УДК 004.056 DOI: 10.18698/0236-3933-2017-3-95-106

БЕЗОПАСНЫЙ ДОСТУП К ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СМАРТ-КАРТ

Т.И. Булдакова[1] buldakova@bmstu.ru
А.В. Ланцберг[2] nurka_nuska@mail.ru
К.А. Смолянинова[1] kriszzztina@yandex.ru

[1] МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
[2] Институт проблем точной механики и управления РАН, Саратов, Российская Федерация

Аннотация

Рассмотрена проблема защиты данных пациента в медицинских информационных системах, содержащих электронные истории болезни. Показано, что доступ к данным о состоянии человека может получить любой сотрудник, зарегистрированный в системе, без ведома пациента. Для обеспечения конфиденциальности и целостности информации предложено использовать смарт-карты, позволяющие однозначно идентифицировать пациента в единой базе электронных медицинских карт. Описаны возможности смарт-карт и особенности их применения в здравоохранении. В качестве примера рассмотрен процесс приема врачом пациентов со смарт-картами. Сформулированы требования к структуре данных, хранящихся на карте пациента. Создано программное обеспечение для работы со смарт-картами. Приведены блок-схема разработанного приложения, а также его особенности. Описаны режимы работы приложения, приведены примеры

Ключевые слова

Медицинская информационная система, электронная история болезни, информационная безопасность, смарт-карта

Поступила в редакцию 14.11.2016

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

Введение. В настоящее время в здравоохранении активно внедряются информационно-коммуникационные технологии, обеспечивающие переход на автоматизированные системы, которые позволяют хранить информацию в электронном виде [1–3]. Это повышает эффективность информационного обмена между медицинскими учреждениями, дает возможность удаленного доступа к медицинским информационным системам, облегчает и ускоряет запись пациентов на прием к врачам с помощью электронной регистратуры [4–6]. В связи с этим можно утверждать, что медицинская информация в электронной форме является основой многих процессов в современном здравоохранении.

Так, в ряде организаций начинается переход на системы электронных историй болезней, предоставляющие возможность разным специалистам совместно использовать информацию о состоянии здоровья пациентов [7, 8]. Наиболее

активно этот процесс реализуется в США и Германии [9, 10]. В этих странах выполняется большое число проектов в целях поддержки перехода к использованию электронных медицинских карт (Electronic Health Record, EHR), обеспечивающих обмен информацией между различными медицинскими организациями. К числу преимуществ целенаправленного использования EHR относится обеспечение пациентов и медицинских работников полной и точной медицинской информацией. Например, в Германии создана Ассоциация электронных медицинских карт, включающая в себя основные больницы и клиники, а также локальные ассоциации здравоохранения и региональные сети здравоохранения. Ассоциация разработала новую концепцию развертывания технологии электронных историй болезни (Electronic Case Record, ECR) — ECR in a Box [11]. Разработанный подход облегчает привлечение к здравоохранению новых действующих лиц, позволяя им проще включаться в региональные сети здравоохранения (рис. 1).

