УДК 004.056
Мурадова Г.И.
Азербайджанский Технический Университет, Азербайджан, Баку
gulara_m@hotmail.com

КОНЦЕПЦИЯ REDIS ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ МЕДИЦИНСКИХ ДАННЫХ ПАЦИЕНТОВ

Безопасность персональных медицинских данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. Инструменты и решения Redis ориентированы на скоростную обработку данных. В статье показана целесообразность использования технологии Redis для поступающих в режиме онлайн и быстро меняющихся персональных медицинских данных. Применение Redis устраняет неконтролируемое ознакомление с конфиденциальной информацией.

Ключевые слова: *электронное здравоохранение, защита информации, безопасность, конфиденциальность, персональные медицинские данные, базы данных, управляемая служба кэша.*

Введение

В здравоохранении информатизация необходима на этапах лечебно-диагностического процесса при сборе информации о пациенте, диагностике, принятии решений о необходимых действиях, их реализации и организации медицинской помощи населению и управлении здравоохранением. Информатизация − комплекс мероприятий для полного и своевременного обеспечения участников процесса нужной информацией, переработанной и при необходимости преобразованной. Информатизация здравоохранения осуществляется путем создания и внедрения компьютеризированных систем. Использование инструментов информационной технологии в медицинской практике позволяет не только улучшить качество и доступность услуг, но и трансформировать саму модель предоставления медицинской помощи. Растущие ожидания граждан о повышении качества медицинской помощи стимулируют использование компьютерных приложений в здравоохранении. Кроме того, современная система здравоохранения опирается на концепции расширения прав и возможностей пациентов, совместного обслуживания и непрерывности услуг. Использование компьютерных решений в настоящее время воспринимается также как одно из эффективных средств правовой защиты [1]. Традиционные методы не могут реагировать на быстрорастущие потребности в обеспечении конфиденциальности пациентов в среде электронного здравоохранения [2].

Электронное здравоохранение

Электронное здравоохранение **(***E-health)* нацелено на решение всех задач охраны здоровья населения. Оно основано на общем электронном документообороте, включающем персональные медицинские данные, оперативный доступ к информации о пациенте, возможность ее совместного дистанционного анализа врачами и контакт врача с пациентом. В настоящее время все большее внимание уделяется проблеме отношения больного к своему здоровью. Это подразумевает интегральную характеристику физического, психологического, эмоционального и социального состояния больного, основанную на его субъективном восприятии. Право человека на жизнь и здоровье − неотъемлемое право каждого. Государство гарантирует гражданам охрану здоровья независимо от пола, расы, национальности, языка, социального происхождения, должностного положения, места жительства, отношения к религии, убеждений, принадлежности к общественным объединениям, а также других обстоятельств.

Современная концепция отношения к своему здоровью основана на трех составляющих:

- многомерность − это применение методик, связанных и не связанных непосредственно с заболеванием, что позволяет дифференцированно определить влияние болезни и лечения на состояние больного;
- изменяемость во времени − постоянный мониторинг состояния больного помогает проводить коррекцию лечения в зависимости от изменения состояния больного во времени;
- участие больного в оценке своего состояния – это показатель общего состояния, сделанный самим больным. Наряду с традиционным врачебным заключением составляется более полная картина болезни и дается прогноз ее течения [3, 4].

Большое число программ клинических исследований направлено на выбор оптимального алгоритма лечения заболеваний. При этом качество жизни рассматривают как важный интегральный критерий эффективности лечения. Данные пациента, полученные до лечения, используют для прогноза заболевания, его исхода и, таким образом, помогают врачу в выборе наиболее эффективной программы лечения. Исследования качества жизни больного играют важную роль в контроле качества оказываемой населению медицинской помощи. Эти исследования − дополнительный инструмент оценки эффективности медицинской помощи на основе мнения главного ее потребителя − больного [5, 6]. В связи с этим широкое использование технологий дистанционного анализа данных в оперативном режиме предполагает наличие E-health, которое часто называют «распределенным здравоохранением», подчеркивая отсутствие принципиального значения места нахождения пациента и врача.

