1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації. Метрологічне забезпечення систем ТЗІ. Стандартизація, сертифікація та випробовування засобів ТЗІ

УДК 680.3

НАПРАВЛЕНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ВОПРОСОВ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Владимир Гребнев, Алексей Скиба
ДСТСЗИ СБ Украины

Анотація: **Аналізуються моделі розвитку національних законодавств в сфері електронного документообігу та електронного підпису. Проводиться короткий огляд проекту Закону України "Про електронний цифровий підпис", прийнятого Верховною Радою в першому читанні, умови прирівнення електронного цифрового підпису до власноручного, можливі схеми правових взаємовідносин з використанням електронного цифрового підпису тощо.**
Summary: **In this article are analyzed models of the development national legislation in sphere of the electronic document workflow and electronic signature. The survey of the project of the Law of the Ukraine "About electronic digital signature", accepted by Verchovna Rada in the first reading is done, condition of the bill equating electronic digital signature to handmade, possible schemes of the legal relations with use electronic digital signature etc.**
Ключові слова: **Електронний цифровий підпис, електронний документообіг, електронний документ, сертифікат ключа, центр сертифікації ключів, акредитація.**

Двадцать первый век – время интенсивного развития информационных технологий. Международные сети и системы, прежде всего сеть Интернет, являются технологической основой международного информационного обмена. Кроме этого, на Интернет сейчас ложится большая экономическая нагрузка, которая возрастает буквально в геометрической прогрессии.

Устойчивая тенденция значительного роста информационных потоков, необходимых для принятия управленческих решений, приводит к тому, что, с одной стороны, резко растет обмен документами, а с другой стороны, требуется сокращать сроки переписки. Задача осложняется ещё и тем, что информация может иметь различную форму и масштабы представления: текст, графика, картография, табличные данные, фотоматериалы, видеоинформация и т. п., причем документы не имеют жестких предопределенных форматов. Традиционные методы работы с документами становятся при этом малоэффективными.

По экспертным оценкам, применение полноценного электронного документооборота позволит сократить время обработки документов более чем в два раза, а также добиться огромного экономического эффекта. Например, суммарное годовое снижение издержек при внедрении электронного документооборота в Норвегии оценивается в сумму около одного миллиарда долларов.

Развитие компьютерных сетей и телекоммуникаций в Украине значительно расширяет возможности применения современных информационных технологий и делает возможным создание систем юридически значимого электронного документооборота, осуществляемого с использованием информационных систем. Уже сейчас эти информационные технологии внедряются во многие сферы деятельности: от поддержки функционирования товарных и финансовых рынков и взаимодействия населения с органами государственной власти до розничной торговли и сферы услуг, образования и досуга. Широкое распространение получают электронные платежные системы (коммунальные платежи, заказы и покупка товаров и т. д.), а также системы обмена электронными документами (предоставление финансовой отчетности, налоговые декларации, заключение договоров и т. д.) при взаимодействии между гражданами, организациями и государственными органами.

Уровень развития общества вплотную подошел к необходимости использования электронной цифровой подписи (ЭЦП) как удостоверения подлинности и аутентичности электронных данных. Поэтому перед

государством стоит задача создания правового и технологического механизма, который обеспечивал бы необходимый уровень защиты электронных данных, учитывая, что сфера электронных сетей в целом не контролируются государством и позволяет каждому пользователю практически без проблем включаться в общедоступные глобальные процессы.

Современные тенденции развития национальной экономики, задачи сохранения единого экономического и финансового пространства на территории Украины диктуют необходимость создания инфраструктуры с открытыми ключами на национальном уровне. Такая национальная инфраструктура должна стать основой для обеспечения юридически значимого и безопасного информационного обмена по открытым сетям связи между всеми субъектами информационного взаимодействия – от органов государственной власти различных уровней до коммерческих организаций и отдельных физических лиц.

В данной статье хотелось бы абстрагироваться от технических вопросов построения и функционирования национальной системы ЭЦП и остановиться исключительно на юридических аспектах применения ЭЦП.