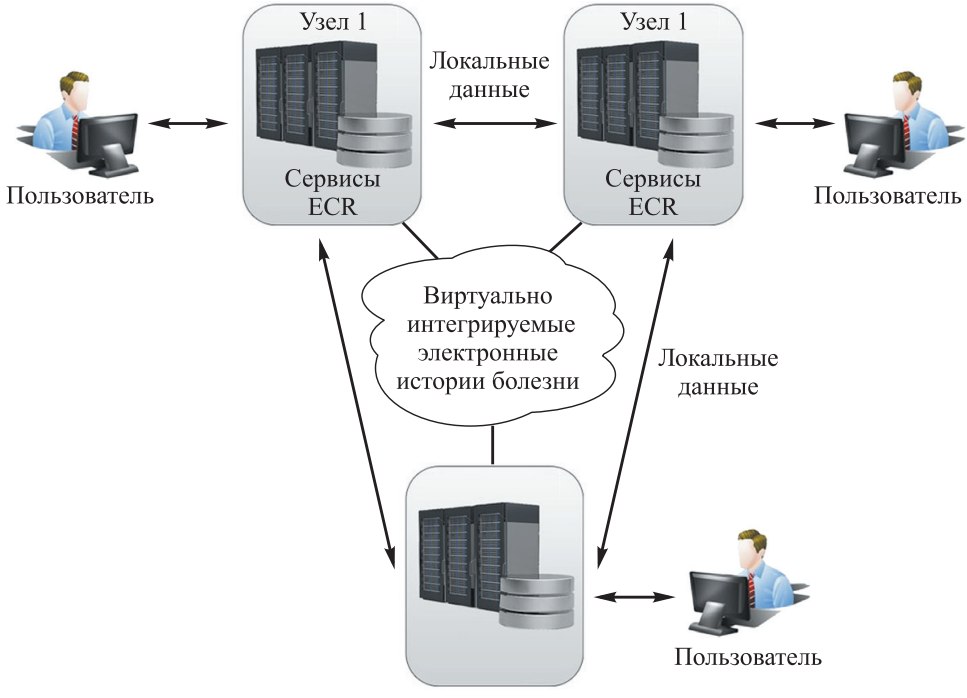

Рис. 1. Одноранговая архитектура платформы ECR

Однако в подобных системах доступ к истории болезни пациента может получить любой сотрудник, имеющий доступ к системе, без ведома пациента. Эти системы позволяют внести, удалить или изменить любую информацию, поэтому они не являются безопасными, так как в них нарушаются принципы конфиденциальности и целостности информации. Системы, которые оперируют такими важными данными, как информация о здоровье человека, должны быть надежно защищены.

Определяющую роль в этом процессе играет безопасный доступ к информации, а также обеспечение защиты при передаче данных и применение электронных подписей [12–14]. Решением этих проблем является использование смарт-карты, которая хранится у пациента и позволяет однозначно идентифицировать его в единой базе электронных медицинских карт.

В настоящей статье представлены особенности работы со смарт-картами для обеспечения конфиденциальности и целостности данных пациентов.

Применение смарт-карт в здравоохранении. Смарт-карта — пластиковая карточка, по внешнему виду идентичная карте полиса медицинского страхования или кредитной карте. Чип, встроенный в смарт-карту, имеет энергонезависимую память и криптопроцессор (микрокомпьютер, имплантированный в пластиковую карту). В память чипа записывается уникальный сертификат пользователя и другая персонифицированная информация (сведения о пациенте и о состоянии его здоровья). Криптопроцессор обеспечивает логику работы карты, в том числе, генерацию ключевых пар и электронной подписи.

В настоящее время популярность электронных персональных карт постоянно возрастает, в ряде зарубежных стран применение смарт-карт в медицине уже стало обычным делом. Во Франции, Германии, Италии, Японии, Турции, Тайване, Словении используются десятки миллионов смарт-карт в сфере медицинского обслуживания.

Применение смарт-карт значительно упрощает идентификацию пациента в компьютерной системе медицинского учреждения, уменьшает вероятность ошибок при учете оказанных пациенту услуг и ускоряет время оборота медицинской информации (рис. 2).

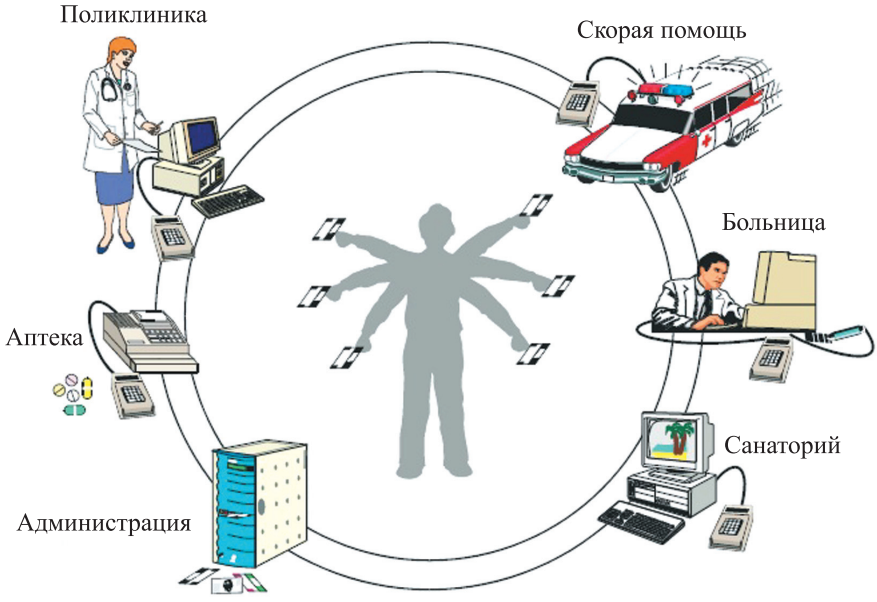

Рис. 2. Возможные применения смарт-карт как носителей информации

Для начала работы с медицинской информационной системой, содержащей электронные истории болезни (ЭИБ), пользователь соединяет смарт-карту со считывателем и вводит PIN-код. При этом последовательно осуществляются 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.

