УДК 004.056.55

Переход на криптографические алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в программных продуктах линейки «1С: Медицина»

© А.С. Балюк, В.А. Попова
Иркутский государственный университет,
г. Иркутск, Российская Федерация

С 1 января 2019 года в Российской Федерации введены в использование стандарты ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 для электронной подписи и хеширования соответственно. Ранее использовавшиеся стандарты ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 могут применяться до конца текущего года. Таким образом, исходя из требований законодательства, все системы электронного документооборота в 2019 году должны иметь возможность использовать два стандарта как для электронной подписи, так и для хеширования. В данной работе описывается реализованная поддержка криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в программных продуктах линейки «1С: Медицина», которые относятся к системам электронного документооборота и используются в медицинских организациях по всей России. Перечисляются факторы, ввиду которых замена стандартов является достаточно длительным процессом. Описываются основные принципы работы электронной подписи и шифрования. Приводятся схемы подписания и шифрования в программах линейки «1С: Медицина». Определяется применение в схеме шифрования стандартов линейки ГОСТ Р 34.10. Описываются внесённые изменения в схемы электронной подписи и шифрования для обеспечения возможности использовать алгоритмы ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 в программных продуктах линейки «1С: Медицина».

Ключевые слова: криптографические алгоритмы, электронная подпись, шифрование, хеширование

Transition to Cryptographic Algorithms GOST R 34.10-2012 and GOST R 34.11-2012 in Software Products of the «1C: Medicine» line

© Alexander S. Balyuk, Victoria A. Popova
Irkutsk State University,
Irkutsk, Russian Federation

Since January 1, 2019, the Russian Federation has introduced GOST R 34.10-2012 and GOST R 34.11-2012 standards for electronic signature and hashing, respectively. Previously existing standards GOST R 34.10-2001 and GOST R 34.11-94 can be applied until the end of 2019. Thus, according to the requirements of the legislation, all electronic document management systems in 2019 should be able to use two state standards for both electronic signature and hashing. This article describes the implemented support of cryptographic algorithms GOST R 34.10-2012 and GOST R 34.11-2012 in the software products of the line «1C: Medicine», which relate to electronic document management systems and are used in medical organizations in Russia. The article lists the factors in view of which the replacement of standards is a rather lengthy process and describes the basic principles of electronic signature and encryption. It also provides the schemes of signing and encryption in the software products of the line «1C: Medicine». The authors revealed the use of encryption scheme standards GOST R 34.10. This article also describes the changes in the electronic signature and encryption schemes to enable the use of algorithms GOST R 34.10-2012 and GOST R 34.11-2012 in the software products of the line «1C: Medicine».

Keywords: cryptographic algorithms, electronic signature, encryption, hashing

Современные информационные технологии позволяют полностью перейти на системы электронного документооборота, тем самым предоставляя возможность отказаться от использования традиционных бумажных носителей информации.

Электронный документооборот – это механизм, который включает в себя приём, рассылку, хранение и повторное использование документов в электронном виде [1]. Он позволяет снизить затраты на распечатку, пересылку и хранение документов.

Несмотря на преимущества, в электронные документы, в отличие от бумажных аналогов, легче внести изменения и труднее доказать факт их подлинности [2]. Также требуется, чтобы электронный документ обладал юридической силой [3, 1].

Для осуществления наиболее безопасного обмена электронными документами следует применять криптографические алгоритмы электронной подписи и шифрования. Электронная подпись позволяет подтвердить личность автора документа [4], а шифрование обеспечивает конфиденциальность передаваемой информации [5].

В настоящий момент алгоритмы электронной подписи и шифрования работают по двум видам схем: симметричной и асимметричной [6]. В первой применяется один криптографический ключ как для шифрования и расшифровки сообщений, так и для формирования и проверки подписи. Во второй данные шифруются при помощи открытого ключа, а процедура их расшифровки может быть произведена только при наличии закрытого. Подписание документов в асимметричных схемах электронной подписи осуществляется при помощи закрытого ключа, а проверка – с применением открытого.

