Электро́нная по́дпись (ЭП), **Электро́нная цифровая по́дпись** (ЭЦП), **Цифровая подпись** (ЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).

1 Назначение и применение**.**

Квалифицированная электронная подпись предназначена для определения лица, подписавшего электронный документ, и является аналогом собственноручной подписи в случаях, предусмотренных законом[1].

Квалифицированная электронная подпись применяется при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Использование ЭП предполагается для осуществления следующих важных направлений в электронной экономике:

- Полный контроль целостности передаваемого электронного платежного документа: в случае любого случайного или преднамеренного изменения документа цифровая подпись станет недействительной, потому как вычисляется она по специальному алгоритму на основании исходного состояния документа и соответствует лишь ему.
- Эффективная защита от изменений (подделки) документа. ЭП даёт гарантию, что при осуществлении контроля целостности будут выявлены всякого рода подделки. Как следствие, подделывание документов становится нецелесообразным в большинстве случаев.
- Фиксирование невозможности отказа от авторства данного документа. Это аспект вытекает из того, что вновь создать правильную электронную подпись

можно лишь в случае обладания так называемым закрытым ключом, который, в свою очередь, должен быть известен только владельцу этого самого ключа (автору документа). В этом случае владелец не сможет сформировать отказ от своей подписи, а значит — от документа.
- Формирование доказательств подтверждения авторства документа: исходя из того, что создать корректную электронную подпись можно, как указывалось выше, лишь зная Закрытый ключ, а он по определению должен быть известен только владельцу-автору документа, то владелец ключей может однозначно доказать своё авторство подписи под документом. Более того, в документе могут быть подписаны только отдельные поля документа, такие как «автор», «внесённые изменения», «метка времени» и т. д. То есть, может быть доказательно подтверждено авторство не на весь документ.

Перечисленные выше свойства электронной цифровой подписи позволяют использовать её в следующих основных целях электронной экономики и электронного документального и денежного обращения:

- Таможенное декларирование товаров и услуг (таможенные декларации).
- Электронная регистрация сделок по объектам недвижимости.
- Использование в банковских платежных системах.
- Электронная коммерция (торговля).
- Контролирующие функции исполнения государственного бюджета (если речь идет о стране) и исполнения сметных назначений и лимитов бюджетных обязательств (в данном случае если разговор идет об отрасли или о конкретном бюджетном учреждении).
- Управление государственными заказами.
- В электронных системах обращения граждан к органам власти, в том числе и по экономическим вопросам (в рамках таких проектов как «электронное правительство» и «электронный гражданин»).
- Формирование обязательной налоговой (фискальной), бюджетной, статистической и прочей отчетности перед государственными учреждениями и внебюджетными фондами.
- Организация юридически легитимного внутрикорпоративного, внутриотраслевого или национального электронного документооборота.
- Применение ЭЦП в различных расчетных и трейдинговых системах.
- Управление акционерным капиталом и долевым участием.
- Контроль над объёмом производства и оборота этилового спирта, алкогольной продукции и пива посредством системы ЕГАИС.

- В глобальных системах межбанковского рынка обмена валют по определённому курсу (Forex).

2 История возникновения**.**

В 1976 году Уитфилдом Диффи и Мартином Хеллманом было впервые предложено понятие «электронная цифровая подпись», хотя они всего лишь предполагали, что схемы ЭЦП могут существовать.

В 1977 году Рональд Ривест, Ади Шамир и Леонард Адлеман разработали криптографический алгоритм RSA, который без дополнительных модификаций можно использовать для создания примитивных цифровых подписей.

Вскоре после RSA были разработаны другие ЭЦП, такие, как алгоритмы цифровой подписи Рабина, Меркле.

В 1984 году Шафи Гольдвассер, Сильвио Микали и Рональд Ривест первыми строго определили требования безопасности к алгоритмам цифровой подписи. Ими были описаны модели атак на алгоритмы ЭЦП, а также предложена схема GMR, отвечающая описанным требованиям (Криптосистема Гольдвассер — Микали).

