ПРИМЕНЕНИЕ СМАРТ-КАРТ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ

Булдакова Т.И.[1], Ланцберг А.В.[2], Смолянинова К.А.[3]

Статья посвящена проблеме защиты данных пациента в телемедицинской системе, содержащей электронные истории болезни. Показано, что в современных системах доступ к данным о состоянии здоровья человека может получить любой зарегистрированный сотрудник медицинского учреждения, без ведома пациента. Поэтому подобные системы позволяют внести, удалить или изменить любую информацию. В результате нарушаются принципы безопасного доступа к информационным ресурсам телемедицинской системы. Для решения этих проблем и обеспечения конфиденциальности и целостности информации в данной работе предложено использовать смарт–карты пользователей, обеспечивающие безопасный доступ к телемедицинской системе. Применение смарт–карт в телемедицинских системах позволит обеспечить надежное хранение конфиденциальных данных пациента. Описаны возможности и функции смарт–карт пациента и врача, а также особенности их применения в телемедицинских системах. Безопасность информационных ресурсов обеспечивается с помощью криптографических методов. Обсужден процесс авторизации врача в телемедицинской системе, содержащей электронные истории болезней, с помощью электронной подписи. Подробно рассмотрены процедуры подписания документов электронной цифровой подписью. Приведены блок–схемы алгоритмов создания и проверки электронной подписи. По результатам исследований создано приложение с пользовательским интерфейсом для работы со смарт–картами.

***Ключевые слова**: телемедицина, смарт–карта, электронная история болезней, электронная подпись, хэш–код*

DOI: 10.21681/2311-3456-2017-4-40-46

Введение

В настоящее время в здравоохранении активно внедряются автоматизированные системы, позволяющие хранить информацию в электронном виде [1, 2]. Это способствует повышению эффективности информационного обмена между медицинскими учреждениями, возможности удаленного доступа к медицинским информационным системам, облегчению и ускорению записи пациентов на прием с помощью электронной регистратуры [3, 4]. Поэтому можно утверждать, что медицинская информация в электронном виде является основой многих процессов в современном здравоохранении.

Например, переход на системы электронных историй болезней дает возможность разным специалистам совместно использовать информацию о состоянии здоровья пациентов [5, 6]. Наиболее активно данный процесс развивается в Германии и США, где реализуется большое количество проектов для перехода к электронным медицинским картам (Electronic Health Record, EHR), обеспечивающим обмен данными между различными медицинскими организациями.

Так, в Германии создана Ассоциация электронных медицинских карт, которая объединяет основные клиники и больницы, а также локальные ассоциации и региональные сети здравоохранения. Указанная Ассоциация создала новую концепцию внедрения технологии электронных историй болезни (electronic case record, ECR) – "ECR in a Box" [7]. Предложенный подход облегчает привлечение к здравоохранению новых действующих лиц и включение их в региональные сети здравоохранения (рис. 1).

Однако недостаток современных телемедицинских систем заключается в том, что доступ к истории болезни для ввода, изменения или удаления любой информации предоставляется без ведома самого пациента. В результате подобные системы не являются безопасными, поскольку в них нарушаются принципы конфиденциальности и целостности информации. Системы, которые оперируют такими важными данными, как информация о состоянии здоровья человека, должны быть надежно защищены [8, 9].

Основное внимание должно быть направлено на обеспечение безопасного доступа к информации, защиту передаваемых данных и применению электронных подписей [10]. Решением этих проблем является использование смарт-карт

1 Булдакова Татьяна Ивановна, д.т.н., профессор, МГТУ имени Н.Э. Баумана, Москва, buldakova@bmstu.ru

2 Ланцберг Анна Вильямовна, к.т.н., научный сотрудник, Институт проблем точной механики и управления РАН, Саратов, nurka_nuska@mail.ru

3 Смолянинова Кристина Александровна, студент МГТУ имени Н.Э. Баумана, Москва, kriszzztina@yandex.ru