Основными направлениями здравоохранения, на которые нацелено E-health, являются:

- оценка состояния пациента и ее динамики на основе оперативного доступа ко всей информации о пациенте:
- слежение за состоянием пациента на дому;
- дистанционные консультации, консилиумы;
- удаленный доступ пациента к ресурсам лечебно-профилактических учреждений и сервисов, предоставляемым на различных административных уровнях;
- анализ данных на основе оперативного доступа к медико-статистической информации по нозологической, половозрастной и социальной структурам;
- проведение форумов медицинских работников по широкому кругу вопросов, включая совместный анализ и обсуждение медицинской информации [7].

E-health требует согласованных усилий на общегосударственном уровне по целому ряду проблем:

- нормативно-правовое обеспечение;
- информационно-коммуникационная инфраструктура;
- единая система идентификации пациента;
- разработка и применение международных стандартов структуры медицинских документов и протоколов обмена ими;
- единые принципы хранения информации [8].

Отношения между пациентами и больницами традиционно были случайными, т.е. люди посещали медицинские учреждения только тогда, когда они болели, и прекращали их посещать, как только выздоравливали. Сегодня акцент сменяется на действия предупредительного характера − профилактику состояния здоровья, чтобы предотвратить болезнь и сохранить в старости хорошее здоровье [9]. Это так называемая «Медицина 4 P»: Predictive, Personalized, Preemptive and Participatory − Прогнозирование, Профилактика, Участие и Персонализация [10]. Медицинские службы предоставляют ряд услуг через

Интернет и прочие современные каналы связи − интерактивное цифровое телевидение, центры обработки вызовов и общественные киоски. В этой связи получают распространение специальные средства, в частности, электронное назначение лекарства, электронное лечение и доступ к медицинской информации через электронные медицинские карточки. Предоставление услуг в онлайновом режиме дает возможность пациентам взаимодействовать с медицинскими службами в любое время, через любой канал связи на свой выбор. В условиях развития электронной медицины, широкого внедрения компьютерных технологий обработки персональных медицинских данных и трансграничного обмена последними требуется комплексный инновационный подход к разработке правовых, организационных и технологических гарантий защиты медицинской информации, в том числе составляющей врачебную тайну, от несанкционированного доступа [11].

Защита конфиденциальности данных

Вопросы обеспечения конфиденциальности медицинских персональных данных являются предметом пристального внимания во всех странах, вступивших на путь электронного здравоохранения. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, является при этом неукоснительным условием. Персональные данные − это любая информация, относящаяся к физическому лицу, в том числе фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, образ жизни и другая информация. Следить за всеми деталями и решать сложные проблемы со здоровьем, при этом предоставлять пользователям возможность выбирать, какие именно данные они готовы предоставить, а какие − нет. Кроме того, такие данные не всегда можно сделать анонимными. Трудно работать с персональными данными и находить нужную информацию, которая постоянно обновляется и которой можно на 100% доверять. Анализ персональных данных позволяет выявить влияние различных причин на заболеваемость и определить факторы риска в динамике. Наличие фактора риска свидетельствует о повышенной вероятности развития того или иного неблагоприятного события, а его величина — об уровне этой вероятности. Появление различных видов мобильных приложений помогает пациенту осуществлять диагностику и облегчает процесс самостоятельного лечения или лечения с помощью удаленного консультанта.

Частота получения информации, сокращение периода времени от запроса до получения результата дают лучшие результаты, а именно: качество, достоверность, простоту, наглядность, полноту информации. Слежение за состоянием пациентов на дому уменьшает число посещений их медицинскими работниками, и, как следствие, снижаются расходы. Дистанционная оценка динамики состояния пациента на дому предполагает широкий диапазон решаемых задач − от мониторинга физиологических параметров до психотерапевтической помощи разным категориям пациентов (лежачие больные, престарелые, инвалиды, беременные женщины и др.).