Для шифрования следует использовать комбинированные схемы [7], в которых применяются два алгоритма: симметричный и асимметричный. Это связано с тем, что использование симметричных и асимметричных схем шифрования по отдельности сопровождается рядом существенных недостатков. При симметричном шифровании возникает сложность передачи секретного ключа, поскольку для этого нужны защищённые каналы связи. Асимметричные алгоритмы обеспечивают высокую степень защиты информации, но их следует применять только для обмена сообщениями небольшого объёма. Связано это с тем, что такие алгоритмы реализуют сложные математические вычисления и требуют больше вычислительных ресурсов, чем симметричные алгоритмы, на выполнение процедур шифрования и расшифровки.

Для подписания следует использовать асимметричные схемы, так как до настоящего времени не удалось реализовать эффективные симметричные алгоритмы формирования электронной подписи. Поскольку подписываемые документы чаще всего имеют достаточно большой объем, электронная подпись ставится не на сам документ, а на его хеш [8], который формируется при помощи хеш-функции [9, 10].

В настоящее время в Российской Федерации действуют стандарты электронной подписи и хеширования линейки ГОСТ Р 34.10 и ГОСТ Р 34.11 соответственно. До 2019 года для электронной подписи использовался стандарт ГОСТ Р 34.10-2001[1], а для хеширования – ГОСТ Р 34.11-94[2]. Согласно выписке из документа ФСБ России[3], стандарт ГОСТ Р 34.10-2001 действителен до 31 декабря 2018 года, а формирование электронной подписи с 2019 года должно осуществляться только по ГОСТ Р 34.10-2012[4]. Однако 7 сентября 2018 года был опубликован документ[5], согласно которому действие ГОСТ Р 34.10-2001 продлевается до конца 2019 года, но при этом с 1 января 2019 года вводится в использование стандарт ГОСТ Р 34.10-2012. Таким образом, в 2019 году действуют два стандарта электронной подписи. Следует отметить, что при использовании электронной подписи по ГОСТ Р 34.10-2012 необходимо применять алгоритм хеширования по ГОСТ Р 34.11-2012[6].

Переход на алгоритм электронной подписи ГОСТ Р 34.10-2012 отложен ввиду того, что замена стандартов всегда является достаточно длительным процессом, поскольку должны быть внесены изменения во все системы электронного документооборота, лицензированы средства криптографической защиты информации и подготовлены к выпуску сертификаты по новым алгоритмам.

Одними из систем электронного документооборота, в которых было необходимо реализовать поддержку алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 к началу 2019 го-

[1] ГОСТ Р 34.10-2001. Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Взамен ГОСТ Р 34.10-94; введ. 01.07.2002. М.: ИПК Изд-во стандартов, 2001. 16 с.

[2] ГОСТ Р 34.11-94. Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования. Введ. 01.01.95. М.: Изд-во стандартов, 1994. 16 с.

[3] О порядке перехода к использованию новых стандартов ЭЦП и функции хэширования: выписка из документа ФСБ России № 149/7/1/3-58 от 31.01.2014 [Электронный ресурс]. URL: https://tc26.ru/upload/medialibrary/5f7/5f724550477 (15.10.2018).

[4] ГОСТ Р 34.10-2012. Информационная технология (ИТ). Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. Взамен ГОСТ Р 34.10-2001; введ. 01.01.2013. М.: Стандартинформ, 2012. 33 с.

[5] Уведомление об организации перехода на использование схемы электронной подписи по ГОСТ Р 34.10-2012 [Электронный ресурс]. URL: https://goo.gl/4rfW2m (15.10.2018).

[6] ГОСТ Р 34.11-2012. Информационная технология (ИТ). Криптографическая защита информации. Функция хэширования. Взамен ГОСТ Р 34.11-94; введ. 01.01.2013. М.: Стандартинформ, 2013. 24 с.

да, являются программные продукты линейки «1С: Медицина». Под продуктами линейки «1С: Медицина» подразумеваются программы «1С: Медицина. Поликлиника», «1С: Медицина. Больница» и «1С: Медицина. Больничные».

Электронная подпись в программах линейки «1С: Медицина» применяется в:

- электронных листках нетрудоспособности (ЭЛН);
- медицинских документах;
- сообщениях, отправляемых в Реестр электронных медицинских документов (РЭМД).

Перечисленные документы и сообщения создаются в формате XML, а их подпись должна соответствовать стандарту XML Digital Signature (XMLDSig) [11], который разработан консорциумом W3C (World Wide Web Consortium) в 2002 году. Стандарт XMLDSig определяет синтаксис представления электронной подписи, который включает в себя правила её обработки, а также обеспечивает целостность данных, установление подлинности сообщений и подтверждение принадлежности документа подписавшему лицу. После формирования подпись XMLDSig является частью структуры самого XML-документа.

