П О С Т А Н О В Л Е Н И Е

Парламентской Ассамблеи
Организации Договора о коллективной безопасности

О Рекомендациях по гармонизации законодательства государств – членов ОДКБ о цифровых подписях в целях обеспечения информационной безопасности

Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:

1. Принять Рекомендации по гармонизации законодательства государств – членов ОДКБ о цифровых подписях в целях обеспечения информационной безопасности (далее – Рекомендации) (прилагаются).

2. Направить Рекомендации в парламенты государств – членов ОДКБ для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.

3. Опубликовать текст Рекомендаций на официальном сайте и в материалах Парламентской Ассамблеи ОДКБ.

Председатель
Парламентской Ассамблеи ОДКБ **В.В.ВОЛОДИН**

Москва
9 декабря 2024 года
№ 17-7.1

Приложение
к постановлению ПА ОДКБ
от 9 декабря 2024 года № 17-7.1

РЕКОМЕНДАЦИИ
по гармонизации законодательства государств – членов ОДКБ о цифровых подписях в целях обеспечения информационной безопасности

Современный этап развития всех сфер человеческой деятельности характеризуется активнейшим проникновением цифровых технологий во все области государственной жизни, экономики и личной жизни граждан. Данная тенденция с течением времени будет только нарастать, и законодательство должно адекватным образом отвечать на потребности социума.

Одной из существенных проблем в информационной сфере, которую к настоящему времени удалось частично решить, является обеспечение обмена юридически значимыми документами в электронной форме отображения с определенной гарантией обеспечения неизменности их содержания. Эту задачу решил правовой институт цифровых (электронно-цифровых, электронных) подписей, сформированный после появления соответствующих математических алгоритмов и компьютерных программ их реализации. Как правило, регулирование данных отношений осуществляется на уровне национальных законов, большинство из которых принято после появления Типового закона ЮНСИТРАЛ[1] об электронных подписях (Вена, 5 июля 2001 года). Общая направленность принятых законов заключается в легитимации цифровых подписей преимущественно для целей осуществления предпринимательской деятельности.

Практика применения технологии цифровых подписей в государствах – членах ОДКБ показывает, что наибольшее развитие защищенный таким образом электронный документооборот получил прежде всего в публичной сфере, то есть в деятельности органов государственной власти и органов местного самоуправления.

Из этого вытекает необходимость более углубленного правового регулирования отношений по организации обмена между уполномоченными субъектами государственно значимой информацией в электронной форме отображения, достоверность которой подтверждается цифровыми подписями.

Помимо сказанного, в рамках межгосударственного взаимодействия имеется постоянно возрастающая потребность в обмене государственно значимой информацией в электронной форме отображения на разных уровнях, что существенным образом влияет на оперативность информационного обмена и скорость принятия соответствующих решений. Очевидным также является позитивное влияние расширения обмена сведениями в такой форме

---

[1] Комиссия ООН по праву международной торговли.

отображения между органами военного управления государств – членов ОДКБ.

Цель настоящих Рекомендаций – разработка правовых ориентиров в совершенствовании национального законодательства государств – членов ОДКБ, регулирующего отношения в области использования цифровых подписей для целей государственного управления и обмена государственно значимой информацией между органами государственной власти и органами военного управления государств – членов ОДКБ.

1. Система правового регулирования использования цифровых подписей в государствах – членах ОДКБ

В Республике Армения основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Закон Республики Армения от 15 января 2005 года № ЗР-40 «Об электронном документе и электронной цифровой подписи».

В Республике Беларусь основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Закон Республики Беларусь от 28 декабря 2009 года № 113-З «Об электронном документе и электронной цифровой подписи».

Помимо данного законодательного акта, интерес представляет также приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 года № 118 «Об утверждении Положения о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь».

В Республике Казахстан основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Закон Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи».

Помимо данного законодательного акта, интерес представляет приказ и. о. Министра по инвестициям и развитию Республики Казахстан от 26 июня 2015 года № 727 «Об утверждении Правил выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи корневым удостоверяющим центром государственных органов и национальным удостоверяющим центром Республики Казахстан».

В Кыргызской Республике основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Закон Кыргызской Республики от 19 июля 2017 года № 128 «Об электронной подписи».

Помимо данного законодательного акта, интерес представляет также постановление Правления Национального банка Кыргызской Республики от 15 июня 2016 года № 25/6 «Об утверждении Положения “О деятельности

Национального банка Кыргызской Республики в качестве удостоверяющего центра открытых ключей электронной цифровой подписи”».

В Российской Федерации основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Помимо данного законодательного акта, интерес представляет прекративший свое действие Федеральный закон от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи».

В Республике Таджикистан основным законодательным актом, регулирующим отношения в сфере использования цифровых подписей, является Закон Республики Таджикистан от 15 марта 2023 года № 1965 «Об электронном документе и электронной подписи».

2. Анализ дефинитивного аппарата

Гармонизация дефинитивного (понятийного) аппарата является важной научной и практической задачей, так как позволяет сблизить содержание определенных групп юридически значимых понятий, используемых в национальном законодательстве, что облегчает уяснение юридических норм субъектами правоприменения в других государствах, а также способствует более быстрому достижению консенсуса при заключении международных договоров и межправительственных соглашений.

1. Понятие «цифровая подпись».

Профильный законодательный акт Республики Армения определяет рассматриваемое понятие следующим образом: «электронная цифровая подпись – полученная посредством криптографического преобразования информации и представленная в электронно-цифровой форме уникальная последовательность символов для создания данных электронной цифровой подписи и данного электронного документа, которая приобщена к электронным документам либо логически связана с ними и используется для идентификации подписывающего лица, а также для защиты электронного документа от подделок и искажений».

Профильный законодательный акт Республики Беларусь определяет рассматриваемое понятие следующим образом: «электронная цифровая подпись – 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».

Профильный законодательный акт Республики Казахстан определяет рассматриваемое понятие следующим образом: «электронная цифровая подпись – набор электронных цифровых символов, созданный средствами

цифровой подписи и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания».

Профильный законодательный акт Кыргызской Республики определяет рассматриваемое понятие следующим образом: «электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме и (или) логически связана с ней и которая используется для определения лица, от имени которого подписана информация».

Профильный законодательный акт Российской Федерации определяет рассматриваемое понятие следующим образом: «электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию».

Профильный законодательный акт Республики Таджикистан определяет рассматриваемое понятие следующим образом: «защищенная электронная подпись (электронная цифровая подпись) – реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи, позволяющий идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе и направленный на защиту электронного документа от несанкционированного исправления».

Анализ приведенных определений показывает, что в них присутствуют сходные черты, однако имеются и существенные различия.

