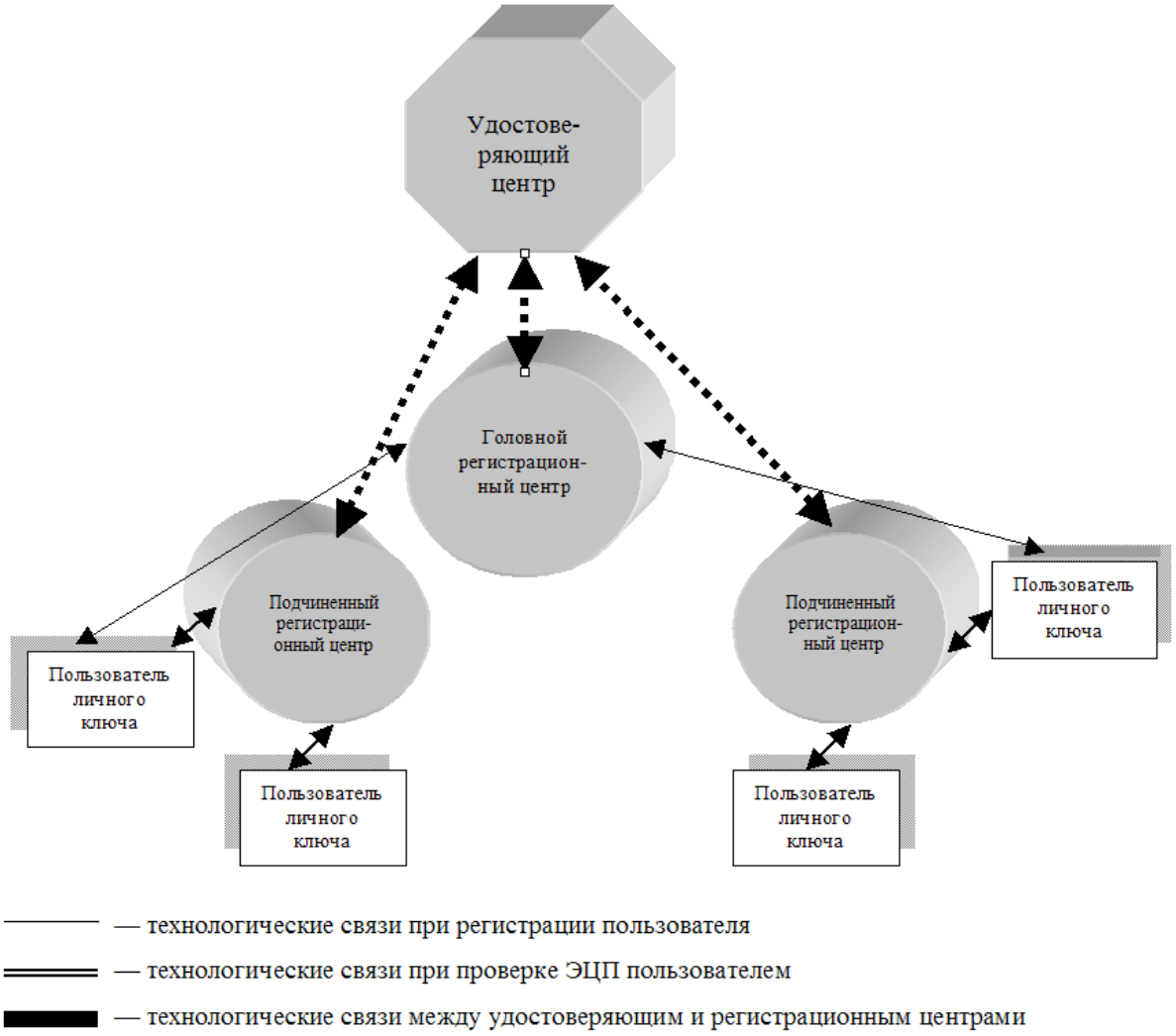

Рис. 3. Технологические связи системы применения ЭЦП в территориально распределенной структуре

Понятие подчиненного регистрационного центра не введено в действующих нормативах по созданию и функционированию систем применения ЭЦП в силу того, что в отечественной практике нет прецедентов развертывания подобных систем широкого применения в крупных организациях с территориально распределенной структурой, предполагающих организационно-техническую централизацию. Вместе с тем, практика разработки указанного вопроса на железнодорожном транспорте Республики Беларусь свидетельствует, что объединение принципов централизованной генерации ключей и управления сертификатами с вынесением в зоны сосредоточения абонентов функций, направленных на повышение оперативности проверки ЭЦП (не связанных с лицензируемой деятельностью, т.е. правами и полномочиями удостоверяющего центра) позволит добиться наилучших практических результатов использования возможностей применения ЭЦП. Это справедливо в условиях:

– организационно-технической централизации системы применения ЭЦП;

– территориально распределенной структуры организации, эксплуатирующей систему применения ЭЦП;

– отсутствия, либо недостатка качественных телекоммуникационных систем во всех регионах, охваченных системой применения ЭЦП.

