МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ ЭЛЕКТРОННОГО ОБМЕНА СТАНДАРТИЗОВАННЫМИ МЕДИЦИНСКИМИ ДОКУМЕНТАМИ*

В.В. Кириллов, Г.Ю. Громов

В статье приведены результаты исследования средств организации защиты информации в автоматизированной системе электронного обмена стандартизованными медицинскими документами. В качестве инструментальной среды системы используются Microsoft Office 2003 и средство криптографической защиты информации компании КриптоПро. Рассматриваются методы их взаимодействия и результаты использования медицинскими работниками.

Введение

Технические требования к автоматизированной системе электронного обмена стандартизованными медицинскими документами (АС ОСМД) предлагают использовать конкретный инструментарий для визуализации и доступа авторизованных пользователей системы к стандартизованным медицинским документам (СМД) – это проводник Интернета Microsoft Internet Explorer 6.0 SP1 и пакет офисной автоматизации Microsoft Office 2003 Pro Rus SP2, включая InfoPath 2003. Там же указывается, что должна быть предусмотрена возможность электронной подписи СМД (одним или несколькими лицами) и их шифрование при передаче по незащищенным каналам связи. При этом следует применять сертифицированные в России программные средства криптографической защиты информации.

Исследование предлагаемых средств подготовки, пересылки и просмотра СМД показало, что в них предусмотрены механизмы, позволяющие пользователям подписать СМД или его части, а также зашифровать пересылаемый СМД (рис. 1). Естественно, что они позволяют расшифровать зашифрованный СМД и проверить наличие цифровой подписи на СВД, а также определить автора подписи и время подписания.

В связи с этим основное внимание было уделено выбору сертифицированных в России программных средств криптографической защиты информации и их использования совместно с Microsoft Office 2003.

Электронная подпись

Основное назначение электронной подписи документа – обеспечение аутентичности как самого документа, так его автора, т.е. доказательство, что документ действительно заверен отправителем и что содержимое этого документа не было изменено в процессе пересылки по каналам связи. Технология электронных подписей является основой для безопасного функционирования систем документооборота. Эта подпись отличается от обычной подписи на бумажном документе тем, что она не только подтверждает личность отправителя документа, но также и гарантирует, что его содержание не модифицировалось по пути от отправителя к адресату.

Электронная подпись – это данные в электронной форме, которые содержатся в документе, приложены к нему или логически связаны с ним и которые могут быть использованы для идентификации подписавшего и указания на то, что подписавший согласен с информацией, содержавшейся в сообщении [1]. Отправитель формирует ее, обрабатывая исходный документ соответствующей процедурой, называемой функцией

* Работа выполнена в рамках ГК №02.467.11.1007 от "10" октября 2005 года "N2005-ИТ-00.2/002 Разработка системы электронного обмена стандартизованными документами на основе Интернет- и Интранет-порталов для ускорения документооборота в медицинских учреждениях страны"

«Электронной подписи». Внешне электронная подпись выглядит как случайные данные и имеет смысл только при использовании совместно с исходным документом. Получатель этого документа проверяет электронную подпись с помощью другого набора вычислений – так называемой функции «проверки электронной подписи». Результат этой проверки должен подтвердить аутентичность как самого отправителя, так и полученного от него документа.