Для более углубленного понимания кратко обратимся к теории данного вопроса. В течение многих веков собственноручная подпись уполномоченного лица, проставленная на бумажном документе, придавала ему должную юридическую силу на основании того, что данное уполномоченное лицо фактом проставления собственноручной подписи подтверждало свое согласие с текстом документа. Бумага или иной сходный носитель информации сами по себе обеспечивали защиту зафиксированной на них информации от подделки. Воспроизводство собственноручной подписи одного лица другим лицом при определенном уровне развития графологии сравнительно легко определялось как подделка.

Обратим также внимание на тот факт, что процедура проставления собственноручной подписи никоим образом не может быть отделена от конкретного физического лица.

С появлением компьютерных технологий подготовки документов и развитием безбумажного обмена документированной информацией все вышеуказанные очевидные преимущества документа на бумажном носителе исчезли, что вызвало необходимость разработки новых методов подтверждения факта волеизъявления уполномоченного субъекта в виде проставления его подписи в документе и подтверждения факта отсутствия каких-либо изменений в направленном документе.

Таких способов довольно много, однако подавляющее большинство из них не могло решить основную юридическую задачу однозначной «привязки» нового вида подтверждения к конкретному физическому лицу, так как только это в конечном итоге позволило бы сделать новый вид подписи аналогом собственноручной подписи лица, воспроизведенной на бумажном документе.

Выход был найден в применении математических алгоритмов, основанных на односторонних функциях дискретного логарифмирования, благодаря которым стало возможным получение пары математически связанных между собой криптографических ключей, один из которых используется для зашифрования, другой – для расшифрования, но при этом восстановление содержания ключа, используемого для зашифрования, по данным, содержащимся в ключе, используемом для расшифрования, является практически невыполнимой задачей.

Именно эта логика и заложена в настоящее время почти во все виды криптографически стойких цифровых подписей. Сам алгоритм «проставления» цифровой подписи сводится в основном к следующему: подписываемый текст сжимается посредством хеш-функции, полученный результат (хеш-сумма) зашифровывается ключом для зашифрования (закрытым ключом). Полученная криптограмма передается вместе с текстом. Получатель сообщения сжимает полученный текст посредством точно такой же, как и у отправителя, хеш-функции, расшифровывает ключом для расшифрования (открытым, проверочным ключом) криптограмму, полученную от отправителя, сравнивает полученные хеш-суммы. В случае их полного совпадения цифровая подпись признается подлинной. Именно криптограмму, содержащую зашифрованную посредством закрытого ключа отправителем документа хеш-сумму документа, ныне законодательно принято признавать цифровой (электронной, электронной цифровой) подписью.

Таким образом, упоминание в определении цифровых подписей понятия «криптографическое преобразование» является вполне уместным. В связи с тем, что все вышеуказанные математические преобразования возможно провести не только посредством компьютерных программ, но и на листе бумаги, употребление таких понятий, как «набор электронных цифровых символов», не представляется научно обоснованным. Некорректным также представляется упоминание о наличии «логической или иной» связи между текстом и цифровой подписью – между ними существует однозначное математическое тождество.

Приведенные выше рассуждения, однако, не являются исчерпывающим основанием для формулирования научно приемлемого определения цифровой подписи, так как в ряде профильных законодательных актов государств – членов ОДКБ, а именно в законодательстве Кыргызской Республики и Российской Федерации, имеется градация цифровых подписей по уровням. В Законе Кыргызской Республики об электронной подписи выделяются *простая электронная подпись*, *неквалифицированная электронная подпись* и *квалифицированная электронная подпись*. В Федеральном законе Российской

Федерации об электронной подписи выделяются *простая электронная подпись* и *усиленная электронная подпись*. Последняя, в свою очередь, подразделяется на *усиленную неквалифицированную электронную подпись* и *усиленную квалифицированную электронную подпись*. Такая дробная градация, как представляется, связана со стремлением законодателей этих государств расширить ареал использования электронных подписей в различных правоотношениях.

Однако применительно к задачам, поставленным перед настоящими Рекомендациями, речь может идти только об усиленной квалифицированной электронной подписи, которая обладает рядом признаков, непосредственно определенных вышеуказанными законодательными актами.

Анализ также показал, что в профильных законодательных актах остальных государств – членов ОДКБ речь идет о видах электронных подписей, которые в Кыргызской Республике и Российской Федерации признаются усиленными квалифицированными. Именно этот вид электронных подписей и предлагается считать цифровой подписью в целях гармонизации подходов к формулированию законодательных дефиниций.

Вышесказанное позволяет сформулировать следующую модельную дефиницию цифровой подписи, предназначенной для целей использования в системе государственной власти и обмена государственно значимой информацией с другими государствами:

«***цифровая подпись*** **– уникальный отрезок информации, представленный в виде цифровой последовательности символов (число), созданный средством цифровой подписи, допущенным в соответствии с законодательно определенной процедурой для выработки цифровых подписей с использованием алгоритмов криптографического преобразования, математически связанный с текстом подписываемого электронного документа, предназначенный для защиты данного текста от изменений и для идентификации лица, подписавшего электронный документ».**

2. Вторым блоком основных понятий являются определения ключей цифровой подписи.

Профильный законодательный акт Республики Армения определяет эти понятия следующим образом:

данные для создания электронной цифровой подписи – специфическая последовательность символов, которую подписывающее лицо использует при каждом применении своей электронной цифровой подписи;

данные проверки электронной цифровой подписи (данные проверки) – специфическая последовательность символов, которая используется для подтверждения подлинности каждой электронной цифровой подписи.

Профильный законодательный акт Республики Беларусь определяет эти понятия следующим образом:

личный ключ – последовательность символов, принадлежащая определенным организации или физическому лицу и используемая при выработке электронной цифровой подписи;

открытый ключ – последовательность символов, соответствующая определенному личному ключу, доступная для всех заинтересованных организаций или физических лиц и применяемая при проверке электронной цифровой подписи.

Профильный законодательный акт Республики Казахстан определяет эти понятия следующим образом:

закрытый ключ электронной цифровой подписи – последовательность электронных цифровых символов, предназначенная для создания электронной цифровой подписи с использованием средств электронной цифровой подписи;

открытый ключ электронной цифровой подписи – последовательность электронных цифровых символов, доступная любому лицу и предназначенная для подтверждения подлинности электронной подписи в электронном документе.

Профильный законодательный акт Кыргызской Республики определяет эти понятия следующим образом:

ключ подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

ключ проверки подписи – уникальная последовательность символов, однозначно связанная с ключом подписи и предназначенная для проверки электронной подписи.

Профильный законодательный акт Российской Федерации определяет эти понятия следующим образом:

ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Профильный законодательный акт Республики Таджикистан определяет эти понятия следующим образом:

закрытый ключ электронной цифровой подписи – последовательность символов, известная владельцу сертификата ключа подписи;

открытый ключ электронной цифровой подписи – последовательность символов электронной подписи, доступная любому пользователю, предназначенная для подтверждения подлинности электронной цифровой подписи в электронном документе.

