МЕДИЦИНСКИЕ И БИОЛОГИЧЕСКИЕ ИЗМЕРЕНИЯ

УДК 004.75: 616.12-07

С. А. Балахонова

ОСОБЕННОСТИ РЕАЛИЗАЦИИ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ КАРДИОДИАГНОСТИКИ

S. A. Balakhonova

IMPLEMENTATION FEATURES OF DISTRIBUTED CARDIO DIAGNOSIS SYSTEM

А н н о т а ц и я. ***Актуальность и цели***. Целью работы является разработка структуры распределенной системы кардиодиагностики, обеспечивающей своевременность и качество медицинской помощи при снижении затрат на аппаратное обеспечение. ***Материалы и методы***. Рассмотрены возможности оптимизации оказания медицинской помощи, особенности и проблемы построения распределенных систем. Особое внимание уделено необходимости повышения надежности и отказоустойчивости системы для противодействия DDoS-атакам. Предложен подход к построению распределенной системы кардиодиагностики, учитывающий требования к высоким показателям эксплуатационных характеристик. ***Результаты***. Предложен подход к организации распределенной системы кардиодиагностики. Разработанная структура системы обеспечивает следующие преимущества: высокую степень доступности, возможность аппаратного масштабирования, защищенность от воздействия злоумышленников, надежность, отказоустойчивость. Предложенный подход к построению распределенной системы кардиодиагностики позволяет снизить себестоимость затрат на защиту от DDoS-атак. ***Выводы***. Предложенный подход к построению структуры распределенной системы кардиодиагностики позволяет снизить ее себестоимость при сохранении высоких эксплуатационных характеристик.

A b s t r a c t. ***Background.*** The aim is to develop a structure of a distributed cardio diagnosis system, ensuring the timeliness and quality of care while reducing costs on hardware. ***Materials and methods***. The article discusses the possibility of optimizing patient care. The features and problems of building distributed systems is considered. Particular attention is paid to need to improve reliability and fault tolerance of system to counter DDoS-attacks. Approach to construction of distributed cardio diagnosis system is offered. ***Results***. The organization of distributed heart state diagnosis system is offered. Advantages of distributed system implementing are proved: high degree of availability, possibility of hardware scaling, protection from malicious impact, reliability, fault tolerance. The proposed approach to the construction of distributed system reduces the cost of protection against DDoS-attacks. ***Conclusions***. The proposed approach to building distributed cardio diagnosis system structure reduces cost of system, while maintaining high performance.

Ключевые слова: медицинская информационная система, распределенная система, облачный сервис, надежность, доступность.

Key words: medical information system, distributed system, cloud service, fault tolerance, availability.

Введение

Важнейшими показателями уровня жизни населения являются доступность и качество медицинского обслуживания. В последние годы на государственном уровне уделяется особое внимание развитию здравоохранения. Одним из направлений реформирования системы медицинского обслуживания стало повсеместное внедрение информационных технологий. Компьютеризация, проведение высокоскоростного Интернета в больницах и поликлиниках, использование медицинских информационных систем (МИС) в работе персонала – неотъемлемые части современного здравоохранения. В течение ближайших двух лет планируется стопроцентная информатизация лечебных учреждений [1]. В итоге данное реформирование призвано повысить качество оказания медицинской помощи, оптимизировать использование трудовых ресурсов, повысить уровень жизни населения.

Одним из возможных путей повышения доступности и качества оказания медицинской помощи, по мнению автора, является построение технологического процесса обмена данными между персональным портативным устройством кардиодиагностики, службой экстренной медицинской помощи и лечебно-профилактическим учреждением (ЛПУ). Реализовать данный технологический процесс предлагается в рамках распределенной системы кардиодиагностики.

При реализации распределенной системы особое внимание необходимо уделить надежности системы, отказоустойчивости, возможности масштабирования, защищенности от несанкционированного воздействия [2].

Одной из нерешенных проблем современных МИС является недостаточная устойчивость к DDoS-атакам. Это связано с высокой стоимостью оборудования, необходимого для противодействия DDoS-атакам. Ограниченность бюджета при развертывании МИС учреждениями здравоохранения приводит к снижению устойчивости перед хакерскими атаками. По мнению автора, необходимо искать пути снижения себестоимости разрабатываемой распределенной кардиодиагностической системы (РКДС) с сохранением эксплуатационных характеристик.