Реализация вышеуказанной схемы требует проведения дополнительных программно-технических, технологических и организационных доработок регистрационного центра, так как изначально передача персонифицированным средствам ЭЦП адресата открытого ключа отправителя письма в функции регистрационного центра не входит. При этом должны быть

учтены некоторые принципиальные моменты, связанные с обеспечением правового качества системы, такие как необходимость немедленной генерации удостоверяющим центром списка отозванных сертификатов при любом изменении реестра сертификатов, автоматически, в "принудительном" порядке, в режиме реального времени рассылающегося подчиненным регистрационным центрам с квитированием. Кроме того, наличие единого центра генерации ключей (головного регистрационного центра) наряду с территориально распределенной структурой обуславливает сложность регистрации пользователей системы применения ЭЦП и, соответственно, генерации ключей.

При решении этой проблемы необходимо учитывать следующие аспекты:

– пользователь личного ключа не является его владельцем;

– владельцем личного ключа является организация, в которой работает пользователь;

– право пользования личным ключом работнику делегировано для выполнения служебных обязанностей;

– пользователь личного ключа несет персональную ответственность за выполнение своих служебных обязанностей, в том числе связанных с хранением и использованием личного ключа.

С учетом изложенного на первый взгляд допустимым представляется создание системы, при которой работнику организации — пользователю личного ключа выдается заранее сгенерированный и записанный на носитель личный ключ, т.е. процесс генерации происходит по схеме, представленной на рис. 4, где свойства, правила и принципы функционирования среды передачи определяются организацией — владельцем личного ключа.

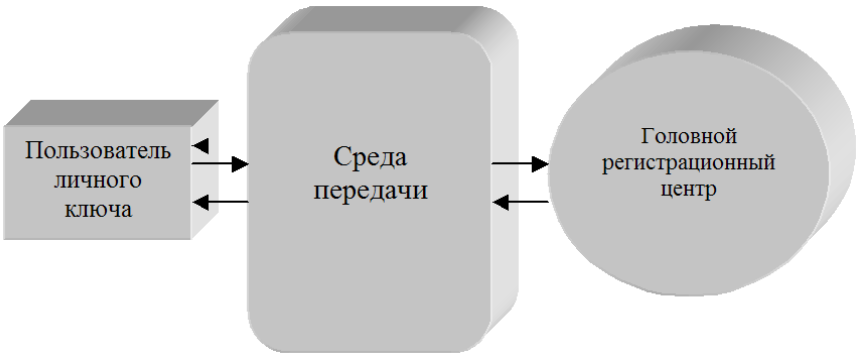

Рис. 4. Генерация ключа в варианте владелец — организация, пользователь — ее работник

Однако данная схема содержит серьезный недостаток, связанный со следующей коллизией: организация-владелец ключа требует от работника гарантий обеспечения безопасности личного ключа и его носителя, при этом передавая полномочия по генерации ключа и транспортировке его носителя третьему лицу. Это обстоятельство, в случае возникновения нештатной ситуации с документом, подписанным ЭЦП, может серьезно усложнить претензионные процедуры, проводимые заинтересованными сторонами, а при определенных обстоятельствах сделать невозможным однозначное заключение о юридической, организационной и иной достоверности ЭЦП.

Для решения этой проблемы при создании системы применения ЭЦП в организации с территориально распределенной структурой необходимо:

– минимизировать и нормативно определить круг лиц, которым организацией-владельцем личного ключа предоставлено право генерации ключей в головном регистрационном центре;

– обеспечить механизм транспортировки носителя личного ключа из головного регистрационного центра до пользователя ключа, предполагающий максимально возможную степень надежности, с достоверной фиксацией всех этапов транспортировки;

– разработать и в нормативно установленном порядке ввести в действие подробный регламент генерации ключа, транспортировки носителя ключа, его использования, решения возникающих процедурных вопросов и т.д.;

– предусмотреть схему претензионной работы по вопросам, связанным с использованием ЭЦП, учитывающей особенности функционирования конкретного юридического лица с территориально распределенной структурой.

Заключение

Результаты работ, ведущихся в данной области на Белорусской железной дороге, являющейся территориально распределенной структурой, показывают, что реализация изложенных в статье принципов создает основу для создания и успешного функционирования системы применения ЭЦП в самых различных задачах — от простого разового обмена электронными документами до сложных систем документооборота и использования криптографической защиты информации в форме применения электронной цифровой подписи в критических производственных процессах.

FEATURES OF SYSTEM APPLICATION OF THE DIGITAL SIGNATURE IN THE ORGANIZATIONS, WHICH HAVE TERRITORIALLY ALLOCATED STRUCTURE

S.P. KALIUTCHYK

Abstract

Principles of expansion and functioning of system the digital signature that take into account requirements of the legislation of Belarus in conditions of corporation which has territorially allocated structure with the central management by the example of the Belarus railway are considered. The organizational, technical and technological methods are described, allowing realizing a principle of legal reliability of system the digital signature in the organization, which has territorially allocated structure.

Литература

1. Закон Республики Беларусь "Об электронном документе", от 10.01.2000 года, статья 7.
2. *Калютчик С.П.* // Вестн. БелГУТ. Наука и транспорт. 2006. № 1–2.
3. "Банковские технологии. Технология электронной цифровой подписи. Термины и определения". РД РБ 07040. 2004. п. 5.2.
4. "Банковские технологии. Технология электронной цифровой подписи. Термины и определения". РД РБ 07040. 2004. п. 5.4.
5. "Банковские технологии. Технология электронной цифровой подписи. Термины и определения", РД РБ 07040. 2004. п. 5.5.