Основное правовое препятствие, стоящее на пути развития юридически значимого электронного документооборота, в том числе электронной торговли – невозможность предоставлять электронные документы, например договоры, в качестве доказательств в суде при возникновении споров. В некоторых случаях, например на фондовом рынке, эту проблему решают с помощью соглашений между самими участниками торговли, прописывая возможность использовать электронные документы в качестве доказательств при возникновении конфликтных ситуаций. Но такой подход удобен далеко не всегда. Например, покупка компакт-диска в электронном магазине не должна осложняться подписанием горы бумаг.

Другую группу проблем порождает анонимность пользователей в глобальных сетях. Например, в сети Интернет, общаясь с контрагентом, невозможно быть полностью уверенным в том, что полученный по открытым каналам электронный документ идентичен отправленному оригиналу, а отправитель и есть вторая сторона в информационном обмене.

В общем виде юридические функции электронной подписи заключаются в следующем:

гарантировать, что электронный документ подписан уполномоченным лицом;

гарантировать подлинность и целостность подписанного документа;

предотвращать негативные последствия отсутствия собственноручной подписи;

символизировать выражение воли стороны по сделке;

символизировать необходимую письменную форму сделки, заключенной посредством электронного документооборота.

Удобная, быстрая и дешевая практика использования электронных подписей стала внедряться на Западе с середины 90-х годов.

Мировой опыт показал, что на настоящий момент сложились три модели развития законодательной базы в сфере электронного документооборота и электронной подписи.

Первая модель принята в США. Правительство США оставляет право самостоятельно регулировать внутренние процессы в сфере электронной коммерции. Данная модель основана на принципах бизнес-выбора, концепции свободы заключения контракта и использовании при этом любой конкретной технологии. Выбор любой технологии подписи электронных документов сторон, участвующих в сделке, признается законным. Стороны могут решить – использовать или не использовать электронную цифровую подпись, причем они не обязаны обращаться к третьей независимой организации, удостоверяющей сертификаты ключа.

Вторая модель принята в России и в Индии. Там существуют законы об ЭЦП, которые жестко регулируют рынок услуг в сфере электронной цифровой подписи путем лицензирования деятельности по предоставлению таких услуг. Принцип модели – признание ЭЦП действенной и необходимой везде, в том числе и на международном уровне. Данный подход лишен гибкости и не способен своевременно реагировать на меняющиеся условия и механизмы развития информационной сферы. Примером может стать тот факт, что в Индии первая лицензия на деятельность по предоставлению услуг в сфере ЭЦП выдана через три года после принятия закона об ЭЦП. В итоге электронная торговля была заморожена, в гражданском суде Индии скопилось около 40 млн. дел по поводу споров по контрактам.

Третья модель принята в Европейском Союзе. Принцип соответствующей директивы об ЭЦП – система лицензирования не должна быть обязательной. Правительство может создавать структуры, регулирующие процесс добровольного лицензирования, для того, чтобы сформировать у клиентов или потенциальных деловых партнеров авторитет и доверие к организации, которая предоставляет услуги в сфере ЭЦП.

По степени детализации требований к самой электронной подписи можно выделить три подхода.

Первый, самый общий, основан на признании в отношении электронной подписи тех же требований, что и в отношении обычной, включая уникальность, возможность верификации подписи и "подконтрольность" использующему ее лицу.

Второй подход, кроме того, предполагает, что электронная подпись должна быть связана с передаваемыми данными таким образом, что если они изменяются, то электронная подпись становится недействительной.

Третий подход выдвигает наиболее детализированные требования к электронной подписи, в частности, предусматривает использование технологии асимметричных криптографических преобразований. Именно такой тип электронной подписи называется электронной цифровой подписью.

Какой из трех подходов принимается на уровне национального законодательства – в конечном итоге зависит от общей политики государства, которое может либо доверить поиск наиболее подходящего средства безопасной передачи данных самому рынку, либо взять эту ответственность на себя, чтобы уберечь агентов рынка электронной коммерции от возможных "проколов".