Затем происходит регистрация пользователя в информационной системе медицинского учреждения. Начиная с этого момента, история всех его действий, при необходимости, может быть восстановлена.

Существуют два типа карт: карта пациента и карта врача. На карте пациента имеются две области памяти: открытая и закрытая. В открытой области памяти хранится базовая информация о пациенте (фамилия, имя, отчество, дата рождения, группа крови, наименование страховой компании и т. п.). Эти данные должны быть доступны любому медработнику для оказания неотложной медицинской помощи, но они должны быть защищены от несанкционированного внесения изменений. В закрытой области хранятся данные, необходимые для аутентификации пациента, и прочие персональные данные. Эта область доступна только медицинским специалистам по предъявлению смарт-карт. Другая информация о состоянии здоровья (истории болезни) пациента хранится не на карте, а на сервере медицинского учреждения и доступна соответствующим медицинским специалистам.

Второй тип смарт-карт — карта врача (или карта специалиста). На этой карте записаны фамилия, имя, отчество специалиста, название лечебного учреждения, в котором он работает, специализация, персональный номер, электронная подпись. Карта дает право доступа к закрытой информации, как на карте пациента, так и на серверах медицинских учреждений (специалист может получить доступ лишь к той информации, на которую имеет право в соответствии с его специализацией).

Отметим, что при обеспечении взаимодействия карточных систем с информационными системами здравоохранения важно 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 [15–17]. Одной из главных причин распространения этого стандарта является использование технологии XML, удобной для описания архитектуры клинических документов [18].

Защита данных пациента при работе со смарт-картами. Рассмотрим особенности приема врача при использовании смарт-карт (рис. 3). Каждый участник процесса имеет личную смарт-карту, на которую записана его персональная

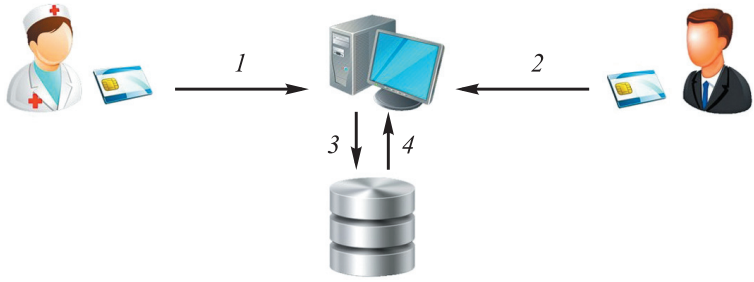

Рис. 3. Схема, описывающая прием врача:
1 — смарт-карта врача; *2* — смарт-карта пациента; *3* — поиск ЭИБ пациента; *4* — предоставление информации врачу

информация. В начале приема врач авторизуется с помощью своей смарт-карты *1* для получения доступа к системе ЭИБ.

Приходя в медицинское учреждение, пациент предоставляет карту *2* и вводит свой PIN-код. Затем медицинский сотрудник, авторизованный в системе, получает доступ к идентификатору пациента, хранящемуся на карте. По этому идентификатору в базе данных (БД) осуществляется поиск ЭИБ пациента *3*, далее полученная информация предоставляется медицинскому сотруднику, который может создавать электронные персональные медицинские записи, затем в соответствии с ГОСТ Р 52636–2006 обязан их подписать квалифицированной электронной подписью. Изменение записей может выполняться только до момента подписания. После подписания изменение или удаление записей из БД проводится в особом порядке, прописанном в политике безопасности учреждения здравоохранения. Таким образом, медицинский сотрудник несет ответственность за подписанные им электронные документы. Для обеспечения целостности и достоверности информации в системе должен использоваться сервер доверенного времени.