2.1 Россия

В 1994 году Главным управлением безопасности связи ФАПСИ был разработан первый российский стандарт ЭЦП — ГОСТ Р 34.10-94 «Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма».

В 2002 году для обеспечения большей криптостойкости алгоритма взамен ГОСТ Р 34.10-94 был введён одноимённый стандарт ГОСТ Р 34.10-2001, основанный на вычислениях в группе точек эллиптической кривой. В соответствии с этим стандартом, термины «электронная цифровая подпись» и «цифровая подпись» являются синонимами.

1 января 2013 года ГОСТ Р 34.10-2001 заменён на ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.»

3 Алгоритмы

Существует несколько схем построения цифровой подписи:

- На основе алгоритмов симметричного шифрования. Данная схема предусматривает наличие в системе третьего лица — арбитра, пользующегося доверием обеих сторон. Авторизацией документа является сам факт зашифрования его секретным ключом и передача его арбитру.
- На основе алгоритмов асимметричного шифрования. На данный момент такие схемы ЭП наиболее распространены и находят широкое применение.

Кроме этого, существуют другие разновидности цифровых подписей (групповая подпись, неоспоримая подпись, доверенная подпись), которые являются модификациями описанных выше схем.[6] Их появление обусловлено разнообразием задач, решаемых с помощью ЭП.

3.1 Использование хэш-функций

Поскольку подписываемые документы — переменного (и как правило достаточно большого) объёма, в схемах ЭП зачастую подпись ставится не на сам документ, а на его хэш. Для вычисления хэша используются криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэш-функции не являются частью алгоритма ЭП, поэтому в схеме может быть использована любая надёжная хэш-функция.

Использование хэш-функций даёт следующие преимущества:

- Вычислительная сложность. Обычно хэш цифрового документа делается во много раз меньшего объёма, чем объём исходного документа, и алгоритмы вычисления хэша являются более быстрыми, чем алгоритмы ЭП. Поэтому формировать хэш документа и подписывать его получается намного быстрее, чем подписывать сам документ.
- Совместимость. Большинство алгоритмов оперирует со строками бит данных, но некоторые используют другие представления. Хэш-функцию можно использовать для преобразования произвольного входного текста в подходящий формат.
- Целостность. Без использования хэш-функции большой электронный документ в некоторых схемах нужно разделять на достаточно малые блоки для применения ЭП. При верификации невозможно определить, все ли блоки получены и в правильном ли они порядке.

Использование хэш-функции не обязательно при электронной подписи, а сама функция не является частью алгоритма ЭП, поэтому хэш-функция может использоваться любая или не использоваться вообще.

В большинстве ранних систем ЭП использовались функции с секретом, которые по своему назначению близки к односторонним функциям. Такие системы уязвимы к атакам с использованием открытого ключа (см. ниже), так как, выбрав произвольную цифровую подпись и применив к ней алгоритм верификации, можно получить исходный текст. Чтобы избежать этого, вместе с цифровой подписью используется хэш-функция, то есть, вычисление подписи осуществляется не относительно самого документа, а относительно его хэша. В этом случае в результате верификации можно получить только хэш исходного текста, следовательно, если используемая хэш-функция криптографически стойкая, то получить исходный текст будет вычислительно сложно, а значит атака такого типа становится невозможной.

3.2 Симметричная схема

Симметричные схемы ЭП менее распространены, чем асимметричные, так как после появления концепции цифровой подписи не удалось реализовать эффективные алгоритмы подписи, основанные на известных в то время симметричных шифрах. Первыми, кто обратил внимание на возможность симметричной схемы цифровой подписи, были основоположники самого понятия ЭП Диффи и Хеллман, которые опубликовали описание алгоритма подписи одного бита с помощью блочного шифра. Асимметричные схемы цифровой подписи опираются на вычислительно сложные задачи, сложность которых ещё не доказана, поэтому невозможно определить, будут ли эти схемы сломаны в ближайшее время, как это произошло со схемой, основанной на задаче об укладке ранца. Также для увеличения криптостойкости нужно увеличивать длину ключей, что приводит к необходимости переписывать программы, реализующие асимметричные схемы, и в некоторых случаях перепроектировать аппаратуру. Симметричные схемы основаны на хорошо изученных блочных шифрах.

