ЭЛЕКТРОННАЯ ПОДПИСЬ: НАЗНАЧЕНИЕ, ФУНКЦИИ И ПРИМЕНЕНИЕ В СОВРЕМЕННОМ ДОКУМЕНТООБОРОТЕ

Цуканова Д.В.
Областное бюджетное профессиональное образовательное учреждение "Курский государственный техникум технологий и сервиса"
kgtts@mail.ru

Письменные документыи данные, полученные археологами и лингвистами, показывают, что уже в X в. в Древнерусском государстве присутствовала культура написания документов, а также велась процедура подтверждения их юридической силы.Большой вклад в делопроизводство ввёл Петр l. Он создал 12 коллегий, они контролировали определенную отрасль или сферу управления. Появились первые секретари. В конце XVIIIв. уже существовали пособия по составлению документов.[3, 15] С тех пор по настоящее время существовала необходимость подтверждения подлинности документов. Это были собственноручные подписи, различного вида оттиски и печати и т.п. С развитием информационных технологий и электронного документооборота стала постепенно внедряться так называемая электронно-цифровая подпись (ЭЦП).

Цифровая подпись предназначена для аутентификации лица, подписавшего электронный документ или сообщение. Кроме того, использование ЭЦП предоставляет возможность обеспечить следующие свойства при передаче в системе подписанного сообщения:

- осуществление контроля целостности передаваемого подписанного сообщения;
- доказательное подтверждение авторства лица, подписавшего сообщение;
- защита сообщения от возможной подделки.[1, 83]

Ещё до появления цифровой подписи, существовала факсимиле. Это воспроизведение любого графического оригинала (рисунка, чертежа, рукописи, гравюры, и т.д.) передающее его точно, со всеми подробностями. Если быть проще, то при помощи факсимиле создают копию, которая максимально соответствует оригиналу.Живая подпись используется для физических лиц. Для юридических лиц, требуется заверение живой подписи печатью организации. Как подписи, так и печать не сложно было подделать. Если ситуация не выходила за рамки конфликта, то подделку не замечали. В случае конфликта, требовалась экспертиза подписи, печати и почерка. Исходя из всего вышесказанного, можно сделать вывод, что данная система подписи была не надёжна и не защищена юридически.В 1976 году УитфилдомДиффи и Мартином Хеллманом было впервые предложено понятие "электронная цифровая подпись". В основу ЭЦП входил алгоритм обмена ключами. Он возник благодаря идее передачи информации от одного лица другому лицу так, чтобы посторонние лица, получив доступ к ней, не могли ее подделать.

В Россию электронная подпись пришла в начале 90-ых и была введена в 1995 году. Эти изменения были внесены в Гражданский кодекс РФ. Где в статье

160 пункте 2 говорилось о возможностииспользования электронной подписи при оформлении сделок, как аналогов собственноручной подписи (АСП).

Принцип цифровой подписи состоит из криптографических символов, которые связанны с определённым документом. С помощью цифровой подписи, возможно, идентифицировать его пользователя. Предназначением ЦП является электронный документооборот. Сама цифровая подпись создается при помощи криптографических символов (наборов нулей и единиц).Одним из самых распространенных алгоритмов шифрования является алгоритм RSA, длина ключа которого обычно 1024 бита. Но могут применяться и укороченные ключи 256 и 512 бит.[2]

Цифровая подпись состоит из двух ключей, закрытого и открытого. Закрытый ключ хранится только у владельца цифровой подписи, а открытый ключ – это сертификат, который формируется уполномоченной на это организацией на основе хэш-функций закрытого ключа, естественно с соответствующими ссылками на сертификаты доверенных корневых центров, промежуточных корневых центров и самого сертификата пользователя. Если закрытый ключ никому не передаётся, а хранится только у владельца, то сертификат служит для передачи заинтересованным лицам, между которыми идёт документооборот. То есть если есть владелец цифровой подписи А, ему необходимо наладить документооборот с пользователями Ви С, тогда владелец закрытого ключа передает свой сертификат, полученный от удостоверяющего центра, В и С, при отправке документов от А к В, В может проверить, с помощью открытого ключа или сертификата, что это именно от А, но также, что документ не был изменён третьим лицом. Открытый ключ может находиться в свободном доступе.

Носителей закрытого ключа может быть много, начиная с дискеты, дисков, флешки, память компьютера, но все эти носители не защищены от кражи закрытого ключа, потому что они допускают копирование. Для того чтобы обезопасить пользователя существуютносители с повышенной степенью защищиты информации, такие как Рутокен, eTokenPro, «Соболь» и другие. Принцип работы этих носителей состоит в том, что они не позволяют копировать закрытый ключ. Обмен информации идет со специальным программным обеспечением: КриптоПро, ViPNet CSP, КриптоАРМ. Рутокен позволяет не хранить цифровую подпись в открытом доступе.