Анализ вышеприведенных дефиниций показывает, что в целом определения ключей цифровой подписи по формулировкам близки друг к другу, за исключением законодательства Республики Армения, где сделана попытка более углубленно описать функциональное назначение каждого из видов ключей. Вместе с тем ни одно из определений не содержит указания на то, что данные числовые последовательности математически связаны между

собой. С лингвистической точки зрения также важным моментом является указание на принадлежность ключа выработки цифровой подписи, как это установлено профильным законодательным актом Республики Беларусь. Понятийная пара «закрытый ключ – открытый ключ» в законодательстве государств – членов ОДКБ появилась после принятия в Российской Федерации Федерального закона «Об электронной цифровой подписи» в 2002 году. В этом законодательном акте данные понятия были воспроизведены на основе принятой в определенных разделах математики терминологии.

В связи со сказанным, для более четкого восприятия широкими кругами правоприменителей специфической терминологии, представляется целесообразным предложить следующие модельные дефиниции:

«***личный ключ для выработки цифровой подписи (закрытый ключ)*** **– уникальная последовательность символов (число), предназначенная для создания цифровой подписи в электронном документе»**;

«***ключ для проверки цифровой подписи (открытый ключ)*** **– уникальная последовательность символов (число), математически связанная с личным ключом для выработки цифровой подписи, предназначенная для проверки подлинности цифровой подписи в электронном документе».**

Необходимость указания на то, что ключ для выработки цифровой подписи является именно личным ключом, будет раскрыта при рассмотрении категории «сертификат ключа подписи».

К терминам, гармонизацию дефиниций которых представляется целесообразным осуществить, относится «удостоверяющий центр». Сразу следует оговориться: данное понятие означает специфическую функцию, исполняемую субъектом, суть которой состоит в том, что он получает право изготавливать сертификаты ключей для проверки цифровой подписи и тем самым официально подтверждать принадлежность данных ключей определенному физическому лицу (проблема принадлежности ключей юридическим лицам будет раскрыта при рассмотрении вопроса об определении понятия «сертификат ключа подписи»). Говоря иначе, право исполнять функцию удостоверяющего центра может быть предоставлено как организации, так и физическому лицу.

Профильный законодательный акт Республики Армения определяет данную категорию следующим образом:

удостоверяющий центр – организация, выдающая сертификаты электронной цифровой подписи и оказывающая другие услуги, связанные с электронными цифровыми подписями.

В профильном законодательном акте Республики Беларусь данное понятие отсутствует, оно заменено следующей категорией:

поставщик услуг – организация, осуществляющая одну или несколько из следующих функций: издание, распространение и хранение сертификатов открытых ключей, атрибутных сертификатов, списков отозванных

сертификатов открытых ключей и списков отозванных атрибутных сертификатов; достоверное подтверждение принадлежности открытого ключа определенным организации или физическому лицу; предоставление информации о действительности сертификатов открытых ключей, атрибутивных сертификатов; отзыв сертификатов открытых ключей, атрибутивных сертификатов; проставление штампа времени, выработка личных ключей для организаций или физических лиц.

В профильном законодательном акте Республики Казахстан данная категория определена следующим образом:

удостоверяющий центр – юридическое лицо, удостоверяющее соответствие открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, а также подтверждающее достоверность регистрационного свидетельства.

В профильном законодательном акте Кыргызской Республики данная категория определена следующим образом:

удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие деятельность по созданию и выдаче сертификатов ключа проверки подписи.

В профильном законодательном акте Российской Федерации данная категория определена следующим образом:

удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным законом (речь идет о Федеральном законе «Об электронной подписи»).

В профильном законодательном акте Республики Таджикистан данная категория определена следующим образом:

центр сертификации открытых ключей электронной цифровой подписи (далее – удостоверяющий центр) – юридическое лицо, обладающее правомочиями на удостоверение соответствия открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи, на чье имя выдано регистрационное свидетельство (владелец свидетельства).

Анализ вышеприведенных дефиниций показывает следующее.

1. Большинство государств – членов ОДКБ для обозначения рассматриваемой функции используют понятие «удостоверяющий центр». Исключение составляет Республика Беларусь. Однако по смыслу используемого в профильном законодательном акте данного государства понятия «поставщик услуг» речь все же идет о функции удостоверяющего центра.

2. Во многих государствах – членах ОДКБ законодательно установлено, что в качестве удостоверяющего центра выступает юридическое лицо. В Республике Армения и Республике Беларусь используется более широкое понятие – организация. В Российской Федерации установлена возможность

выступать в данном качестве, помимо юридических лиц, также индивидуальным предпринимателям, государственным органам и органам местного самоуправления.

3. Сложнее обстоит дело с описанием функций удостоверяющего центра. Наиболее просто и четко такая деятельность определяется в профильном законе Республики Армения: выдача сертификатов электронной цифровой подписи и оказание других услуг, связанных с электронными цифровыми подписями. Близкими являются определения профильных законов Кыргызской Республики и Российской Федерации. Наиболее сложно набор правомочий описан в определении, содержащемся в профильном законодательном акте Республики Беларусь.

Несколько обособленным от всех вышеуказанных представляется определение, использованное в профильном законодательном акте Республики Казахстан, согласно которому удостоверяющий центр выполняет следующие основные функции:

– удостоверение соответствия открытого ключа электронной цифровой подписи закрытому ключу электронной цифровой подписи;

– подтверждение достоверности регистрационного свидетельства.

Если подойти к анализу данного определения более детально, то следует отметить, что основной смысл сертификата ключа цифровой подписи заключается прежде всего в установлении принадлежности ключа проверки цифровой подписи конкретному лицу. Соответствие личного ключа для выработки цифровой подписи (закрытого ключа) ключу проверки цифровой подписи в данном случае презюмируется. Еще раз подчеркнем: создание инфраструктуры проверочных (открытых) ключей, чем, собственно, и занимаются удостоверяющие центры в первую очередь, имеет своей основной целью однозначное, юридически подтвержденное закрепление проверочных ключей за конкретными физическими лицами. Иначе невозможно говорить о юридической тождественности цифровых подписей собственноручным подписям в бумажных документах. Подтверждение достоверности регистрационного свидетельства (сертификата ключа подписи) является важной функцией удостоверяющего центра, однако она вторична по отношению к его основной функции.

При оценке качества определения, установленного профильным законом Республики Беларусь, следует отметить, что оно перегружено лингвистически. Учитывая тот факт, что статус удостоверяющих центров, как правило, определяется отдельным разделом в профильном законодательном акте, вряд ли целесообразно перегружать первичное определение.

В Республике Беларусь такой подход следует признать вынужденным, поскольку раскрытие функций удостоверяющих центров (в терминологии данного государства – поставщиков услуг) в профильном законе не осуществляется, в нем определяется статус Государственной системы управления открытыми ключами (ГосСУОК) в целом.