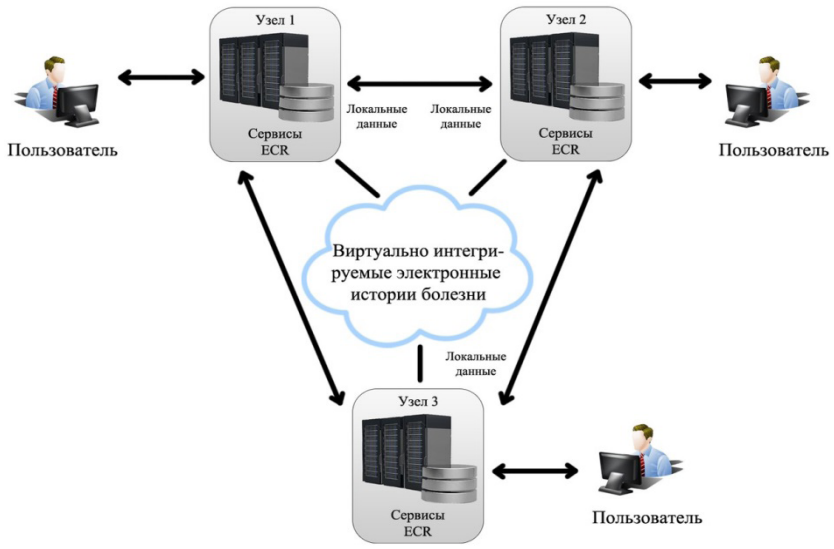

***Рис. 1**. Архитектура платформы ECR*

врача и пациента для его однозначной идентификации в единой базе электронных медицинских карт. Применение смарт-карт в телемедицинских системах позволит обеспечить безопасный доступ к информации и надежное хранение конфиденциальных данных пациента. Безопасность информационных ресурсов обеспечивается криптографическими методами.

В данной статье представлены возможности криптографических методов при работе со смарт-картами для обеспечения конфиденциальности и целостности данных пациентов.

Особенности применения смарт-карт в телемедицинских системах

Смарт-карта является пластиковой карточкой, по внешнему виду идентичной карте полиса медицинского страхования или кредитке. В нее встроен чип, содержащий энергонезависимую память и криптопроцессор (микрокомпьютер, встроенный в пластиковую карту). В памяти чипа хранится уникальный сертификат пользователя и другая персонифицированная информация (например, сведения о пациенте и состоянии его здоровья). Криптопроцессор обеспечивает логику работы карты, в том числе генерацию ключевых пар и электронной подписи.

В настоящее время электронные персональные карты становятся все популярнее, и в ряде зарубежных стран использование смарт-карт в здравоохранении стало уже обычным делом. Например, во Франции, Германии, Италии, Японии, Турции, Тайване, Словении применяются десятки миллионов смарт-карт в области медицинского обслуживания [11].

Применение карточек способствует значительному упрощению идентификации пациента в автоматизированной медицинской системе, уменьшению вероятности ошибок при учете оказанных пациенту услуг и ускорению времени оборота медицинской информации (рис. 2).

Чтобы начать работу с телемедицинской системой, содержащей электронные истории болезни (ЭИБ), пользователь соединяет смарт-карту со считывателем и вводит PIN-код. При этом последовательно выполняются три связанных процесса:

1) идентификация (процедура распознавания пользователя по его идентификатору);

2) аутентификация (процедура доказательства того, что пользователь на самом деле является тем, за кого себя выдает);

3) авторизация (процедура предоставления пользователю определенных прав доступа к ресурсам системы).

В результате происходит регистрация пользователя в телемедицинской системе. Далее, при необходимости, история всех его действий может быть восстановлена.

Существуют два типа карт – карта пациента и карта врача. На карте пациента имеются открытая

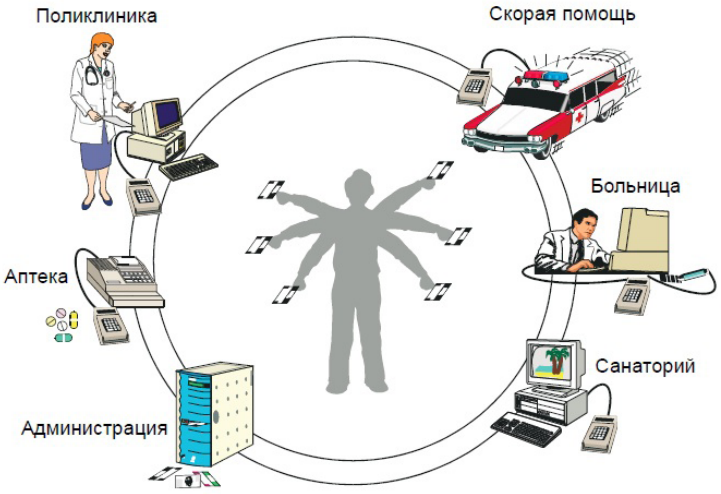

***Рис. 2**. Возможные применения смарт-карт как носителей информации*

и закрытая области памяти. В открытой области хранится базовая информация (ФИО, дата рождения, группа крови, наименование страховой компании и т.п.). Эти данные должны быть доступны любому медработнику для оказания неотложной помощи пациенту, однако эта информация должна быть защищена от несанкционированного внесения изменений. В защищенной области памяти хранятся данные, необходимые для аутентификации пациента, прочие персональные данные, а также сертификат открытого ключа врача, подписавшего эту карту. Закрытая область доступна только медицинским специалистам по предъявлению ими своих смарт-карт. Другая информация о состоянии здоровья (истории болезни) пациента хранится на сервере медицинского учреждения и доступна соответствующим специалистам.

