

УДК 681.324.067

А.С. Поляков, В.Е. Самсонов

## ПРОБЛЕМЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ В БЕЛАРУСИ

*Рассмотрены вопросы применения на практике электронных документов и электронной цифровой подписи, отмечены недостатки существующих правовых актов, препятствующих их широкому внедрению.*

### Введение

Применение электронных документов (ЭД) и электронной цифровой подписи (ЭЦП) регламентируется законами и стандартами Республики Беларусь [1–5]. Однако многие вопросы применения ЭД и ЭЦП остаются нерешёнными, что фактически сдерживает практическое использование ЭД и ЭЦП.

В данной статье анализируются положения Закона об электронном документе (в дальнейшем – Закон) [4], в которых, по нашему мнению, имеются некоторые недоработки, затрудняющие практическое применение ЭД.

### 1. Анализ общих положений Закона об электронном документе

В ст. 2 Закона указано, что «электронный документ может использоваться во всех сферах деятельности, где применяются программные и технические средства, необходимые для создания, обработки, хранения, передачи и приёма информации. С помощью электронных документов могут совершаться сделки (заключаться договоры), производиться расчеты, осуществляться переписка и передача документов и иной информации». В ст. 11 это положение ещё более усиливается: «электронный документ на машинном носителе приравнивается к документу на бумажном носителе и имеет одинаковую с ним юридическую силу».

К сожалению, несмотря на закреплённую в ст. 11 Закона юридическую значимость ЭД, его статус реально не поддерживается статьями, касающимися применения ЭД и ЭЦП. Отметим лишь некоторые из таких положений.

В ст. 9 вводится понятие «оригинал электронного документа» и указано, что «все экземпляры электронного документа, зафиксированные на машинном носителе и идентичные один другому, являются оригиналами и имеют одинаковую юридическую силу». Это положение противоречит устоявшемуся определению «оригинал» (начальный, подлинный). Поэтому непонятно, каким образом может существовать произвольное количество «оригиналов», если оригинал, по определению, должен быть в единственном числе. К тому же в Законе не указано, кто и каким образом устанавливает идентичность экземпляров ЭД и каким образом определяется тот факт, что данный экземпляр является оригиналом ЭД. В связи с отсутствием этих правил у пользователей не может быть уверенности в том, что полученный ими экземпляр ЭД является оригиналом этого документа.

Поскольку согласно Закону все оригиналы ЭД имеют одинаковую юридическую силу, то это положение Закона предоставляет возможность для различных махинаций, в том числе незаконного получения денег. Например, можно предъявлять к оплате любое количество созданных оригиналов электронного платёжного поручения и каждое из них должно быть оплачено, поскольку является оригиналом ЭД и имеет юридическую силу.

Проблемы, связанные с некорректным использованием понятий «оригинал», «подлинник», «копия», существуют и в законодательствах других стран СНГ. Подробно они рассмотрены в работе [6].

Нигде не оговорены правовые вопросы применения ЭД, например, в случае проведения проверок контролирующими органами, в процессе которых могут производиться арест, изъятие

документов и т. д. Не учтены и другие вопросы, связанные с рассмотрением ЭД в судебных и правоохранительных органах. Непонятно, например, каким образом можно найти, арестовать или изъять все никем не учтённые экземпляры ЭД, разосланные в неизвестном количестве и в неизвестные адреса, каждый из которых, в соответствии с Законом, является оригиналом ЭД и имеет одинаковую с ним юридическую силу.

В Законе не предусмотрены требования к качеству личного ключа ЭЦП. Сказано лишь (ст. 12), что выработка личного ключа осуществляется владельцем личного ключа. Следствием такого положения может быть ситуация, когда пользователи будут выработать «слабые» криптографические ключи, что создаст возможность их лёгкой раскрываемости, а это вызовет, естественно, недоверие пользователей к применяемым ЭЦП и практическую невозможность их использования в ЭД.

Основным элементом ЭД, с помощью которого производится проверка его подлинности и целостности, является ЭЦП, входящая в «особенную часть ЭД» (ст. 7). Подтверждение подлинности и целостности ЭД производится путём применения средств ЭЦП с использованием открытых ключей проверки подписей (ст. 12). Таким образом, именно открытый ключ проверки подписи является главным информационным элементом при проверке подлинности и целостности ЭД, в связи с чем процедуры его создания, хранения, передачи и использования должны обеспечивать абсолютную надёжность применения. К сожалению, предусмотренные в Законе положения не обеспечивают гарантированного выполнения этих требований, следовательно, не обеспечивают полноценного подтверждения статуса ЭД как юридического документа.