На основании вышеизложенного, для более четкого восприятия широкими кругами правоприменителей специфической терминологии, представляется целесообразным предложить следующую модельную дефиницию:

«***удостоверяющий центр*** **– организация, обладающая статусом юридического лица, в том числе государственный орган или орган местного самоуправления, осуществляющая функции по созданию и выдаче сертификатов ключа для проверки цифровой подписи, а также иные функции, предусмотренные законодательством»**.

Логической связи данного определения с другими (ключей и сертификатов) будет достаточно для четкого понимания основной функции такой организации. Предоставление возможности исполнять эту функцию такому субъекту, как индивидуальный предприниматель, является уникальным подходом Российской Федерации по отношению к другим государствам – членам ОДКБ, поэтому из модельной дефиниции данный субъект исключен.

С учетом важности проблемы определения статуса удостоверяющих центров в целом и выделения из их числа тех, на основе которых следует обеспечивать использование цифровых подписей для обмена государственно значимой информацией между органами государственной власти государств – членов ОДКБ, на что и направлены настоящие Рекомендации, целесообразно рассмотреть разновидности таких организаций, определенные в профильном законодательстве указанных государств.

Профильный закон Республики Армения выделяет два вида удостоверяющих центров – обычные и аккредитованные. Аккредитованные удостоверяющие центры, в сравнении с обычными, обладают расширенным набором полномочий, за ними установлен более строгий контроль со стороны государства. Очевидно, что инфраструктура ключей для проверки цифровых подписей, которая обеспечивает обмен государственно значимыми документами между государствами – членами ОДКБ, должна опираться именно на деятельность аккредитованных удостоверяющих центров.

В профильном законе Республики Беларусь вместо удостоверяющих центров выделяется ГосСУОК. Из норм данного закона следует, что Государственная система управления открытыми ключами строится как иерархическая инфраструктура открытых ключей и состоит из корневого удостоверяющего центра, подчиненного ему республиканского удостоверяющего центра и регистрационных центров.

Постановлением Совета Министров Республики Беларусь и Национального банка Республики Беларусь от 19 июля 2010 года № 1077/8 данная система была несколько скорректирована и представлена следующими тремя видами субъектов: корневой удостоверяющий центр – удостоверяющий центр – регистрационный центр.

Рассмотрим основные функции данных субъектов более подробно.

В качестве основных функций *корневого удостоверяющего центра* вышеуказанным постановлением определены:

– разработка и утверждение нормативных правовых и технических нормативных правовых актов, организационно-распорядительных документов, регулирующих деятельность корневого удостоверяющего центра;

– изготовление и обеспечение жизненного цикла (хранение, приостановление действия, возобновление, отзыв) самоподписанного сертификата открытого ключа;

– обеспечение международного взаимодействия с использованием электронной цифровой подписи;

– ведение реестра аккредитованных удостоверяющих и регистрационных центров и обеспечение к нему доступа;

– издание, распространение и хранение сертификатов открытых ключей и списков отозванных сертификатов открытых ключей всех аккредитованных удостоверяющих и регистрационных центров;

– ведение реестров действующих и отозванных сертификатов открытых ключей ГосСУОК;

– ведение архивов сертификатов открытых ключей и списков отозванных сертификатов открытых ключей;

– обеспечение доступа к базам данных, архивам сертификатов открытых ключей и спискам отозванных сертификатов открытых ключей для всех аккредитованных удостоверяющих и регистрационных центров.

В качестве основных функций *удостоверяющего центра* определены:

– издание сертификатов открытых ключей и списков отозванных сертификатов;

– распространение и хранение сертификатов и списков отозванных сертификатов открытых ключей, выданных данным удостоверяющим центром;

– оказание услуг по распространению открытых ключей в соответствии с законодательством Республики Беларусь.

В качестве основных функций *регистрационного центра* определены:

– регистрация владельцев личных ключей;

– проверка информации, размещаемой в сертификате открытого ключа;

– регистрация заявок на выпуск и отзыв сертификатов открытых ключей;

– обеспечение взаимодействия с удостоверяющим центром;

– достоверное подтверждение принадлежности открытого ключа определенной организации или определенному физическому лицу.

Анализ вышеприведенных положений показывает, что корневой удостоверяющий центр обеспечивает легитимность иных удостоверяющих и регистрационных центров путем издания сертификатов ключей цифровых подписей этих организаций и ведения соответствующего реестра данных организаций. Для целей настоящих Рекомендаций также важно, что

обеспечение международного взаимодействия с использованием цифровых подписей тоже возложено на корневой удостоверяющий центр.

Функциональные задачи удостоверяющих центров в Республике Беларусь предельно сужены, они заключаются в издании сертификатов ключей для проверки цифровых подписей, а также в распространении и хранении данных сертификатов и списков отозванных сертификатов, выданных данным удостоверяющим центром.

Подготовительная работа (регистрация будущего владельца, проверка информации о нем, регистрация заявок на выпуск и отзыв сертификатов и самое основное – достоверное подтверждение принадлежности ключа для проверки цифровой подписи определенной организации или определенному физическому лицу) возложена на регистрационные центры.

В соответствии с профильным законом Республики Казахстан выделяются удостоверяющий центр государственных органов Республики Казахстан, национальный удостоверяющий центр Республики Казахстан и корневой удостоверяющий центр Республики Казахстан. В настоящий период функции и задачи всех указанных субъектов обеспечивает *оператор информационно-коммуникационной инфраструктуры «электронного правительства»*, определенный в соответствии с Законом Республики Казахстан «Об информатизации». В этом качестве, в соответствии с постановлением Правительства Республики Казахстан от 29 января 2016 года № 40, выступает акционерное общество «Национальные информационные технологии».

В профильном законе Кыргызской Республики предусмотрено деление удостоверяющих центров на обычные и главные (корневые). Последние вправе иметь доверенных лиц, которые могут выдавать сертификаты ключей для проверки цифровых подписей. Какого-либо корневого удостоверяющего центра данный законодательный акт не предусматривает.

Профильный закон Российской Федерации выделяет собственно удостоверяющие центры и доверенные лица (доверенная третья сторона), которые наделяются полномочиями по приему заявлений на выдачу сертификатов ключей проверки цифровых подписей, а также вручению сертификатов ключей проверки цифровых подписей от имени удостоверяющего центра. Наличие такой системы обусловлено тем, что профильное законодательство Российской Федерации устанавливает обязательность личного присутствия заявителя при его идентификации в качестве будущего владельца сертификата ключа для проверки цифровой подписи.

Профильный закон Республики Таджикистан определяет, что удостоверяющие центры могут быть созданы в виде государственных и негосударственных (частных) удостоверяющих центров.

Следующим термином, гармонизацию дефиниций которого представляется целесообразным осуществить, является *«сертификат ключа проверки цифровой подписи»*.

Данный документ играет одну из самых важных ролей в системе организации электронного документооборота с использованием цифровых подписей, так как именно в нем обеспечивается юридическая связь между ключом для проверки цифровой подписи и лицом, которому он принадлежит (за которым он закреплен). Для обеспечения такой юридической связи, собственно, и создается национальная система удостоверяющих центров.