В связи с этим симметричные схемы имеют следующие преимущества:

- Стойкость симметричных схем ЭП вытекает из стойкости используемых блочных шифров, надежность которых также хорошо изучена.

- Если стойкость шифра окажется недостаточной, его легко можно будет заменить на более стойкий с минимальными изменениями в реализации.

Однако у симметричных ЭП есть и ряд недостатков:

- Нужно подписывать отдельно каждый бит передаваемой информации, что приводит к значительному увеличению подписи. Подпись может превосходить сообщение по размеру на два порядка.
- Сгенерированные для подписи ключи могут быть использованы только один раз, так как после подписывания раскрывается половина секретного ключа.

Из-за рассмотренных недостатков симметричная схема ЭЦП Диффи-Хелмана не применяется, а используется её модификация, разработанная Березиным и Дорошкевичем, в которой подписывается сразу группа из нескольких бит. Это приводит к уменьшению размеров подписи, но к увеличению объёма вычислений. Для преодоления проблемы «одноразовости» ключей используется генерация отдельных ключей из главного ключа.

3.3 Асимметричная схема

Асимметричные схемы ЭП относятся к криптосистемам с открытым ключом. В отличие от асимметричных алгоритмов шифрования, в которых шифрование производится с помощью открытого ключа, а расшифровка — с помощью закрытого, в асимметричных схемах цифровой подписи подписание производится с применением закрытого ключа, а проверка подписи — с применением открытого.

Для того, чтобы использование цифровой подписи имело смысл, необходимо выполнение двух условий:

- Верификация подписи должна производиться открытым ключом, соответствующим именно тому закрытому ключу, который использовался при подписании.
- Без обладания закрытым ключом должно быть вычислительно сложно создать легитимную цифровую подпись.

Общепризнанная схема цифровой подписи охватывает три процесса:

- Генерация ключевой пары. При помощи алгоритма генерации ключа равновероятным образом из набора возможных закрытых ключей выбирается закрытый ключ, вычисляется соответствующий ему открытый ключ.

- Формирование подписи. Для заданного электронного документа с помощью закрытого ключа вычисляется подпись.
- Проверка (верификация) подписи. Для данных документа и подписи с помощью открытого ключа определяется действительность подписи.

Следует отличать электронную цифровую подпись от кода аутентичности сообщения (MAC).

Виды асимметричных алгоритмов

Как было сказано выше, чтобы применение ЭП имело смысл, необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

Обеспечение этого во всех асимметричных алгоритмах цифровой подписи опирается на следующие вычислительные задачи:

- Задачу дискретного логарифмирования (EGSA)
- Задачу факторизации, то есть разложения числа на простые множители (RSA)

Вычисления тоже могут производиться двумя способами: на базе математического аппарата эллиптических кривых (ГОСТ Р 34.10-2012, ECDSA) и на базе полей Галуа(ГОСТ Р 34.10-94, DSA). В настоящее время самые быстрые алгоритмы дискретного логарифмирования и факторизации являются субэкспоненциальными. Принадлежность самих задач к классу NP-полных не доказана.

Алгоритмы ЭП подразделяются на обычные цифровые подписи и на цифровые подписи с восстановлением документа[9]. При верификации цифровых подписей с восстановлением документа тело документа восстанавливается автоматически, его не нужно прикреплять к подписи. Обычные цифровые подписи требуют присоединение документа к подписи. Ясно, что все алгоритмы, подписывающие хэш документа, относятся к обычным ЭП. К ЭП с восстановлением документа относится, в частности, RSA.

