



# Теория и практика применения электронной подписи



**Кустов**  
Владимир Николаевич,  
заместитель  
генерального директора  
ООО «Газинформсервис»



**Петров**  
Сергей Владимирович,  
начальник отдела  
разработки средств  
защиты департамента  
разработки и испытаний  
ООО «Газинформсервис»

## Введение

Замысел настоящей статьи, по мнению авторов, состоял в том, чтобы простым и понятным языком изложить достаточно сложные процессы, сопровождающие использование электронной подписи (ЭП), касающиеся ее теоретических основ и практического применения.

## Теоретические основы ЭП

Изложение теоретических основ ЭП будет полезным начать с описания, некоторых понятий, таких как: алфавит, сообщение, ключ, шифрование, расшифрование, криптографическая система.

**Алфавит** — конечное множество используемых для кодирования информации знаков (символов алфавита).

**Сообщение (С)** — некоторая последовательность символов алфавита.

**Ключ (К)** — уникальная секретная информация, необходимая для беспрепятственного шифрования и расшифрования текстов.

**Шифрование** (функция  $F$ ) — процесс преобразования исходного сообщения (С), в шифрованное сообщение (ШС) с использованием ключа (К) — можно записать в виде:  $ШС = F(C, K)$ .

**Расшифрование** — обратный шифрованию процесс, в котором на основе ключа шифрованное сообщение преобразуется в исходное сообщение — можно записать в виде  $C = F^{-1}(ШС, K)$ .

**Криптографическая система (КС)** — полное множество всех преобразований исходного сообщения (С) в шифрованное сообщение (ШС), причем каждое преобразование выполняется с использованием уникального секретного ключа (К).

## Классификация криптографических систем (КС)

Все КС делятся на три больших класса:

1. Бесключевые (Хэш-функции), условно обозначаются Н.
2. Одноключевые или симметричные КС.
3. Многоключевые (чаще всего двухключевые) или асимметричные КС.

## Бесключевые КС — Хэш-функции

Функция  $H=h(C)$  — является хэш-функцией (или просто хэшем), если она удовлетворяет следующим условиям:

1. Исходное сообщение может быть произвольной длины.
2. Само значение Н имеет фиксированную длину.
3. Значение функции Н легко вычисляется для любого аргумента С.
4. Восстановить аргумент С по значению Н с вычислительной точки зрения — практически невозможно (функция Н — односторонняя функция).
5. Функция Н — однозначна.

Для вычисления хэш-функции ключ не нужен, поэтому



хэш-функция относится к классу бесключевых КС. Для любой хэш-функции есть отличающиеся друг от друга сообщения-близнецы ( $C_1$  и  $C_2$ ), имеющие одинаковое значение  $H$ . Однако для хорошей хэш-функции вероятность такого события близка к 0. Такой факт получил название «эффект близнецов». Все свойства хэш-функции можно для образного восприятия проиллюстрировать на рис. 1. На данном рисунке роль исходного сообщения выполняет автомобиль, сдаваемый на утилизацию. После процесса хэширования (побывав под прессом) он превращается в небольшой по размеру кусок металлолома (в хэш-функцию). Из спрессованного куска металла восстановить автомобиль невозможно. Получить два совершенно одинаковых, спрессованных куска из разных автомобилей практически невозможно.

### Одноключевые — симметричные КС

**Одноключевые** (симметричные) КС представляют собой системы, в которых для шифрования и для расшифрования сообщений используют один

и тот же ключ. Напомним, что формально данные процессы соответственно описываются в виде следующих выражений:

- шифрование сообщений:  $ШС = F(C, K)$ ;
- расшифрование сообщений или обратное преобразование:  $С = F^{-1}(ШС, K)$ .

### Многочисленные — асимметричные КС

Не останавливаясь подробно на описании многочисленных КС, определим основной из них класс — двухключевые или асимметричные КС.

**Двухключевые** или асимметричные КС, а также КС с открытым ключом используют два ключа для каждого абонента — открытый ( $K_0$ ) и закрытый ( $K_3$ ), которые математически связаны друг с другом очень сложной зависимостью. Ключи являются парными и создаются одновременно. Знание открытого ключа не позволяет вычислить значение закрытого ключа. Информация шифруется с помощью любого из ключей, а расшифровывается только с помощью парных им ключей. То есть информация, зашифро-

ванная с помощью открытого ключа, может быть расшифрована только с помощью парного ему закрытого ключа, который абонент обязан хранить в тайне. Формально использование такой КС (функция  $f$ ) можно представить в виде:

- шифрование сообщений:  $ШС = f(C, K_0)$ ;
- расшифрование сообщений или обратное преобразование:  $С = f^{-1}(ШС, K_3)$ .