Кроме идентификатора на медицинской карте хранится информация, доступная без ввода PIN-кода, никак не идентифицирующая пациента, но позволяющая оказать экстренную медицинскую помощь (например, группа крови, резус-фактор, имеющиеся хронические заболевания и др.).

Открытые и закрытые данные, которые должны храниться на карте, их формат и размер занимаемой памяти, приведены в таблице.

Открытые и закрытые данные, которые должны храниться на карте, их формат и размер занимаемой памяти

Наименование элементов	Допустимые значения	Размер занимаемой памяти, байт
Идентификатор пациента	12-значный номер	12
PIN-код	8-значный номер	8
Идентификатор ЭМА	4-значный номер	4
Фамилия, имя, отчество владельца карты	Строка не более 50 символов	50

Окончание таблицы

Наименование элементов	Допустимые значения	Размер занимаемой памяти, байт
Группа крови и резус фактор	0+, 0–, A+, A–, B+, B–, AB+, AB–	3
Сахарный диабет и его тип	0 — нет, 1 или 2 — тип диабета	1
ВИЧ-статус	Один символ (+, –)	1
Гепатит	Один символ (0 — нет гепатита, A, B, C, D, E, F, G)	1
Хронические заболевания	Коды, соответствующие заболеваниям по Международной классификации болезней	10
Непереносимость лекарственных препаратов	Коды веществ из непереносимых пациентом лекарственных препаратов	10
Сертификат открытого ключа	Открытый ключ	64
Дайджест	Хэш всех данных карты	64

По результатам исследований авторами создано приложение, которое работает с базой данных *Medical_card*, содержащей информацию о медицинских сотрудниках, пациентах и их электронных персональных медицинских записях.

Описание работы приложения. Программное обеспечение, которое осуществляет доступ к карте, разработано на языке программирования C++ в среде разработки *QtCreator*. Для работы с базой данных была выбрана СУБД *MySQL*.

Приложение предусматривает работу с двумя смарт-картами: картой врача и картой пациента. На карте врача хранится идентификатор и ключевая пара, на карте пациента — идентификатор, фамилия, имя, отчество, базовая информация, подпись врача, сертификат открытого ключа.

При запуске программы и на протяжении ее работы происходит проверка наличия подключенной карты врача. Если при запуске программы карта отсутствует, то появляется сообщение с просьбой подключить карту. После подключения карты происходит авторизация. Врачу предлагается ввести PIN-код карты. Если PIN-код корректен, то происходит проверка подлинности карты методом *Challenge-Response* [12, 14]. Суть данного метода заключается в следующем. На карте врача хранится идентификатор, по которому в БД выбирается открытый ключ, соответствующий врачу, для проверки подписи. Приложение генерирует случайное число, хэширует его алгоритмом в соответствии с ГОСТ34.11–94. Затем хэш аппаратно подписывается картой по алгоритму, приведенному в ГОСТ34.10–2001. Далее с помощью открытого ключа из БД подпись проверяется. Если подпись верна, то врачу предоставляется доступ к системе. Для того чтобы продолжить работу с приложением, необходимо подключить вторую карту.

После подключения второй карты приложение предоставляет врачу три режима работы с картой пациента: «Режим записи»; «Режим частичного чтения»;

«Режим полного чтения». Режимы записи и полного чтения доступны только после ввода PIN-кода пациентом. Режим частичного чтения доступен сразу после подключения карты пациента.

Блок-схема алгоритма работы приложения представлена на рис. 4.