На сегодняшний момент ЭЦП достаточно защищена, ведь при каком-либо изменении в документе, он теряет свою юридическую силу. Сама цифровая подпись работает по системе необратимых функций. То есть при заданном значении a и b мы легко можем вычислить c, обратно же, имея значение c, a и bвычислить, будет затруднительно. Группа ученых из Швейцарии, Японии, Франции, Германии, Нидерландах и США в 2010 году удалось успешно вычислить данные зашифрованные при помощи криптографического ключа стандарта RSA длинной 768 бит. По словам исследователей, в качестве надёжной системы шифрования можно рассматривать RSA длинной 1024 бита и более. С 2013 года некоторые браузеры перестали поддерживать сертификаты удостоверяющих центров с ключами RSA меньше 2048 бит.[5]

Единственный доступный метод дешифрования, это перебор символов, но он достаточно длителен и неэффективен. Из этого можно сделать вывод, что суть ЭЦП состоит в практической невозможности вычислить обратное значение. Так как даже при шестидесяти четырех битном шифровании, на расшифровку потребуется 217908031 год.

Время полного перебора всех возможных паролей заданного алфавита при скорости перебора 10,000,000 паролей в секунду

алфавит	6 символов	8 символов	10 символов	12 символов
26 (латиница все маленькие или все большие)	31 сек	5 часов 50 мин	163.5 суток	303 года
52 (латиница с переменным регистром)	33 мин	62 суток	458 лет	1,239,463 года
62 (латиница разного регистра плюс цифры)	95 мин	252 суток 17 часов	2,661 год	10,230,425 лет
68 (латиница разного регистра плюс цифры плюс знаки препинания .,;:!?)	2 часа 45 мин	529 суток	6703 года	30,995,621 лет
80 (латиница разного регистра плюс цифры плюс знаки препинания .,;:!? плюс скобки ()[]{} плюс #$%&*~)	7 часов 30 мин	5 лет 4 месяца	34048 лет	217,908,031 год

Цифровая подпись имеет ограниченный период действия. Срок жизни цифровой подписи начинается с момента получения сертификата ключа собственником и обычно выдаётся сроком на один год. Окончаниедействия ЭЦП может возникнуть по разным причинам: если цифровая подпись требует продления, (период действия сертификата ключа окончен),владелец ЭЦП пожелал прекратить использование, организация прекратила своё функционирование, цифровая подпись внесена в реестр недостоверных.[4,]

Изначально цифровая подпись неразрывно связана с документооборотом. При помощи документооборота ЭЦП получает юридическую значимость. В основу цифровой подписи входит защита от перехвата информации и защита файла от изменений, посторонним лицом.

С увеличением электронного документооборота всё чаще возникает необходимость в применении цифровой подписи, на настоящий момент существует ряд программных продуктов(TrustedJava, КриптоПро PDF, КриптоПро OfficeSignature), которые позволяют подписывать как файлы,архивы, так и документы.

Цифровая подпись также применяется для работы с защищёнными сайтами, для размещенияофициальной информации об организации, проведения государственных и тендерных закупок, доступа к государственным услугам, предоставляемым в электронном виде юридическими физическим лицам, для удалённой работыс банками в учреждениях и предприятиях, и т.д.

Согласно постановлениюправительства РФ от 31 декабря 2020года, к 2024 году планируется перевести в электронный вид весь государственный и межведомственный документооборот, что соответственно будет способствовать развитию использования ЭЦП в ближайшем будущем.

Сегодня субъекты предпринимательской деятельности взаимодействуют посредством электронного документооборота как между собой, так и с конечными потребителями и органами власти.

В качестве практического примера использования ЭЦП физическим лицом можно привести то, что на настоящий момент любой гражданин, имеющий личный кабинет на сайте налоговой инспекции может подключить для себя цифровую подпись и передавать документы, заявления, обращения, а также подписывать их в электронном виде,не посещая лично самой налоговой инспекции. Данная ЭЦП хранится на серверах ФНС, а доступ к цифровой подписи пользователь получает через ввод пароля.

Таким образом, использование ЭЦП становится неотъемлемой частью нашей жизни,как и тенденция на успешное и безопасное её применение.

Список использованныхисточников:

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.Основы криптографии.— «Гелиос АРВ», 2018.— 480с.—ISBN 5-85438-137-0.
2. ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
3. РябкоБ.Я., Фионов А.Н.Основы современной криптографии для специалистов в информационных технологиях—Научный мир, 2019. — 173с. —ISBN 978-5-89176-233-6
4. Федеральный закон Российской Федерации от 6 апреля 2011г. N 63-ФЗ «Об электронной подписи»
5. ФороузанБ. А. Схема цифровой подписи Эль-Гамаля//Управление ключами шифрования и безопасность сети / Пер. А. Н. Берлин.— Курс лекций.