Вторым типом смарт-карт является карта врача (или карта специалиста). На ней записаны ФИО специалиста, название учреждения здравоохранения, в котором он работает, специализация, персональный номер, электронная подпись. Смарт-карта врача дает право доступа к закрытой информации, как на карте пациента, так и на серверах медицинских учреждений. Однако специалист может получить доступ лишь к той информации, на которую он имеет право в соответствии со своей специализацией.

Заметим, что для обеспечения взаимодействия карточных систем с телемедицинскими системами необходимо следовать стандартам электронной передачи медицинских данных, например, стандарту Health Level Seven (HL7). В настоящее время стандарт электронного обмена медицинскими данными HL7 охватывает наиболее широкую предметную область передачи текстовых, качественных и количественных медицинских данных [12-14]. Распространению данного стандарта способствовало использование технологии XML, которая оказалась удобной для описания архитектуры клинических документов [15].

Авторизация врача в телемедицинской системе с помощью электронной подписи

Смарт-карта врача применяется для авторизации его в телемедицинской системе и дальнейшего подписания документов. Аутентификация производится методом Challenge-Response [16]. По идентификатору в базе данных выбирается открытый ключ, соответствующий врачу. Сервер генерирует случайное число размером 32 бита и передает его клиентскому приложению, которое, в свою очередь, получив секретный ключ со смарт-карты, подписывает его в соответствии с ГОСТ34.10-2012.

Электронная подпись (ЭП) реализуется с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем. Параметрами схемы цифровой подписи являются:

- простое число p – модуль эллиптической кривой;

- эллиптическая кривая E, задаваемая коэффициентами $a, b \in F_p$;

- целое число m – порядок группы точек эллиптической кривой E;

- простое число q – порядок циклической подгруппы группы точек эллиптической кривой E, для которого выполнены следующие условия:

$$\begin{cases} m = nq, n \in Z, n \geq 1; \\ 2^{254} < q < 2^{256} \text{ или } 2^{508} < q < 2^{512}; \end{cases} \quad (1)$$

- точка $P \neq 0$ эллиптической кривой E, с координатами (x_p, y_p), удовлетворяющая равенству $qP=0$;

- хэш-функция $V^* \rightarrow V_l$, отображающая сообщения, представленные в виде двоичных векторов произвольной конечной длины, в двоичные векторы длины l бит.

Каждый пользователь схемы цифровой подписи должен обладать двумя личными ключами:

1) ключом подписи – целым числом d, удовлетворяющим неравенству $0<d<q$;

2) ключом проверки подписи – точкой эллиптической кривой Q с координатами (x_p, y_p), удовлетворяющей равенству $dP=Q$.

Процесс формирования подписи представлен на рис. 3.

Процедура получения хэш-кода в соответствии с ГОСТ Р 34.11-2012 «Криптографическая защита информации. Функция хэширования» представлена ниже. В данном случае на вход поступает случайное значение M, размером 32 бита. В процессе хэширования применяются следующие преобразования: X-преобразование; S-преобразование; P-преобразование; L-преобразование.

На вход функции X подаются две последовательности длиной 512 бит каждая, а выходом функции является *XOR* этих последовательностей:

$$X[k]: V_{512} \rightarrow V_{512}, \; X[k](a) = k \oplus a. \quad (2)$$

Функция S - это обычная функция подстановки. Каждый байт из 512-битной входной последовательности заменяется соответствующим байтом из таблицы подстановок ψ:

$$S: V_{512} \rightarrow V_{512}, S(a) = S(a_{63} \| \cdots \| a_0) = \psi(a_{63}) \| \cdots \| \psi(a_0). \quad (3)$$