Схемы электронной подписи могут быть одноразовыми и многоразовыми. В одноразовых схемах после проверки подлинности подписи необходимо провести замену ключей, в многоразовых схемах это делать не требуется.

Также алгоритмы ЭП делятся на детерминированные и вероятностные[9]. Детерминированные ЭП при одинаковых входных данных вычисляют одинаковую

подпись. Реализация вероятностных алгоритмов более сложна, так как требует надежный источник энтропии, но при одинаковых входных данных подписи могут быть различны, что увеличивает криптостойкость. В настоящее время многие детерминированные схемы модифицированы в вероятностные.

В некоторых случаях, таких как потоковая передача данных, алгоритмы ЭП могут оказаться слишком медленными. В таких случаях применяется быстрая цифровая подпись. Ускорение подписи достигается алгоритмами с меньшим количеством модульных вычислений и переходом к принципиально другим методам расчёта.

3.4 Перечень алгоритмов ЭП

Асимметричные схемы:

- FDH (Full Domain Hash), вероятностная схема RSA-PSS (Probabilistic Signature Scheme), схемы стандарта PKCS#1 и другие схемы, основанные на алгоритме RSA
- Схема Эль-Гамаля
- Американские стандарты электронной цифровой подписи: DSA, ECDSA (DSA на основе аппарата эллиптических кривых)
- Российские стандарты электронной цифровой подписи: ГОСТ Р 34.10-94 (в настоящее время не действует), ГОСТ Р 34.10-2001 (не рекомендован к использованию после 31 декабря 2017 года), ГОСТ Р 34.10-2012
- Евразийский союз: ГОСТ 34.310-2004[10] полностью идентичен российскому стандарту ГОСТ Р 34.10-2001
- Украинский стандарт электронной цифровой подписи ДСТУ 4145-2002
- Белорусский стандарт электронной цифровой подписи СТБ 1176.2-99 (в настоящее время не действует), СТБ 34.101.45-2013
- Схема Шнорра
- Pointcheval-Stern signature algorithm
- Вероятностная схема подписи Рабина
- Схема BLS (Boneh-Lynn-Shacham)
- Схема DLR (Donna-Lynn-Rivest)
- Схема GMR (Goldwasser-Micali-Rivest)

На основе асимметричных схем созданы модификации цифровой подписи, отвечающие различным требованиям:

- Групповая цифровая подпись

- Неоспоримая цифровая подпись
- «Слепая» цифровая подпись и справедливая «слепая» подпись
- Конфиденциальная цифровая подпись
- Цифровая подпись с доказуемостью подделки
- Доверенная цифровая подпись
- Разовая цифровая подпись

4. Подделка подписей

Анализ возможностей подделки подписей — задача криптоанализа. Попытку сфальсифицировать подпись или подписанный документ криптоаналитики называют «атака».

4.1 Модели атак и их возможные результаты.

В своей работе Гольдвассер, Микали и Ривест описывают следующие модели атак, которые актуальны и в настоящее время[5]:

- Атака с использованием открытого ключа. Криптоаналитик обладает только открытым ключом.
- Атака на основе известных сообщений. Противник обладает допустимыми подписями набора электронных документов, известных ему, но не выбираемых им.
- Адаптивная атака на основе выбранных сообщений. Криптоаналитик может получить подписи электронных документов, которые он выбирает сам.

Также в работе описана классификация возможных результатов атак:

- Полный взлом цифровой подписи. Получение закрытого ключа, что означает полный взлом алгоритма.
- Универсальная подделка цифровой подписи. Нахождение алгоритма, аналогичного алгоритму подписи, что позволяет подделывать подписи для любого электронного документа.
- Выборочная подделка цифровой подписи. Возможность подделывать подписи для документов, выбранных криптоаналитиком.
- Экзистенциальная подделка цифровой подписи. Возможность получения допустимой подписи для какого-то документа, не выбираемого криптоаналитиком.