Данные от интеллектуальных устройств позволяют в режиме реального времени проводить мониторинг хронических заболеваний, оптимизировать дозировку препаратов и улучшать результаты лечения пациентов. С помощью специальной аппаратуры, которая передает данные электрокардиограммы врачу, пациент, перенесший инсульт или травму головного мозга, может получать круглосуточные консультации и сеансы тестирования на дому. Реагирование на изменения важнее следования плану. Это позволяет оценивать больного в данный момент и делать сравнительную оценку влияния различных медицинских препаратов. Они позволяют улавливать изменения у больного, произошедшие за короткий промежуток времени − 2−4 мин. Применяются они и для оценки

эффективности схем лечения конкретного заболевания. Например при бронхиальной астме, для больных с острым инфарктом миокарда и т.д. Для каждого можно прокорректировать норму препарата и в дальнейшем проводить сравнение с ней. При лечении определяется не тяжесть течения болезни, а то, как пациент ее переносит. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, публикует в соответствующей информационно-телекоммуникационной сети документы, определяющие политику безопасности в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных. Например, в местном госпитале хранится история болезни. Но если в другой стране попасть в аварию, то врачу скорой помощи будет очень важна информация о хронических болезнях или аллергии на лекарства. Легкий и быстрый поиск с автоматическими подсказками таких данных поможет оказать квалифицированную помощь. Конфиденциальность данных означает, что данные, принадлежащие отдельному лицу, никогда никому не будут раскрыты [12]. Потенциальные угрозы конфиденциальности и информационной безопасности персональных медицинских данных связаны с опасностью нецелевого использования последних. Еще одна серьезная угроза безопасности персональных медицинских данных появилась после широкой доступности генетической информации, однозначно указывающей на конкретного пациента. Поскольку эту информацию практически невозможно анонимизировать, а деидентифицированные геномные данные легко восстановить, то в этом случае вопросы конфиденциальности должны быть решены на законодательном уровне. Позволят ли люди компаниям обрабатывать их персональные данные и вообще всю поступающую от клиентов информацию? Информация предоставляется бесплатно, потом анализируется, обрабатывается компьютером, производится новый продукт, который затем снова продается людям. Вопрос в том, корректно ли использовать таким образом «собственность» клиента [13–15]. Больные не догадываются, что данные о них и их действиях могут быть повторно использованы для других целей. Коммуникация избегает социального контроля, и возникает угроза негативного влияния на человека. На основе оценок Американской ассоциации управления информацией о здоровье на рис.1 дается диаграмма наиболее распространенных причин крупномасштабных утечек данных о здоровье. Это кража (55%), несанкционированный доступ (20%), потеря информации (11%), взлом (6%), неправильное использование (5%) и неизвестные другие причины (3%).

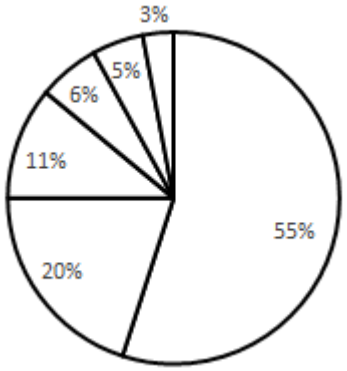

Рис 1. Утечки персональных данных [16]

Безопасность данных и конфиденциальность стали серьезной проблемой. Конфиденциальные сырые данные, хранящиеся и используемые, являются основным препятствием для внедрения различных методик, таких как сбор, систематизация, накопление, хранение биометрических данных. Анализ современной научной литературы позволил выделить следующие меры, такие как защита паролем, шифрование данных, разграничение прав доступа, а также защищенные виртуальные сети. Во многих случаях

этих средств оказывается недостаточно, и тогда используются разнообразные методы защиты, начиная от проектирования систем управления базами данных со встроенными механизмами защиты и заканчивая интеграцией последних со специальными программными продуктами по защите информации [17, 18]. Эти сложности вызывают ряд следующих проблем:

1. Администраторам баз данных трудно правильно определить права доступа, что порождает ошибки.

2. Другому администратору базы данных более сложно впоследствии поддерживать ограничения доступа.

Существует повышенная возможность непредвиденных побочных эффектов, когда сложные права интерпретируются системой.