## 2. Анализ вопросов практического применения электронного документа

Открытый ключ проверки подписи, вырабатываемый на базе личного ключа подписи, распространяется в соответствии со ст. 15 «владельцем личного ключа подписи для пользования всем заинтересованным лицам» в виде карточки открытого ключа проверки подписи (КОКПП), подлинность которой удостоверяется (ст. 14) путём постановки этим лицом подписи (как вариант подписи и печати) на КОКПП. Учитывая, что основная часть пользователей сети, которые будут использовать в своей работе ЭЦП, не имеют оформленных и зарегистрированных в установленном порядке личных печатей, в случае возникновения каких-либо споров или конфликтных ситуаций, связанных с применением ЭЦП, юридическое разрешение этих споров на основе КОКПП, удостоверенных лишь подписью рядового пользователя сети, естественно, будет невозможным в силу недостаточной юридической силы такой подписи. Следовательно, и юридическая сила ЭД в таком случае будет утрачена.

Открытый ключ проверки подписи в соответствии со ст. 15 должен распространяться для пользования всем заинтересованным лицам в виде КОКПП. Как определить круг заинтересованных лиц? Фактически любой из абонентов сети в какой-то момент времени может оказаться заинтересованным лицом.

Распространение КОКПП среди заинтересованных лиц производится (ст. 15) владельцем личного ключа или «уполномоченным им лицом». Каким образом оформляется «уполномочивание», в Законе не сказано. Логично предположить, по аналогии с КОКПП, что имеется в виду подпись владельца личного ключа под каким-то созданным им самим бумажным документом, в котором будут делегироваться права на распространение открытого ключа проверки подписи некоторому физическому лицу. Естественно, что такого уровня юридические гарантии для пользователей сети недостаточны и поэтому доверие к полученной КОКПП будет небольшим.

В Законе не определяются ни содержание и структура КОКПП, ни содержание и структура особенной части ЭД (ст. 7). Эти вопросы, в соответствии со ст. 14, решаются «собственником информационных систем и сетей». Естественно, что в каждой сети будут выбраны свои содержание и структура указанных объектов. Следовательно, понимания ЭД, созданных в полном соответствии с законами Республики Беларусь в разных информационных сетях, за пределами этих сетей не будет. Таким образом, вопрос всеобщего применения ЭД на территории Республики Беларусь остаётся нерешённым.

В ст. 1 Закона содержание КОКПП ограничено лишь значением открытого ключа проверки подписи. На самом деле, в соответствии с [3], КОКПП должна содержать гораздо больше

информации: полные данные о владельце личного ключа подписи (его сетевой идентификатор, фамилию, имя, отчество, официальное название организации, должность абонента, телефоны и т. п.), значения параметров  $p$ ,  $q$ ,  $a$ ,  $l$ ,  $g$  и т. д.

Согласно ст. 14 пользователь обязан «обеспечить идентичность используемого им открытого ключа проверки подписи тому ключу, который зафиксирован в карточке открытого ключа проверки подписи». Для выполнения этого требования пользователю необходимо знать, с помощью какого открытого ключа он должен проверять значение ЭЦП под полученным ЭД. Фактически это означает следующее: вместе с ЭД в его особенной части должно передаваться всё содержание КОКПП, чтобы получатель ЭД при выполнении процедуры проверки ЭЦП имел возможность убедиться в том, что значение КОКПП, полученной в виде бумажного документа непосредственно от владельца этой карточки, совпадает со значением КОКПП, которую он получил вместе с ЭД. Поскольку объём проверяемых данных достаточно велик, каждый пользователь для облегчения и ускорения своей работы будет вынужден создавать электронный вариант КОКПП и соответствующую программу, которая позволит ему производить сверку идентичности используемого им в данный момент открытого ключа проверки подписи с тем ключом, который зафиксирован в КОКПП. Обеспечение подлинности и целостности создаваемых при этом электронных вариантов открытых ключей никем и никак не гарантировано.

Практическое применение ЭЦП с использованием предусмотренной в Законе КОКПП может оказаться затруднённым также по следующим причинам.

1. Существуют проблемы с подготовкой бумажного документа (КОКПП), подписанием его у руководителя организации, постановкой на этом документе гербовой печати и рассылкой всем предполагаемым пользователям (которые заранее могут быть неизвестны). В отношении КОКПП в ст. 14 Закона предусмотрена следующая норма: «принадлежность открытого ключа проверки подписи владельцу личного ключа подписи удостоверяется путём постановки подписи (подписи и печати) на карточке открытого ключа проверки подписи». Требование о создании КОКПП практически означает необходимость подготовки соответствующих бумажных документов для каждого из предполагаемых абонентов, подписания этих карточек у руководителя организации, постановки гербовой печати на подпись руководителя организации и рассылки удостоверенных таким образом КОКПП всем предполагаемым абонентам.