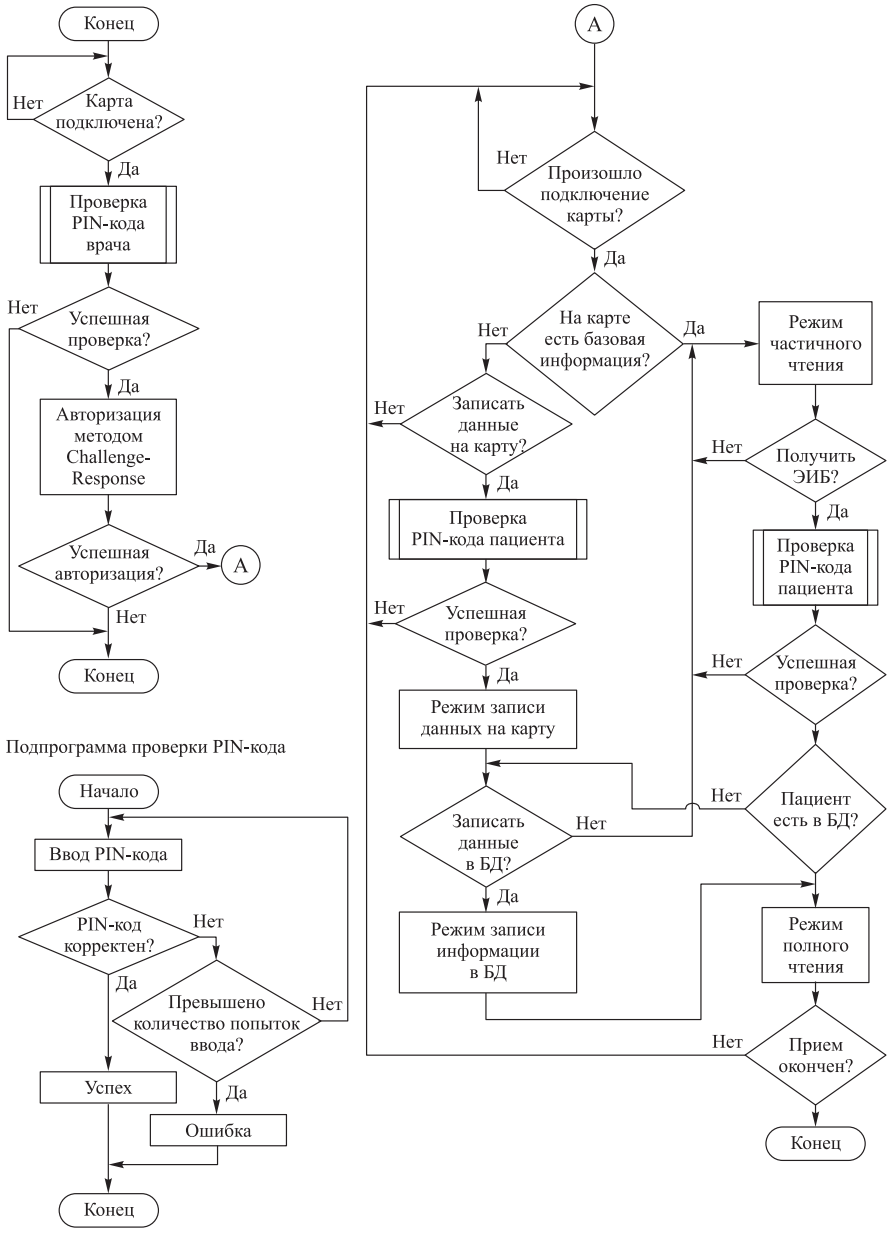

Рис. 4. Блок-схема алгоритма работы приложения

Если на карте пациента уже записана информация, то окно с базовыми данными пациента появляется сразу. При открытии окна происходит проверка подписи с использованием ключа, извлеченного из сертификата. Если после

подписания данные были изменены, то появится предупреждение об этом. Для того чтобы перейти к полному чтению информации, необходимо нажать на кнопку «Получить историю болезни». Если такого пациента нет в БД, врачу будет предложено создать запись.

В режиме полного чтения можно просмотреть информацию о враче, который записывал данные на карту и подписал ее. Получив идентификатор, программа отправляет в БД запрос для получения ЭИБ пациента. Затем медицинский сотрудник может работать с ЭИБ. Интерфейс приложения максимально приближен к бумажной версии истории болезни (рис. 5).

