5. *Оленко, Е.С.* Особенности висцеропатий у больных опийной наркоманией / Е.С.Оленко, Ю.И. Скворцов, Л.Ф.Панченко // Вопросы наркологии. – 2001. – №2. – С.65–75.
6. *Кошкина, Е.А.* Современные эпидемиологические методы мониторинга распространенности употребления наркотиков / Е.А.Кошкина // Вопросы наркологии. –2006. – №1. – С.64–73.
7. *Кошкина, Е.А.* Исследование "скрытого" контингента потребителей наркотических веществ методом "повторного захвата" в г. Чапаевске Самарской области в 2000–2001 гг. / Е.А.Кошкина, С.А.-Корякин, С.А.Царев // Вопросы наркологии. – 2002. – №4. – С.56–59.
8. *Мелешко, Л.А.* Результаты дозорного эпидемиологического надзора за ВИЧ–инфекцией в Республике Беларусь. Отчет об исследовании, проведенном в 2006 году / Л.А.Мелешко, Е.А.Кечина, О.М. Ждановская, С.В.Сергиенко, В.П.Зелюткин. – Минск: ООО "Ковчег", 2007. – 43 с.
9. Национальный отчет о выполнении Декларации о приверженности делу борьбы с ВИЧ/СПИДом: Республика Беларусь. Отчетный период: январь 2006 – декабрь 2007 г. / сост. В.М.Быкова [и др.] под общ. ред. М.И.Римжи. – Минск: Альтиора – Живые Краски, 2008. – С.11–13.

Поступила 14.07.2008 г.

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ В ТЕЛЕМЕДИЦИНЕ

Л.Н.Величко, Л.П.Качура, Ю.Н.Метлицкий, В.О.Чернышев

ЗАО "НПП БелСофт", г. Минск

Описаны процесс формирования электронной цифровой подписи (ЭЦП), информационная технология создания ЭЦП, технология построения автоматизированных систем электронного документооборота (АСЭД), основные преимущества, угрозы и проблемные вопросы при использовании ЭЦП.

Современные информационные технологии, подтверждающие авторство и целостность электронного документооборота в здравоохранении, основываются на формировании цифровой подписи (digital signature), которая уникальна для каждого автора. Особое значение электронная цифровая подпись (ЭЦП) приобретает при реализации территориально-распределенного документооборота, когда требуется признание ее аналогом собственноручной подписи с возможностью проверки третьей стороной (удостоверяющим центром), не участвующей в самом процессе документооборота и пользующейся доверием его участников.

ЭЦП представляет собой реквизит медицинского электронного документа, предназначенный для удостоверения источника и целостности документального сообщения и его защиты от подделок. Она применяется в качестве средства для идентификации и подтверждения юридической значимости медицинских документов. ЭЦП выполняется в виде последовательности символов, полученной в результате криптографического преобразования электронных данных.

В общем случае формирование ЭЦП, подтверждающей авторство документального сообщения, основывается на знании уникальных закрытого (известен только автору подписи) и открытого (известен всем) криптографических ключей. При этом закрытый ключ представляет собой некоторую информацию длиной 256 бит, которая хранится у пользователя в недоступном другим лицам месте на дискете, смарт-карте и т.п. С его помощью производится шифрование электронных медицинских документов и формируется ЭЦП. Открытый ключ используется для проверки ЭЦП получаемых документов-файлов длиной 1024 бита. Дубликат открытого ключа находится в удостоверяющем центре, который обеспечивает его регистрацию и надежное хранение во избежание внесения искажений или попыток подделки. Закрытый и открытый ключи работают только в паре. При этом необходимо вычислить значение ЭЦП на закрытом ключе, а открытый ключ сообщить всем участникам документооборота и проверяющим ЭЦП.