Принимаются дополнительные меры для вычисления и устранения неработоспособности во время выполнения, когда необходимо проверить привилегии для данного запроса [19, 20].

Техники и инструменты Redis кэш

Кэширование сегодня является неотъемлемой частью любого веб-проекта. Веб-приложения не могут мгновенно реагировать на воздействия пользователя, так как требуется время для обмена данными с серверами этих приложений, а также необходимо сделать некоторые вычисления перед отправкой ответа. Сюда входят и время, необходимое для передачи данных от сервера клиенту и поиска нужных данных на диске, и сетевые задержки, и обработка очередей запросов, и механизмы регулирования полосы пропускания сетей, и многое другое. Если учесть, что все это может происходить на множестве компьютеров, находящихся между клиентом и сервером, то можно говорить о том, что все эти задержки способны серьезно увеличить время, необходимое для прихода запроса на сервер и получения клиентом ответа.

Правильно настроенная система кэширования способна значительно улучшить общую производительность сервера. Кэши сокращают задержки, неизбежно возникающие при передаче данных по сети, помогают экономить сетевой трафик и, в результате, уменьшают время, необходимое для того, чтобы браузер вывел запрошенную у сервера веб-страницу. Запросы к базам данных могут быть медленными и требовать серьезных системных ресурсов для формирования ответа. Если запросы повторяются, кэширование их средствами базы данных поможет уменьшить время отклика. Кэширование полезно в ситуациях, когда несколько компьютеров работают с базой данных, выполняя одинаковые запросы. Большинство серверов баз данных по умолчанию настроено с учетом оптимальных параметров кэширования.

Однако существует множество настроек, которые могут быть модифицированы для того, чтобы подсистема баз данных лучше соответствовала особенностям конкретного приложения. Ответы веб-сервера кэшируются в оперативной памяти. Кэш-приложение может храниться либо локально, в памяти, либо на специальном кэширующем сервере. Redis − это разновидность кэширования, применяемая для оптимизации работы с ресурсоемкими функциями.

Redis − *remote dictionary server* − хранилище объектов в памяти − довольно простой и быстрый способ кэширования данных [21]. Преимущество кэширования данных в веб-приложениях с использованием отдельного кэширующего сервиса Redis в том, что данные поступают из разных источников. Один раз сгенерированный код хранится в оперативной памяти, и при каждом обращении вместо того, чтобы генерировать все заново, он выдает копию (кэш), хранящуюся в оперативной памяти. Главным преимуществом является то, что это простой кэш с простой структурой, а также то, что запрос занимает не больше 10 мс.

Программное обеспечение, предназначенное для кэширования данных в оперативной памяти Redis, обеспечивает сервис по хранению значений, ассоциированных с ключами. Доступ к кэшу мы получаем через простой сетевой протокол, клиентом может выступать программа, написанная на произвольном языке программирования. Это сетевое журнальное хранилище данных типа «ключ – значение» с открытым исходным кодом, ориентированное на скоростную обработку данных [22]. Ключ – это то, чем мы помечаем части информации. Значение – это данные, ассоциированные с ключом. Redis сохраняет снимки базы данных на диске в зависимости от того, сколько ключей было изменено. Настройка процесса идет таким образом, что если X – количество изменившихся ключей, то базу данных нужно сохранять каждые Y секунд. По умолчанию Redis сохраняет базу с интервалами от 60 секунд, если 1000 или более ключей изменились, до 15 минут, если изменились хотя бы 9 ключей. Кроме того, Redis может быть запущен в режиме дозаписи (*append mode*). Каждый раз, когда ключ меняется, на диске дописывается запись в файле, открытом в режиме дозаписи (новые записи добавляются в конец файла) [23]. Redis-сервис для кэширования данных в оперативной памяти обладает высокой производительностью. В общем случае кэширование выглядит следующим образом: если в результате запроса требуется получить данные какой-то выборки, то обращаются к быстрому серверу Redis (*get*-запрос) и соответствующий ключ будет обнаружен. В противном случае идет обращение к базе данных. Полученный результат сразу же записывается в Redis в качестве кэша (*set*-запрос). При этом для ключа задается максимальное время жизни (срок годности). Операциями являются: получить значение указанного ключа (*get*), установить значение ключа (*set)* и удалить ключ (*del).*