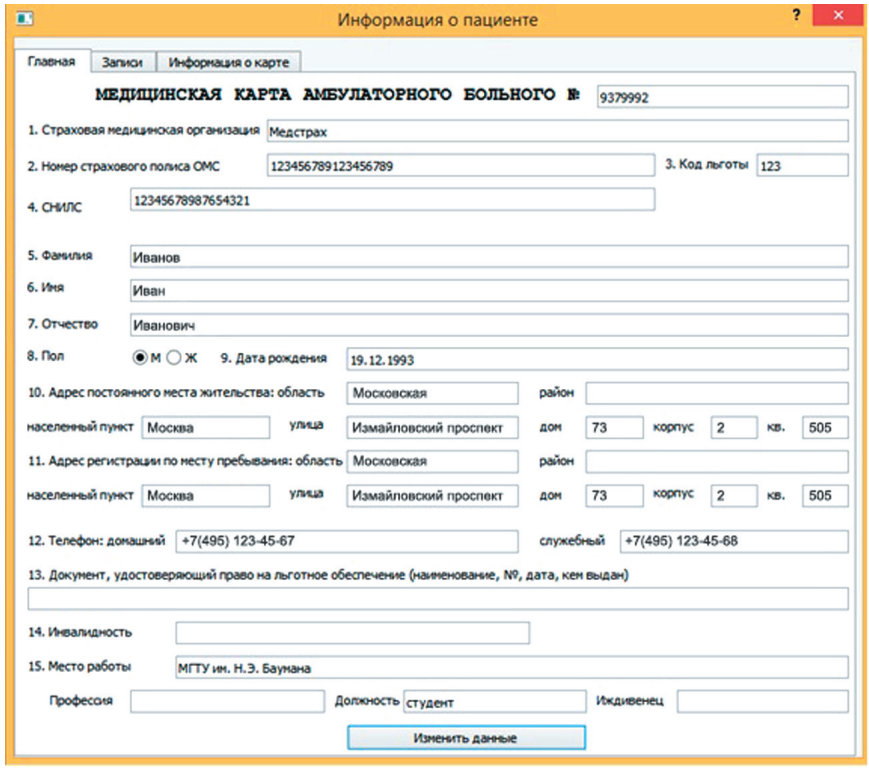

Рис. 5. Электронная история болезни

В режиме полного чтения можно изменять и перезаписывать данные. После ввода изменений информация, хранящаяся на карте, удаляется, записывается заново и подписывается.

В режиме частичного чтения пользователю предоставляются минимальные данные, необходимые для оказания экстренной помощи пациенту.

Заключение. Применение смарт-карт в здравоохранении обеспечивает защиту данных пациентов в базе ЭИБ. Создано программное обеспечение с пользовательским интерфейсом для работы со смарт-картой пациента. Реализованное приложение позволит повысить эффективность работы медицинского персонала, а также обеспечить надежное хранение данных о состоянии здоровья

пациентов. Для обеспечения целостности данных использована электронная подпись по алгоритму, приведенному в ГОСТ34.10–2001, для обеспечения конфиденциальности — аутентификация врача и пациента. Аутентификация врача выполняется методом *Challenge-Response*, аутентификация пациента — вводом PIN-кода.

ЛИТЕРАТУРА

1. *Вопросы* создания Единого информационного пространства в системе здравоохранения РАН / Н.Г. Гончаров, Я.И. Гулиев, Ю.В. Гуляев, Ю.М. Кавинская, А.А. Каменщиков, А.Я. Олейников, М.И. Хаткевич // Информационные технологии и вычислительные системы. 2006. № 4. С. 83–95.

2. *Lantsberg A.V., Troitzch K.G., Buldakova T.I.* Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources) // Automatic Documentation and Mathematical Linguistics. 2011. Vol. 45. No. 2. P. 74–80. DOI: 10.3103/S0005105511020075

URL: http://link.springer.com/article/10.3103/S0005105511020075

3. *Ланцберг А.В., Тройч К., Булдакова Т.И.* Особенности оценки качества медицинской электронной услуги // Информационное общество. 2011. № 4. С. 28–37.

4. *Гусев А.В.* Обзор электронных регистратур // Врач и информационные технологии. 2010. № 6. С. 4–15.

5. *Llinás G., Rodríguez-Iñesta D., Lorenzo S., Aibar C.* Comparison of websites from Spanish, American and British hospitals // Methods of Information in Medicine. 2008. Vol. 47. No. 2. P. 124–130.

6. *Ланцберг А.В., Тройч К., Булдакова Т.И.* Развитие системы электронных услуг муниципальной поликлиники (на основе анализа зарубежных web-ресурсов) // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2011. № 4. С. 1–7.

7. Электронная история болезни — важнейшее звено медицинских информационных систем / В.А. Монич, О.И. Кушников, Р.Р. Алакаев, А.Я. Косоногов, Д.П. Коротин, Е.В. Медоваров // Современные технологии в медицине. 2010. № 3. С. 73–74.

