DESIGNING OF PUBLIC CATERING ESTABLISHMENTS WITH THE HELP OF COMPUTER TECHNOLOGY

Khalilova V.K., Bunina N. E.

Keywords: modeling, computers, catering establishments, program.

The article presents one type of modeling – computer. It examined the characteristics, properties and opportunities, as well as codes for simulation of public catering establishments and trade.

Контактная информация: ha_venera@mail.ru 89876366564

УДК 004.738.5

ЭЛЕКТРОННАЯ ПОДПИСЬ И ЕЕ ПРИМЕНЕНИЕ

Хамзина Э.И., студентка 2 курса экономического факультета
Научный руководитель – Голубев С.В.,
кандидат экономических наук, доцент
ФГБОУ ВО Ульяновская ГСХА

Ключевые слова: *электронная цифровая подпись, информационные технологии, хэш, хэш-функция, открытый ключ, закрытый ключ.*

Работа посвящена актуальной в наше время проблеме применения электронной цифровой подписи юридическими и физическими лицами.

Жизнь современного общества уже сложно представить без информационных технологий: книжки и журналы стали электронными, а почтальонов заменил Интернет. Всемирная сеть крепко опутала фактически все " уголки " нашей жизни — совсем обычным смотрятся электрические средства, покупки в виртуальных магазинах, интернет-приемные представителей государственной власти и электронная цифровая подпись, схемы и главные аспекты которой мы рассмотрим в предоставленной статье.

Электронная цифровая подпись (ЭЦП) – это особенный реквизит документа, который дает возможность определить, была ли изменена информация в электронном документе с момента формирования ЭП и подтвердить принадлежность ее обладателю. Значение реквизита выходит в последствии криптографического преображения информации. Электронная подпись необходима для идентификации лица, подписавшего электронный документ, и считается настоящей заменой оригинальной ручной подписи.

Применение электронной цифровой подписи позволяет осуществить:

Обеспечение целостности передаваемого документа: при любом изменении документа подпись становится недействительной, потому что сформирована она на основании первоначального состояния документа и будет соответствовать только ему.

Недопустимость отказа от авторства: так как создать правильную подпись может только владелец закрытого ключа, то в дальнейшем он не может отказаться от своей электронной подписи под документом.

Неоспоримое доказательство авторства документа: так как сформировать точную подпись возможно, лишь зная закрытый ключ, который известен только владельцу подписи, он может доказать подлинность подписи под документом.

Так как многие подписываемые документы — обычно довольно значительного объёма, подпись в схемах ЭП ставится не на сам документ, а на его хэш. Хэш-функция защищенного электронного документа – это число, получаемое из первоначального документа посредством его преобразования при помощи сложного, но известного алгоритма. Такая функция чувствительна к разнообразным изменениям исходного электронного документа, то есть изменение хотя бы одного символа в исходном документе приводит к искажению в среднем половины символов хэш-значения.

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. Но 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 последствии было введено определение трех видов электронных подписей:

Простая ЭП-это подпись, которая подтверждает факт создания электронной подписи определенным лицом при помощи паролей, кодов или иных средств.

Усиленной неквалифицированной электронной подписью называется подпись, которая: получена в результате криптографического преобразования информации с применением открытого и закрытого ключа, а усиленной квалифицированной электронной подписью является электронная подпись, соответствующая всем свойствам неквалифицированной электронной подписи, но охватывает дополнительные признаки: ключ проверки электронной подписи должен быть задан в квалифицированном сертификате и при создании и проверке подписи.

На сегодняшний день имеется несколько схем шифрования электронной подписи: на основе алгоритмов асимметричного и симметричного шифрования.

Асимметричная схема шифрования относится к криптосистемам с открытым ключом. В данной схеме подписание совершается с применением закрытого ключа, а проверка подписи — с применением открытого ключа.(Рис.1)