Рассмотрим концепцию Redis для реализации определенных функций. Redis-кэш является хорошим выбором для приложений, требующих быстрого просмотра данных, помогает корректировать сведения о состоянии пациентов в соответствии с показаниями приборов, меняющиеся каждую минуту:

1. Персональная информация о состоянии пациента отображается как запрос на вход, затем она автоматически перенаправляется в Redis.

2. После обработки в Redis получаем результат запроса − рекомендации для пациента. Если врачу необходима дополнительная информация для диагностики, то делается еще запрос в Redis. В этом случае принимается объединение этих множеств и пользователь получает требуемые данные.

3. Вся необходимая информация кэшируется в течение определенного, заранее заданного короткого периода времени (в нашем коде это 1 минута).

4. После решения поставленной задачи персональная информация исчезает и через 1 минуту появляются обновленные данные.

Преимущества использования концепции Redis в медицинских приложениях заключаются в том, что необходимая информация кэшируется гораздо быстрее, чем работа с MySQL.

Ниже представлен код:

```
// Save patient info for (TTL)1 minute
string patientAsString = JsonConvert.SerializeObject(firstPatient);
cache.StringSet("patient-id-" + firstPatient.Id, patientAsString,
    new TimeSpan(0 /* hours */, 1 /* minutes */, 0 /* seconds */));
// Read patient info
Patient patient1 = JsonConvert.DeserializeObject<Patient>(patient1AsString).
```

Запись с указанным TTL (Time to live) может быть удалена по истечении заданного времени. Все записи TTL в пределах 60 секунд и устаревшие данные гарантированно не придерживаются дольше минуты**.**

Было бы желательно иметь более простое решение, которое легче настраивать, поддерживать и надежно выполнять. В настоящей статье основное внимание уделяется ограничению времени доступа к данным. Во всех этих случаях лучшая защита данных − это «осуществлять политику и процедуры», касающиеся окончательной ликвидации электронной информации о пациентах. Поэтому наилучшими методами являются, по нашему мнению, обеспечение корректного удаления и невозможность повторного восстановления, в том числе из резервных копий. Это осуществляется при помощи управляемой службы кэша Redis, которая позволяет привязывать к значению срок его действия. Технологии доступа к данным постоянно совершенствуются. Концепция Redis этому подтверждение. Здесь решается специфический класс задач, которые в то же время являются достаточно универсальными. Традиционные дисковые базы данных для большинства операций требуют циклического обращения к диску. Хранилища данных в памяти, такие как Redis, свободны от этого ограничения, а потому могут выполнять в единицу времени на порядок больше операций и обеспечивают лучшее время отклика. Благодаря своей скорости и удобству веб-технология Redis часто используется для игровых и рекламных приложений, финансовых сервисов, приложений для сферы здравоохранения.

Redis отличается своей исключительной скоростью, что делает его оптимальным выбором для определенного класса задач:

1. Постановка диагнозов на основе полученных в режиме онлайн данных с участием специалистов. Все больше пациентов приобретают носимую электронику, а мобильные девайсы постоянно развиваются и наращивают функционал (уровень сахара, частота сердечных сокращений, давление, активность, диагностические анализы и прочее). Существуют гаджеты для раннего диагностирования заболеваний и повседневного контроля здоровья организма. Больные диабетом могут использовать различные устройства с подключением к сети, которые помогли бы пациентам периодически отправлять такие данные, как уровень сахара в крови. Таким образом, информация, поступающая в режиме реального времени, отслеживается в соответствии со сложившимся состоянием пациента, принимаются решения, а затем промежуточные данные очищаются.

