УДК 003.26

ЭЛЕКТРОННАЯ ПОДПИСЬ: ПРЕИМУЩЕСТВА И НЕДОСТАТКИ

А.С. СИВОГРАКОВ
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В данной работе были проанализированы преимущества и недостатки электронной подписи.

В настоящее время что бы упростить подписание документов и заключение договоров без личного присутствия лиц, заключавших различного рода акты, используют электронные подписи. Но не смотря на преимущества данной технологии имеется и ряд её недостатков.

Эта тема востребована, ввиду широким внедрением в повседневную жизнь новых электронных технологий, в том числе внедрение технологии электронной цифровой подписи (ЭЦП) идет активно в различных государственных структурах. Само определение электронной подписи имеет следующую формулировку: это информация в электронно-цифровой форме, с помощью которой можно идентифицировать физическое или юридическое лицо без его личного присутствия [1].

Применение электронной цифровой подписи. Наиболее активное применение электронной цифровой подписи можно встретить в таких областях как:

1. система делопроизводства в электронном формате;
2. цифровая торговля;
3. ведение бухгалтерии;
4. бизнес;
5. платежные системы.

Назначение ЭП:

1. позволяет осуществить контроль целостности документа в электронном виде;
2. обеспечивает защиту данных от подделки и внесения изменений;
3. обеспечивает возможность подтверждения авторства владельца ЭП.

Существуют различные способы сформировать электронную подпись. Самым удобным и распространенным из них является создание ЭП с помощью электронного ключа.

Электронный ключ – ключевая пара, которая состоит из двух частей: открытой и закрытой. Оба этих ключа выдаются и создаются удостоверяющими центрами с помощью специальной программы шифрования (например, «Крипто-про»).

Закрытый ключ – или «Ключ электронной подписи» – уникальная последовательность символов, предназначенная для создания ЭП и для расшифровки сообщений. Это частная, приватная информация, которая известна только ее владельцу.

Закрытый ключ генерируется на рабочем месте пользователя с помощью средства криптографической защиты информации и сохраняется (только у пользователя) на съемный носитель (дискета, токен, смарт-карта) или в реестр Windows. Такой закрытый ключ необходимо хранить в секретном месте со всеми мерами предосторожностей.

На основе закрытого ключа создается открытый ключ (стоит сказать, что обратный процесс здесь невозможен, так как подобрать закрытый ключ по открытому ключу нельзя).

Открытый ключ – он же «Ключ проверки электронной подписи» – уникальная последовательность символов, предназначенная для проверки подлинности ЭП. Это открытая, общеизвестная информация доступна любому пользователю системы электронного документооборота.

Открытый ключ вычисляется из закрытого ключа и отправляется в Удостоверяющий центр в виде запроса на сертификат.

Сертификат является электронным (и/или бумажным) документом:

1. выдаётся на ФИО конкретного человека (должностного лица) - содержит персональные данные;
2. подписывается ЭП Удостоверяющего центра, который тем самым подтверждает его действительность;
3. сертификат в себе содержит открытый ключ Пользователя (поэтому открытый ключ называют сертификатом).

Определяются следующие виды ЭП: простая и усиленная электронные подписи. В свою очередь усиленная электронная подпись подразделяется на усиленную неквалифицированную электронную подпись (именуемую неквалифицированная электронная подпись) и усиленную квалифицированную электронную подпись (именуемую квалифицированная электронная подпись).

Простая электронная подпись. Простая ЭП – это максимально упрощенный вариант электронной подписи. Для ее создания не используются криптографические модули. Наиболее ярким примером, попадающим под определение простой электронной подписи, являются SMS-пароли, а также данные для доступа к различным информационным сервисам.

Часто используется вариант простой электронной подписи в банковских системах для подтверждения платежей и других операций. Она может также применяться в следующих случаях:

1. при получении госуслуг через официальный портал (доступны не все операции);
2. во внутренних системах документооборота (обмен между сотрудниками компании);
3. во внешних системах при наличии дополнительного соглашения;
4. при входе на различные сайты.

Данный вариант цифровой подписи недопустимо применять в системах, где приходится сталкиваться с гостайной. Это ограничение установлено на законодательном уровне.

Усиленная неквалифицированная электронная подпись. Усиленная неквалифицированная ЭП создается уже с помощью криптографического ПО. При этом используется закрытый ключ ЭП. Она позволяет проверить личность владельца, а также отсутствие изменений в подписанном файле.

При получении подписи владельцу передаются открытый и закрытый ключи ЭП. Открытый ключ ЭП нужен для проверки подлинности подписи, а закрытый используется в момент подписания файла (документа). Фактически открытый ключ доступен всем. Выдавать НЭП могут различные УЦ. Аккредитация для этого не требуется.

Довольно часто НЭП используется для участия в различных торгах.

Усиленная квалифицированная электронная подпись. Это самая защищенная разновидность ЭП; это ЭП, которая создается с применением криптографических средств, подтвержденных компетентными органами. Гарантом подлинности такой подписи служит специальный сертификат, который выдаётся аккредитованным удостоверяющим центром.

Применение КЭП значительно шире. Она применяется при участии в различных торгах в качестве поставщика и заказчика, с использованием нее может проводиться документооборот внутри компании и с партнерами. А также с помощью нее сдаются отчеты в различные госорганы.

Существуют специальные криптопрограммы для работы с ЭП:

1. КриптоПро CSP
2. ViPNet CSP
3. КриптоАРМ

Схема ЭП предусматривает следующие процессы:

1. генерация ключей ЭП и ключей проверки ЭП;
2. формирование ЭП;
3. проверка ЭП.

Механизм ЭП определяется реализацией двух важных процессов:

1. формирование ЭП;
2. проверка ЭП.

Применение ЭП позволяет осуществить следующие функции при передаче в системе подписанного ЭП сообщения:

1. осуществление контроля целостности передаваемого подписанного ЭП сообщения;
2. доказательная идентификация лица, подписавшего сообщение при помощи ЭП;
3. защита сообщения от возможной подделки.

Взлом ЭП на практике представляет собой взлом алгоритма шифрования. Для полной защиты своих данных недостаточным является защита выполнения алгоритма RSA и применение мер математической безопасности, иными словами, использование ключа достаточной длины, поскольку на практике наилучший результат имеют те атаки, которые производятся на незащищенные этапы управления ключами системы RSA.

Вывод. В результате научно-практического исследования были проанализированы преимущества и недостатки электронной цифровой подписи. Несмотря на имеющиеся недостатки ЭП, можно сделать вывод о подавляющем количестве преимуществ её использования.

ЛИТЕРАТУРА

1. Электронный ресурс «Подводные камни» простой электронной подписи». – Режим доступа: https://habr.com/ru/post/313982. Дата обращения: 25.08.2020.
2. Электронный ресурс «Применение электронной подписи». – Режим доступа: http://elektronnayapodpis.ru/wiki/primenenie. – Дата доступа: 25.08.2020.
3. Электронный ресурс «Виды электронной подписи (ЭЦП)». – Режим доступа: https://ca.kontur.ru/articles/vidy-ehlektronnoj-podpisi-ecp. – Дата доступа: 25.08.2020.
4. Электронный ресурс «Неквалифицированная электронная подпись». – Режим доступа: http://elektronnayapodpis.ru/wiki/nekvalifitsirovannaya. – Дата доступа: 25.08.2020.
5. Электронный ресурс «Программы и приложения для ЭЦП». – Режим доступа: https://ececp.ru/programmy-i-prilozheniya-dlya-ecp. – Дата доступа: 25.08.2020.