Профильный законодательный акт Республики Армения содержит следующую дефиницию: «сертификат электронной цифровой подписи – документ на бумажном, электронном или ином носителе, который подтверждает принадлежность данных проверки электронной цифровой подписи и электронной цифровой подписи подписывающему лицу и служит средством проверки подлинности электронной цифровой подписи».

Профильный законодательный акт Республики Беларусь содержит следующую дефиницию: «сертификат открытого ключа – электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенным организации или физическому лицу, и иную информацию, предусмотренную настоящим Законом и иными актами законодательства Республики Беларусь».

Профильный законодательный акт Республики Казахстан содержит следующую дефиницию: «регистрационное свидетельство – электронный документ, выдаваемый удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным настоящим Законом».

Профильный законодательный акт Кыргызской Республики содержит следующую дефиницию: «сертификат ключа проверки подписи – электронный документ или документ на бумажном носителе, выданный удостоверяющим центром и подтверждающий принадлежность ключа проверки подписи владельцу сертификата ключа проверки подписи».

Профильный законодательный акт Российской Федерации содержит следующую дефиницию: «сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи».

Профильный законодательный акт Республики Таджикистан содержит следующие дефиниции:

«сертификат ключа защищенной электронной подписи – документ на бумажном носителе или электронный документ с защищенной электронной подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ защищенной электронной подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности защищенной электронной подписи и идентификации владельца сертификата ключа подписи»;

«сертификат усиленной электронной подписи – документ на бумажном носителе или электронный документ с защищенной электронной подписью уполномоченного лица, выдавшего усиленную электронную подпись, которые включают в себя открытый ключ усиленной электронной подписи и которые выдаются уполномоченным лицом участнику информационной системы для подтверждения подлинности усиленной электронной подписи и идентификации владельца сертификата ключа подписи».

Анализ вышеуказанных дефиниций показывает следующее.

1. Профильное законодательство всех государств – членов ОДКБ, за исключением Республики Казахстан, в рассматриваемом определении использует категорию «сертификат» (происходит от французского слова certificate, объединяющего латинские термины certum (верно) и facere (делать), в словарях русского языка толкуется как «свидетельство, удостоверение»).

2. Большинство профильных законов государств – членов ОДКБ дают правильную функциональную трактовку данного документа – удостоверять принадлежность ключа для проверки цифровой подписи конкретному лицу. Исключение составляют профильные законодательные акты Республики Армения и Республики Казахстан (первый полагает, что этот документ предназначен для подтверждения принадлежности данных проверки электронной цифровой подписи подписывающему лицу; второй – что данный документ предназначен для подтверждения электронной цифровой подписи требованиям, установленным Законом Республики Казахстан «Об электронном документе и электронной цифровой подписи»).

3. Большинство профильных законодательных актов государств – членов ОДКБ указывают на то, что сертификат может быть изготовлен в виде документа на бумажном носителе или электронного документа (соответствующий Закон Республики Армения также предусматривает возможность отображения данного документа на ином носителе). Как представляется, такое указание является важным в связи с тем, что этим подчеркивается одинаковость юридической силы данных документов в любой форме их отображения.

4. Законодательство всех государств – членов ОДКБ, за исключением Республики Беларусь, однозначно связывает сертификат ключа для проверки цифровой подписи с деятельностью удостоверяющих центров, на что также следует обратить внимание при формулировании модельной дефиниции. Однако возможно и предоставление такого полномочия иным лицам, если правонаделение происходит на законодательном уровне, поскольку в результате данной деятельности может возникнуть гражданско-правовая ответственность лица, выдавшего сертификат, за достоверность его содержания.

На основании вышеизложенного, для более четкого восприятия широкими кругами правоприменителей специфической терминологии, представляется целесообразным предложить следующую модельную дефиницию:

«***сертификат ключа для проверки цифровой подписи*** **– электронный документ или документ на бумажном носителе, выдаваемый удостоверяющим центром или иным уполномоченным законом лицом, подтверждающий принадлежность ключа для проверки цифровой подписи конкретному лицу».**

Следующей проблемой, которая должна найти свое разрешение для формирования комплекса предложений по совершенствованию законодательства о цифровых подписях, является вопрос о принадлежности ключей цифровой подписи, имеющий практическое преломление. Дело в том, что собственноручная подпись физического лица, которая моделируется посредством системы цифровой подписи, физиологически принадлежит этому физическому лицу и неотделима от него. Логично было бы предположить, что цифровая подпись должна иметь точно такую же привязку. Именно эта логика и была заложена при выборе математического алгоритма, используемого для создания и проверки цифровой подписи (ключ цифровой подписи существует в единственном экземпляре, тогда как в других криптосистемах ключей как минимум два).

Отсюда следует, что «привязка» ключа цифровой подписи к юридическому лицу весьма проблематична, так как она не позволяет полностью уравнять между собой собственноручную подпись и цифровую подпись по юридической силе в связи с исчезновением презумпции о согласии уполномоченного лица с содержанием документа, возникающей при подписании его собственноручной подписью. Юридическое лицо с теоретической точки зрения является юридической фикцией, и от его имени может выступать довольно значительное число представителей – физических лиц.

Попытка разрешения данной проблемы, в частности, в профильном законодательстве Республики Беларусь осуществляется следующим образом (статья 23 Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи»):

«Электронная цифровая подпись, владельцем личного ключа которой является физическое лицо, является аналогом собственноручной подписи.

Электронная цифровая подпись, владельцем личного ключа которой является организация, может применяться:

в качестве аналога оттиска печати организации;

совместно с электронной цифровой подписью, владельцем личного ключа которой является физическое лицо, если информация о полномочиях этого физического лица, предоставленных ему от имени этой организации, не содержится в атрибутивном сертификате;

для создания и (или) подписания электронных документов посредством автоматизированных информационных систем без участия физического лица;

в иных случаях, предусмотренных законодательством».

Анализ показывает, что схема применения цифровой подписи юридическими лицами, за исключением создания и подписания электронных

документов в автоматизированных системах без участия физических лиц, выглядит несколько громоздкой.

Еще более сложная схема использования квалифицированной цифровой подписи при участии в правоотношениях юридических лиц предусмотрена профильным законом Российской Федерации (статья 17.2 Федерального закона «Об электронной подписи»), что также не представляется вполне оправданным. Исключение опять же составляет применение цифровой подписи в автоматизированных системах без участия физических лиц.

Более однозначно и вполне приемлемо для практического применения реализовано правовое регулирование в этом отношении в профильном законе Республики Казахстан. Согласно части третьей статьи 10 этого акта «владелец регистрационного свидетельства электронной цифровой подписи юридического лица – руководитель юридического лица или лицо, его замещающее, вправе передавать работнику данного юридического лица или назначенному им лицу полномочия на использование электронной цифровой подписи от имени данного юридического лица». Эта норма фактически приравнивает цифровую подпись юридического лица к печати организации.