2. Медицинская компания имеет веб-сайт, что дает возможность клиентам общаться в интерактивном режиме через компьютер. Пациенты могут безопасно вводить на сайте свои реквизиты (например адреса). Клиенты получают преимущества от улучшенных интерактивных возможностей сайта, например, могут безопасно сообщать свои административные реквизиты через Интернет. В результате людям предоставляется возможность быстрее и легче находить нужную информацию о назначениях врачей, а также быть уверенными в том, что конфиденциальная информация будет удалена.

3. Обработка телефонных звонков в службу скорой помощи. По истечении времени персональные данные удаляются.

4. Ключевыми аспектами при обмене медицинской информацией в виртуальных сообществах являются безопасность и надежность медицинской информации. Способы общения контролируются и персональная переписка имеет временный характер.

5. Применение в скриннинге − при массовом обследовании населения и выявление лиц с заболеваниями, для которых необходима разработка персональных лекарств. В этом случае результаты обследований пациентов изымаются.

6. Здоровым людям могут встраиваться USB-порты для диагностики. Анализы делаются дома самостоятельно, клиническая картина сохраняется в облаке, а общение с врачом происходит дистанционно – через Интернет. Данные пациентов, измеряемые в домашних условиях, могут своевременно удаляться.

В больших высокозагруженных проектах для снижения нагрузки на базы данных целесообразны инструменты кэширования Redis. Применение управляемого Redis-кэша обеспечивает своевременное удаление конфиденциальной информации, тогда как

аппаратные, программные и другие решения не всегда гарантируют надежность и безопасность персональных данных в компьютерных сетях.

Заключение

Анализ персональных данных в динамике позволяет выявить влияние различных причин на заболеваемость и смертность населения, определить факторы риска. Обязательным условием предоставления и поручения обработки персональных данных другому лицу является обязанность сторон по соблюдению конфиденциальности и обеспечению безопасности персональных данных при их обработке. В статье изложен метод защиты от неправомерных действий в отношении персональных данных, позволяющий своевременно уничтожить последние. Приведен код, который обеспечивает время отклика на уровне долей секунд и дает возможность приложениям, работающим в режиме реального времени, выполнять миллионы запросов в секунду. Резюмируя выше изложенное, можно сделать заключение о том, что система защиты персональных данных на базе Redis-кэша позволяет ускорить выполнение запросов и улучшить возможности масштабирования, снижая нагрузку на основную базу данных. Такие компании, как Redis Labs, Amazon, Microsoft Azure и другие, предлагают множество полезных инструментов и услуг Redis. Веб-технологии Redis успешно могут быть использованы в мобильных и интернет-приложениях, а также в приложениях для электронного здравоохранения.

Литература

1. Duplaga M. The Impact of Information Technology on Quality of Healthcare Services Computational Science - ICCS 2004, vol. 3039. Springer, Berlin, Heidelberg, pp.1118–1125.
2. Мурадова Г.И. Большие данные в системе здравоохранения // Проблемы информационных технологий, Баку, 2016, №2, pp.98–105.
3. Fekri O., Macarayan E., Klazinga N. Health system performance assessment in the WHO European Region: which domains and indicators have been used by Member States for its measurement? Copenhagen: WHO Regional Office for Europe; 2018 (Health Evidence Network synthesis report 55), pp.4-6.
4. Global strategy and plan of action on public health, innovation and intellectual property ISBN: 978 92 4 150290 0 World Health Organization 2011 www.who.int
5. Wilson I., Cleary P. Linking Clinical Variables With Health-Related Quality of LifeA Conceptual Model of Patient Outcomes 1995,vol.27,N1, pp.59-65.
6. Spil T., LeRouge C.,Trimmer K.,Wiggins C. Back to the future of IT adoption and evaluation in healthcare International Journal of Healthcare Technology and Management ,2011,vol.12, Issue 1, pp.85–109.
7. Усанов В. Федеральный закон «О персональных данных», Издательство: Эксмо-Пресс, 2018, с.12–20.
8. Keeping Promises, Measuring Results. Commission on Information and Accountability for Women's and Children's Health. Geneva. World Health Organization. 2011, p.12.
9. Sibona C., Walczak S., Brickey J., Parthasarathy M.Patient perceptions of electronic medical records: physician satisfaction, portability, security and quality of care, International Journal of Healthcare Technology and Management 2011 12:1, pp.62–84.
10. Bradley W.,Golding S. Globalization of P4 Medicine: Predictive, Personalized, Preemptive, and ParticipatoryRadiology, 2011,vol. 287 No. 2, pp.571–582.
11. Мамедова М.Г. Информационная безопасность персональных медицинских данных в электронной среде // Проблемы информационных технологий, Баку, 2015, №2, с.6–30.
12. Кучин И.Ю. «Защита конфиденциальности персональных данных с помощью обезличивания». Вестник Астраханского государственного технического