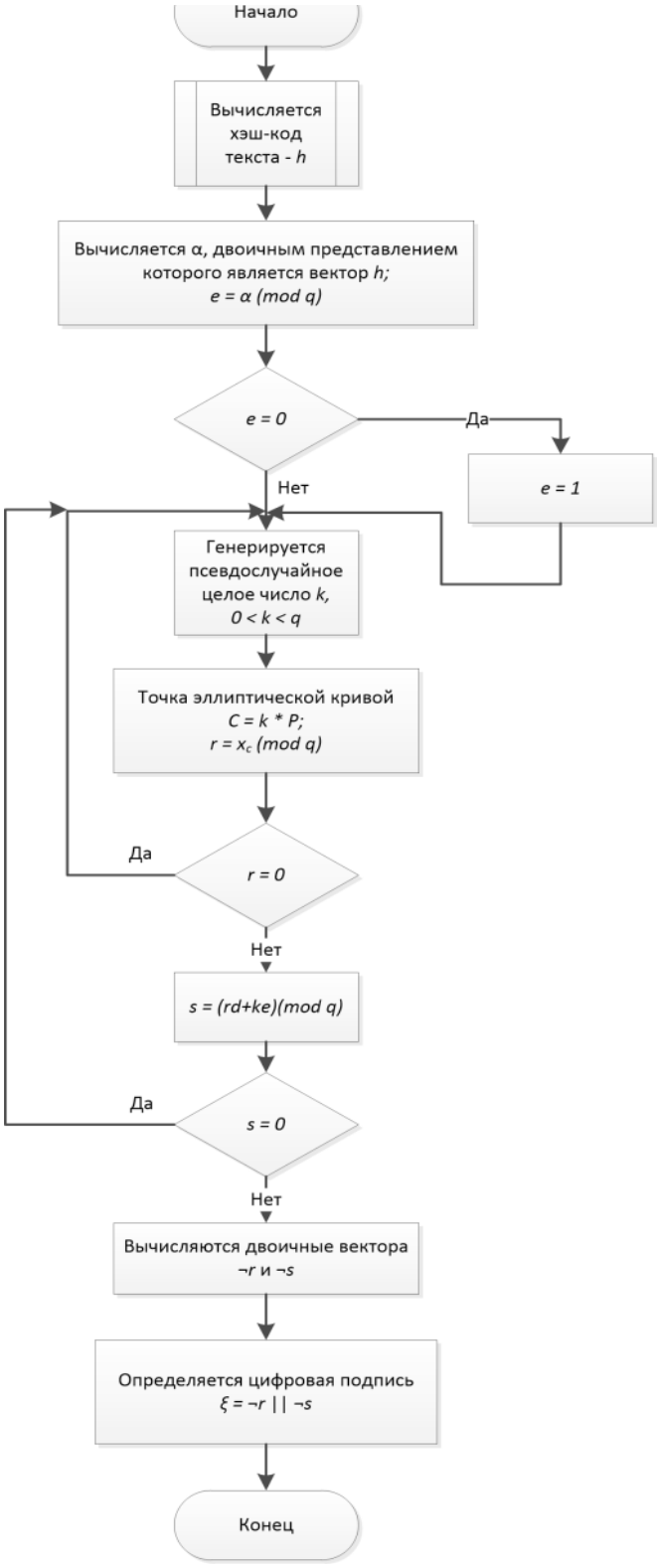

***Рис. 3**. Алгоритм создания электронной подписи*

Таблица ψ приведена в ГОСТ Р 34.11-2012, является неизменной и может быть записана в виде массива констант.

P-преобразование фактически является функцией перестановки. Для каждой пары байт из входной последовательности выполняется замена одного байта другим:

$$P: V_{512} \to V_{512}, P(a) = P(a_{63} \| \cdots \| a_0) = a_{\tau(63)} \| \cdots \| a_{\tau(0)}. \quad (4)$$

Отметим, что таблица перестановок τ также является неизменной.

L-преобразование - это умножение 64-битного входного вектора на бинарную матрицу A размерами 64x64:

$$L: V_{512} \to V_{512}, L(a) = L(a_7 \| \cdots \| a_0) = l(a_7) \| \cdots \| l(a_0). \quad (5)$$

Входными значениями для процедуры вычисления хэш-кода являются подлежащее хэшированию значение M и инициализационный вектор IV. Процесс вычисления хэш-функции выглядит следующим образом:

1. Присваиваются начальные значения внутренних переменных: $h=IV$; $N = 0^{512} \in V_{512}$; $\Sigma = 0^{512} \in V_{512}$

2. Выполняется проверка условия $|M|<512$ бит. Если оно выполняется, переходим к шагу 3. В данном случае условие выполняется (M=32), невыполнение условия рассматриваться не будет;

3. Производится дополнение M до 512 бит по следующему правилу:

$$m = 0^{511-|M|} \| 1 \| M. \quad (6)$$

где $|M|$ — длина сообщения M в битах;