В данной статье автором предложены концептуальные особенности построения медицинской системы на примере построения РКДС «Кардиовид».

На рис. 1 представлена схема организации облачного сервиса РКДС «Кардиовид» [3].

Как видно из рис. 1, сервис РКДС «Кардиовид» представляет собой сложную распределенную систему, состоящую из множества серверов, одни из которых являются внутренними (функциональными) и недоступными для сетевых обращений из «внешнего» мира, а другие серверы являются внешними (транзитными) и служат для организации сетевого взаимодействия между клиентами и активным функциональным сервером. Клиентами РКДС являются портативные кардиоанализаторы (ПКА), лечебно-профилактические учреждения и др. Приведенная схема организации облачного сервиса РКДС «Кардиовид» обладает следующими преимуществами: распределенность, аппаратная масштабируемость, высокая степень доступности, защищенность каналов связи [3].

Обладание свойством распределенности позволяет РКДС использовать ресурсы множества серверов и МИС ЛПУ для организации хранения и обработки медицинской информации. При этом реализуется фундаментальный принцип построения распределенной базы данных (БД): для пользователя распределенная система должна выглядеть как нераспределенная [4]. Это обеспечивается путем организации асинхронного доступа к данным за счет использования трехзвенной клиент-серверной архитектуры и распределенной БД [5].

Среди указанных преимуществ одним из наиболее важных, с точки зрения автора, является высокая степень доступности. Данное преимущество достигается в результате применения следующих технологических приемов:

1. Защита функциональных серверов от DDoS-атак, что достигается благодаря отсутствию известных злоумышленнику доменных имен и IP-адресов.

2. Защита транзитных серверов (ТС) от DDoS-атак, что достигается за счет использования значительного количества «внешних» серверов, вероятность организации одновременной успешной DDoS-атаки на которые близка к нулю.

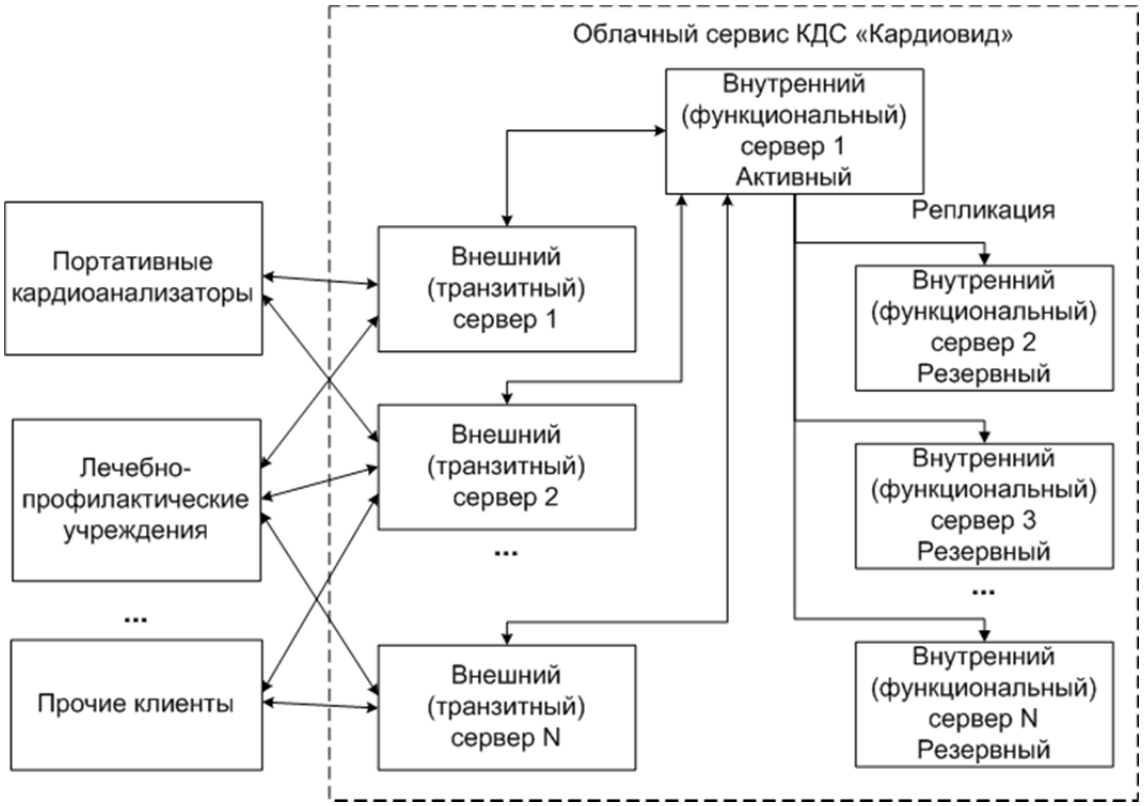

Рис. 1. Схема организации облачного сервиса РКДС «Кардиовид»