Для обеспечения доверия к открытым ключам и их защиты от подмены в общедоступных медицинских автоматизированных системах электронного документооборота (АСЭД) используется механизм распределения ключей, называемый инфраструктурой открытых ключей, основанный на цифровых сертификатах, выдаваемых удостове-

ряющим центром. Цифровой сертификат содержит в себе открытый ключ, данные, позволяющие идентифицировать его владельца и дополнительную информацию (срок действия открытого ключа и т.п.). Сам сертификат подписывается ЭЦП удостоверяющего центра, открытый ключ которого получает каждый из участников электронного документооборота при первоначальном подключении к АСЭД. При этом вводится система обязательного лицензирования деятельности удостоверяющего центра, поскольку от качества его услуг зависит безопасность электронного документооборота в здравоохранении. Управлением ключами занимаются центры распространения сертификатов, осуществляющие выдачу сертификата какого-либо пользователя, а также проверку наличия или отзыва того или иного открытого ключа.

При установке ЭЦП под электронным медицинским документом на основе закрытого ключа происходит криптографическое преобразование, в результате которого вырабатывается некоторое большое число, являющееся ЭЦП данного пользователя под данным конкретным документом. В ЭЦП закладывается следующая информация: имя файла открытого ключа, информация об отправителе и дата формирования подписи. Получатель на основе текста документа и открытого ключа отправителя выполняет обратное криптографическое преобразование, обеспечивающее проверку ЭЦП отправителя.

Информационная технология создания ЭЦП включает в себя следующие составляющие:

• алгоритм (в Российской Федерации определяется ГОСТ Р 34.10/34.11-94) генерации ключевых пар пользователя;

• функцию вычисления подписи;

• операцию проверки подписи.

На основе электронного документа и закрытого ключа осуществляется функция вычисления ЭЦП, которая в зависимости от алгоритма может быть детерминированной или вероятностной. Детерминированная функция всегда обеспечивает вычисление одинаковой ЭЦП по одинаковым входным данным. Практически в настоящее время детерминированные решения не используются. Даже в изначально детерминированные алгоритмы сейчас вносятся модификации, превращающие их в вероятностные. Вероятностные функции вычисления ЭЦП вносят в подпись элемент случайности, что повышает криптостойкость алгоритмов ключевых пар пользователя. Для этого необходим надежный источник случайных цифр, который может быть включен в виде генератора шума либо генератора псевдослучайных бит. Операция проверки ЭЦП призвана выяснить соответствует ли данная подпись конкретному документу и открытому ключу пользователя, который доступен всем.

В случае, кода подписываемый электронный документ достаточно больших размеров (длины), ЭЦП ставится не на сам документ, а на его хэш (отдельный файл), для вычисления которого используются любые криптографические хэш-функции, что гарантирует выявление изменений документа при проверке подписи. Хэширование - это преобразование входного потока данных в хэш, представляющий собой короткое число фиксированной длины. При этом необходимо, чтобы это число было значительно короче исходных данных и однозначно с большой вероятностью им соответствовало.

Алгоритмы ЭЦП подразделяются на два больших класса:

1. Обычные цифровые подписи, которые необходимо присоединять к подписываемому документу.

2. Цифровые подписи с восстановлением документа, в процессе проверки которых автоматически вычисляется и “тело” подписываемого документа.

Следует заметить, что в последние годы наблюдается устойчивая тенденция снижения количества АСЭД, в которых используются более дешевые средства ЭЦП, встроенные в операционные системы с последующим их переводом на сертифицированные платформы ЭЦП. Наряду с выбором алгоритма и реализующей его технологии, немаловажную роль играет механизм распределения и обмена ключей, т.е. криптопротокол. Конфиденциальность закрытого ключа ЭЦП и целостность доступного для всех участников электронного документооборота открытого ключа позволяют аутентифицировать автора сообщения.

Технологию построения АСЭД можно представить следующим образом: между каждой организацией здравоохранения и центром заключается договор, и стороны подключаются к услугам удостоверяющего центра с возможностью подписания электронных документов ЭЦП. При этом если у удостоверяющего центра есть региональные представительства, то стороны могут быть территориально удалены друг от друга. На эффективности электронного документооборота не сказываются разовые взаимоотношения сторон, так как, единожды заключив договор с удостоверяющим центром, обеспечивается возможность работы с любым из его клиентов.