4. Вычисляется $h= g_n(h,m)$. На каждой итерации вычисления хэш-кода применяется функция сжатия, полученная следующим образом:

$$g_n(h,m) = E(LPS(h \oplus N), m) \oplus h \oplus m, \quad (7)$$
$$E(k,m) = X[K_{13}]LPSX[K_{12}] \ldots LPSX[K_2]LPSX[K_1](m). \quad (8)$$

Значения $K_i \in V_{512}$, $i=1\ldots13$, вычисляются по формулам: $K_1=K$; $K_i=LPS(K_{i-1} \oplus C_{i-1})$, $i=2\ldots13$, где Ci – итерационные константы, записанные в шестнадцатеричном виде;

5. Вычисляется $N=(N+|M|) \bmod 2^{512}$;

6. Вычисляется $\Sigma=(\Sigma+m) \bmod 2^{512}$;

7. Вычисляется $h= g_{0^{512}}(h,N)$;

8. Вычисляется $h= g_{0^{512}}(h,\Sigma)$. Значение h полученное на 8 шаге и есть значение хэш-кода.

После получения электронной подписи клиентское приложение передает двоичный вектор ξ, полученный на последнем этапе алгоритма создания электронной подписи, серверному приложению, которое с использованием ключа проверки электронной подписи, хранящегося в базе данных, выполняет проверку подписи. Проверка подписи выполняется по алгоритму, приведенному на рис. 4.

Таким образом, на смарт-карте врача должны храниться идентификатор и ключевая пара (ключ электронной подписи и ключ проверки электронной подписи). Следовательно, данная карта долж-

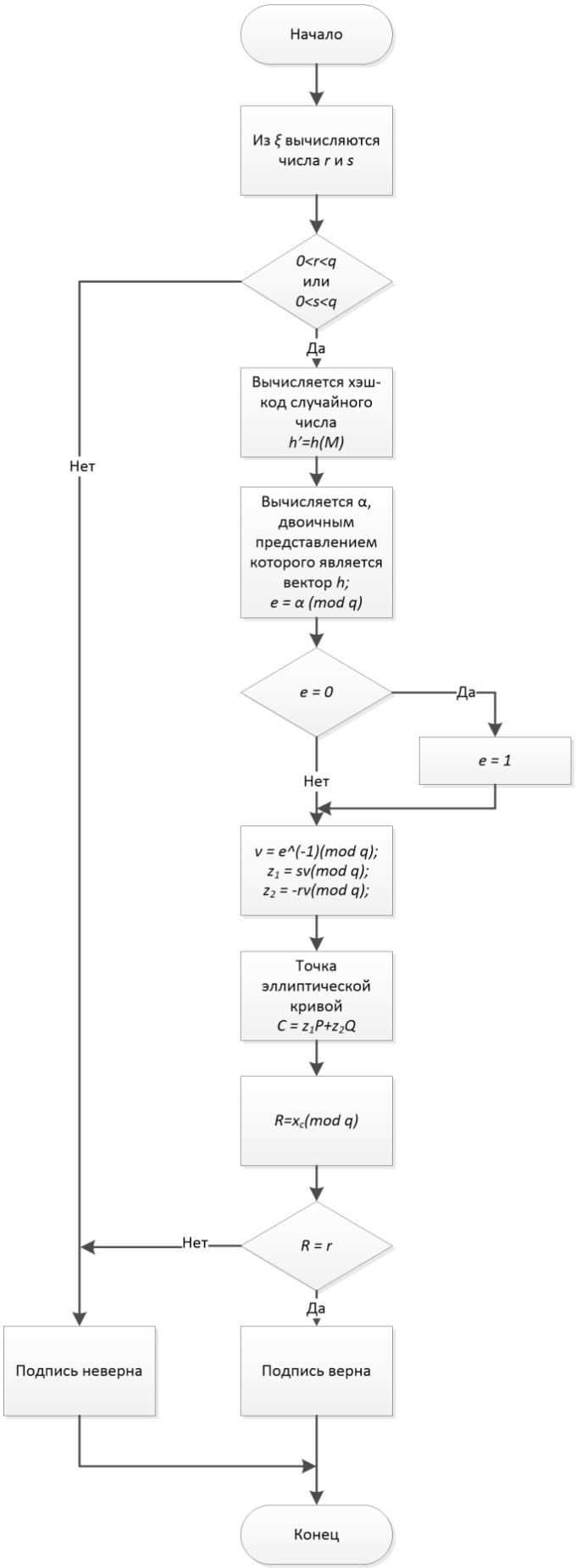

Рис. 4. *Алгоритм проверки электронной подписи*

на иметь защищенные области памяти для безопасного хранения ключевой информации.

