2012 Математические методы криптографии №3(17)
DOI 10.17223/20710410/17/7
УДК 004.34

О СОДЕРЖАНИИ ПОНЯТИЯ «ЭЛЕКТРОННАЯ ПОДПИСЬ»

А. В. Черемушкин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: avc238@mail.ru

Сравниваются подходы к определению понятия и стандартизации электронной подписи в нашей стране и Евросоюзе.

Ключевые слова: *электронная подпись, цифровая подпись.*

8 апреля 2011 г. вступил в силу Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [1] (далее ФЗ). В нём введены новые для российского нормативного регулирования технические понятия усиленной и квалифицированной электронной подписи, квалифицированного сертификата и др.

Поскольку данная терминология заимствована из зарубежных технических стандартов, то представляет интерес сравнить содержание данных понятий в западном и российском нормативном и техническом регулировании.

Наиболее проработанными эти вопросы являются в документах Евросоюза, поэтому остановимся на применяющихся там подходах.

1. Определение электронной подписи

Основным исходным документом для стран Евросоюза в этой области является Директива 1999/93/ЕС Европейского парламента и совета от 13 декабря 1999 г. о порядке использования электронных подписей в Европейском сообществе [2] (далее Директива).

Электронная подпись (ЭП) определяется в Директиве как данные в электронной форме, которые добавлены либо логически ассоциированы с другими данными в электронной форме и служат методом аутентификации этих данных.

Это соответствует расширенному пониманию термина ЭП в международных правовых документах, где в качестве ЭП могут выступать биометрические данные, запись голоса, фото, пароли или другие данные, которые можно использовать для определения лица, подписавшего электронный документ. Сюда же попадают и коды аутентичности сообщений, применяемые в системах с симметричными ключами для защиты от навязывания или подмены передаваемых данных. Использование термина «электронная подпись» не привязано к какой-либо технологии. Могут применяться не только асимметричные, но и симметричные криптографические системы, а также системы, вообще не использующие криптографические алгоритмы.

Сразу следует заметить, что понятие «электронная подпись» предназначено, в основном, для юридического использования, в том смысле, что использование этого термина предполагает фактическое соответствие установленным юридическим нормам. Поэтому Директива, фактически, вводит юридическую категорию, определяющую рамки применения и юридической значимости для различных технологий подписи, верификации, подтверждения и принятия цифровых электронных данных.

ЭП может выступать в качестве основного механизма для реализации различных сервисов безопасности. Приведём технические определения некоторых сервисов безопасности из международных стандартов:

— *Аутентификация*: обеспечение гарантий идентичности предъявленной сущности [ISO/IEC 10181-2].
— *Аутентификация источника данных*: подтверждение подлинности источника полученных данных [ISO 7498-2].
— *Аутентификация сторон*: подтверждение того, что взаимодействующая сторона является той, за которую себя выдаёт [ISO 7498-2].
— *Целостность данных*: свойство, означающее, что данные не были модифицированы или уничтожены неавторизованным образом [ISO 7498-2].
— *Отрицание* (*отречение*) (*Repudiation*): отрицание одним из участвующих в коммуникации субъектов своего участия во всей или части коммуникации [ISO 7498-2].
— *Невозможность отрицания авторства* (*Non-repudiation of origin*): этот сервис предназначен для защиты от отрицания автором факта создания или отправления им сообщения [ISO/IEC 13888-1].
— *Невозможность отрицания* (*Non-repudiation*): этот сервис предназначен для сбора, обработки и обоснования неопровержимой очевидности информации, касающейся предъявленного события или действия, с целью разрешения спора о том, что событие или действие имело место в реальности [ISO/IEC 10181-4].

Заметим, что в определении ЭП не уточняется, о каком типе аутентификации идёт речь. Обычно различают два важных случая: аутентификацию источника данных и аутентификацию сторон. Если первая относится к случаю передачи подписанного сообщения с последующей отложенной проверкой подписи, то вторая выполняется в режиме on-line в рамках протокола идентификации.

Применение подписи для обеспечения целостности гарантирует, что все изменения в передаваемых данных будут обнаружены независимо от того, чем они вызваны — ошибками при передаче или целенаправленным воздействием противника в канале.

Целостность данных, взаимная аутентификация сторон и аутентификация источника представляют примеры сервисов безопасности, которые исчерпывающе описываются техническими определениями в стандартах. Для того чтобы гарантировать выполнение данных свойств, достаточно обеспечить правильную техническую реализацию. При этом соответствие требованиям законов и нормативных документов основано на научной и технологической очевидности проверки:

а) является ли подпись аутентичной, т. е. она соответствует конкретному человеку и не подделана;

б) являются ли подписываемые данные оригинальными, т. е. они соответствуют данным, представленным подписывающему, и они не были изменены.

Стандарты ISO 7498-2 и ISO/IEC 13888-1 определяют несколько типов сервиса «невозможность отрицания». Общее определение сервиса дано в ISO/IEC 10181-4. То, которое обычно ассоциируется с ЭП, называется «невозможность отрицания авторства». Если пользоваться этим определением, то следует помнить, что «отрицание автором факта создания или отправления им сообщения» относится, как правило, только к самой подписи, а не обязательно к исходному подписанному сообщению.

Невозможность отрицания является более сложным сервисом, и поэтому технологические решения должны дополняться нормативными требованиями. Термин «невозможность отрицания» в нормативном применении относится не столько к самой подписи, сколько к словесным декларациям и поведению. Юридически невозможность отрицания факта подписи обеспечивается:

а) соответствующим законом (для открытых систем), и/или

б) соглашением (для специальных систем, которые могут быть открытыми или закрытыми в зависимости от их политики).