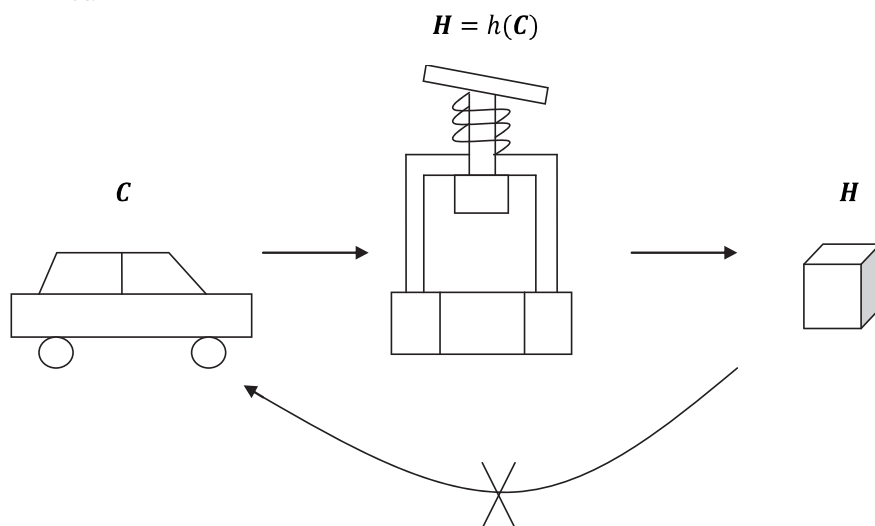
Асимметричные КС представляют собой математическую основу использования ЭП.

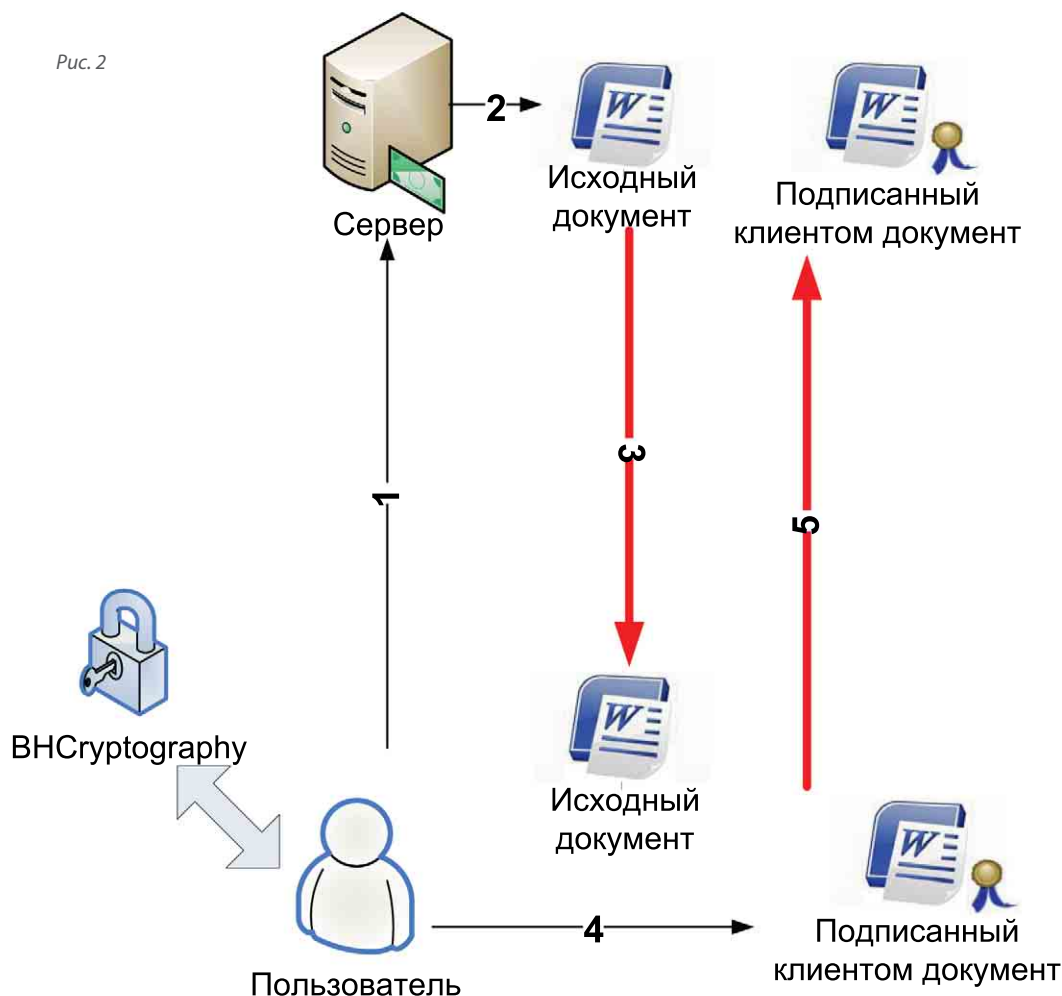
Далее рассмотрим практическое применение ЭП для систем электронного документооборота.