Помимо аутентификации, смарт-карта врача используется также для подписания электронных персональных медицинских записей (ЭПМЗ) и смарт-карт пациентов. Для этого применяются приведенные выше алгоритмы, только входным значением теперь будет текст ЭПМЗ и данные смарт-карты пациента. В соответствии с ГОСТ Р 52636-2006 «Электронная история болезни», документы подписанные электронной подписью в данной системе, должны иметь такую же юридическую силу, как и бумажные документы, подписанные собственноручно. Поэтому для подписания электронных документов, а также данных, хранящихся на смарт-карте пациента, необходимо применять квалифицированную электронную подпись.

Разработка программного обеспечения

По результатам исследований авторами создано приложение, которое предусматривает работу с двумя смарт-картами: врача и пациента. Программное обеспечение для доступа к карте разработано на языке программирования C++ в среде разработки QtCreator. Для работы с базой данных телемедицинской системы выбрана СУБД MySQL. Алгоритм работы приложения приведен на рис. 5.

Созданное приложение с пользовательским интерфейсом для работы со смарт-картами позволит повысить эффективность работы медицинского персонала в телемедицинской системе, а также обеспечить надежное хранение информации о состоянии здоровья пациентов.

Выводы

Применение смарт-карт в телемедицинских системах ограничивает несанкционированный доступ к данным пациента в базе ЭИБ. Для обеспечения целостности данных применена электронная подпись по алгоритму ГОСТ34.10-2001, для обеспечения конфиденциальности – аутентификация врача и пациента. Аутентификация врача выполняется методом Challenge-Response, аутентификация пациента – вводом PIN-кода.

Кроме того, использование смарт-карт в процессе взаимодействия врача и пациента позволит ускорить время работы медицинского персонала.