Ясно, что самой «опасной» атакой является адаптивная атака на основе выбранных сообщений, и при анализе алгоритмов ЭП на криптостойкость нужно рассматривать именно её (если нет каких-либо особых условий).

При безошибочной реализации современных алгоритмов ЭП получение закрытого ключа алгоритма является практически невозможной задачей из-за вычислительной сложности задач, на которых ЭП построена. Гораздо более вероятен поиск криптоаналитиком коллизий первого и второго родов. Коллизия первого рода эквивалентна экзистенциальной подделке, а коллизия второго рода — выборочной. С учётом применения хэш-функций, нахождение коллизий для алгоритма подписи эквивалентно нахождению коллизий для самих хэш-функций.

4.2. Подделка документа (коллизия первого рода)

Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. Причина в следующем:

- документ представляет из себя осмысленный текст;
- текст документа оформлен по установленной форме;
- документы редко оформляют в виде txt-файла, чаще всего в формате DOC или HTML.

Если у фальшивого набора байт и произойдет коллизия с хэшем исходного документа, то должны выполниться три следующих условия:

- случайный набор байт должен подойти под сложно структурированный формат файла;
- то, что текстовый редактор прочитает в случайном наборе байт, должно образовывать текст, оформленный по установленной форме;
- текст должен быть осмысленным, грамотным и соответствующим теме документа.

Впрочем, во многих структурированных наборах данных можно вставить произвольные данные в некоторые служебные поля, не изменив вид документа для пользователя. Именно этим пользуются злоумышленники, подделывая документы. Некоторые форматы подписи даже защищают целостность текста, но не служебных полей.[11]

Вероятность подобного происшествия также ничтожно мала. Можно считать, что на практике такого случиться не может даже с ненадёжными хэш-функциями, так как документы обычно большого объёма — килобайты.

4.3. Получение двух документов с одинаковой подписью (коллизия второго рода)

Куда более вероятна атака второго рода. В этом случае злоумышленник фабрикует два документа с одинаковой подписью, и в нужный момент подменяет один другим. При использовании надёжной хэш-функции такая атака должна быть также вычислительно сложной. Однако эти угрозы могут реализоваться из-за слабостей конкретных алгоритмов хэширования, подписи, или ошибок в их реализациях. В частности, таким образом можно провести атаку на SSL-сертификаты и алгоритм хэширования MD5.

4.4. Социальные атаки

Социальные атаки направлены не на взлом алгоритмов цифровой подписи, а на манипуляции с открытым и закрытым ключами[13].

- Злоумышленник, укравший закрытый ключ, может подписать любой документ от имени владельца ключа.
- Злоумышленник может обманом заставить владельца подписать какой-либо документ, например, используя протокол слепой подписи.
- Злоумышленник может подменить открытый ключ владельца на свой собственный, выдавая себя за него.

Использование протоколов обмена ключами и защита закрытого ключа от несанкционированного доступа позволяет снизить опасность социальных атак.

5. Управление ключами

5.1. Управление открытыми ключами

Важной проблемой всей криптографии с открытым ключом, в том числе и систем ЭП, является управление открытыми ключами. Так как открытый ключ доступен любому пользователю, то необходим механизм проверки того, что этот ключ принадлежит именно своему владельцу. Необходимо обеспечить доступ любого пользователя к подлинному открытому ключу любого другого пользователя,

защитить эти ключи от подмены злоумышленником, а также организовать отзы́в ключа в случае его компрометации.

Задача защиты ключей от подмены решается с помощью сертификатов. Сертификат позволяет удостоверить заключённые в нём данные о владельце и его открытый ключ подписью какого-либо доверенного лица. Существуют системы сертификатов двух типов: централизованные и децентрализованные. В децентрализованных системах путём перекрёстного подписывания сертификатов знакомых и доверенных людей каждым пользователем строится сеть доверия. В централизованных системах сертификатов используются центры сертификации, поддерживаемые доверенными организациями.