URL: http://www.stm-journal.ru/ru/numbers/2010/3/648

8. *Зингерман Б.В., Шкловский-Корди Н.Е.* Электронная медицинская карта и принципы ее организации // Врач и информационные технологии. 2013. № 2. С. 37–58.

9. *Медицинские* информационные технологии: глобальный прогноз развития. М.: ООО «АКСИМЕД», 2011. 18 с.

10. *Кузнецов С.* Электронные медицинские карты — реальность // Открытые системы. СУБД. 2012. № 10. С. 60–62. URL: https://www.osp.ru/os/2012/10/13033128

11. *Kuhlisch R., Kraufmann B., Restel H.* Electronic case records in a box: Integrating patient data in healthcare networks // Computer. 2012. Vol. 45. No. 11. P. 34–40. DOI: 10.1109/MC.2012.294 URL: http://ieeexplore.ieee.org/document/6287500

12. *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. P. 27–33. DOI: 10.1109/MC.2012.285
URL: http://ieeexplore.ieee.org/document/6353451

13. *Булдакова Т.И., Суятинов С.И., Миков Д.А.* Анализ информационных рисков виртуальных инфраструктур здравоохранения // Информационное общество. 2013. № 4. С. 6.

14. *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. URL: http://cyberrus.com/wp-content/uploads/2015/02/vkb_08_04.pdf

15. *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.

16. *Швырев С.Л.* Внедрение стандартов HL7 в России // Врач и информационные технологии. 2009. № 6. С. 71–72.

17. *Weiss G.* You have to have standards // IEEE Spectrum. 2002. Vol. 39. No. 3. P. 48.

18. *Ahn Ch., Nah Yu., Park S., Kim Ju.* An integrated medical information system using XML // Lecture Notes in Computer Science. 2001. Vol. 2105. P. 307–322.

Булдакова Татьяна Ивановна — д-р техн. наук, профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Ланцберг Анна Вильямовна — канд. техн. наук, научный сотрудник Института проблем точной механики и управления РАН (Российская Федерация, 410028, Саратов, ул. Рабочая, д. 24).

Смолянинова Кристина Александровна — студентка кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Просьба ссылаться на эту статью следующим образом:

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. DOI: 10.18698/0236-3933-2017-3-95-106

SECURE ACCESS TO INFORMATION USING SMART CARD

T.I. Buldakova[1] buldakova@bmstu.ru
A.V. Lantsberg[2] nurka_nuska@mail.ru
K.A. Smolyaninova[1] kriszzztina@yandex.ru

[1] Bauman Moscow State Technical University, Moscow, Russian Federation
[2] Institute of Precision Mechanics and Control, Russian Academy of Sciences, Saratov, Russian Federation

Abstract

The article is devoted to the protection of patient data in medical information systems containing electronic medical records. The study shows that the access to the patient's health data is available to any employee registered in the system, without notifying the patient. To ensure the information confidentiality and integrity, we suggest using smart cards to uniquely identify the patient in the unified electronic medical record database. We describe

Keywords

Medical information system, electronic medical records, information security, smart card

possibilities of smart cards and characteristic features of their application in health care. As an example, we consider the process when a doctor sees patients with smart cards. In this work we lay down the requirements to the data stored on the patient's card. Moreover, we provide the software for operation with smart cards, give the flowchart of the developed application. Finally, we describe the application operating modes and give examples

REFERENCES

[1] Goncharov N.G., Guliev Ya.I., Gulyaev Yu.V., Kavinskaya Yu.M., Kamenshchikov A.A., Oleynikov A.Ya., Khatkevich M.I. Problems of creation of Common information area in RAS health care system. *Informatsionnye tekhnologii i vychislitel'nye sistemy*, 2006, no. 4, pp. 83–95 (in Russ.).

[2] Lantsberg A.V., Troitzch K.G., Buldakova T.I. Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources). *Automatic Documentation and Mathematical Linguistics*, 2011, vol. 45, no. 2, pp. 74–80.
DOI: 10.3103/S0005105511020075 Available at: http://link.springer.com/article/10.3103/S0005105511020075

[3] Lantsberg A.V., Troych K., Buldakova T.I. Quality control features of medical E-services. *Informatsionnoe obshchestvo*, 2011, no. 4, pp. 28–37 (in Russ.).