Одновременное использование множества транзитных серверов, обладающих различной степенью устойчивости к DDoS-атакам, повышает доступность облачного сервиса РКДС (P):

$$P = 1 - \prod_{i=1}^{n} (1 - p_i), \quad (1)$$

где p_i – вероятность доступности i-го ТС при организации на него DDoS-атаки; при $p_1 = p_2 = p_3 = 0{,}5$, $P = [1 - (1 - p)^3] = 1 - 0{,}125 = 0{,}875$.

Очевидно, что при увеличении количества транзитных серверов n и их устойчивости к DDoS-атакам максимальная доступность сервиса РКДС: $P \to 1$.

3. Использование резервных функциональных серверов, каждый из которых готов в любой момент принять роль активного сервера. При этом актуальность информации на резервных функциональных серверах обеспечивается благодаря использованию механизма репликации данных.

4. Размещение транзитных и функциональных серверов в разных data-центрах, что позволяет сервису РКДС оставаться доступным даже в случае организации DDoS-атаки непосредственно на data-центр либо при возникновении технических неполадок в его работе.

Защищенность канала связи в РКДС обеспечивается благодаря использованию технологии организации защищенного соединения TLS (Transport Layer Security) [6].

Для снижения количества сетевых запросов, требуемых для установки и поддержания защищенного соединения, автором разработан алгоритм установки защищенного соединения между клиентом и транзитным сервером, представленный на рис. 2.