Шифрование в программах линейки «1С: Медицина» применяется при обмене данными ЭЛН с Фондом социального страхования (ФСС) для получения номеров, открытия, продления и закрытия ЭЛН, а также поиска ранее зарегистрированных сведений в базе ФСС.

Программные продукты линейки «1С: Медицина» реализованы на платформе «1С: Предприятие», а работа с электронной подписью и шифрованием организована при помощи:

- встроенных средств криптографии платформы «1С: Предприятие»;
- методов конфигурации «1С: Библиотека стандартных подсистем» (БСП) версии 2.4;
- подсистемы «Электронный документооборот с контролирующими органами» (ЭДКО);
- методов собственных общих модулей.

Следует отметить, что методы и средства криптографии платформы «1С: Предприятие» не содержат реализации алгоритмов подписи, хеширования и шифрования, а предоставляют набор объектов и методов, позволяющих обеспечить взаимодействие с внешними модулями криптографии. К таким модулям относятся средства криптографической защиты информации (СКЗИ)[7]. Наиболее распространёнными и сертифицированными Федеральной службой безопасности России являются программные СКЗИ (криптопровайдеры) КриптоПро CSP и ViPNet CSP, которые содержат реализацию алгоритмов линейки ГОСТ Р 34.10 и ГОСТ Р 34.11. Для выполнения операций подписания и шифрования также необходимо получить в аккредитованном удостоверяющем центре сертификат электронной подписи с контейнером закрытого ключа.

Схема подписания XML-документов, ранее применявшаяся в конфигурациях линейки «1С: Медицина» при использовании алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94, представлена на рис. 1.

В такой схеме при выполнении подписания сначала формируется XML-шаблон SignedInfo, содержащий области для дальнейшего помещения в них значений хеша и подписи. Затем создаётся структура XMLDSig, которая содержит параметры алгоритмов по ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94. Далее выбирается сертификат для подписания и вызывается метод GetSignOIDFromCert (...) компоненты XMLDSIG, который извлекает из сертификата идентификатор алгоритма подписи – OID (Object Identifier). Внешняя компонента XMLDSIG входит в состав БСП и используется для формирования хеша, подписания и проверки подписи XML-документов. Необходимость использования внешних компонент заключается в решении задач, которые невозможно реализовать на встроенном в «1С: Предприятие» языке программирования.

Метод GetSignOIDFromCert (...) вызывался ранее только для того, чтобы проверить совпадает ли алгоритм сертификата с алгоритмом подписи, указанным в параметрах XMLDSig. Если алгоритм сертификата отличался от алгоритма в структуре XMLDSig, то хеш

[7] Бутакова Н.Г. Криптографические методы и средства защиты информации: учебное пособие / Н.Г. Бутакова, Н.В. Федоров. СПб.: ИЦ «Интермедия», 2016. С. 212.

и электронная подпись не формировались, а весь процесс подписания завершался с ошибкой.