Элементы нормативного регулирования невозможности отрицания также различаются в зависимости от функции подписи и от типа подписываемого документа/данных. Они могут быть подразделены на три типа [3]:

а) несемантические (т. е. чисто технические) элементы (например, аутентичность, целостность);

б) контекстуальные или семантические элементы, являющиеся предметом как технического, так и семантического рассмотрения (типа знание, преднамеренность, намерение, понимание, интерпретация, принуждение, ошибка, ложь, невозможность действия и т. п.);

в) чисто нормативные элементы (типа легальная валидность/невалидность, способность/неспособность, полномочие).

Чисто технический подход к определению невозможности отрицания, проведённый без рассмотрения учёта нормативных вопросов, введённых законом или контрактным соглашением, может приводить к заблуждению и неприменим для человеческих поступков. Как показывает пример заключения двустороннего контракта, даже если с технической точки зрения все очевидно, то сторонам может быть недостаточно информации для окончательного заключения контракта.

2. Технологии электронной подписи

Рассмотрим основные технологии, позволяющие реализовать ЭП.

Цифровая подпись. Стандарт ISO 7498-2:1989 определяет *цифровую подпись* как данные, присоединённые к набору данных либо являющиеся результатом криптографического преобразования исходного набора данных и позволяющие получателю подтвердить подлинность источника и целостность набора данных и обеспечить защиту против подделки, например, со стороны получателя.

Различают цифровые подписи без восстановления сообщения (когда подпись присоединяется с помощью конкатенации к исходному набору данных) и с восстановлением сообщения (когда передается одна подпись, а исходный набор данных получается в результате обратного преобразования).

Термин «цифровая подпись» предполагает наличие двух алгоритмов — для вычисления и проверки цифровой подписи, обычно называемых в математике схемой цифровой подписи [4]. Алгоритм вычисления цифровой подписи должен быть секретным, чтобы исключить возможность вычисления правильного значения подписи (например, определяться закрытым ключом), и зависеть от всех подписываемых данных. Алгоритм проверки — открытым для гарантирования возможности проверки подписи любым из участников без знания какой-либо закрытой информации.

Такое определение позволяет применять его в самых различных контекстах, например для защищённых систем передачи информации и автоматизированных систем, контролирующих работу удалённых объектов, функционирующих полностью в автоматическом режиме.

Цифровая подпись позволяет осуществить аутентификацию источника данных и обеспечить их целостность, а при взаимодействии людей — обеспечивает ещё и невозможность отрицания от авторства. Причём это — единственная технология, которая решает сразу три проблемы.

Использование термина «подпись» в данном контексте оправдано тем, что цифровая подпись имеет много общего с обычной собственноручной подписью на бумажном

документе. Собственноручная подпись также решает перечисленные выше задачи, однако между обычной и цифровой подписями имеются существенные различия. Сведём основные различия между обычной и цифровой подписями в таблицу (табл. 1).

Таблица 1

Сравнение цифровой и собственноручной подписи

Собственноручная подпись	*Цифровая подпись*
Не зависит от подписываемого текста, всегда одинакова	Зависит от подписываемого текста, разная для различных текстов
Неразрывно связана с подписывающим лицом, однозначно определяется его психофизическими свойствами, не может быть утеряна	Определяется секретным ключом, принадлежащим подписывающему лицу, который может быть утерян владельцем
Неотделима от носителя (бумаги), поэтому отдельно подписывается каждый экземпляр документа	Легко отделима от документа, поэтому верна для всех его копий
Не требует для реализации дополнительных механизмов	Требует дополнительных механизмов, реализующих алгоритмы её вычисления и проверки
Не требует создания поддерживающей инфраструктуры	Требует создания доверенной инфраструктуры сертификатов открытых ключей
Не имеет срока давности	Имеет ограничения по сроку действия

Надёжность схемы цифровой подписи оценивается сложностью решения следующих задач:

— *подделка подписи*, то есть нахождение значения подписи под заданным документом лицом, не являющимся владельцем секретного ключа;
— *подделка документа*, то есть модификации подписанного сообщения без знания секретного ключа;
— *подмена сообщения*, то есть подбор двух различных сообщений с одинаковыми значениями подписи без знания секретного ключа;
— *генерация подписанного сообщения*, то есть нахождение хотя бы одного сообщения с правильным значением подписи без знания секретного ключа.

Защита от данных атак обеспечивается выбором схемы цифровой подписи, обладающей соответствующими криптографическими свойствами.

Приведённое выше определение не ограничивает цифровую подпись применением только одной технологии асимметричных криптосистем, хотя эта технология и является сегодня доминирующей.

При использовании асимметричных криптосистем цифровая подпись не позволяет:

— знать владельца открытого ключа;
— знать, что закрытый ключ во время создания подписи находился у владельца закрытого ключа подписи.

Для достижения первого свойства приходится создавать инфраструктуру (сертификатов) открытых ключей. Второе обычно достигается введением информации о статусе сертификата с помощью проставления токенов с временны́ми штампами или временны́ми метками. Токены с временны́ми штампами представляют собой структуру данных, содержащую доверенную временную метку и подписанную специальным центром временных штампов. Временна́я метка — это запись в файле аудита, включающая доверенное значение времени и хешированное представление даты.

Поэтому для реализации схемы цифровой подписи, как правило, используют либо системы с открытыми ключами, что соответственно приводит к необходимости созда-

вать инфраструктуру (сертификатов) открытых ключей и центры временных штампов, либо прибегают к использованию услуг третьей стороны — доверенного центра, выступающего посредником в процедурах подписания и проверки подписи.

При этом должны выполняться два условия — временна́я метка и токен с временны́м штампом должны соответствовать периоду действия, указанному в сертификате, и сам сертификат не должен быть аннулирован.