Естественно, что такая процедура, в силу отмеченных выше ограничений, не может быть удобной и приемлемой в практической работе. Поэтому в случае её принудительного навязывания, как показывает опыт применения неудобных в организационном отношении правил, бланки с подписью руководителя и соответствующей печатью будут лежать у сотрудников как обычный рабочий материал. Таким образом, исчезает гарантия выполнения функции удостоверения открытых ключей проверки ЭЦП.

2. Для обеспечения взаимодействия с предполагаемыми абонентами каждый пользователь системы, имеющий право производства ЭЦП, будет вынужден организовывать у себя и постоянно поддерживать базу данных своих абонентов. Учитывая достаточно высокую трудоёмкость этого процесса, легко предположить, что корректное ведение базы данных для пользователей, работающих с большим числом абонентов, окажется непосильной задачей, поэтому на практике это будет означать, что обмен ЭД, сопровождаемыми ЭЦП, будет производиться в известной степени бесконтрольно.

Проблемы, аналогичные рассмотренным выше, существуют практически во всех странах СНГ, в которых производится внедрение ЭД, приняты некоторые законы и разрабатываются новые в сфере электронного взаимодействия [7–10].

## **Заключение**

На основании проведенного анализа можно сделать следующие выводы.

1. Обмен ЭД, созданными в соответствии с Законом, но в разных информационных и вычислительных сетях, будет невозможен в связи с различными содержанием и структурой КОКПП, а также самого ЭД и его особенной части.

2. Применение ЭД, возможно только внутри отдельно взятой корпоративной сети, в которой установлены собственные правила изготовления личных ключей подписи, открытых ключей проверки подписи, передачи и использования открытых ключей проверки подписи.

Как отмечалось в [11, 12], в Республике Беларусь разрабатываются и сертифицируются средства ЭЦП, разрабатываются проекты нормативных документов, готовится внедрение ЭД в ряде министерств и ведомств. Естественно, в каждом из этих министерств и ведомств должны быть разработаны собственные ведомственные руководящие материалы, определяющие и конкретизирующие вопросы применения ЭД и ЭЦП.

3. Для полноценного применения ЭД требуются внесение соответствующих изменений и дополнений в Закон об электронном документе, разработка дополнительных нормативных материалов, однозначно определяющих все вопросы, связанные с использованием ЭД и ЭЦП.

### Список литературы

1. Закон Республики Беларусь «Об информатизации» от 06.09.1995 г. № 3850-ХП.
2. СТБ 1176.1-99. Информационная технология. Защита информации. Функция хэширования.
3. СТБ 1176.2-99. Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи.
4. Закон Республики Беларусь «Об электронном документе» от 10.01.2000 г. № 357-3.
5. СТБ 1121-2000. Документы электронные. Правила выполнения, обращения и хранения.
6. Гадасин В.А., Конявский В.А. От документа к электронному документу. Системные основы. – М.: РФК-Имидж Лаб., 2001. – 192 с.
7. Ткачев А.В. Законодательное регулирование правового статуса ЭЦП // Защита информации. Конфидент. – № 1(43). – 2003. – С. 18–22.
8. Волчков А.А. Закон «Об электронной подписи» – за и против // Защита информации. Конфидент. – № 3(45). – 2003. – С. 19–25.
9. Соловьяненко Н.И. Федеральный закон «Об ЭЦП»: проблемы применения и юридические риски // Защита информации. Конфидент. – № 3(45). – 2003. – С. 26–29.
10. Дутов М.М. Сравнительный анализ европейского законодательства в области электронного документооборота // Предпринимательство, государство и право. – 2002. – № 8. – С. 25–28.
11. Полевиков Э. Проблемы внедрения электронных документов в Беларуси // Тез. докл. VII Междунар. конф. «Комплексная защита информации» (25–28 февраля 2003 г., Раубичи). – Мн.: ОИПИ НАН Беларуси. – 2003. – С. 147, 148.
12. Рыбкин Ю.Е., Коледа В.В., Резников Г.К. Сертификация программных средств защиты от воздействия вредоносных программ // Там же. – С. 82–83.

Поступила 15.11.04

*Объединенный институт проблем  
информатики НАН Беларуси  
Минск, Сурганова, 6  
e-mail: sveby@mail.ru*

**A. S. Poljakov, V. E. Samsonov**

### THE PROBLEMS OF PRACTICAL APPLICATION IN BELARUS OF ELECTRONIC DOCUMENTS AND ELECTRONIC DIGITAL SIGNATURE

The questions of electronic documents and digital signature use were examined. Some weakness of current legislation, which make the obstacles for widespread application of electronic documents are discussed.