Так, американское федеральное правительство считает законными все электронные подписи, признаваемые обоими контрагентами по сделке, будь то хоть отпечаток пальца. В частности, файл с текстом закона "Об электронных подписях в глобальной и национальной торговле" (американский аналог закона “Об электронной цифровой подписи”) был подписан фотографической копией собственной подписи Билла Клинтона, которую он вывел на компьютерном графическом планшете.

Европейское законодательство более жестко подходит к вопросу о том, какой должна быть электронная подпись. Соответствующая Директива Европарламента рекомендует использовать второй по степени детализации подход из названных выше. На нем основаны соответствующие законы европейских стран, например, ФРГ, Великобритании, Австрии.

Проблемы правового регулирования отношений, связанных с использованием электронных подписей, связаны именно с регулированием применения технологий. Каждая страна решает, насколько тот или иной способ электронного документооборота надежен, как велика вероятность искажения воли стороны в электронном документе, кто обладает правом решать в каждом конкретном случае вопрос об аутентичности и на основании каких критериев.

В системе ООН работа по юридическому регулированию отношений в областях электронной коммерции и электронной подписи в основном сосредоточена в Комиссии по международному торговому праву – UNCITRAL. Правовой режим электронного обмена данными в международных коммерческих операциях представлен в виде примерного свода правил в модельных законах UNCITRAL “Об электронной коммерции” 1996 года и “Об электронной подписи” 2001 года.

Другим международным центром разработки базовых правил регулирования электронной коммерции стало Европейское сообщество. Работа также шла в двух областях – собственно электронная коммерция и электронные подписи. Были разработаны и приняты Европейские директивы “О заочной торговле” 1997 года и “Об электронной коммерции” 2000 года. В сфере, касающейся регулирования вопросов применения электронных подписей, принят базовый европейский закон – упомянутая выше Директива Европейского парламента и Совета Министров Европейского Союза 1999/93/ЕС от 13 декабря 1999 года “О политике Европейского союза по электронным подписям”.

В Украине, как и во многих странах Европейского союза и государств СНГ, также достаточно долго ведутся работы, направленные на законодательное урегулирование правовых взаимоотношений, связанных с использованием электронного документооборота и электронных подписей.

Законом Украины “О платежных системах и переводе денег в Украине” определен юридический статус электронных документов, подписанных ЭЦП. Речь идет о банковской сфере, в частности, о платежных системах и переводе денег в Украине, то есть о платежных электронных документах.

Разработаны проекты законов “Об электронной цифровой подписи” и “Об электронных документах и электронном документообороте”, цель которых – определить организационно-правовые основы создания электронных документов, правовой статус электронной подписи, порядок ее использования, организационно-правовые основы деятельности по предоставлению услуг в сфере ЭЦП и т. д.

На данный момент эти законопроекты приняты Верховной Радой Украины в первом и во втором чтении соответственно.

Хотелось бы более подробно остановиться на проекте закона “Об электронной цифровой подписи”, основываясь на редакции законопроекта, принятого в первом чтении, а также тексте законопроекта, подготовленного для внесения на последующее чтение рабочей группой профильного комитета по вопросам науки и образования Верховной Рады.

Разработчиками проекта закона “Об электронной цифровой подписи” была принята общая концепция соответствующей директивы Европейского Союза, основанная на определении единых правил относительно признания юридической силы цифровой подписи и добровольной аккредитации центров сертификации ключей. В законопроекте основное внимание, помимо вопросов приравнивания электронной подписи к собственноручной подписи, уделяется регламентированию работы организационно-технического аппарата,

позволяющего применять технологию ЭЦП, установлению рамок для функционирования этого аппарата, определению прав и обязанностей субъектов сферы ЭЦП.