Код аутентичности сообщения. Представляет собой значение некоторой определяемой ключом хеш-функции, вычисленное для данного сообщения [4]. Является разновидностью симметричных криптографических систем, поскольку у подписывающего и проверяющего ключи должны быть одинаковыми.

Позволяет проверить целостность и аутентифицировать источник данных и отправителя, так как получатель может убедиться в том, что это сообщение, помимо него самого, мог создать и отправить только отправитель, обладающий тем же ключом. В то же время код аутентичности не может обеспечить невозможность отрицания авторства отправителем, так как получатель не сможет доказать третьей стороне, что он не сам создал подписанное сообщение.

3. Виды подписей

На практике встречаются самые различные системы ЭП. Требования к типу ЭП во многом зависят от условий применения, которые, в свою очередь, влияют на процессы формирования и проверки (верификации) подписи.

Условия проведения верификации подписи и соответственно данных, ассоциированных с подписью, могут значительно различаться в зависимости от назначения и предполагаемого жизненного цикла подписи. Так, в [5] выделены следующие типы подписи в зависимости от особенностей процесса её верификации:

— одноразовые подписи (ephemeral signature): подписи, значения которых не нужно сохранять после проведения верификации;
— краткосрочные подписи (short term signatures): подписи, верификацию которых необходимо проводить только в период срока годности сертификата;
— долговременные подписи (long term signatures): подписи, верификацию которых необходимо проводить не только в период срока годности сертификата владельца ключа подписи, но, возможно, даже и после окончания срока полномочий выдавшего сертификат удостоверяющего центра.

В [3] сформулированы четыре основных функции электронной подписи:

— подпись для идентификации — соответствует аутентификации сторон, не связана ни с каким документом, обеспечивает доказательство владения закрытым ключом в протоколе идентификации;
— подпись для аутентификации — соответствует аутентификации источника данных, в которых данные представляются как объект, а не как документ с определённым семантическим содержанием;
— подпись для декларации знания — предназначена для обеспечения аутентификации источника данных, причём данные имеют семантическое значение, но никак не связаны с намерениями;
— подпись для декларации намерения — обеспечивает невозможность отрицания событий или действий. Относится к специальным наборам данных и требует чёткой интерпретации содержания данных и наличия контекста для процесса создания подписи.

Директива устанавливает, фактически, три вида подписи: усиленная квалифицированная, усиленная неквалифицированная и не являющаяся усиленной (в российских документах называемая «простой»).

3.1. Усиленная ЭП

Согласно Директиве, усиленная электронная подпись должна удовлетворять следующим требованиям:

a) она однозначно связана с лицом, подписавшим данные;

b) с её помощью можно подтвердить подлинность лица, подписавшего данные;

c) она создана с использованием средств, которые находятся под единоличным контролем лица, подписавшего данные, и

d) она связана с данными, которым она соответствует, таким способом, что с её помощью можно обнаружить любые последующие изменения подписанных данных.

Таким образом, здесь говорится о выполнении свойств однозначной аутентификации источника и обеспечения целостности. Как известно, эти свойства могут быть обеспечены только применением схемы цифровой подписи. Дело в том, что коды аутентификации сообщений, основанные на симметричных криптографических алгоритмах, создают электронную подпись, которая не является усиленной, поскольку ключом создания подписи обладают две стороны (нарушено условие a). Применение некриптографических методов позволяет только указать на лицо, подписавшее данные, не обеспечивая ни аутентификации источника, ни целостности, ни невозможности отрицания.

В то же время, как отмечается в [3], пользоваться таким определением чрезвычайно трудно, так как оно слишком широко и не привязано ни к какой конкретной технологии. Поэтому в случае спора экспертам надо проверить выполнение каждого из четырёх требований.

Условие a можно выполнить, вводя квалифицированные либо неквалифицированные X509 сертификаты, которые должны выпускаться либо доверенной третьей стороной, либо самим подписывающим лицом. Условие b проверяется по сертификату. Условие c реализуется применением специальных средств для вычисления и проверки подписи, представляющих собой независимые защищённые устройства, удовлетворяющие требованиям безопасности. Для выполнения условия d обычно применяют хеш-функции с достаточной длиной ключа.

Усиленная подпись удовлетворяет всем свойствам цифровой подписи из табл. 1, за исключением создания инфраструктуры сертификатов открытых ключей, вместо которой необходимо разработать нормативные документы, регулирующие конфликтные ситуации, связанные с возможностью отрицания факта создания подписи.

В ФЗ определение усиленной неквалифицированной ЭП (п. 3 ст. 5) получено усреднением двух определений — усиленной подписи из Директивы и цифровой подписи из международного стандарта ISO 7498-2: 1989:

1) она получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) она позволяет определить лицо, подписавшее электронный документ;

3) она позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

4) она создаётся с использованием средств электронной подписи.

Здесь в целом говорится о том же самом, но изменённая формулировка первого пункта приводит к существенному отличию: если в формулировке Директивы усло-

вия *a*, *b* и *d* могут быть выполнены только при использовании цифровой подписи на основе асимметричных криптографических систем, то под определение, приведённое в ФЗ, подпадают ещё и коды аутентификации сообщений. Кроме того, формулировка второго пункта некорректна — подпись не позволяет определить лицо, а подтверждает подлинность определённого лица. Наконец, при таком подходе не делается различия между усиленной и неквалифицированной подписями.