### Практическое применение электронной подписи

Наиболее распространенным применением ЭП является создание систем защищенного документооборота. В таких системах ключевую роль играет как сама ЭП, так и средства, позволяющие создавать или проверять ЭП, а также выполняющие другие сервисные функции. Специалистами ООО «Газинформсервис» разработаны программные продукты для работы с ЭП — ПО «Блокхост-ЭЦП» и ПО «ВНСryptography». Программный комплекс «Блокхост-ЭЦП» предназначен для автономной работы и предоставляет пользователям возможность создавать и проверять подписи на своем рабочем месте. Программная библиотека «ВНСryptography» позволяет организовывать автоматизированные системы защищенного документооборота. Продукты успешно внедрены и неизменно пользуются успехом, как у рядовых пользователей, так и у крупных корпоративных клиентов.

Рис. 1





### Электронная подпись документа без предоставления данных

В процессе организации и эксплуатации систем защищенного документооборота с использованием ЭП возникает задача оптимизации времени обслуживания и минимизации трафика. Каждый раз для подписания документа участнику системы требуется скачать документ к себе на рабочее место, подписать и загрузить обратно. Для такого алгоритма становится критичным размер подписываемых файлов, поскольку возрастает нагрузка на канал передачи.

Командой разработчиков ООО «Газинформсервис» было предложено и реализовано

программное решение для минимизации нагрузки на канал. Суть решения заключается в следующем: для подписания документа пользователь не скачивает его к себе на рабочее место, а получает только хэш. Далее, на рабочем месте выполняется подпись хэша и полученная подпись отправляется обратно на сервер, где происходит объединение исходного документа с полученной подписью. Размер передаваемого хэша составляет несколько килобайт.