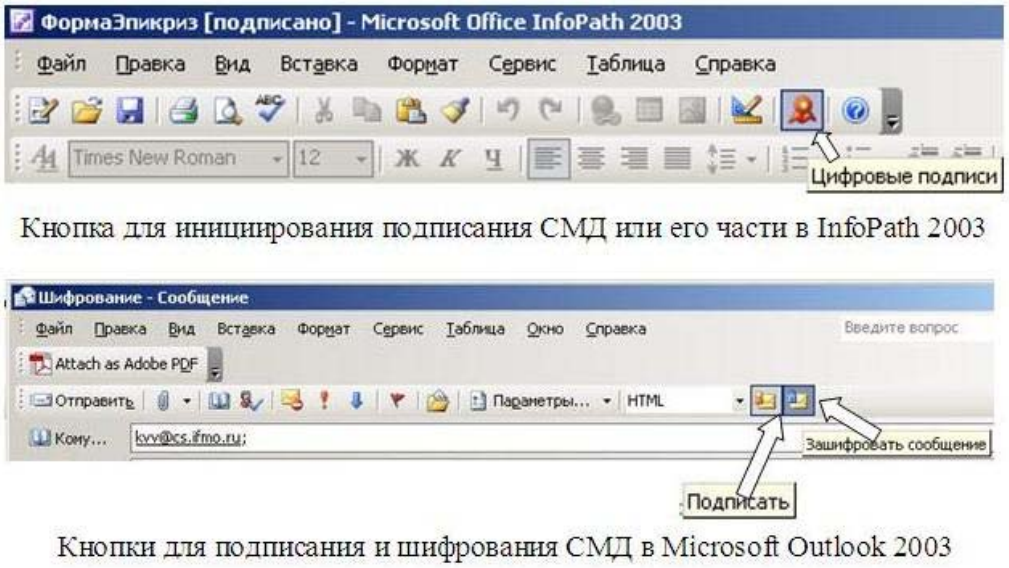


Рис. 1. Средства шифрования и/или подписания СМД

Надо отметить, что существует два почти синонимических понятия: «электронная подпись» и «электронная цифровая подпись», которые на самом деле имеют существенное различие [2]. Большинство мировых нормативных актов в этой области, например, Типовой закон Комиссии ООН по праву в международной торговле ЮНСИТРАЛ оперируют понятием «электронная подпись». Оно объединяет целый спектр электронных технологий: это не только математические алгоритмы, реализованные в цифре на компьютерах, но и такие биометрические, как сканирование отпечатков пальцев, сетчатки глаза, спектральных характеристик голоса, а в перспективе и молекул ДНК. В подлинности электронного сообщения можно убедиться, используя также специальные ПИН-коды, смарт-карты, маркеры, принадлежащие подписывающему лицу. Такое расширенное толкование понятно, оправдано и дальновидно, ведь сейчас невозможно надежно предсказать, какая именно технология электронной подписи будет доминирующей. Современные электронные и программные средства развиваются так быстро, что делать ставку на какой-то один вариант электронной подписи крайне рискованно. Быстрый прогресс может внезапно свести на нет длительные законотворческие усилия и большие затраты на внедрение, тем более, если внедрение будет тотально-принудительным. Однако в Федеральном законе Российской Федерации от 10 января 2002 г. N 1-ФЗ «Об электронной цифровой подписи» она жестко привязана к единственной криптографической технологии, создаваемой методом шифрования с помощью открытых ключей.

Сама по себе эта методика сейчас является одной из самых развитых, и у нее есть серьезные достоинства. Суть шифрования с открытым ключом, частью которого является электронная цифровая подпись, такова. Участники переписки должны иметь одинаковый инструмент шифрования-дешифрования. Обычно это компьютер, снабженный соответствующей программой. В начале программа автоматически создает два ключа, применяющиеся исключительно в паре. Открытый ключ можно послать по почте по-

тенциальным партнерам, разместить в Интернете, отправить в местное отделение ФАПСИ.

Вы подписываете послание с помощью закрытого секретного ключа, а проверить авторство документа может любой, кому вы пошлете или кто не поленится скачать из базы данных в Интернете ваш открытый ключ.

Используя свой закрытый ключ и открытый ключ партнера, вы можете создать ключ шифрования и зашифровывать послание на адрес этого партнера. Для прочтения такого сообщения партнер должен создать ключ расшифровки из своего закрытого и вашего открытого ключей.

Степень защиты цифровой подписи от подделки так же высока, как степень стойкости при шифровании (стойкость оценивается объемами вычислений, которые требуются для ее вскрытия – считается, что ключ шифрования достаточно стоек, если все известные способы его отыскать настолько сложны, что требуют больше времени, чем простой перебор всех возможных ключей). Важно, что можно подписывать сообщение как шифруя, так и не шифруя его – оставляя открытым. Математические алгоритмы шифрования с открытым ключом при длине ключа в несколько килобит делают при нынешних знаниях задачу взлома практически неразрешимой. Такие алгоритмы реализованы практически всеми современными системами.

Итак, схема цифровой подписи или электронно-цифровой подписи – это набор алгоритмов и протоколов, позволяющих построить информационное взаимодействие между двумя и более участниками таким образом, чтобы факт авторства переданного массива данных, «подписанного» одним из участников, мог быть надежно подтвержден или опровергнут третьей стороной – «независимым арбитражем». Любая схема цифровой подписи предполагает добавление к «подписываемому» массиву данных дополнительного кода – собственно «цифровой подписи», выработать который может только автор сообщения, обладающий секретным (закрытым) ключом подписи, а все остальные могут лишь проверить соответствие этой «подписи» подписанным данным. Поэтому каждая схема должна предусмотреть, как минимум, определение трех следующих алгоритмов:

- выработки пары ключей – подписи и проверки подписи с использованием вектора случайных параметров;
- подписи сообщения с использованием ключа подписи;
- проверки подписи с использованием ключа проверки подписи, выдающего в качестве результата булево значение – подтверждается или не подтверждается авторство сообщения.

Цифровые сертификаты

В соответствии с Федеральным законом об электронной цифровой подписи организации, участвующие в документообороте с Федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации и органами местного самоуправления, должны использовать для организации процедуры подписывания только сертифицированное программное обеспечение и иметь лицензию ФСБ России и Государственной Технической комиссии при президенте Российской федерации.