3.2. Квалифицированная подпись

Главная цель Директивы — унификация правил использования электронной подписи и наиболее общая формулировка условий, необходимых для признания юридической равнозначности электронной и собственноручной подписей. На основе анализа законов, принятых в различных странах мира, в Директиве закреплены наиболее существенные моменты. Они сформулированы в ст. 5 Директивы: необходимо использовать усиленную электронную подпись, которая должна быть основана на квалифицированном сертификате и сформирована с помощью защищённого устройства создания подписи. По сути, это — определение квалифицированной электронной подписи, хотя в Директиве этот термин и не вводится. Он появляется только в стандарте CWA 14167 со ссылкой на Директиву. В ст. 5 Директивы утверждается, что такая электронная подпись удовлетворяет всем требованиям к подписи под данными в электронной форме, позволяющим считать её равносильной собственноручной подписи на бумаге.

В Приложениях I – IV к Директиве приведены соответственно:

- требования, предъявляемые к квалифицированным сертификатам;
- требования к службе CSP, выпускающей квалифицированные сертификаты;
- требования, предъявляемые к защищённым устройствам создания электронной подписи;
- рекомендации для безопасной верификации подписи.

В Директиве вводятся формальные определения понятий квалифицированного сертификата, провайдера служб сертификатов и защищённого устройства создания подписи:

- *Квалифицированный сертификат* (Qualified Certificate, QC) — сертификат, удовлетворяющий требованиям, сформулированным в Приложении I, созданный провайдером сертификационных услуг, удовлетворяющим требованиям, сформулированным в Приложении II Директивы.
- *Провайдер сертификационных услуг* (Certification-Service-Provider, CSP) — организация (entity), либо юридическое или физическое лицо, которая выпускает сертификаты либо обеспечивает другие сервисы, связанные с электронной подписью.
- *Защищённое устройство создания подписи* (Secure-Signature-Creation Device, SSCD) — сконфигурированное программное или аппаратное устройство создания подписи, которое удовлетворяет требованиям, сформулированным в Приложении III Директивы.

Таким образом, чтобы удостовериться в том, что подпись квалифицированная, получатель должен убедиться, что:

a) сертификат является квалифицированным (удовлетворяет требованиям Приложения I Директивы);

b) провайдер служб сертификатов удовлетворяет требованиям Приложения II Директивы;

c) технология, использованная для формирования подписи, является безопасной (удовлетворяет требованиям Приложения III Директивы);

d) верификация подписи выполнена в соответствии с требованиями Приложения IV Директивы (в частности, проверено, что в сертификате указана политика QC + SSCD и данные для формирования подписи хранятся в устройстве SSCD).

Аналогичный подход принят в п. 1 ст. 6 ФЗ: «Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, кроме случая, если федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе». В ст. 11 ФЗ приведены условия признания квалифицированной электронной подписи.

Однако можно заметить, что в п. 4 ст. 6 ФЗ вводится немного изменённое определение понятия квалифицированной электронной подписи: «Квалифицированной электронной подписью является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и двум дополнительным признакам:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом».

Заметим, что в европейских документах неквалифицированная электронная подпись — это усиленная, но не квалифицированная, а согласно приведённому выше определению из ФЗ, усиленная и неквалифицированная электронная подписи совпадают, причём квалифицированная электронная подпись является частным случаем неквалифицированной электронной подписи.

3.3. Простая электронная подпись

Согласно п. 2. ст. 5 ФЗ, «простой электронной подписью является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт создания электронной подписи определённым лицом». Такое определение не вносит ясности в понимание того, чем может являться простая электронная подпись и какие технологии допустимы для её реализации, тем более что все последующие уточнения касаются только квалифицированной подписи.

Различные виды таких подписей обсуждаются в работе [6], где отмечается, что в западном законодательстве введение понятия простой подписи было обусловлено её широким использованием на ранних этапах развития технологий. Поэтому автор [6] выражает недоумение, зачем надо в нашей стране реанимировать устаревшие технологии, которые, к тому же, не обеспечивают выполнения свойств невозможности отрицания, а в отдельных случаях — и обеспечения целостности документов.

Формального определения простой электронной подписи не существует. В [3] эта ситуация обсуждается путем логического перебора возможных ситуаций, приводящих к нарушению имеющегося формального определения квалифицированной подписи. Множество подписей, которые не являются квалифицированными и поэтому не могут быть признаны равнозначными собственноручной подписи, распадается на два класса: усиленные и не являющиеся усиленными (в ФЗ они названы «простыми»). Такой подход к определению (через отрицание) предполагает, что к этим классам можно отнести те электронные подписи, которые хотя и имеют электронную форму, но не удовлетворяют основным условиям квалифицированной подписи, то есть для них не выполнено хотя бы одно из условий a, b или c определения квалифицированной подписи.

Рассмотрим два важных случая.

Подписи, не основанные на квалифицированном сертификате. Если сертификат не является квалифицированным, например используется PGP, то проверяющий не сможет доказать, что автором подписи является именно данный субъект. Тем не менее, как показывают следующие примеры, такие системы широко применяются.

При аутентификации источника данные для проверки подписи содержатся в сертификате, заверенном некоторым центром сертификации. Поэтому из признания сертификатов этого центра вытекает доверие к результату проверки электронной подписи, хотя она и не может быть признана равносильной собственноручной подписи.

Если подпись получена с помощью защищённого устройства создания подписи, то обеспечено условие целостности, хотя и не ясно, кто подписал документ. В некоторых случаях, когда не важно, кто подписал документ, а имеет значение только его целостность, такая электронная подпись может оказаться достаточной.

Наконец, в системах групповой подписи для проверяющего не важно, кто из участников группы подписал документ. Главное — он может убедиться в том, что подпись сделана кем-то из участников этой группы от её имени.