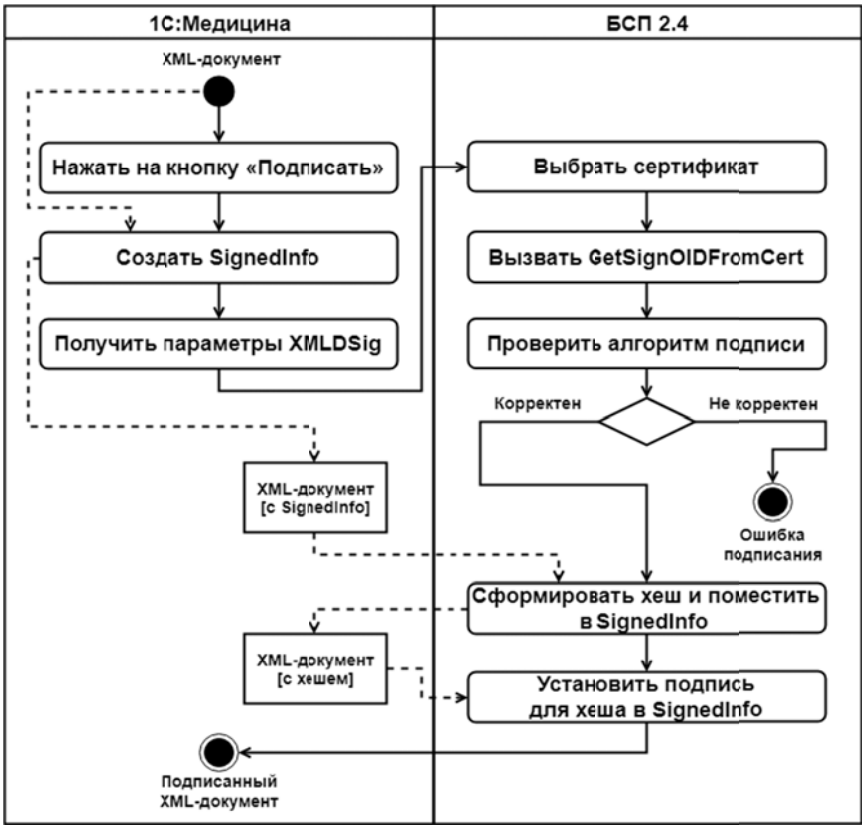

Рис. 1. Схема подписания в конфигурациях «1С: Медицина»

Ранее, при использовании алгоритмов подписи ГОСТ Р 34.10-2001 и хеширования ГОСТ Р 34.11-94, все параметры задавались в явном виде в программном коде конфигураций линейки «1С: Медицина», и поэтому не было возможности использовать какие-либо другие алгоритмы.

В 2019 году может использоваться один из трёх алгоритмов подписи: ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012 в двух вариантах – с длиной хеша 256 или 512 бит. Данные алгоритма подписи содержатся в сертификате открытого ключа. Следовательно, необходимо было определять алгоритм выбранного сертификата и использовать соответствующий ему алгоритм хеширования.

Таким образом, для добавления возможности подписания по ГОСТ Р 34.10-2012 и формирования хеша по ГОСТ Р 34.11-2012 была выполнена следующая последовательность действий:

1. удалены все заранее определённые параметры алгоритмов ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94 из шаблона SignedInfo и структуры XMLDSig;
2. организовано использование OID алгоритма из сертификата открытого ключа для выполнения подписания;
3. определена функция *Получить Параметры Для Формирования ЭП (…)* для получения параметров алгоритма хеширования, который соответствует алгоритму подписи, полученному из сертификата;
4. реализовано заполнение шаблона SignedInfo и структуры XMLDSig полученными параметрами алгоритмов подписи и хеширования;
5. добавлены настройки криптопровайдеров, поддерживающих работу алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

После выполнения вышеперечисленных действий схема подписания XML-документов выглядит так, как показано на рис. 2.