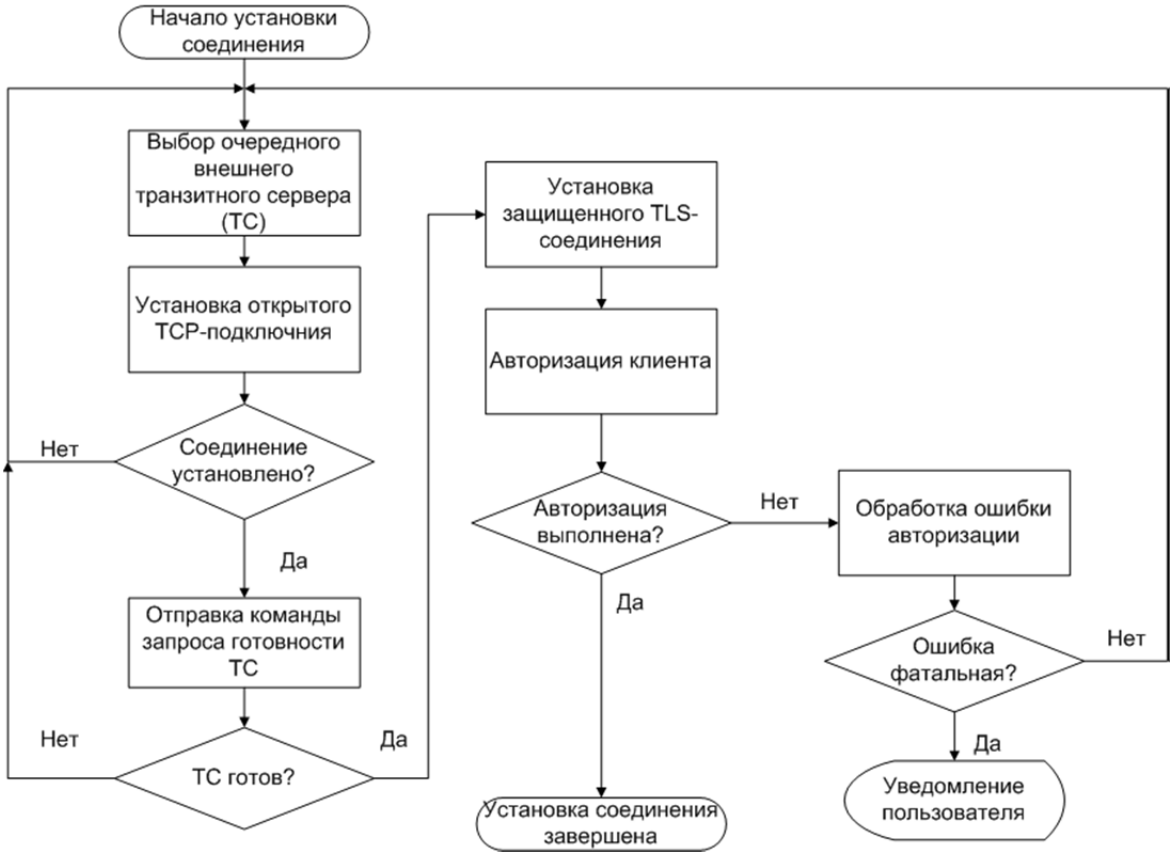

Рис. 2. Алгоритм установки защищенного соединения между клиентом и транзитным сервером

Алгоритм, представленный на рис. 2, учитывает специфику работы транзитных серверов и включает следующие этапы установки защищенного соединения между клиентом и ТС:

1. **Выбор очередного внешнего транзитного сервера**. Предполагается, что в памяти клиента (ПКА, ЛПУ и др.) сохранена таблица всех доступных ТС с указанием их доменного имени (или IP-адреса) и номера TCP-порта. При отсутствии таблицы транзитных серверов с актуальными данными клиент должен запросить ее у известного ТС, который задан в программном обеспечении клиента по умолчанию. При выборе очередного транзитного сервера предпочтение должно отдаваться тому ТС, с которым ранее было успешно установлено защищенное соединение.

2. **Установка открытого TCP-соединения**. Осуществляется установка TCP-соединения [7] с транзитным сервером, выбранным на предыдущем этапе. В случае отказа в установке соединения осуществляется переход к п. 1, иначе переход к п. 3.

3. **Отправка команды запроса готовности транзитного сервера**. Данная команда позволяет оценить наличие у ТС ресурсов, необходимых для установки защищенного соединения и дальнейшего взаимодействия между клиентом и функциональным сервером в рамках этого соединения. Транзитный сервер возвращает ответ «готов» при наличии следующих факторов:

а) установлено соединение между транзитным и функциональным сервером;

б) транзитный сервер запущен в режиме готовности приема и обработки запросов от клиентов;

в) ограничение на максимальное количество подключений не достигнуто;

г) у транзитного сервера достаточно ресурсов для обслуживания запросов от клиента (отсутствует пиковая загрузка процессора, жесткого диска или SSD, а также памяти оперативного запоминающего устройства).

В случае приема от транзитного сервера ответа «готов» осуществляется переход к п. 4, иначе переход к п. 1.

4. **Установка защищенного TLS-соединения**. При этом используются стандартные протоколы установки TLS-соединения с использованием серверного сертификата [6]. Клиен-

там (ЛПУ), предоставляющим функциональному серверу запрашиваемую медицинскую информацию, должны выдаваться клиентские сертификаты, служащие гарантией того, что сервис РКДС получает информацию от доверенного источника.

5. **Авторизация клиента**. Осуществляется в рамках установленного TLS-соединения. При наличии идентификатора сессии, сформированного сервером в ходе предыдущей авторизации, клиент передает его транзитному серверу, который проверяет актуальность идентификатора. В том случае если идентификатор сессии актуален, сервер находит в своей памяти необходимую информацию о клиенте и передает ответ «авторизован», не запрашивая логин и пароль. В противном случае (идентификатор сессии на клиенте не сохранен либо сервер передал ответ «необходима авторизация») клиент должен передать транзитному серверу логин и пароль, после чего ТС должен сформировать новый идентификатор сессии и передать клиенту результат авторизации («авторизован» либо «ошибка авторизации» с указанием кода и расшифровки ошибки).

После успешного завершения этапа «авторизация клиента» сервис РКДС переходит в состояние готовности к обмену с клиентом медицинской информацией.

Необходимо отметить, что информация, передаваемая в ходе обмена между транзитными серверами и функциональным сервером, также надежно защищена от возможных деструктивных действий злоумышленника. Это достигается благодаря использованию технологии VPN (Virtual Private Network). Особенность VPN заключается в том, что, несмотря на организацию коммуникации по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений) [8].