Подписи, не созданные защищённым устройством создания подписи. Если средство создания подписи не является защищённым (не выполнены условия Приложения III Директивы), то подпись может быть как простой, так и усиленной (профиль защиты для таких устройств приведён в [7]). В этом случае можно гарантировать целостность данных и аутентификацию источника, но нельзя обеспечить невозможность отрицания. Иногда этого бывает достаточно. Например, если в системе внутреннего защищённого документооборота, обладающей достаточно высокой защищённостью, для формирования подписи используются идентификационные пластиковые карты, то, хотя сами карты могут и не удовлетворять всем требованиям к защищённым устройствам создания подписи, защита подписи от отрицания будет высокой.

3.4. Условия признания простой и неквалифицированной подписи равнозначной собственноручной подписи

В п. 3 ст. 6. ФЗ установлено, что «информация в электронной форме, подписанная простой электронной подписью или неквалифицированной электронной подписью, признаётся электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в случаях, установленных федеральными законами, принимаемыми в соответствии с ними нормативными правовыми актами или соглашением между участниками электронного взаимодействия. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных неквалифицированной электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны предусматривать порядок проверки электронной подписи. Нормативные правовые акты и соглашения между участниками электронного взаимодействия, устанавливающие случаи признания электронных документов, подписанных простой электронной подписью, равнозначными документам на бумажных носителях, подписанным собственноручной подписью, должны соответствовать требованиям ст. 9 настоящего Федерального закона».

Далее в ст. 9 установлено, что электронный документ считается подписанным простой электронной подписью при выполнении в том числе одного из следующих условий: либо электронная подпись «содержится в самом электронном документе»; либо она получена в результате криптографического преобразования, причём ключ «применяется в соответствии с правилами, установленными оператором информационной

системы, с использованием которой осуществляются создание и (или) отправка электронного документа, и в созданном и (или) отправленном электронном документе содержится информация, указывающая на лицо, от имени которого был создан и (или) отправлен электронный документ».

При этом как для неквалифицированной, так и для простой электронной подписи должны быть разработаны нормативные правовые акты и (или) соглашения между участниками электронного взаимодействия, в которых должны быть оговорены указанные в ФЗ существенные моменты применения таких электронных подписей.

4. Стандартизация технических требований

В основу Директивы положены следующие принципы:

— отказ от дискриминации электронной подписи перед законом;
— признание необходимости информационной защищённости подписи;
— возможность признания квалифицированной электронной подписи как юридически значимой.

Директива определяет следующие правила признания квалифицированной электронной подписи:

— квалифицированная электронная подпись не является синонимом юридически значимой подписи;
— невыполнение требований к квалифицированной электронной подписи не означает отказ от принятия подписи к рассмотрению её юридической значимости;
— выполнение требований к квалифицированной электронной подписи является одним, но не единственными требованием, дающим возможность приравнять электронную подпись к собственноручной подписи.

Технические требования к квалифицированной электронной подписи, сформулированные в Приложениях I – IV, в дальнейшем уточняются и дополняются в многочисленных стандартах серии CWA и ETSI, составляющих нормативную базу разработки, внедрения и использования квалифицированной подписи (см. рис. 1, взятый из работы [8]).

Аббревиатурой CWA (сокр. от CEN Workshop Agreement) обозначается документ, выпущенный Европейским комитетом по стандартизации CEN (Comite Europeende Normalisation (European Committee for Standardization)). Это неофициальный стандарт от независимой организации.

Для электронной подписи основными являются следующие CWA, признаваемые в качестве технических стандартов, соответствующих Директиве, и формулирующие требования по безопасности для доверенных систем управления сертификатами электронных подписей:

— CWA 14167-1: Требования к безопасности системы [9];
— CWA 14167-2: Криптографический модуль CSP для операций подписи с восстановлением — Профиль безопасности [10];
— CWA 14167-3: Криптографический модуль CSP для служб генерации ключей — Профиль безопасности [11];
— CWA 14167-4: Криптографический модуль CSP для операций подписи — Профиль безопасности [12];
— CWA 14169: Защищённое средство создания подписи уровня 'EAL 4+' [13].

В соответствии со стандартом CWA 14167 доверенная система (Trustworthy Systems, TWS) для работы с квалифицированными (QC) и неквалифицированными