Однако, как представляется, в таком сложном регулировании реальная целесообразность отсутствует, поскольку ничто не мешает указывать в сертификате ключа цифровой подписи возможность для физического лица действовать от имени юридического лица без доверенности, что характерно для руководителя исполнительного органа таких субъектов, либо по доверенности, если должным образом оформленная доверенность будет предоставлена удостоверяющему центру. Во всяком случае, для правоотношений, на моделирование регулирования которых направлены настоящие Рекомендации, следует воздержаться от включения в число субъектов, уполномоченных подписывать документы цифровыми подписями, юридических лиц. Применение цифровых подписей юридических лиц в автоматизированных системах без участия физических лиц является исключением.

Следующим термином, гармонизацию дефиниций которого представляется целесообразным осуществить, является *«средство цифровой подписи»*.

В профильном законодательном акте Республики Армения данная категория разделена на следующие две подкатегории:

средства создания электронной цифровой подписи – аппаратные и (или) программные средства, которые применяются в целях создания электронной цифровой подписи лица с использованием данных для создания электронной цифровой подписи;

средства проверки электронной цифровой подписи – аппаратные и (или) программные средства, создающие возможность проверки подлинности электронной цифровой подписи с использованием данных проверки электронной цифровой подписи.

Профильный законодательный акт Республики Беларусь определяет рассматриваемое понятие следующим образом:

средство электронной цифровой подписи – средство криптографической защиты информации, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи; проверка электронной цифровой подписи; выработка личного ключа или открытого ключа.

Профильный законодательный акт Республики Казахстан определяет рассматриваемое понятие следующим образом:

средства электронной цифровой подписи – совокупность программных и технических средств, используемых для создания и проверки подлинности электронной цифровой подписи.

Профильный законодательный акт Кыргызской Республики определяет рассматриваемое понятие следующим образом:

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключей подписи и ключей проверки подписи.

Профильный законодательный акт Российской Федерации определяет рассматриваемое понятие следующим образом:

средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Профильный законодательный акт Республики Таджикистан не содержит определения данного понятия.

Анализ вышеприведенных определений показывает, что в законодательстве государств – членов ОДКБ применительно к понятию средств цифровой подписи можно выделить два подхода: определения общего характера и определения, раскрывающие функциональное назначение данных средств. Не во всех определениях также присутствует акцент на то, что данные устройства или программы являются криптографическими, то есть реализуют криптографические функции.

Применение детализованного подхода обусловлено, скорее всего, особенностями оборота криптографических средств в том или ином государстве (например, в Российской Федерации разработка и производство криптографических средств являются лицензируемым видом деятельности).

Как представляется, детализованный подход является более приемлемым в связи с тем, что позволяет обособить средства цифровой подписи от иных устройств и компьютерных программ в целях дальнейшего упорядочения их гражданского или административного оборота.

Исходя из сказанного можно предложить следующую модельную дефиницию:

«*средства цифровой подписи* – **средства криптографической защиты информации, реализующие одну или несколько из следующих функций: создание цифровой подписи, проверка цифровой подписи, создание личного ключа для выработки цифровой подписи и ключа для проверки цифровой подписи»**.

3. Содержание сертификата ключа для проверки цифровой подписи

Рассмотрение содержания сертификатов ключей для проверки цифровых подписей имеет большое значение при конструировании модельного правового регулирования, так как целесообразным представляется добиться единообразия в основном содержании таких документов во всех государствах – членах ОДКБ, что существенным образом упорядочит межгосударственный обмен электронными документами.

Профильный законодательный акт Республики Армения определяет основное содержание сертификата ключа для проверки цифровой подписи следующим образом:

а) уникальный регистрационный номер сертификата;

б) фамилия, имя лица или его криптоним (псевдоним);

в) данные проверки электронной цифровой подписи;

г) день, месяц, год выдачи сертификата электронной цифровой подписи, а если сертификат электронной цифровой подписи имеет срок действия, то также этот срок;

д) название центра, удостоверяющего электронную цифровую подпись, адрес осуществления им своей деятельности и место нахождения юридического лица.

Профильный законодательный акт Республики Беларусь определяет содержание сертификата ключа для проверки цифровой подписи (в этом акте он именуется как «сертификат открытого ключа») следующим образом:

а) значение открытого ключа;

б) информация, однозначно идентифицирующая организацию или физическое лицо, являющиеся владельцем открытого ключа;

в) информация о сроке действия открытого ключа.

Профильный законодательный акт Республики Казахстан определяет содержание сертификата ключа для проверки цифровой подписи (в этом акте он именуется как «регистрационное свидетельство») следующим образом:

а) номер регистрационного свидетельства и срок его действия;

б) данные, позволяющие идентифицировать владельца электронной цифровой подписи;

в) открытый ключ электронной цифровой подписи;

г) информация о сферах применения и об ограничениях применения электронной цифровой подписи;

д) реквизиты соответствующего удостоверяющего центра.

Профильный законодательный акт Кыргызской Республики определяет содержание сертификата ключа для проверки цифровой подписи (в этом акте он именуется как «сертификат ключа проверки подписи») следующим образом:

а) даты начала и окончания срока действия сертификата;

б) фамилия, имя, отчество (если имеется) – для физических лиц (наименование – для юридических лиц) или иной идентификатор владельца сертификата ключа проверки подписи;

в) ключ проверки подписи;

г) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ подписи и ключ проверки подписи;

д) наименование удостоверяющего центра, который выдал сертификат.

Профильный законодательный акт Российской Федерации определяет содержание сертификата ключа для проверки цифровой подписи (в этом акте он именуется как «сертификат ключа проверки электронной подписи») следующим образом:

а) уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата;

б) фамилия, имя и отчество (если имеется) – для физических лиц, наименование и место нахождения – для юридических лиц или иная информация, позволяющая идентифицировать владельца сертификата ключа проверки электронной подписи;

в) уникальный ключ проверки электронной подписи;

г) наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

д) наименование удостоверяющего центра, который выдал сертификат ключа проверки электронной подписи.

Профильный законодательный акт Республики Таджикистан определяет содержание сертификата ключа для проверки цифровой подписи (в этом акте он именуется как «сертификат ключа защищенной электронной подписи») следующим образом:

а) уникальный регистрационный номер сертификата ключа защищенной электронной подписи;

б) даты начала и окончания срока действия сертификата ключа защищенной электронной подписи, находящегося в реестре удостоверяющего центра;

в) фамилия, имя и отчество (при наличии) владельца сертификата ключа защищенной электронной подписи;

г) открытый ключ защищенной электронной подписи;

д) наименование средств защищенной электронной подписи, в которых используется данный открытый ключ защищенной электронной подписи;

е) сведения об удостоверяющем центре, выдавшем сертификат открытого ключа защищенной электронной подписи, включая его наименование, место нахождения и серию лицензии.

В профильном законе Российской Федерации выделяется и такая категория, как квалифицированный сертификат, к содержанию которого предъявляются дополнительные требования.