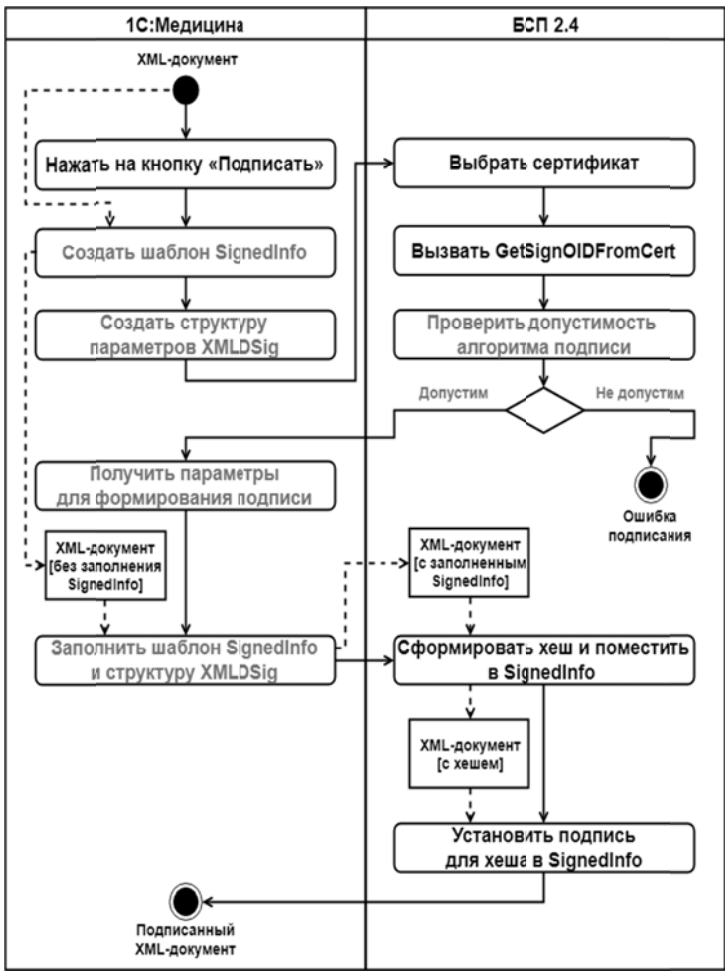

Рис. 2. Схема подписания с использованием алгоритма из сертификата

После реализации подписания по ГОСТ Р 34.10-2012 и формирования хеша по ГОСТ Р 34.11-2012 необходимо было настроить асимметричное шифрование, которое используется в конфигурациях линейки «1С: Медицина» для обмена данными ЭЛН с ФСС. Следует отметить, что в асимметричной схеме используются ключи по стандартам линейки ГОСТ Р 34.10 для шифрования или расшифровки симметричного ключа. Схема шифрования и расшифровки сообщений при обмене данными с ФСС, в которой применялся только алгоритм ГОСТ Р 34.10-2001, представлена на рис. 3.

В такой схеме сначала инициализируется по алгоритму ГОСТ Р 34.10-2001 компонента «Компонента обмена», которая используется для шифрования и расшифровки сообщений. Затем эта компонента производит шифрование XML-сообщения по симметричному методу ГОСТ 28147-89[8], а сгенерированный симметричный ключ зашифровывает при помощи открытого ключа сертификата ФСС. В результате шифрования компонента возвращает четыре объекта: зашифрованный симметричный ключ, вектор инициализации, открытый ключ сертификата ФСС и зашифрованное сообщение. После шифрования создаётся шаблон XML-сообщения для последующей отправки, в который далее добавляется зашифрованное компонентой сообщение, зашифрованный симметричный ключ и сертификат медицинской организации (МО) для того, чтобы ФСС мог зашифровать свой ответ. Далее формируется массив, в который сначала вносится значение симметричного ключа, зашифрованного компонентой, а затем добавляются вектор инициализации и открытый ключ сертификата ФСС, при помощи которого компонента зашифровала симметричный ключ. Затем массив преобразовывается в строку, которая является зашифрованным симметричным ключом для вставки в XML и содержит все параметры, позволяющие в дальнейшем ФСС расшифровать сообщение.

[8] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. Введ. 01.07.90. М.: Изд-во стандартов, 1989. 28 с.