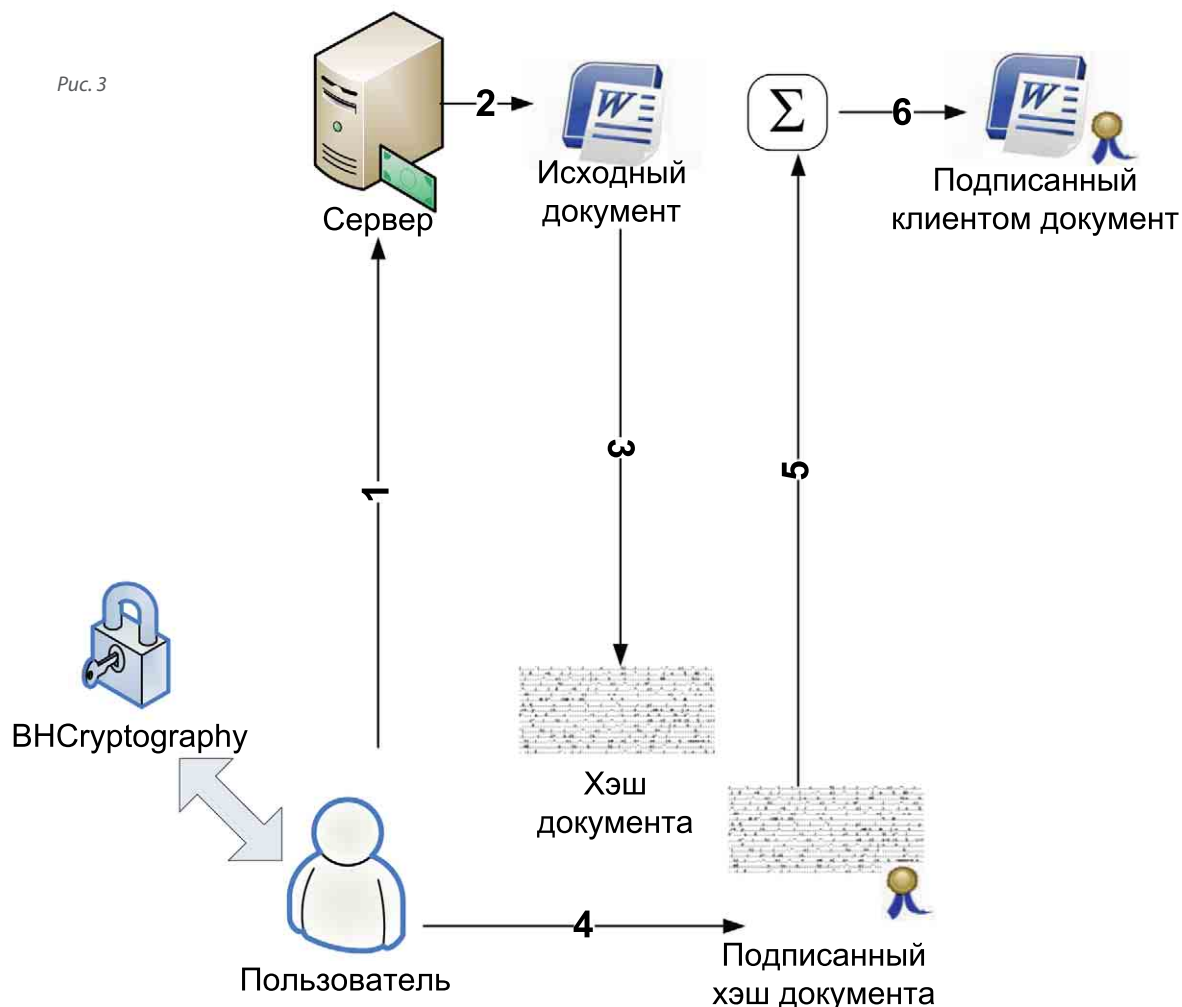
При такой организации документооборота следует учитывать ряд ограничений и допущений, а именно:

- юридическая значимость документооборота;
- защита канала данных;

- программные средства, реализующие подобную функциональность.

Для обеспечения юридической значимости данной схемы необходимо дополнительно разрабатывать регламент, передаваемый конечным пользователям. В регламенте указывается, что пользователь соглашается на данный алгоритм подписи документов, то есть согласен подписывать документы, не видя их вживую. Подпись пользователя под регламентом будет являться гарантом при рассмотрении спорных вопросов.

Для передачи хэша документа необходимо обеспечить доверенное защищенное соединение между клиентом и сервером,



для исключения модификации хэша или подписи в процессе передачи. Следует отметить, что защищенное соединение также необходимо устанавливать и для обычной схемы подписи документов, поскольку документ может передаваться в открытом виде.

Специалистами ООО «Газинформсервис» был разработан алгоритм и реализован в программном решении «VNCryptography» — библиотеке для реализации УЭЦП. Библиотека «VNCryptography» устанавливается на клиентские рабочие места и на сервер, клиентам предоставляется пользовательский интерфейс для подписания документов, на серверной стороне реали-

зованы функции вычисления хэша и инкапсуляции подписи в документ. Все операции по вычислению хэша, объединения документа с подписью и передача по каналам связи выполняются прозрачно для пользователя, который наблюдает на сервере только конечный результат — подписанный его секретным ключом документ.

Таким образом, удаленная подпись документов позволяет решить проблему перегруженности канала, минимизировать временные и материальные затраты в процессе защищенного документооборота и при этом выполняются все требования по безопасности, предъявляемые системе.

Подробнее —  
см. в приложении на CD



ГАЗИНФОРМСЕРВИС

**ООО «Газинформсервис»**  
Россия, 198188, г. Санкт-Петербург, а/я 35  
Тел.: (812) 305–2050  
Факс: (812) 305–2051  
E-mail: resp@gaz-is.ru  
URL: www.gaz-is.ru