Определение термина "электронная подпись" по уровню детализации выдвигаемых к электронной подписи требований, разделено на два понятия. Собственно электронная подпись, которая представляет собой данные в электронной форме, которые присоединяются к другим данным или логически с ними объединяются и предназначены для идентификации подписавшего лица. Второе определение – электронная цифровая подпись конкретизирует используемую технологию и определяется как результат определенного криптографического преобразования некоторого набора данных, который присоединяется к этому набору данных или логически с ним объединяется и дает возможность подтвердить целостность этого набора данных и идентифицировать подписавшее лицо.

В законопроекте однозначно определяются условия, при которых именно ЭЦП приравнивается к собственноручной подписи, в частности:

цифровая подпись проверена с использованием усиленного сертификата ключа (в терминах Директивы ЕС – квалифицированного сертификата) при помощи надежных средств ЭЦП; надежные средства ЭЦП – это средства ЭЦП, которые имеют сертификат соответствия или положительное экспертное заключение по результатам государственной экспертизы в сфере криптографической защиты информации;

во время проверки использовался усиленный сертификат ключа подписи, действующий на момент наложения цифровой подписи; усиленные сертификаты ключа имеют право формировать только аккредитованные центры сертификации ключей;

личный ключ подписавшего лица отвечает открытому ключу, который находится в сертификате.

Юридическое признание электронной подписи, в том числе переведенного в цифровую форму изображения собственноручной подписи, не опровергается. Юридическое признание других видов электронной подписи может регламентироваться на основании отдельных договоров между участниками информационного обмена или определяться другими нормативно-правовыми актами.

Таким образом, электронный документ, подписанный электронной подписью, может служить доказательством в судебном процессе. Споры, которые могут возникнуть между сторонами информационного обмена, разрешаются судами в общем порядке, предусмотренном законодательством Украины. Суд не может однозначно опровергнуть юридическую силу электронной подписи исключительно на основании того, что она:

представлена в электронной форме;

не основана на усиленном сертификате ключа;

сформирована с использованием ненадежных средств цифровой подписи.

Законопроектом также устанавливаются соответствующие требования к усиленному сертификату открытого ключа, к аккредитованным центрам сертификации ключей (ЦСК), которые выдают усиленные сертификаты, а также к надежным средствам цифровых подписей (защищенным устройствам для создания подписей в терминах директивы).

Следует отметить, что деятельность ЦСК, т. е. деятельность по предоставлению услуг в сфере ЭЦП, в соответствии с последней рабочей редакцией законопроекта не предусматривает предварительного получения лицензий или разрешений, кроме случаев добровольной аккредитации. Лицензированию подлежит разработка, производство, сертификационные испытания, тематические исследования, экспертиза, а также ввоз, вывоз средств цифровой подписи для коммерческой эксплуатации.

В зависимости от статуса физических и юридических лиц – участников информационного обмена, возможны три схемы правовых взаимоотношений с использованием ЭЦП.

1. Государственные органы и организации используют надежные средства ЭЦП и усиленные сертификаты, выданные аккредитованными ЦСК.

2. Другие юридические и физические лица кроме вышеуказанной схемы используют механизмы ЭЦП на основе сертификатов ключей, которые формируются не аккредитованным ЦСК.

3. Без использования услуг ЦСК.

В последних двух случаях правовые взаимоотношения регулируются на основе договоров, в которых оговаривается признание юридической силы электронного документа, подписанного одним из вышеуказанных способов.

Ряд норм законопроекта не являются нормами прямого действия и предусматривают регулирование отдельных сфер в области ЭЦП подзаконными нормативно-правовыми актами, а именно – устанавливаются нормативными актами Кабинета Министров Украины. Это, например, случаи, когда ЭЦП не может использоваться, особенности использования ЭЦП органами государственной власти и органами местного самоуправления, порядок аккредитации центров сертификации ключей и требования, которым они должны отвечать, порядок предоставления услуг цифровой подписи аккредитованным ЦСК государственным органам власти и т. п.