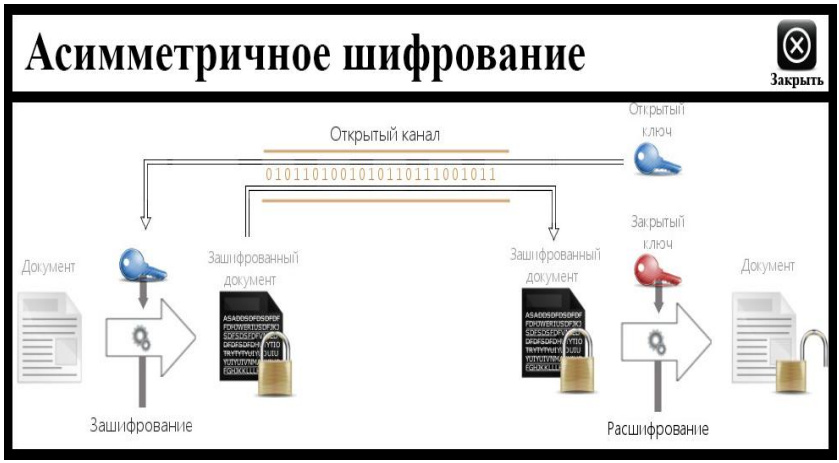

Рис.1.Асимметричная схема шифрования

Симметричная схема шифрования - шифрование выполняется с помощью открытого ключа, а расшифровка - с помощью закрытого Разъясним общую суть схемы подписания цифровой подписи: с помощью криптографической хэш-функции определяется короткая строка знаков фиксированной длины (хэш). Затем этот хэш кодируется закрытым ключом обладателя - результатом будет является подпись документа. После этого полученная подпись прикладывается к документу, в результате чего получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом ключа.(Рис.2) владельца, а также вычисляет хэш документа. При проверке документа на подлинность вычисленный по документу хэш сравнивают с расшифрованным из подписи, в противном случае документ является подделанным. Каждая электронная цифровая подпись выдается на защищенном электронном носителе, похожим на обычную флешку. Такая флешка защищает от случайного или умышленного удаления содержащейся на ней информации, так как

обладает дополнительными функциями ее защиты**.**

Рис.2.Симметричная схема шифрования

Для того, чтобы применение цифровой подписи имело значение, требуется исполнение двух условий:

Во-первых, доказательство подписи должно совершаться открытым ключом, отвечающим именно тому закрытому ключу, который использовался при подписании. Во-вторых, без владения закрытым ключом должно быть вычислительно трудно сформировать неподдельную цифровую подпись.

Наиболее известные средства работы с электронной подписью.

Самый известный - это пакет PGP (Pretty Good Privacy), который позволяет использовать достоверные криптографические схемы для защиты информации в ПК. Данная программа бесплатна, ее интерфейс удобен для использования в широких кругах пользователей, а также он поддерживает различные модели распределения открытых ключей.

Криптон - пакет программ, предназначенный для применения цифровой подписи для электронных документов. Помимо дискет, пакет Криптон дает возможность использования многих других типов ключевых носителей (USB-БРЕЛКИ, смарт-карт, электронных таблеток Touch Memory и др.)

Таким образом можно сделать вывод, что в наше время электронная подпись доступна не только предпринимателям, владельцем сертификата ключа может стать любое физическое лицо и как нам стало известно, процедура оформления такой подписи чрезвычайна проста. Также электронная цифровая подпись является своего рода «анало-

гом» паспорта гражданина РФ. Получив электронную подпись, любой гражданин России сможет отправить в налоговую инспекцию декларацию о доходах физических лиц, подать заявление в ФМС на оформление загранпаспорта и многое другое. Для этого уже не придется ездить по различным инстанциям и тратить время на бесконечные очереди, что во многом облегчит жизнь современного общества.

Библиографический список:

1. Федеральный закон «Об электронной цифровой подписи» от 6 апреля 2011 года № 63-ФЗ.

2. Малофеев С.О применении электронной цифровой подписи в электронном документообороте // Секретарское дело. - 2009. - № 7. - С. 24-28.

3. Лермонтов Ю. Усиленная квалифицированная электронная подпись / Ю. Лермонтов // Аудит и налогообложение. - 2011. - N 10. - С. 12-14.

4. Мещеряков В. Первый российский чип для ключа электронной подписи/ В. Мещеряков // Экономическая безопасность предприятия. - 2015. - N 2. - С. 51.

ELECTRONIC SIGNATURE AND ITS APPLICATION.

Khamzina E.I., Golubev S. V.

Key words: electronic digital signature, information technology, hash, hash function, public key, private key.

This work is devoted to a topical problem of using an electronic digital signature by juristical and individuals and to it's development.

Контактная информация:

e-mail: elwi.khamzina@yandex.ru тел.: 89374542893

УДК 004+631.17

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ПРИНЯТИЯ ОПТИМАЛЬНЫХ РЕШЕНИЙ

Чашлёнкова А.А., Захарова Е.Н., студентки 2 курса экономического факультета

Научный руководитель – Заживнова О.А., кандидат экономических наук, доцент

ФГБОУ ВО Ульяновская ГСХА