университета. Серия: Управление, вычислительная техника и информатика, 2010, no. 2, pp.158–162.
13. Предиктивная медицина и Большие Данные. http://apptractor.ru/info/articles/lektsiya-lorensa-dzheykobsa-prediktivnaya-meditsina-i- bolshie-dannyie.html
14. Magnusson R.S. The Changing Legal and Conceptual Shape of Health Care Privacy// Journal of Law, Medicine & Ethics, 2004, vol.32, pp.685–689.
15. Koufi, V., Malamateniou, F., & Vassilacopoulos, G. Towards Clinical and Operational Efficiency through Healthcare Process Analytics. International Journal of Big Data and Analytics in Healthcare (IJBDAH), 2016,1(1), pp.1–17.
16. Гилмер Э. Конфиденциальность и безопасность данных пациентов в облаке https://www.ibm.com/developerworks/ru/library/cl-hipaa/index.html
17. Stephen S. Yau, Ho G. An, and Arun Balaji Buduru. 2012. An Approach to Data Confidentiality Protection in Cloud Environments, International Journal of Web Services Research 2012, vol 9 Issue 3, pp.67–83.
18. Полтавцева М.А., Хабаров А.Р. «Безопасность баз данных: проблемы и перспективы». Программные продукты и системы, 2016, no. 3 (115), pp.36–41.
19. Omran E., Grandison T., Nelson D., Bokma A. A Comparative Analysis of Chain-Based Access Control and Role-Based Access Control in the Healthcare Domain, International Journal of Information Security and Privacy (IJISP), 2013, 7(3), pp.36–52.
20. Mayuri R. Gawande et al, Analysis of Data Confidentiality Techniques in Cloud Computing, International Journal of Computer Science and Mobile Computing, vol.3 Issue.3, March-2014, pp.169–175.
21. Carlson J., Redis in Action, ManningBooks, 2013, pp.89–110.
22. https://azure.microsoft.com/en-gb/services/cache/
23. Seguin K. The Little Redis Book,2012 http://openmymind.net/redis.pdf

UOT 004.056

Muradova Gülarə İ.
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
gulara_m@hotmail.com

Fərdi tibbi məlumatların təhlükəsizliyi üçün REDIS konsepsiyası

İnformasiya sistemində emalı zamanı fərdi tibbi məlumatların təhlükəsizliyi aktual təhdidləri neytrallaşdıran fərdi verilənlərin müdafiəsi sistemi vasitəsilə həyata keçirilir Redis texnikası və alətləri onlayn rejimində daxil olan və sürətlə dəyişən verilənlərin sürət emalına yönəlmişdir. Redis sisteminin tətbiqi gizli məlumata nəzarət olunmayan girişin qarşısını alır.

***Açar sözlər*:** *Elektron tibb, informasiyanın qorunması, təhlükəsizlik, məxfilik, fərdi tibbi məlumatlar, verilənlər bazaları, keşin idarə olunması*.

Gulara I. Muradova
Azerbaijan Technical University, Baku, Azerbaijan
gulara_m@hotmail.com

Security of personal medical data for the REDIS concept

During processing personnel data, security is provided by personnel data protection system which neutralise actual treats. In the article, techniques and tools of Redis are oriented to speedy data processing for online coming and rapidly changing personal medical data. Application of Redis technology eliminates uncontrolled access to confidential information.

Keywords: *E-health, protection of information, security, confidentiality, personnel medical data, data base, cache management.*