На практике электронный документооборот осуществляется либо между несколькими круп-

ными организациями здравоохранения, где все участники в той или иной степени равноправны, либо между выделенным организатором и большим числом клиентов. В первом случае стоимость электронных транзакций достаточно велика, и участники приобретают коммерческие версии средств криптографической защиты ЭЦП. Во втором случае выбор технологии ЭЦП остается за организатором АСЭД, перед которым стоит непростая задача – предложить информационную технологию, удовлетворяющую всех клиентов.

Использование ЭЦП для подтверждения авторства циркулирующих документов между медицинскими организациями возможно в случае заключения ими предварительного соглашения, что делает АСЭД замкнутой. Как правило, порядок работы в такой системе устанавливается ее организатором. При этом необходимо, чтобы используемые технологии и применяемые алгоритмы ЭЦП удовлетворяли каждую из сторон документооборота. В большинстве случаев необходимый уровень безопасности обеспечивается криптографическими устройствами формирования и проверки ЭЦП, которые встраиваются в операционную систему, что позволяет существенно сократить затраты на создание географически распределенных АСЭД.

Таким образом, ЭЦП обеспечивает:

1. Удостоверение источника документа, при котором могут быть подписаны поля "автор", "внесенные изменения", "метка времени" и т.п.

2. Защиту от изменений документа или подписи, при которой изменяется хэш, следовательно, подпись становится недействительной.

3. Невозможность отказа от авторства, так как закрытый ключ известен только его владельцу.

Основные преимущества ЭЦП заключаются в возможности подписания документов без предварительного соглашения между сторонами и проверки подлинности электронного документа удостоверяющим центром. Для того, чтобы подписанный ЭЦП электронный документ был признан подлинным аналогом бумажного документа, вводятся жесткие ограничения по организации и технологии формирования ЭЦП. Одно из таких ограничений – использование только сертифицированных технологий ЭЦП, так как электронные документы с ЭЦП могут быть представлены третьим лицам, проверяющим органам или затребованы даже судом.

Вполне очевидно, что ЭЦП вовсе не совершенна, информационная технология ее создания не может обеспечить ее абсолютную безопасность. Она может быть подвержена взлому и угрозам. Взлом ЭЦП фактически сводится к взлому алгоритма. При этом наиболее эффективный способ взлома ЭЦП – найти закрытый ключ, соответствующий необходимому открытому ключу, что позволит злоумышленнику читать все сообщения, зашифрованные открытым ключом, и подделывать подписи. Другой способ взлома заключается в нахождении методов вычисления и создания ЭЦП. Существуют и другие способы взлома ЭЦП.

Со стороны злоумышленника возможны следующие угрозы ЭЦП:

• попытаться подделать подпись для выбранного медицинского документа;

• подобрать подходящий документ к данной подписи;

• попытаться подделать подпись хотя бы для какого-нибудь одного документа;

• в случае кражи ключа подписать любой документ от имени его владельца;

• обманным путем заставить владельца ключа подписать какой-либо документ;

• подменить открытый ключ владельца на свой собственный, выдавая себя за него.

При использовании надежной хэш-функции вычислительно сложно создать поддельный документ с таким же хэшем, как у подлинного. Однако перечисленные угрозы могут быть реализованы злоумышленником из-за слабостей принятых алгоритмов хэширования подписи или ошибок при реализации.

Несмотря на схожесть решаемых задач по обеспечению целостности электронного медицинского документа и "неотказуемости" авторства, следует различать ЭЦП и код аутентификации сообщения. Код аутентификации представляет собой закодированное сообщение фиксированной длины, вырабатываемое на основе данных закрытого ключа и добавляемое к документу с целью обнаружения факта изменения хранимой или передаваемой по каналам связи информации. В отличие от асимметричных алгоритмов ЭЦП коды аутентификации вычисляются по симметричным схемам.

Перспективы использования ЭЦП в электронном документообороте здравоохранения как внутри медицинской организации, так и между ними, сомнений не вызывают. Однако реализация ЭЦП связана с решением ряда правовых и лицензионных вопросов ее использования в открытых АСЭД. При этом основное внимание должно быть обращено на обеспечение информационной безопасности, гарантирующее подтверждение авторства и целостности медицинских документов с ЭЦП, циркулирующих в АСЭД здравоохранения.

Поступила 12.08.2008 г.