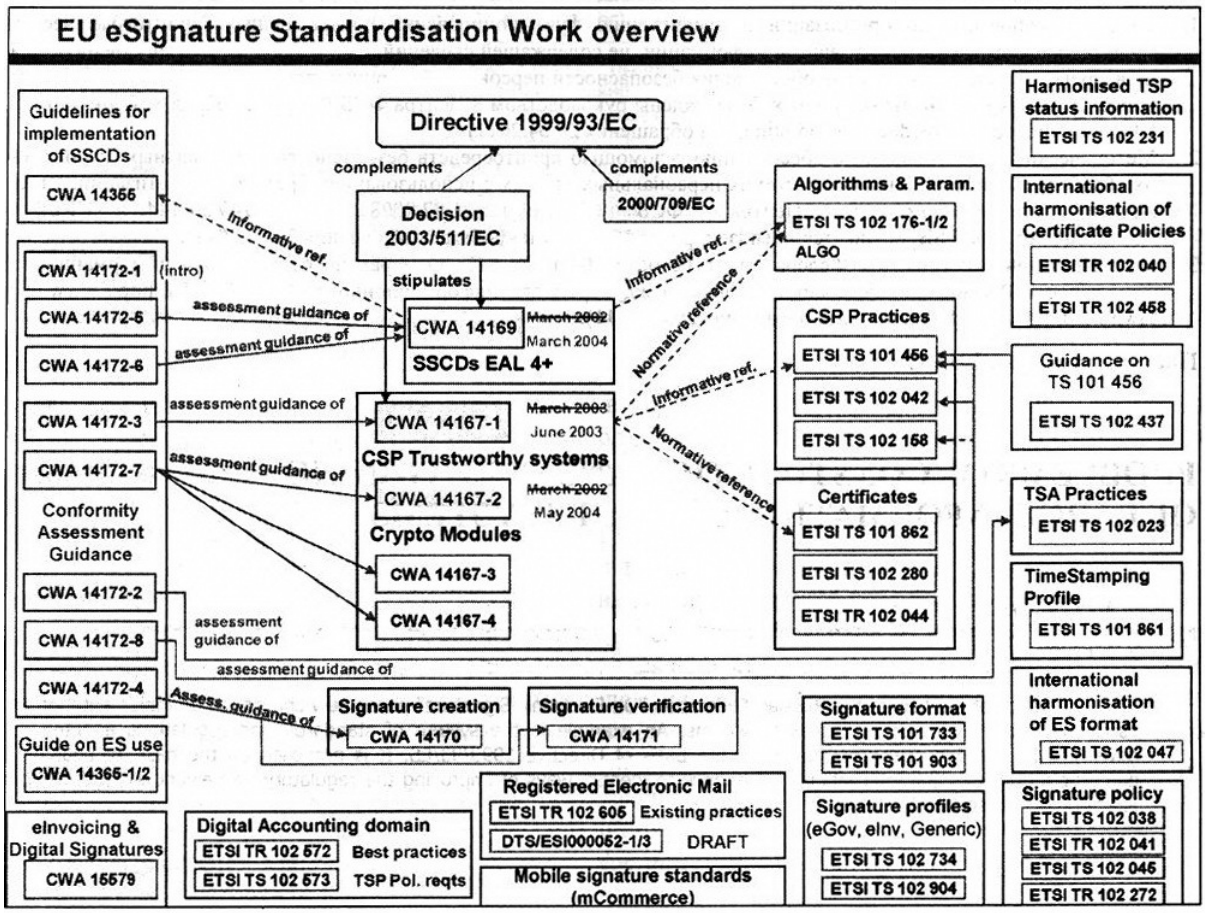

Рис. 1. Стандарты Евросоюза, составляющие нормативную базу разработки, внедрения и использования квалифицированной подписи

(NQC) сертификатами должна включать реализации основных (Core Services) и дополнительных (Supplementary Services) служб.

Основными службами являются:

— служба регистрации (Registration Service) — осуществляет проверку идентичности и, если это необходимо, других специфических атрибутов субъекта;
— служба генерации сертификатов (Certificate Generation Service) — создаёт сертификаты;
— служба распространения (Dissemination Service) — представляет сертификаты и информацию политики безопасности субъектам и доверенным сторонам;
— служба управления отзывом сертификатов (Revocation Management Service) — осуществляет обработку запросов по отзыву сертификатов;
— служба состояния аннулирования (Revocation Status Service) — предоставляет доверенным сторонам информацию о текущем состоянии списка аннулированных сертификатов.

Дополнительными службами являются:

— служба снабжения субъектов устройствами (Subject Device Provision Service) — осуществляет подготовку и снабжение субъектов устройствами создания подписи (SCDev). Включает снабжение защищёнными устройствами создания подписи (SSCD);

— служба штампов времени (Time-stamping Service) — осуществляет простановку меток времени, которые могут понадобиться в процессе проверки подписи.

Стандартом CWA 14169 [13] предусмотрено три варианта построения защищённого устройства создания подписи, соответствующего уровню адекватности EAL 4+:

— т и п 1: специальное устройство для генерации данных для создания и проверки подписи (ключей), которое может управляться только специально выделенным авторизованным лицом (например, системным администратором);
— т и п 2: персональное устройство для создания и проверки подписи, может использоваться только определённым пользователем (например, владельцем смарт-карты). Требует защищённого канала для ввода данных для создания (ключа создания) подписи;
— т и п 3: персональное устройство, сочетающее функции устройств типа 2 и типа 1 (без экспорта данных для создания подписи), например, реализованное в переносном компьютере.

Требования описанных в этом стандарте профилей защиты относятся только к аппаратной платформе, операционной системе и устройствам создания и проверки подписи и генерации и хранения данных для создания и проверки подписи. В них не конкретизируются способы создания защищённых каналов для передачи ключевой информации и защищённых путей и каналов для передачи подписываемой информации между этими устройствами и использующими их приложениями, описанию которых посвящены стандарты серии ETSI TC.

Стандарты CWA 14167 и 14169 были обновлены в 2004 г. после признания их в ЕС в соответствии с решением комиссии (Commission Decision) от 14 июля 2003 г. [14].

В настоящее время выпущено более 40 других CWA, имеющих дело с электронной подписью (см. рис. 1). Среди них:

— CWA 14170: Требования безопасности для приложений, формирующих подпись [15];
— CWA 14171: Общие требования для верификации электронной подписи [5];
— CWA 14172: Согласованные правила оценки в рамках Европейской инициативы по стандартизации электронной подписи EESSI (European Electronic Signature Standardisation Initiative).

Аббревиатурой ETSI TS (сокр. от European Telecommunication Standards Infrastructure Technical Specification) обозначается документ (техническая спецификация), выпущенный независимой профессиональной организацией ETSI, официально признаваемой Евросоюзом наряду с CEN в качестве Европейской организации по стандартизации (European Standards Organization). Стандарты по электронной подписи серии ETSI разрабатываются техническим комитетом по вопросам электронной подписи и инфраструктурам (TC — Technical Committiee / ESI — Electronic Signatures and Infrastructures). Среди документов, выпущенных ETSI TC/ESI, следует прежде всего отметить технические стандарты, содержащие списки рекомендуемых алгоритмов и параметров для безопасных электронных подписей:

— ETSI TS 102 176-1: Хеш-функции и асимметричные алгоритмы [16];
— ETSI TS 102 176-2: Протоколы защищённых каналов и алгоритмы для средств создания подписей [17].