К такому программному обеспечению относится криптопровайдер «Крипто-Про CSP» и удостоверяющий центр «КриптоПро УЦ». С его помощью учреждение может организовать в своем составе локальный центр сертификации, позволяющий обеспечить пользователей средствами и спецификациями для использования сертификатов открытых ключей в целях:

- контроля целостности электронных документов, передаваемых в автоматизированных информационных системах;
- контроля целостности публичных информационных ресурсов;
- проверки подлинности взаимодействующих программных компонентов и конфиденциальности передаваемых данных при информационном взаимодействии;
- создания системы юридически значимой электронной цифровой подписи в системах электронного документооборота;
- обеспечения безопасности и разграничения доступа при взаимодействии субъектов автоматизированных информационных систем;
- создания иерархической системы управления ключами подписи субъектов автоматизированных информационных систем.

Подчеркнем, что самостоятельно созданный в Microsoft InfoPath цифровой сертификат не является сертификатом, выданным официальным центром сертификации, поэтому все формы, подписанные с использованием такого сертификата, рассматриваются как формы с собственной подписью. Такие сертификаты считаются непроверенными и могут быть причиной появления предупреждения системы безопасности, если для формы задан высокий или средний уровень безопасности. Microsoft InfoPath доверяет сертификатам с собственной подписью только в том случае, если сертификат располагается на компьютере, имеющем доступ к закрытому ключу этого сертификата. Как правило, это означает, что Microsoft InfoPath доверяет сертификатам с собственной подписью только на компьютере, на котором создавался сертификат, если только закрытый ключ не предоставлен для общего доступа другим компьютерам.

В лечебном учреждении должна существовать служба криптографической защиты информации, которая, используя возможности собственного локального или другого Центра Сертификации, снабжает пользователей учреждения личными закрытыми и открытыми ключами ЭЦП и шифрования, а также устанавливает на компьютеры пользователей программное обеспечение, необходимое для подписания подготавливаемых ими документов, а также проверки цифровых подписей получаемых документов.

Подписание шаблонов и форм СМД

В автоматизированной системе электронного обмена СМД необходимо иметь в ее составе набор шаблонов для заполнения следующих документов:

- направление на лабораторное исследование;
- направление на диагностическое исследование;
- направление на консультацию;
- результат лабораторного исследования;
- протокол диагностического исследования;
- заключение консультанта;
- рецепт в аптеку;
- выписка из истории болезни (амбулаторной карты) пациента.

Для обеспечения возможности подписания шаблона формы, созданного в InfoPath, необходимо иметь:

- установленное программное обеспечение криптопровайдера КриптоПро CSP, который имеет сертификат ФАПСИ и может использоваться для формирования ключей шифрования и ключей электронной цифровой подписи, шифрования и имитозащиты данных, обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну;
- цифровые сертификаты, полученные у сетевого администратора, занимающегося в учреждении вопросами безопасности.

При разработке шаблона можно разрешить цифровые подписи для всей формы или для ее отдельных частей. Если разрешены подписи для части формы, необходимо определить, какие данные в форме должны быть подписаны. Можно дополнительно связать эти данные с разделом формы. После того, как пользователь подписал форму, данные блокируются, так что их изменение невозможно, и сохраняется их представление с цифровой подписью.

Помимо этого можно указать, разрешается ли использование нескольких подписей для одной формы и, если разрешается, то должны ли это быть совместные подписи (когда каждая подпись не зависит от остальных) или же удостоверяющие подписи (когда каждая следующая подпись удостоверяет как саму форму, так и все предшествующие ей подписи).

Кроме разрешения использования цифровой подписи в формах, благодаря чему пользователи получают возможность подписывать форму, можно подписать цифровой подписью и шаблон формы, что удостоверяет подлинность автора шаблона формы точно таким же образом, как цифровая подпись формы удостоверяет подлинность заполнившего форму.

При заполнении формы можно добавить цифровую подпись ко всей форме или к ее части, в зависимости от настроек в шаблоне формы. Снабжать цифровой подписью можно только те формы и их части, при разработке которых была предусмотрена такая возможность. Можно также удалять или проверять цифровые подписи.

Заключение

Исследование применения Microsoft Office 2003 и средств криптографической защиты информации компании КриптоПро для шифрования и подписания СМД показало, что сотрудники медицинских учреждений, имеющие навыки работы со средствами офисной автоматизации (текстовым редактором, редактором электронных таблиц и т.п.) и стандартными проводниками Интернет, успешно справляются с работой в среде АС ОСМД.

Литература

1. Романец Ю., Тимофеев П., Шаньгин В. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2001. 376 с.
2. Баричев С., Серов С. Основы современной криптографии. М.: Радио и связь, 2001. 121с.