[4] Gusev A.V. Review of solutions “Electronic registry”. *Vrach i informatsionnye tekhnologii* [Information technologies for the Physician], 2010, no. 6, pp. 4–15 (in Russ.).

[5] Llinás G., Rodríguez-Iñesta D., Lorenzo S., Aibar C. Comparison of websites from Spanish, American and British hospitals. *Methods of Information in Medicine*, 2008, vol. 47, no. 2, pp. 124–130.

[6] Lantsberg A.V., Troych K., Buldakova T.I. Developing E-services system of municipal clinic (based on foreign websites analysis). *Nauchno-tekhnicheskaya informatsiya. Seriya 2: Informatsionnye protsessy i sistemy*, 2011, no. 4, pp. 1–7 (in Russ.).

[7] Monich V.A., Kushnikov O.I., Alakaev R.R., Kosonogov A.Ya., Korotin D.P., Medovarov E.V. Electronic case history is a most important link of the medical information system. *Sovremennye tekhnologii v meditsine* [Modern Technologies in Medicine], 2010, no. 3, pp. 73–74. Available at: http://www.stm-journal.ru/en/numbers/2010/3/648

[8] Zingerman B.V., Shklovskiy-Kordi N.E. Electronic health records cards and the principles of its organization. *Vrach i informatsionnye tekhnologii* [Information technologies for the Physician], 2013, no. 2, pp. 37–58 (in Russ.).

[9] Meditsinskie informatsionnye tekhnologii: global'nyy prognoz razvitiya [Medical informational technologies: Global development forecast]. Moscow, OOO “AKSIMED”, 2011. 18 p.

[10] Kuznetsov S. Electronic health records are reality. *Otkrytye sistemy. SUBD* [Open Systems. DBMS], 2012, no. 10, pp. 60–62. Available at: https://www.osp.ru/os/2012/10/13033128

[11] 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.
DOI: 10.1109/MC.2012.294 Available at: http://ieeexplore.ieee.org/document/6287500

[12] 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. DOI: 10.1109/MC.2012.285 Available at: http://ieeexplore.ieee.org/document/6353451

[13] Buldakova T.I., Suyatinov S.I., Mikov D.A. Analysis of information risks of virtual infrastructures in health protection. *Informatsionnoe obshchestvo*, 2013, no. 4, pp. 6 (in Russ.).

[14] Buldakova T.I., Suyatinov S.I., Krivosheeva D.A. Ensuring information security in telemedicine systems on the basis of model approach. *Voprosy kiberbezopasnosti*, 2014, no. 5 (8), pp. 21–29. Available at: http://cyberrus.com/wp-content/uploads/2015/02/vkb_08_04.pdf

[15] Anishchenko V.S., Buldakova T.I., Dovgalevskiy P.Ya., Lifshits V.B., Gridnev V.I., Suyatinov S.I. Conceptual model of virtual centre of public health services. *Informatsionnye tekhnologii*, 2009, no. 12, pp. 59–64 (in Russ.).

[16] Shvyrev S.L. Implementation of HL7 standards in Russia. *Vrach i informatsionnye tekhnologii* [Information technologies for the Physician], 2009, no. 6, pp. 71–72 (in Russ.).

[17] Weiss G. You have to have standards. *IEEE Spectrum*, 2002, vol. 39, no. 3, pp. 48.

[18] Ahn Ch., Nah Yu., Park S., Kim Ju. An integrated medical information system using XML. *Lecture Notes in Computer Science*, 2001, vol. 2105, pp. 307–322.

Buldakova T.I. — Dr. Sc. (Eng.), Professor of Information Security Department, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Lantsberg A.V. — Cand. Sc. (Eng.), Research Scientist of Institute of Precision Mechanics and Control, Russian Academy of Sciences (Rabochaya ul. 24, Saratov, 410028 Russian Federation).

Smolyaninova K.A. — student of Information Security Department, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, srt. 1, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Buldakova T.I., Lantsberg A.V., Smolyaninova K.A. Secure Access to Information using Smart Card. *Vestn. Mosk. Gos. Tekh. Univ. im. N.E. Baumana, Priborostr.* [Herald of the Bauman Moscow State Tech. Univ., Instrum. Eng.], 2017, no. 3, pp. 95–106.
DOI: 10.18698/0236-3933-2017-3-95-106