Цель этих стандартов состоит не в перечислении всех приемлемых алгоритмов и протоколов, а в указании проверенных с точки зрения безопасности и наиболее желательных для использования в схемах усиленных электронных подписей с учётом

достижения интероперабельности, то есть возможности совместимости с наиболее широким спектром приложений. Так, в качестве хеш-функций рекомендовано использовать функции, приведённые в табл. 2, а в качестве схем цифровой подписи — схемы, приведённые в табл. 3. Для каждого варианта «хеш-функция — схема подписи — алгоритм генерации ключей» предложены наиболее подходящие значения параметров в зависимости от предполагаемого срока надёжного использования.

Таблица 2

Рекомендованные хеш-функции

Краткое обозначение	Дата принятия	Нормативная ссылка
sha1	01.01.2001	ISO/IES 10118-3, FIPS Publication 180-2
ripemd160	01.01.2001	ISO/iES 10118-3
sha224	2004	FIPS Publication 180-2
sha256	2004	ISO/IES 10118-3, FIPS Publication 180-2
whirpool	2004	ISO/IES 10118-3,
sha384	31.03.2007	FIPS Publication 180-2
sha512	31.03.2007	FIPS Publication 180-2

Таблица 3

Рекомендованные схемы цифровой подписи

Краткое обозначение	Алгоритмы генерации ключей	Нормативная ссылка
rsa	rsagen1	RFC 3447
dsa	dsagen1	FIPS Publication 180-2, ISO/IES 14888-3:2006
ecdsa-Fp	ecgen1	ANSI X9.62
ecdsa-F2m	ecgen2	ANSI X9.62
ecgdsa-Fp	rsagen1	ISO/IEC 15946-2:2002
ecdsa-F2m	ecgen2	ISO/IEC 15946-2:2002

Вторая часть технического стандарта определяет также список симметричных алгоритмов и протоколов, которые могут использоваться для построения защищённого канала между приложением и защищённым средством создания подписи (SCDev), обеспечивающим как целостность, так и одновременно целостность и конфиденциальность. Такой безопасный канал можно использовать для удалённой загрузки закрытого ключа в средство создания подписей (когда пара ключей не сгенерирована SCDev и необходимо удалённо загрузить в SCDev и личный ключ, и сертификат открытого ключа), удалённого извлечения из него открытого ключа (когда пара ключей сгенерирована средством создания подписи) или/и удалённой загрузки сертификата открытого ключа и связывания его с личным ключом, уже хранимым в средстве создания подписи (когда пара ключей сгенерирована SCDev для удалённой загрузки в SCDev сертификата открытого ключа и необходимо ассоциировать его с ранее сгенерированным личным ключом).

В ФЗ принят другой подход к формированию технических требований, в основе которого лежит передача всех полномочий по формулированию и контролю за выполнением требований по безопасности специальному выделенному федеральному органу исполнительной власти в области обеспечения безопасности, который в соответствии с п. 5 ст. 8:

1) устанавливает требования к форме квалифицированного сертификата;

2) устанавливает требования к средствам электронной подписи и средствам удостоверяющего центра;

3) осуществляет подтверждение соответствия средств электронной подписи и средств удостоверяющего центра требованиям, установленным в соответствии с настоящим Федеральным законом, и публикует перечень таких средств.

Это обусловлено различиями в используемых подходах к стандартизации в Евросоюзе и в нашей стране, связанными с принятием в 2002 г. Федерального закона № 184-ФЗ о техническом регулировании, отменившим с 30.06.2010 г. все государственные стандарты, заменив их на ещё не разработанные специальные технические регламенты (СТР).

Поэтому в соответствии с ФЗ Директором ФСБ России утверждены:

— Требования к средствам электронной подписи и Требования к средствам удостоверяющего центра [18];
— Требования к форме квалифицированного сертификата ключа проверки электронной подписи [19].

В ФЗ и требованиях [18], регламентирующих разработку, производство, реализацию и эксплуатацию средств электронной подписи в Российской Федерации, заложены следующие принципы:

1. Средства электронной подписи (используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи) отнесены к шифровальным (криптографическим) средствам (ФЗ п. 9 ст. 2); средства удостоверяющего центра — программные и/или аппаратные средства, используемые для реализации функций удостоверяющего центра (ФЗ п. 10 ст. 2).

Поэтому на них распространяются требования, закреплённые Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации [20] (Положение ПКЗ-2005).

2. В зависимости от способностей противостоять атакам средства электронной подписи подразделяются на шесть классов: КС1, КС2, КС3, КВ1, КВ2 и КА1 (см. табл. 4) в зависимости от уровней криптографической защиты, определенных в порядке возрастания количества и жесткости предъявляемых к криптосредствам требований, которые точно соответствуют принятым в нашей стране шести типам нарушителей Н1, ..., Н6. Более подробно о методологии создания модели нарушителя см., например, в [21].

В соответствии с уровнем криптографической защиты к средствам ЭП и удостоверяющего центра предъявляются определённые функциональные требования по управлению доступом, контролю целостности, очистке оперативной и внешней памяти, идентификации и аутентификации, защите вводимых и экспортируемых данных, регистрации событий, резервному копированию и восстановлению и т. п.