Следует отметить, что изначально законодательство о цифровых подписях государств – членов ОДКБ ориентировалось преимущественно на отношения, возникающие в гражданско-правовой сфере, в силу чего специфика деятельности органов государственной власти и органов местного самоуправления в области электронного документооборота на законодательном уровне отражена недостаточно четко. Исходя из цели, сформулированной для настоящих Рекомендаций, содержание сертификатов ключей для проверки цифровой подписи, по отношению к общим требованиям, целесообразно определенным образом скорректировать.

Прежде всего, государствам – членам ОДКБ рекомендуется законодательно закрепить требование об уникальности номера такого сертификата (в настоящее время такое законодательное требование отсутствует в профильных законах Республики Казахстан и Кыргызской Республики).

Далее, для организации электронного документооборота между органами публичной власти как внутри государства, так и на межгосударственном уровне недостаточно только фамилии, имени и отчества владельца сертификата, необходимо также указывать его должность в конкретном органе публичной власти.

Кроме того, такого рода сертификаты должны носить срочный характер. Причем, учитывая ротацию государственных служащих, данный срок должен быть относительно небольшим. Например, не более шести месяцев.

Далее, для каждого государственного служащего, которому выдается такой сертификат, необходимо указать объем правомочий на подписание электронных документов (например, все документы, исходящие из определенного департамента; документы, имеющие гражданско-правовое значение; документы только справочного характера и т.д.).

Наконец, обязательным элементом содержания сертификата ключа подписи (что упущено всеми законодателями) должна быть цифровая подпись выдавшего данный сертификат уполномоченного лица удостоверяющего центра, которая подтверждает достоверность перечисленных в нем сведений.

Таким образом, **минимальное содержание модельного сертификата ключа проверки цифровой подписи для органов публичной власти государств – членов ОДКБ должен составлять следующий набор сведений:**

а) уникальный номер сертификата;

б) фамилия, имя, отчество (при наличии последнего) и должность владельца сертификата в конкретном органе публичной власти;

в) объем правомочий владельца сертификата на подписание электронных документов;

г) срок действия сертификата;

д) содержание ключа для проверки цифровой подписи;

е) реквизиты удостоверяющего центра, выдавшего сертификат;

ж) цифровая подпись уполномоченного лица удостоверяющего центра, выдавшего сертификат.

4. Статус удостоверяющих центров для органов публичной власти и межгосударственного обмена электронными документами

При анализе профильных законов государств – членов ОДКБ об электронном документе и цифровой подписи выявились существенные различия в определении статуса таких субъектов, как удостоверяющие центры.

Профильный законодательный акт Республики Армения выделяет собственно удостоверяющие центры и аккредитованные удостоверяющие центры. Основное отличие первых от вторых заключается в том, что только аккредитованным удостоверяющим центрам вменяется в обязанность идентификация лица по документам, удостоверяющим данное лицо, при выдаче сертификата цифровой подписи.

В Республике Беларусь на уровне профильного законодательного акта легитимирована только ГосСУОК. Более детальное регулирование данных отношений осуществляется подзаконными актами, основным из которых является Положение о порядке функционирования Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденное Постановлением Совета Министров Республики Беларусь и Национального банка Республики Беларусь от 19 июля 2010 года № 1077/8. В этой системе выделяются корневой удостоверяющий центр, собственно удостоверяющие центры и регистрационные центры.

Профильный законодательный акт Республики Казахстан легитимирует только аккредитованные удостоверяющие центры, что существенным образом упрощает такую систему и стабилизирует ее деятельность.

Помимо собственно удостоверяющих центров в этом законе упоминаются национальный, корневой и специальный корневой удостоверяющие центры, но без раскрытия особенностей их статуса.

По законодательству данного государства – члена ОДКБ удостоверяющий центр осуществляет следующие основные виды деятельности:

1) создает ключи электронных цифровых подписей по обращению участников системы электронного документооборота с принятием мер для защиты закрытых ключей электронной цифровой подписи от неправомерного доступа;

2) выдает, регистрирует, отзывает, хранит регистрационные свидетельства, ведет регистр регистрационных свидетельств, выданных в установленном порядке;

3) утверждает правила применения регистрационных свидетельств;

4) осуществляет учет действующих и отозванных регистрационных свидетельств;

5) подтверждает принадлежность и действительность открытого ключа электронной цифровой подписи, зарегистрированного удостоверяющим центром в порядке, установленном законодательством Республики Казахстан.

В соответствии с профильным законодательным актом Кыргызской Республики выделяются собственно удостоверяющие центры, полномочия которых близки к вышеприведенным, и аккредитованные удостоверяющие центры. Последние обязаны хранить персональные данные о владельце квалифицированного сертификата. Особенностью правового статуса удостоверяющих центров в данном государстве – члене ОДКБ является то, что удостоверяющие центры вправе наделить иные лица (доверенные лица) полномочиями по созданию и выдаче сертификатов ключей проверки подписи от имени удостоверяющего центра, подписываемых цифровой подписью, основанной на сертификате ключа проверки подписи, выданного такому доверенному лицу этим удостоверяющим центром. При этом данное правомочие может реализовываться как простыми, так и аккредитованными удостоверяющими центрами.

Согласно профильному законодательному акту Российской Федерации также выделяются собственно удостоверяющие центры, полномочия которых близки к вышеприведенным, и аккредитованные удостоверяющие центры. При этом, аналогично с законами Республики Армения и Кыргызской Республики, только аккредитованные удостоверяющие центры в Российской Федерации идентифицируют владельцев ключей цифровой подписи по их документам. Особенностью законодательного регулирования данных отношений является то, что в порядке административного правонаделения статус аккредитованных удостоверяющих центров признается за удостоверяющими центрами Федеральной налоговой службы, Федерального казначейства и Центрального банка Российской Федерации.

Полномочия удостоверяющих центров, установленные профильным законом Республики Таджикистан, сходны с аналогичными правомочиями аккредитованных удостоверяющих центров других государств – членов ОДКБ. Сама административная процедура аккредитации данным законом не предусматривается, так как деятельность удостоверяющих центров является лицензируемым видом деятельности, как это было, в частности, в Российской Федерации в период действия Федерального закона «Об электронной цифровой подписи» 2002 года.

На основании анализа вышеприведенных правоположений возможен вывод, что каждое из государств – членов ОДКБ в своей системе удостоверяющих центров может создать сегмент для использования

цифровых подписей в системе органов исполнительной власти, обеспечивающих оборону и безопасность государства.