Центр сертификации формирует закрытый ключ и собственный сертификат, формирует сертификаты конечных пользователей и удостоверяет их аутентичность своей цифровой подписью. Также центр проводит отзы́в истекших и компрометированных сертификатов и ведёт базы (списки) выданных и отозванных сертификатов. Обратившись в сертификационный центр, можно получить собственный сертификат открытого ключа, сертификат другого пользователя и узнать, какие ключи отозваны.

5.2 Хранение закрытого ключа

Закрытый ключ является наиболее уязвимым компонентом всей криптосистемы цифровой подписи. Злоумышленник, укравший закрытый ключ пользователя, может создать действительную цифровую подпись любого электронного документа от лица этого пользователя. Поэтому особое внимание нужно уделять способу хранения закрытого ключа. Пользователь может хранить закрытый ключ на своем персональном компьютере, защитив его с помощью пароля. Однако такой способ хранения имеет ряд недостатков, в частности, защищённость ключа полностью зависит от защищённости компьютера, и пользователь может подписывать документы только на этом компьютере.

В настоящее время существуют следующие устройства хранения закрытого ключа:

- дискеты,
- смарт-карты,
- USB-брелоки,
- «таблетки» Touch-Memory,
- реестр (в защищённой памяти компьютера).

Кража или потеря одного из таких устройств хранения может быть легко замечена пользователем, после чего соответствующий сертификат должен/может быть немедленно отозван.

Наиболее защищённый способ хранения закрытого ключа — хранение на смарт-карте. Для того, чтобы использовать смарт-карту, пользователю необходимо не только её иметь, но и ввести PIN-код, то есть, получается двухфакторная аутентификация. После этого подписываемый документ или его хэш передаётся в карту, её процессор осуществляет подписывание хэша и передаёт подпись обратно. В процессе формирования подписи таким способом не происходит копирования закрытого ключа, поэтому все время существует только единственная копия ключа. Кроме того, произвести копирование информации со смарт-карты немного сложнее, чем с других устройств хранения.

В соответствии с законом «Об электронной подписи», ответственность за хранение закрытого ключа владелец несёт сам.

6. Использование ЭП в России

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует Федеральный закон Российской Федерации от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

После становления ЭП при использовании в электронном документообороте между кредитными организациями и кредитными бюро в 2005 году активно стала развиваться инфраструктура электронного документооборота между налоговыми органами и налогоплательщиками. Начал работать приказ Министерства по налогам и сборам РФ от 2 апреля 2002 года № БГ-3-32/169 «Порядок представления налоговой декларации в электронном виде по телекоммуникационным каналам связи». Он определяет общие принципы информационного обмена при представлении налоговой декларации в электронном виде по телекоммуникационным каналам связи.

В законе РФ от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи» описаны условия использования ЭП, особенности её использования в сферах государственного управления и в корпоративной информационной системе.

Благодаря ЭП теперь, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете через системы электронной

торговли, обмениваясь с контрагентами необходимыми документами в электронном виде, подписанными ЭП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур[14]. В силу требований Федерального закона от 5 апреля 2013 года № 44-ФЗ «О контрактной системе…» государственные контракты, заключаемые в электронном виде, должны быть подписаны усиленной электронной подписью[15].

С 13 июля 2012 согласно Федеральному закону № 108-ФЗ официально вступила в действие правовая норма, продлевающая действие 1-ФЗ «Об электронной цифровой подписи» до 1 июля 2013 года. В частности, решено в части 2 статьи 20 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036) слова «с 1 июля 2012 года» заменить словами «с 1 июля 2013 года».[16].