Возможность аппаратного масштабирования также является немаловажным преимуществом. Это достигается благодаря использованию технологии «виртуальный выделенный сервер» (VDS), которая предоставляется современными data-центрами. Преимущество использования данной технологии заключается в том, что на начальном этапе работы РКДС можно использовать недорогой VDS со скромными аппаратными возможностями, которые в дальнейшем можно наращивать по мере появления потребностей и соответствующего финансирования.

При разработке современного программного обеспечения (ПО) немаловажное значение имеет выбор среды разработки ПО. Современная среда разработки должна обладать огромным количеством возможностей и особенностей, среди которых автор выделяет следующие:

1) поддержка современных технологий в области разработки ПО;

2) возможность разработки кроссплатформенных приложений, которые могут работать одинаковым образом в разных операционных системах;

3) современный развитый язык программирования;

4) наличие собственной библиотеки компонентов и возможность использования библиотек от сторонних разработчиков;

5) генерация машинного кода, отличающегося высокой производительностью и низкими требованиями к аппаратным ресурсам компьютера;

6) стоимость среды разработки, простота ее развертывания и высокая скорость компиляции и сборки программных проектов;

7) наличие сообщества разработчиков ПО, осуществляющих активное развитие среды разработки и устранение выявленных ошибок.

Анализ современных средств разработки ПО показал, что указанными возможностями и особенностями обладает свободно доступная интегрированная среда разработки программного обеспечения Lazarus IDE, использующая язык программирования Object Pascal и кроссплатформенный компилятор Free Pascal [9]. Использование Lazarus IDE позволяет снизить издержки при разработке РКДС и реализовать кроссплатформенное ПО, работающее под управлением различных операционных систем, таких как Windows и Linux. Одна из экранных форм реализации распределенной системы кардиодиагностики представлена на рис. 3.