Законопроект также устанавливает права и обязанности сторон. Основной обязанностью лица, которое подписывает электронный документ, является сохранение конфиденциальности информации, на основе которой формируется электронная подпись, т. е. личного (секретного) ключа. При этом, в случае утраты контроля над этим ключом оно должно немедленно поставить об этом в известность ЦСК.

С целью повышения и усовершенствования уровня услуг, а также международного признания цифровой подписи предусмотрены механизмы добровольной аккредитации центров сертификации ключей, а также создание системы, которая осуществляет процедуру аккредитации и надзор за работой аккредитованных ЦСК. Данные нормы основываются на соответствующих требованиях Директивы ЕС, где говорится, что каждая страна – член ЕС должна обеспечить создание соответствующей системы для осуществления надзора за деятельностью поставщиков услуг по сертификации, которые созданы на территории этой страны и осуществляют выдачу квалификационных сертификатов населению.

Таким образом, определяются два типа поставщиков услуг в сфере ЭЦП – центр сертификации ключей и аккредитованный центр сертификации ключей. Центром сертификации ключей может быть юридическое или физическое лицо – субъект предпринимательской деятельности, который удостоверил свой открытый ключ в органе технического управления сферы ЭЦП – центральном удостоверяющем органе. К таким центрам в законопроекте не выдвигается практически никаких требований. При этом юридическая сила цифровой подписи, проверенной с использованием сертификата ключа, который сформирован центром сертификации ключей, а также при помощи ненадежных средств ЭЦП, не может быть опровергнута.

Аккредитованному центру сертификации ключей, т. е. центру сертификации, который прошел добровольную процедуру аккредитации, подтверждающую способность данного центра выполнять взятые на себя обязанности, детально определены права и обязанности.

В соответствии с требованиями проекта Закона центры сертификации ключей несут ответственность за невыполнение своих обязанностей перед юридическими и физическими лицами согласно законодательству Украины. В некоторых аналогичных иностранных законодательных актах предусмотрена финансовая ответственность центров сертификации перед своими клиентами и третьими лицами за несоответствующее выполнение своих обязанностей. Возможно, одним из требований к аккредитованному ЦСК будет обязательное наличие страховой суммы определенного размера, которая даст возможность гарантировать способность центров сертификации ключей нести финансовую ответственность перед третьими лицами вследствие невыполнения требований законодательства в сфере ЭЦП.

Законопроектом не предусматривается ограничение центров сертификации ключей относительно возможности генерации открытых и личных (закрытых) ключей пользователям. Ключи могут генерироваться самим пользователем или по его желанию в центре сертификации ключей. В то же время хранение личных ключей клиентов и ознакомление с ними в центре сертификации ключей запрещается.

Центры сертификации ключей могут предоставлять дополнительные услуги в сфере ЭЦП, которые не противоречат требованиям проекта Закона, например, выступать в роли арбитра в спорных вопросах, предоставлять свои средства цифровой подписи или свои технические площадки для формирования/проверки клиентами цифровой подписи и т. д.

Конечные пользователи могут обладать любым количеством сертификатов, имеющих одинаковое или различное юридическое значение в зависимости от правоспособности их обладателя в отношениях, в которых они используются.

В проекте Закона определяется и контролирующий орган в сфере ЭЦП – специально уполномоченный центральный орган исполнительной власти в сфере криптографической защиты информации, который проверяет выполнение ЦСК требований законодательства в сфере ЭЦП центральным удостоверяющим органом, а также отвечает за оценку соответствия средств цифровой подписи установленным требованиям.

В целом, проект Закона получился более либеральным, чем, например, аналогичный российский закон, который не предусматривает другие виды электронной подписи, кроме как ЭЦП, жестко регламентирует деятельность по предоставлению услуг в сфере ЭЦП, предусматривает обязательное лицензирование деятельности по предоставлению услуг в сфере цифровой подписи. Законопроект не устанавливает практически никаких требований к деятельности не аккредитованных центров сертификации ключей относительно предоставления услуг физическим и юридическим лицам. В то же время четко определяются права и обязанности аккредитованных центров сертификации ключей, порядок отмены, блокирование и возобновление усиленных сертификатов.