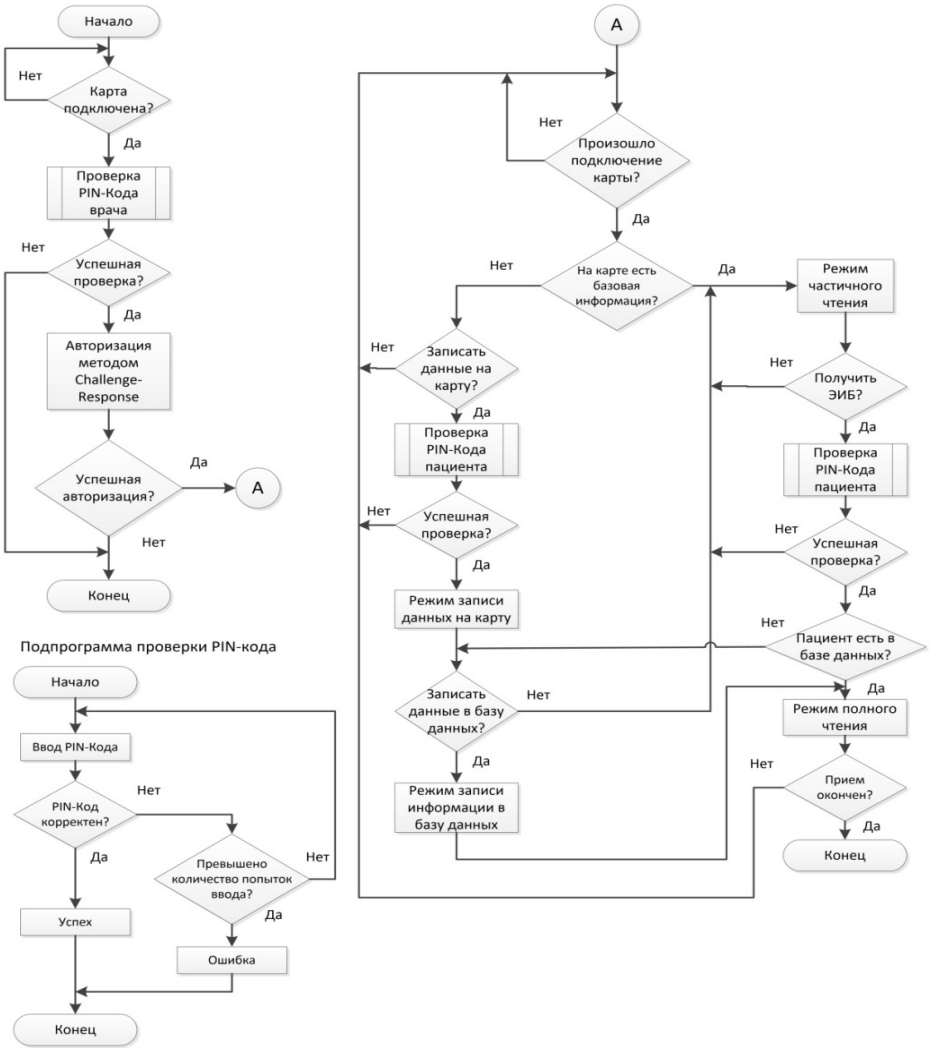

Рис. 5. *Блок-схема алгоритма работы приложения*

Работа выполнена при финансовой поддержке РФФИ (грант 16-07-00878).

Литература:

1. Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources) / A.V. Lantsberg, Klaus G. Troitzch, T.I. Buldakova // Automatic Documentation and Mathematical Linguistics. 2011. N. 2. V. 45. P. 74-80.
2. Ланцберг А.В., Тройч К., Булдакова Т.И. Особенности оценки качества медицинской электронной услуги // Информационное общество. 2011. № 4. С. 28-37.
3. Гусев А.В. Обзор электронных регистратур // Врач и информационные технологии. 2010. № 6. С. 4-15.
4. Llinás G., Rodríguez-Iñesta D. et al. Comparison of Websites from Spanish, American and British Hospitals // Methods of Information in Medicine. 2008. Vol. 47; Issue 2. P. 124-130.
5. Монич В.А., Кушников О.И., Алакаев Р.Р., Косоногов А.Я., Коротин Д.П., Медоваров Е.В. Электронная история болезни - важнейшее звено медицинских информационных систем // Современные технологии в медицине. 2010. № 3. С.73-74.
6. Зингерман Б.В., Шкловский-Корди Н.Е. Электронная медицинская карта и принципы ее организации // Врач и информационные технологии. 2013. № 2. С. 37-58.
7. Kuhlisch R., Kraufmann B., Restel H. Electronic Case Records in a Box: Integrating Patient Data in Healthcare Networks // Computer. 2012. Vol. 45, No. 11. Pp. 34-40.
8. Булдакова Т.И., Суятинов С.И., Кривошеева Д.А. Обеспечение информационной безопасности в телемедицинских системах на основе модельного подхода // Вопросы кибербезопасности. 2014. № 5(8). С. 21-29.
9. Анализ информационных рисков виртуальных инфраструктур здравоохранения / Т.И. Булдакова, С.И. Суятинов, Д.А. Миков // Информационное общество. 2013. № 4. С. 6.
10. Aleman J.L.F., Senor Carrion I., Toval A. Personal Health Records: New Means to Safely Handle Health Data? // Computer. 2012. Vol. 45, No. 11. Pp. 27-33.
11. Булдакова Т.И., Ланцберг А.В., Смолянинова К.А. Безопасный доступ к информации с использованием смарт-карт // Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение. 2017. № 3. С. 95–106.
12. Швырев С.Л. Внедрение стандартов HL7 в России // Врач и информационные технологии. 2009. № 6. С. 71-72.
13. Концептуальная модель виртуального центра охраны здоровья населения / В.С. Анищенко, Т.И. Булдакова, П.Я. Довгалевский, В.Б. Лифшиц, В.И. Гриднев, С.И. Суятинов // Информационные технологии. 2009. № 12. С. 59-64.

14. Weiss G. You Have to Have Standarts // IEEE Spectrum. 2002. T. 39. № 3. C. 48.
15. Ahn Ch., Nah Yu., Park S., Kim Ju. An Integrated Medical Information System Using XML // Lecture Notes in Computer Science. 2001. V. 2105. Pp. 307-322.
16. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / Под ред. А. А. Шелупанова и др. 2-е изд. М.: Горячая линия – Телеком, 2012.

USING SMART CARDS IN TELEMEDICAL SYSTEMS

Buldakova T.[4], Lantsberg A.[5], Smolyaninova K.[6]

The article is devoted to protecting patient data in the telemedical system which store electronic health records. It shows that in modern systems access to data from the health records may be obtained by any registered employee of the healthcare facility without patient's knowledge. Therefore, any information can be entered, deleted or changed in such systems. This results in violation of principles of safe access to the information resources of the telemedical system. To solve these problems and ensure confidentiality and integrity of the information this work suggests the use of user smart card, which ensures safe access to the telemedical system. The use of smart cards in the telemedical systems will ensure reliable storage of the confidential patient data. The article describes the capabilities and functions of the smart cards of the patient and physician, and the specifics of their use in the telemedical systems. Security of the information resources is ensured with the help of cryptographic methods. The article discusses the process of the physician's authorization in the telemedical system, which contains electronic health records. It reviews in detail the procedures of signing documents with electronic digital signature. The article provides block diagrams of the algorithms for creating and verification of the electronic signature. Based on the results of the study, we created an application with a user interface for work with the smart cards.