Однако Федеральным законом от 02.07.2013 № 171-ФЗ внесены изменения в статью 19 Федерального закона от 06.04.11 № 63-ФЗ «Об электронной подписи». В соответствии с этим электронный документ, подписанный электронной подписью, сертификат ключа проверки которой выдан в период действия федерального закона № 1-ФЗ, признаётся подписанным квалифицированной электронной подписью. При этом использовать старый сертификат можно до 31 декабря 2013 года включительно. Это значит, что в указанный период документы могут подписываться электронной цифровой подписью, сертификат ключа проверки которой выдан до 1 июля 2013 года.

С 1 июля 2013 года Федеральный закон от 10 января 2002 года № 1-ФЗ утратил силу, на смену ему пришёл Федеральный закон от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи». В результате было введено определение трех видов электронных подписей:

- **Простой электронной подписью** является электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определённым лицом.
- **Усиленной неквалифицированной электронной подписью** является электронная подпись, которая:

1. получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2. позволяет определить лицо, подписавшее электронный документ;

3. позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4. создается с использованием средств электронной подписи.

- **Усиленной квалифицированной электронной подписью** является электронная подпись, которая соответствует всем признакам неквалифицированной электронной подписи и следующим 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 63-ФЗ

С 1 января 2013 года гражданам выдаётся универсальная электронная карта, в которую встроена усиленная квалифицированная электронная подпись (выпуск карт прекращён с 1 января 2017 года).

8 сентября 2015 года в Крымском федеральном округе (КФО) аккредитован первый удостоверяющий центр на базе Государственного унитарного предприятия «Крымтехнологии». Соответствующие полномочия утверждены приказом Министерства связи и массовых коммуникаций Российской Федерации № 298 «Об аккредитации удостоверяющих центров» от 11 августа 2015 года.

Манипуляции с электронными подписями в России

Известны незаконные действия с электронными подписями через центры сертификации РФ[19]. Коллегия Счетной палаты под председательством Татьяны Голиковойвыявила участие некоторых УЦ в неправомерном применении электронной подписи застрахованного лица в интересах негосударственных пенсионных фондов, а также оформления документов без участия гражданина[20]. «Проверка Счетной палаты в очередной раз выявила массовые нарушения даже при наличии усиленных мер защиты электронной подписи», прокомментировал ситуацию президент НАПФ Сергей Беляков, его советник утверждает, что массовая фальсификация электронных подписей в повторных заявлениях производилась путем повторного использования удостоверяющим центром электронной подписи клиента.

- Другой способ манипуляции с электронными подписями заключается в том, что клиенту предлагают дистанционный выпуск квалифицированного сертификата без личного контакта заявителя и сотрудника регистрационного отдела удостоверяющего центра, в этом случае оформление электронной подписи производится удаленно, на основании документов заявителя, представленных через интернет центру сертификации. В результате подобных действий, вызванных, по мнению специалистов правовой системы «Гарант», тем что «IT-функции в деятельности УЦ преобладают над его юридической сущностью», электронная подпись может быть использована недобросовестными третьими лицами. Однако, в 2017 году предложение Минкомсвязи передать функции выдачи усиленной квалифицированной электронной подписи (УКЭП) от частных компаний государству не нашло понимания других министерств и ведомств.

7. Литература

- Рябко Б. Я.*, Фионов А. Н.* Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — 173 с. — ISBN 978-5-89176-233-6
- *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. — «Гелиос АРВ», 2002. — 480 с. — ISBN 5-85438-137-0.
- Нильс Фергюсон*,* Брюс Шнайер*.* Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004. — 432 с. — 3000 экз. — ISBN 5-8459-0733-0, ISBN 0-4712-2357-3.
- *Б. А. Фороузан.* Схема цифровой подписи Эль-Гамаля // Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин. — Курс лекций.
- Menezes A. J.*, Oorschot P. v.,* Vanstone S. A. Handbook of Applied Cryptography — CRC Press, 1996. — 816 p. — (Discrete Mathematics and Its Applications) — ISBN 978-0-8493-8523-0
- Мао В. Современная криптография: Теория и практика — М.: Вильямс, 2005. — 768 с. — ISBN 978-5-8459-0847-6