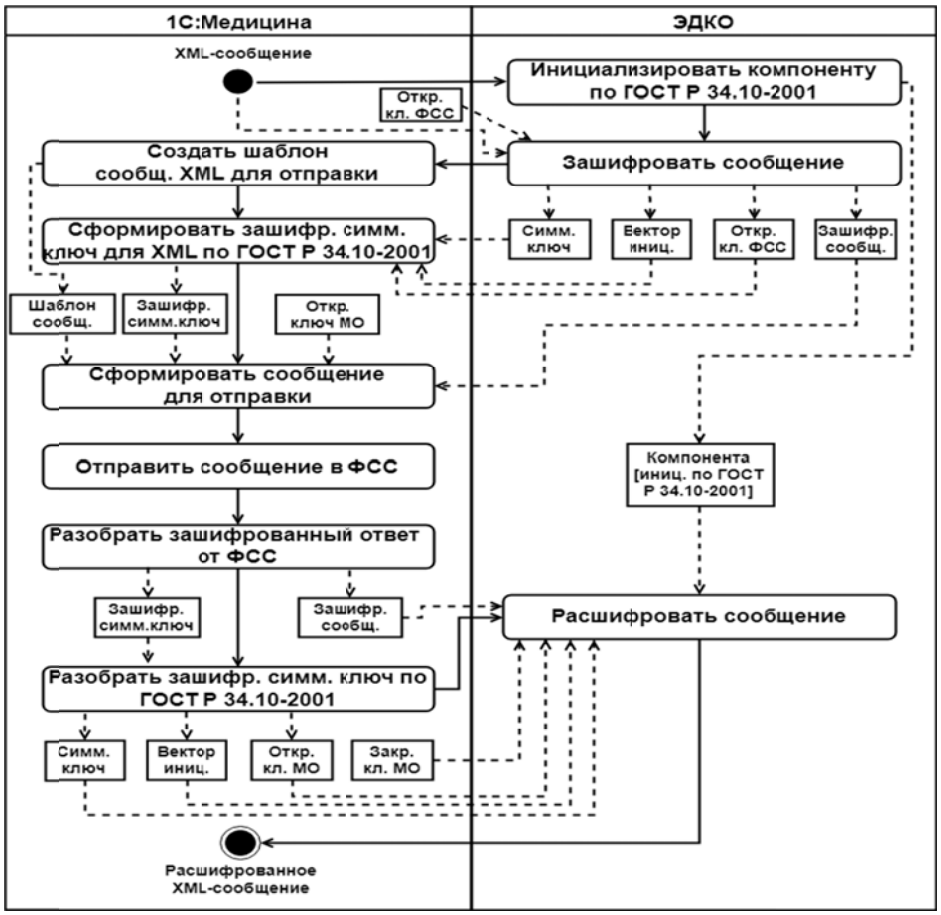

Рис. 3. Схема шифрования и расшифровки сообщений

После получения ответа от ФСС происходит разбор принятого сообщения. Результатом является вложенное зашифрованное сообщение и зашифрованный симметричный ключ. Он затем преобразовывается в массив, который разбивается на три объекта: симметричный ключ, зашифрованный открытым ключом МО вектор инициализации и открытый ключ сертификата МО, при помощи которого был зашифрован симметричный ключ. После этих операций компонента, инициализированная ранее по ГОСТ Р 34.10-2001, производит вычисление симметричного ключа закрытым ключом МО, а затем выполняет расшифровку сообщения при помощи вычисленного симметричного ключа.

Для добавления возможности использовать в асимметричном шифровании ключи по ГОСТ Р 34.10-2012 для схем шифрования и расшифровки была выполнена следующая последовательность действий:

1. добавлено определение алгоритмов сертификатов ФСС и МО перед выполнением процедур шифрования и расшифровки;
2. реализованы методы инициализации компоненты, а также шифрования и расшифровки сообщений по указанному алгоритму;
3. добавлена схема формирования зашифрованного симметричного ключа для вставки в XML при использовании ГОСТ Р 34.10-2012;
4. реализован разбор зашифрованного симметричного ключа из XML при использовании ГОСТ Р 34.10-2012.

После добавления возможности использовать в асимметричном шифровании ключи по ГОСТ Р 34.10-2012 схема шифрования и расшифровки в конфигурациях линейки «1С: Медицина» выглядит так, как показано на рис. 4.