УДК 681.3

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ВОПРОСЫ ПОСТРОЕНИЯ И ФУНКЦИОНИРОВАНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ ЭЦП

Даниил Мялковский, Алексей Скиба
ДСТСЗИ СБ Украины

Анотація: **Розглядаються деякі організаційно-технічні аспекти побудови та функціонування національної системи електронного цифрового підпису, в тому числі структура системи, функції та обов'язки її суб'єктів, питання стандартизації і сумісності форматів даних, криптографічних протоколів тощо.**
Summary: **In this article are considered some organizing-technical aspects of the building and operating the national system of the electronic digital signature, including structure of the system, functions and duties its subject, questions to standardizations and compatibility data format, cryptographic protocol and etc.**
Ключові слова: **Електронний цифровий підпис, сертифікат ключа, центр сертифікації ключів, центр реєстрації, загальнодоступний каталог, національна інфраструктура відкритих ключів, центральний засвідчувальний орган, засвідчувальний центр.**

Оставляя в стороне вопросы юридического характера, связанные с правовыми вопросами использования электронной цифровой подписи (ЭЦП), рассмотрим некоторые технические аспекты национальной инфраструктуры с открытым ключом (НИОК), в частности общую технологию функционирования, взаимодействие в этой инфраструктуре конечных пользователей с поставщиками услуг ЭЦП, а также вопросы стандартизации и совместимости различных криптографических приложений и протоколов.

Анализ этих вопросов основывается на редакции проекта закона "Об электронной цифровой подписи", принятого в первом чтении, тексте законопроекта, подготовленного для вынесения на последующее чтение, а также общей технологии применения цифровой подписи в глобальных сетях с неограниченным количеством пользователей.

В основе использования механизмов ЭЦП на основе асимметричных криптографических преобразований лежат открытые и секретные ключи. Как известно, секретный ключ используется для наложения цифровой подписи, открытый – для ее проверки. В силу тех или иных причин требуется их смена, отзыв, распределение и т. д. Если речь идет о нескольких пользователях небольшой организации, то эти операции, как правило, совершаются "вручную" администратором системы безопасности. Если же пользователей сотни и более, то процесс управления ключами становится очень сложным и громоздким. Вероятность ошибок в таком случае сильно возрастает, что непременно приведет к снижению уровня безопасности в целом. Когда же речь идет о больших корпоративных и глобальных сетях, где имеют место тысячи и более пользователей, которые зачастую не имеют личного контакта или гарантированного безопасного канала обмена открытыми ключами, организовать процесс управления ключами "вручную" практически невозможно. Для решения этих проблем требуется создание специальной системы или инфраструктуры поддержки управления ключами, в основе которой лежит независимый специальный субъект, ответственный за управление ключами в общей инфраструктуре (в терминах законопроекта – центр сертификации ключей).

Общепринятым названием этой системы, которое используется в иностранной литературе, является инфраструктура открытых ключей (Public Key Infrastructure).

Инфраструктура открытых ключей (ИОК) представляет собой комплекс программно-аппаратных средств и организационно-технических мероприятий, необходимых для использования асимметричных криптографических схем в прикладных сферах, где могут использоваться механизмы ЭЦП.

Таким образом, основной целью создания и функционирования ИОК является обеспечение безопасного обмена открытыми ключами между участниками электронного взаимодействия.

Структурно ИОК состоит из субъектов и объектов, а также нормативных документов, которые регламентируют порядок работы субъектов и использование объектов ИОК (политика сертификации, политика безопасности, профайл (формат) сертификата и списков отозванных сертификатов и т. д.). К субъектам относятся центры сертификации ключей, центр регистрации, общедоступные каталоги или сетевые справочники, конечные пользователи. К объектам – сертификат ключа, документ (может быть в электронном или бумажном виде), который однозначно связывает определенное лицо (владельца сертификата) и его открытый ключ, подписанный ЭЦП независимой третьей стороной в информационном