***Keywords**: telemedicine, smart card, electronic medical records, electronic signature, hash code*

Reference

1. Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources) / A.V. Lantsberg, Klaus G. Troitzch, T.I. Buldakova // Automatic Documentation and Mathematical Linguistics. 2011. No. 2. V. 45. Pp. 74-80.
2. Lantsberg A.V., Troych K., Buldakova T.I. Osobennosti otsenki kachestva meditsinskoy elektronnoy uslugi // Informatsionnoe obschestvo. 2011. No. 4. Pp. 28-37.
3. Gusev A.V. Obzor elektronnyih registratur // Vrach i informatsionnyie tehnologii. 2010. No. 6. Pp. 4-15.
4. Llinás G., Rodríguez-Iñesta D. et al. Comparison of Websites from Spanish, American and British Hospitals // Methods of Information in Medicine. 2008. Vol. 47; Issue 2. Pp. 124-130.
5. Monich V.A., Kushnikov O.I., Alakaev R.R., Kosonogov A.Ya., Korotin D.P., Medovarov E.V. Elektronnaya istoriya bolezni - vazhneyshee zveno meditsinskih informatsionnyih sistem // Sovremennyie tehnologii v meditsine. 2010. No. 3. Pp.73-74.
6. Zingerman B.V., Shklovskiy-Kordi N.E. Elektronnaya meditsinskaya karta i printsipyi ee organizatsii // Vrach i informatsionnyie tehnologii. 2013. No. 2. Pp. 37-58.
7. Kuhlisch R., Kraufmann B., Restel H. Electronic Case Records in a Box: Integrating Patient Data in Healthcare Networks // Computer. 2012. Vol. 45, No. 11. Pp. 34-40.
8. Buldakova T.I., Suyatinov S.I., Krivosheeva D.A. Obespechenie informatsionnoy bezopasnosti v telemeditsinskih sistemah na osnove modelnogo podhoda // Voprosyi kiberbezopasnosti. 2014. No. 5(8). Pp. 21-29.
9. Analiz informatsionnyih riskov virtualnyih infrastruktur zdravoohraneniya / T.I. Buldakova, S.I. Suyatinov, D.A. Mikov // Informatsionnoe obschestvo. 2013. No. 4. P. 6.
10. Aleman J.L.F., Senor Carrion I., Toval A. Personal Health Records: New Means to Safely Handle Health Data? // Computer. 2012. Vol. 45, No. 11. Pp. 27-33.
11. Buldakova T.I., Lantsberg A.V., Smolyaninova K.A. Bezopasnyiy dostup k informatsii s ispolzovaniem smart-kart // Vestnik MGTU im. N.E. Baumana. Ser. Priborostroenie. 2017. No. 3. Pp. 95–106.
12. Shvyirev S.L. Vnedrenie standartov HL7 v Rossii // Vrach i informatsionnyie tehnologii. 2009. No. 6. Pp. 71-72.
13. Kontseptualnaya model virtualnogo tsentra ohranyi zdorovya naseleniya / V.S. Anischenko, T.I. Buldakova, P.Ya. Dovgalevskiy, V.B. Lifshits, V.I. Gridnev, S.I. Suyatinov // Informatsionnyie tehnologii. 2009. No. 12. Pp. 59-64.
14. Weiss G. You Have to Have Standarts // IEEE Spectrum. 2002. T. 39. № 3. C. 48.
15. Ahn Ch., Nah Yu., Park S., Kim Ju. An Integrated Medical Information System Using XML // Lecture Notes in Computer Science. 2001. V. 2105. Pp. 307-322.
16. Autentifikatsiya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informatsionnyim resursam / Pod red. A. A. Shelupanova i dr. 2-e izd. M.: Goryachaya liniya – Telekom, 2012.

4 Tatyana Buldakova, Dr.Sc., Professor , Bauman Moscow State Technical University, Moscow, buldakova@bmstu.ru
5 Anna Lantsberg, Ph.D., Institute of Precision Mechanics and Control, Russian Academy of Sciences, Saratov, nurka_nuska@mail.ru
6 Kristina Smolyaninova, Bauman Moscow State Technical University, Moscow, kriszzztina@yandex.ru