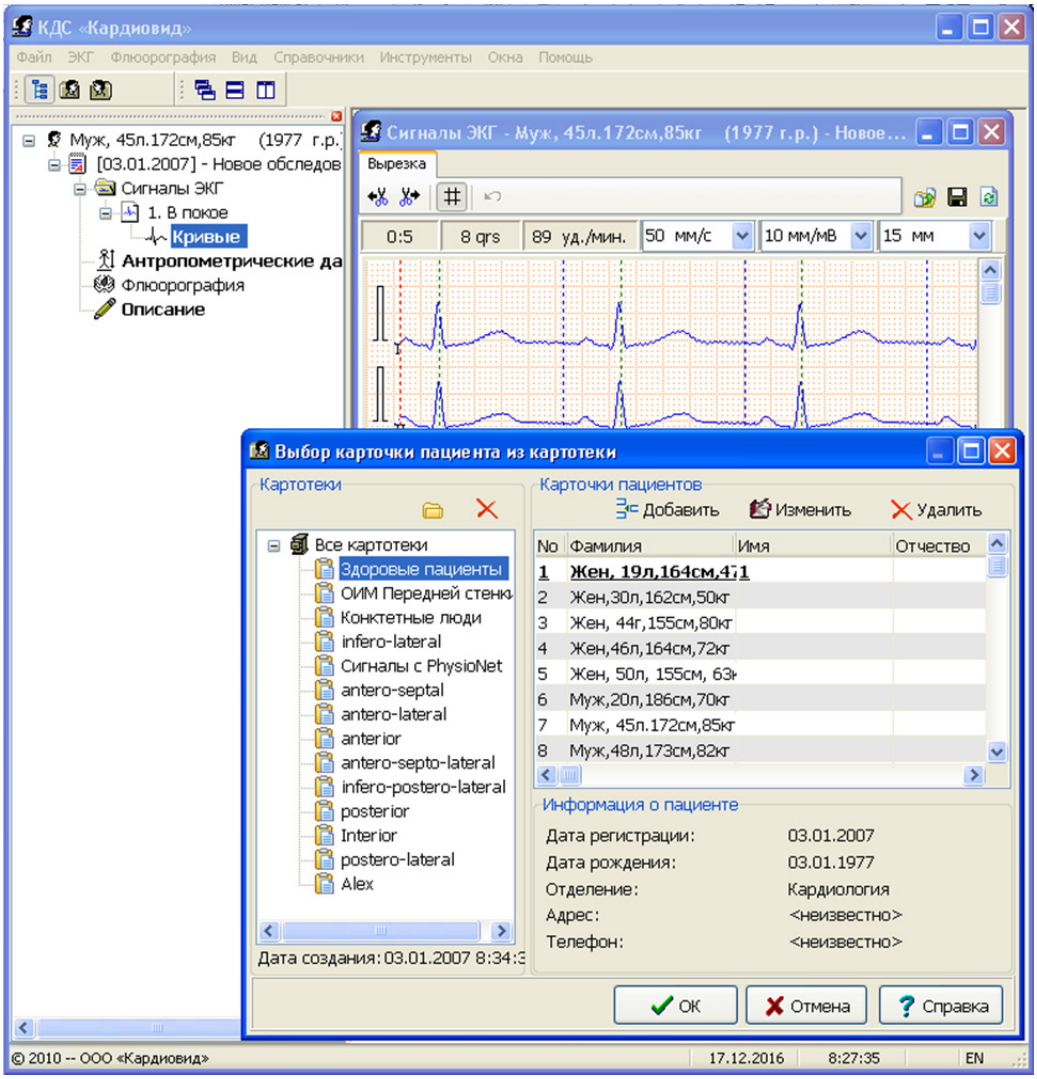

Рис. 3. Экранная форма распределенной системы кардиодиагностики

Заключение

Благодаря предложенному подходу к организации распределенной системы кардиодиагностики обеспечивается необходимый уровень надежности системы, отказоустойчивости, аппаратного масштабирования, защищенности от несанкционированного воздействия. Предложенный подход позволяет снизить себестоимость РКДС с сохранением эксплуатационных характеристик.

Библиографический список

1. Доклад министра здравоохранения РФ. – URL: https://www.rosminzdrav.ru/news/2016/12/14/3334-rabochaya-vstrecha-prezidenta-s-ministrom-veronikoy-skvortsovoy (дата обращения: 25.12.2016).
2. Медицинские информационные системы: Теория и практика / Г. И. Назаренко, Я. И. Гулиев, Д. Е. Ермаков ; под ред. Г. И. Назаренко, Г. С. Осипова. – М. : Физматлит, 2005. – 320 с.
3. Организация распределенной системы диагностики состояния сердца / С. А. Балахонова, О. Н. Бодин, Д. С. Логинов, Е. А. Ломтев // Измерение. Мониторинг. Управление. Контроль. – 2016. – № 2. – С. 129–136.
4. Распределенные системы, принципы и парадигмы / Э. Таненбаум, М. ван Стеен. – СПб. : Питер, 2003. – 877 с.
5. Пат. 2586854 Российская Федерация. Способ предоставления данных, относящихся к пациентам медицинского учреждения / Бодин О. Н., Балахонова С. А., Иванчуков А. А.,

Касимов А. О., Ожикенов К. А., Полосин В. Г., Рахматуллов Ф. К., Сафронов М. И., Сергеенков А. С. – №2015100793/14 ; заявл. 12.01.2015 ; опубл. 10.06.2016, Бюл. № 16.
6. Спецификация протокола TLS. Версия 1.2. – URL: http://www.webcitation.org/65JSRyvms (дата обращения: 20.12.2016).
7. Спецификация протокола TCP. – URL: https://tools.ietf.org/ html/rfc793 (дата обращения: 23.12.2016).
8. Virtual Private Network. – URL: https://ru.wikipedia.org/wiki/VPN (дата обращения: 23.12.2016).
9. Среда разработки программного обеспечения Lazarus. – URL: http://www.lazarus-ide.org (дата обращения: 27.12.2016).

Балахонова Светлана Александровна
аспирант,
Пензенский государственный университет
(Россия, г. Пенза, ул. Красная, 40)
E-mail: svetlanapage@mail.ru

Balakhonova Svetlana Aleksandrovna
postgraduate student,
Penza State University
(40 Krasnaya street, Penza, Russia)

УДК 004.75: 616.12-07

Балахонова, С. А.

Особенности реализации распределенной системы кардиодиагностики / С. А. Балахонова // Измерение. Мониторинг. Управление. Контроль. – 2017. – № 2 (20). – С. 70–76.