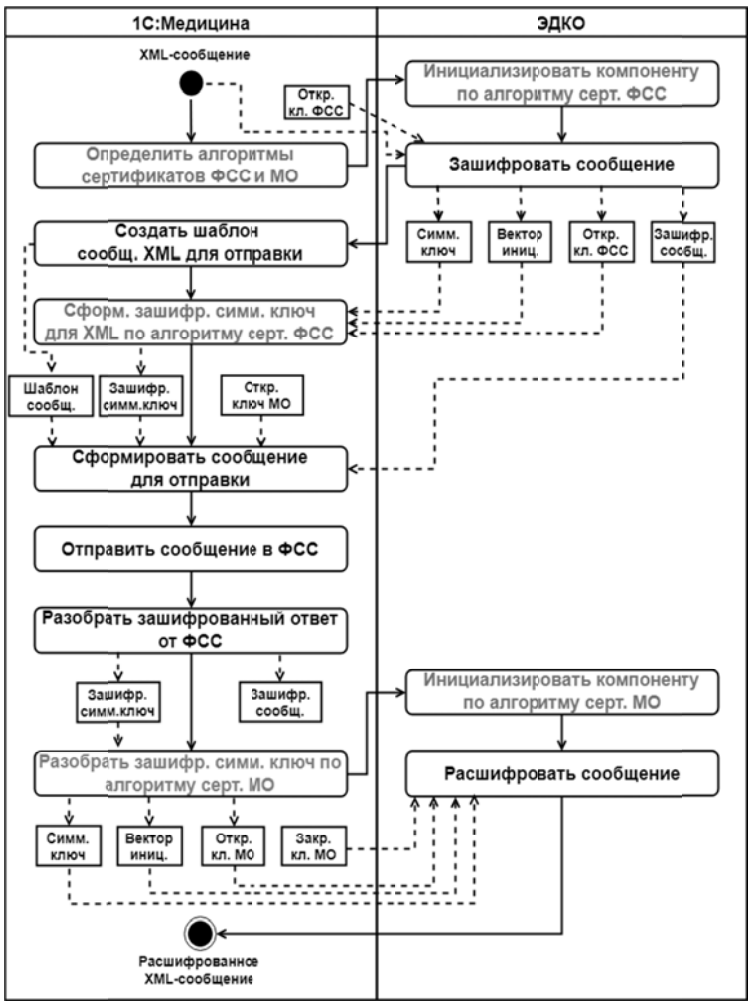

Рис. 4. Схема шифрования и расшифровки с применением ключей сертификатов

Реализованная поддержка криптографических алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012 вошла в следующие релизы программных продуктов:

- «1С: Медицина. Больничные» версии 2.0.3.1 от 17.12.2018;
- «1С: Медицина. Поликлиника» версии 2.1.5.1 от 25.12.2018;
- «1С: Медицина. Больница» версии 1.4.5.1 от 26.12.2018.

Библиографический список

1. Жильников А.Ю., Михайлова А.С. Электронный документооборот // Территория науки. 2017. № 2. С. 116–120.

2. Курченков К.Б. Критерии разработки систем электронного документооборота // Вестник Воронежского Института высоких технологий. 2014. № 12. С. 102–106.

3. Астахова А.С., Чадаева Е.П. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа // Известия Томского политехнического университета. 2012. № 6. С. 153–157.

4. Трофимов Е.И. Электронная подпись как средство защиты электронных документов от подделки // Педагогическое образование на Алтае. 2014. № 2. С. 446–447.

5. Секушина С.А., Сапрыкин А.А. Возможности использования алгоритмов шифрования в системах обработки электронных документов // Вестник Воронежского Института высоких технологий. 2014. № 13. С. 120–122.

6. Лаврова О.С. Симметричные и асимметричные схемы электронной цифровой подписи // Известия Юго-Западного государственного университета. 2011. № 1. С. 84–85.

7. Ильинская Е.В., Павленко К.А. Безопасный обмен электронными документами // Экономическая безопасность социально-экономических систем: вызовы и возможности: сб. науч. тр. Междунар. науч.-практич. конф. Белгород: Белгородский государственный национальный исследовательский университет, 2018. С. 275–277.

8. Жуковина О.А., Зубова Н.Г. Система электронного документооборота, её назначение и проблемы внедрения // Вестник Белгородского университета кооперации, экономики и права. 2012. № 2. С. 246–251.

9. Ланских В.Г., Ланских А.М., Пешнина Л.В. Повышение криптографической стойкости функций хеширования // ИТ Арктика. 2016. № 3. С. 21–35.

10. Чернова А.Я. Анализ системы формирования и проверки электронной подписи // Вестник Пензенского государственного университета. 2017. № 3. С. 108–111.

11. XML Signature Syntax and Processing Version 1.1. W3C Recommendation 11 April 2013 [Электронный ресурс]. URL: https://www.w3.org/TR/xmldsig-core/ (19.10.2018).

Сведения об авторах / Information about the Authors

Балюк Александр Сергеевич,
кандидат физико-математических наук,
доцент кафедры алгебраических и информационных систем,
Институт математики, экономики и информатики,
Иркутский государственный университет,
664003, г. Иркутск, бул. Гагарина, 20, Российская Федерация,
e-mail: sacha@hotmail.ru
Alexander S. Balyuk,
Cand. Sci. (Physics and Mathematics),
Associate Professor of Algebraic and Information Systems,
Institute of Mathematics, Economics and Informatics,
Irkutsk State University,
20 Gagarin Blvd., Irkutsk, 664003, Russian Federation,
e-mail: sacha@hotmail.ru

Попова Виктория Алексеевна,
студентка 4 курса,
Институт математики, экономики и информатики,
Иркутский государственный университет,
664003, г. Иркутск, бул. Гагарина, 20, Российская Федерация,
e-mail: victorypopova1@gmail.com
Victoria A. Popova,
Student,
Institute of Mathematics, Economics and Informatics,
Irkutsk State University,
20 Gagarin Blvd., Irkutsk, 664003, Russian Federation,
e-mail: victorypopova1@gmail.com