Однако, как представляется, в интересах обеспечения национальной безопасности данная система должна быть определенным образом скорректирована. **Среди удостоверяющих центров должен быть выделен один удостоверяющий центр (например, по аналогии со специальным корневым удостоверяющим центром Республики Казахстан), который обеспечивал бы изготовление сертификатов ключей проверки цифровых подписей должностных лиц для использования во внутреннем электронном документообороте органов государственной власти и в документальном взаимодействии между органами государственной власти, в том числе в документообороте, в котором фигурируют сведения, составляющие государственные секреты. Эти сертификаты должны быть недоступны гражданам, а также любым организациям, не входящим в систему органов государственной власти. Возможность учреждения таких удостоверяющих центров может быть отражена в нормах профильных законодательных актов государств – членов ОДКБ в области электронного документооборота и цифровых подписей. Они также должны иметь статус аккредитованных удостоверяющих центров, приобретаемый ими в порядке административного правонаделения.**

5. Регулирование межгосударственного обмена электронными документами, удостоверенными цифровыми подписями

Профильный законодательный акт Республики Армения содержит всего одно правоположение, которое затрагивает проблему организации межгосударственного обмена электронными документами, удостоверенными цифровыми подписями:

«Сертификаты электронных цифровых подписей, выданные удостоверяющими центрами, действующими в других государствах, приравниваются к сертификатам, выданным удостоверяющими центрами, аккредитованными в Республике Армения, при наличии соответствующих ратифицированных международных договоров между этими государствами и Республикой Армения».

Профильный законодательный акт Республики Беларусь содержит следующие нормы, затрагивающие рассматриваемые правоотношения:

«Иностранный сертификат открытого ключа, соответствующий требованиям законодательства иностранного государства, в котором этот сертификат издан, признается на территории Республики Беларусь в случаях и порядке, определенных международным договором Республики Беларусь, предусматривающим взаимное признание сертификатов открытых ключей, или путем установления доверия к нему доверенной третьей стороной. Доверенной третьей стороной является определенная Президентом Республики Беларусь организация, осуществляющая функции по признанию

подлинности электронных документов при межгосударственном электронном взаимодействии.

Сертификат открытого ключа, изданный поставщиком услуг иностранного государства, аккредитованным в Государственной системе управления открытыми ключами, признается на территории Республики Беларусь».

Профильный законодательный акт Республики Казахстан следующим образом определяет порядок признания иностранной цифровой подписи:

«Иностранная электронная цифровая подпись, имеющая иностранное регистрационное свидетельство, признается на территории Республики Казахстан в следующих случаях:

1) удостоверена подлинность иностранной электронной цифровой подписи доверенной третьей стороной Республики Казахстан;

2) лицо, подписавшее электронный документ, правомерно владеет закрытым ключом иностранной электронной цифровой подписи;

3) иностранная электронная цифровая подпись используется в соответствии со сведениями, указанными в регистрационном свидетельстве;

4) сформирована средствами электронной цифровой подписи иностранного удостоверяющего центра, зарегистрированного в доверенной третьей стороне Республики Казахстан, или иностранного удостоверяющего центра, зарегистрированного в доверенной третьей стороне иностранного государства, зарегистрированной в доверенной третьей стороне Республики Казахстан».

Профильный законодательный акт Кыргызской Республики следующим образом определяет порядок признания иностранных цифровых подписей:

«1. Электронные подписи, созданные в соответствии с нормами права иностранного государства, в Кыргызской Республике признаются электронными подписями того вида, признакам которого они отвечают в соответствии с настоящим Законом.

2. Электронная подпись и подписанный ею электронный документ не могут считаться не имеющими юридической силы только на том основании, что сертификат ключа проверки подписи выдан в соответствии с нормами права иностранного государства».

Профильный законодательный акт Российской Федерации, помимо норм, полностью аналогичных законодательству Кыргызской Республики, содержит также следующее правоположение:

«Признание электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами, соответствующими признакам усиленной электронной подписи, и их применение в правоотношениях в соответствии с законодательством Российской Федерации осуществляется в случаях, установленных международными договорами Российской Федерации. Такие электронные подписи признаются действительными в случае подтверждения соответствия их требованиям указанных международных договоров аккредитованной

доверенной третьей стороной, аккредитованным удостоверяющим центром, иным лицом, уполномоченными на это международным договором Российской Федерации, с учетом настоящего Федерального закона».

Профильный законодательный акт Республики Таджикистан содержит следующие правоположения, определяющие условия признания иностранного сертификата ключа цифровой подписи:

«Признание иностранных сертификатов ключей электронной цифровой подписи осуществляется в соответствии с действующим законодательством Республики Таджикистан и международными договорами, признанными Таджикистаном.

Международные договоры Республики Таджикистан применяются к отношениям, указанным в части первой настоящей статьи, непосредственно, кроме случаев, когда из международного договора следует, что для его применения требуется издание внутригосударственного акта».

Анализ вышеприведенных правоположений показывает, что такие государства – члены ОДКБ, как Республика Армения, Республика Беларусь, Российская Федерация и Республика Таджикистан, предусматривают легитимацию иностранных цифровых подписей на основании международных договоров. Профильный закон Республики Казахстан устанавливает иной порядок признания иностранных сертификатов. Профильный закон Кыргызской Республики содержит только общие правила, не имеющие конкретного юридического наполнения.

Как представляется, установление порядка обмена электронными документами между органами государственной власти государств – членов ОДКБ по вопросам, касающимся обеспечения обороны и безопасности, требует заключения отдельного международного договора.

Для легитимации этого электронного документального взаимодействия предлагается следующая примерная модель содержания основных положений данного договора.

1. В каждом государстве – члене ОДКБ определяется один удостоверяющий центр, ответственный за организацию и осуществление обмена электронными документами между органами государственной власти.

2. Каждое государство четко определяет круг должностных лиц, имеющих право подписи электронных документов при межгосударственном электронном взаимодействии, удостоверенных цифровой подписью, и круг вопросов для каждого должностного лица, по которым он вправе вести такую переписку.

3. Все государства – члены ОДКБ в вышеуказанных целях принимают единый стандарт содержания сертификата ключа для проверки цифровой подписи и единую модель средства выработки и проверки цифровой подписи.

4. Уполномоченный удостоверяющий центр каждого государства – члена ОДКБ изготавливает для каждого уполномоченного должностного лица сертификат ключа для проверки цифровой подписи и направляет его в уполномоченные удостоверяющие центры тех государств – членов ОДКБ, с которыми предполагается вести соответствующую переписку. Данный сертификат удостоверяется цифровой подписью уполномоченного лица этого удостоверяющего центра (сертификаты ключей для проверки этих цифровых подписей заблаговременно высылаются в уполномоченный удостоверяющий центр каждого государства – члена ОДКБ).

5. При лишении уполномоченного должностного лица права подписи соответствующих электронных документов сертификат ключа для проверки его цифровой подписи в срок, определенный данным международным договором, отзывается и заменяется сертификатом ключа для проверки цифровой подписи того лица, которому данные полномочия переданы.

6. Юридическая ответственность за достоверность содержания сертификатов ключей для проверки цифровых подписей, используемых в данных правоотношениях, а также за своевременность замены сертификатов лежит на государстве – члене ОДКБ, удостоверяющий центр которого изготовил такие сертификаты.