Например, в отношении ключевой информации для средств удостоверяющего центра всех классов, начиная с КС1, не допускается копирование информации ключевых документов (криптографических ключей, в том числе ключей ЭП) на носители (например, жёсткий диск), не являющиеся ключевыми носителями, без её предварительного шифрования (которое должно осуществляться встроенной функцией используемой системы криптографической защиты информации). В то же время для средств удостоверяющего центра классов КВ1, КВ2 и КА1 должны быть приняты организационно-

Таблица 4

Возможности нарушителя

Возможности нарушителя	КС1	КС2	КС3	КВ1	КВ2	КА1
Проведение атак внутри контролируемой зоны (КЗ)	–	+	+	+	+	+
Проведение лабораторных исследований вне КЗ	–	+	+	+	+	+
Доступ к средствам вычислительной техники, на которых реализованы средства ЭП	–	–	+	+	+	+
Наличие аппаратных компонент средства ЭП и среды функционирования	–	–	+	+	+	+
Привлечение специалистов по анализу сигналов	–	–	–	+	+	+
в т. ч. по недокументированным возможностям программного обеспечения (ПО)	–	–	–	–	+	+
Наличие исходных текстов прикладного ПО	–	–	–	–	+	+
Наличие всей документации на аппаратуру и ПО	–	–	–	–	–	+
Наличие всех аппаратных компонент	–	–	–	–	–	+

технические меры, исключающие возможность компрометации ключа ЭП, используемого для подписи сертификатов ключей проверки ЭП и списков аннулированных сертификатов, при компрометации ключевой информации, доступной одному, двум и трём лицам соответственно (п. 27 Приложения 2 к [18]).

Построение документов и терминология в западных и отечественных документах различны. Соответствие основных понятий приведено в табл. 5.

Таблица 5

Сравнение терминологии

Директива 1999/93/EC	№ 63-ФЗ
Провайдер сертификационных услуг (CSP)	Удостоверяющий центр
Устройство создания подписи (SCDev)	Средство электронной подписи
Защищённое устройство создания подписи (SSCD)	Средство электронной подписи
CSP SSCD	Средство удостоверяющего центра
Данные для создания подписи (SCD)	Ключ электронной подписи
Данные для верификации подписи (SVD)	Ключ проверки электронной подписи

Заключение

Приведённый краткий обзор подходов к нормативному и техническому регулированию вопросов использования электронной подписи в нашей стране и за рубежом показывает, что, несмотря на сходство, имеются принципиальные отличия, заключающиеся в несовпадении определений основных понятий и систем стандартизации технических требований. Кроме того, следует обращать внимание на отличия в определениях основных терминов, вводимых в математической литературе и в технических стандартах, обусловленных ориентированностью последних на применения в юридической сфере.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации от 06.04.2011 г. № 63-ФЗ «Об электронной подписи».
2. Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures // Official J. European Communities. OJ L 13. 19.01.2000. P. 12.

3. CEN CWA 14365-1: Guide on the Use of Electronic Signatures. Part 1: Legal and Technical Aspects. March 2004. 28 p. (Ref. No.: CWA 14365-1:2004 E).
4. *Menezes A. J., van Oorschot P. C., and Vanstone S. A.* Handbook of applied cryptography. Boca Raton; New York; London; Tokyo: CRC Press, 1997.
5. CEN CWA 14171: General guidelines for electronic signature verification. May 2004. 46 p. (Ref. No.: CWA 14171:2004 D/E/F).
6. *Пазизин С. В.* От цифровой подписи через электронную цифровую подпись к простой «не подписи» // BIS J. — Информационная безопасность банков. 2012. № 1. С. 54–61.
7. CEN CWA 14365-2: Guide on the Use of Electronic Signatures. Part 2: Protection Profile for Software Signature Creation Devices. March 2004. 63 p. (Ref. No.: CWA 14365-2:2004 E).
8. *Попов В. О.* Проблемы построения и функционирования больших систем защиты информации // Системы высокой доступности. 2011. Т. 7. № 2. С. 6—64.
9. CEN CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures. Part 1: System Security Requirements. June 2003. 47 p. (Ref. No.: CWA 14167-1:2003 D/E/F).
10. CEN CWA 14167-2: Cryptographic module for CSP signing operations with backup — Protection profile — CMCSOB PP. May 2004. 89 p. (Ref. No.: CWA 14167-2:2004 E).
11. CEN CWA 14167-3: Cryptographic module for CSP key generation services — Protection profile (CMCKG-PP). May 2004. 69 p. (Ref. No.: CWA 14167-3:2004 E).
12. CEN CWA 14167-4: Cryptographic module for CSP signing operations — Protection profile (CMCSO PP). May 2004. 83 p. (Ref. No.: CWA 14167-4:2004 E).
13. CEN CWA 14169: Secure signature-creation devices 'EAL 4+'. May 2004. 219 p. (Ref. No.: CWA 14169:2004 E).
14. COMMISSION DECISION of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council (notified under document number C(2003) 2439) // Official J. European Union. 15.07.2003. L 175/45–46.
15. CEN CWA 14170: Security requirements for signature creation applications. May 2004. 63 p. (Ref. No.: CWA 14170:2004 E).
16. ETSI TS 102 176-1: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. V 2.0.0 (2007-11) (Ref. No.: RTS/ESI-000054-1).
17. ETSI TS 102 176-2: Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices. V1.2.1. (2005-07). (Ref. No.: RTS/ESI-000039-2).
18. Приказ ФСБ № 796 от 27 декабря 2011 г. «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра». (Зарегистрировано в Минюсте РФ 27 января 2012 г., рег. № 23041.)
19. Приказ ФСБ № 795 от 27 декабря 2011 г. «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи». (Зарегистрировано в Минюсте РФ 9 февраля 2012 г., рег. № 23191.)
20. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну. (Положение ПКЗ-2005.) Утверждено приказом ФСБ России от 9 февраля 2005 г. № 66. (Зарегистрировано Минюстом России 3 марта 2005 г., рег. № 6382) (с изменениями, внесёнными приказом ФСБ России от 12 апреля 2010 г. № 173 (зарегистрировано Минюстом России 25 мая 2010 г., рег. № 17350).)

21. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. № 149/54–144.