ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ТЕЛЕМЕДИЦИНЕ

В настоящее время активно создаются виртуальные инфраструктуры здравоохранения, объединяющие на базе единого информационного пространства (ЕИП) все составляющие элементы системы охраны здоровья населения. Внедрение информационно-коммуникационных технологий обеспечивает формирование каналов устойчивых коммуникаций между специалистами разных лечебно-профилактических учреждений (ЛПУ), удаленный доступ к медицинским информационным системам (МИС), облегчение и ускорение записи пациентов на прием к врачам.

В России крупные медицинские информационно-аналитические центры развертывают площадки своих центров обработки данных, используя различные платформы виртуализации (например, VMware vSphere), и создают инфраструктуру виртуальных рабочих мест для работников ЛПУ, предоставляя им прямой доступ к МИС. В первую очередь в виртуальную среду переносятся приложения и инфраструктурные сервисы, используемые при обработке биомедицинской информации.

Создаваемые виртуальные инфраструктуры позволяют решить актуальную задачу дистанционного мониторинга состояния здоровья населения. При этом остро стоит вопрос с обеспечением информационной безопасности передаваемых данных.

Проблема защиты данных в системах мониторинга

Развитие микроэлектроники и телекоммуникаций позволяют включить человека в единое информационное пространство системы здра воохранения, независимо от его местоположения. Сделать это можно, например, путём регистрации биосигналов сердечно-сосудистой системы с помощью датчиков, вмонтированных в нательную одежду. Биосигналы должны передаваться по каналам связи в медицинские центры мониторинга и обработки информации (рис. 1), где посредством математических моделей элементов и подсистем организма создаётся виртуальный физиологический образ пациента, описывающий физиологическую деятельность подсистем человека.

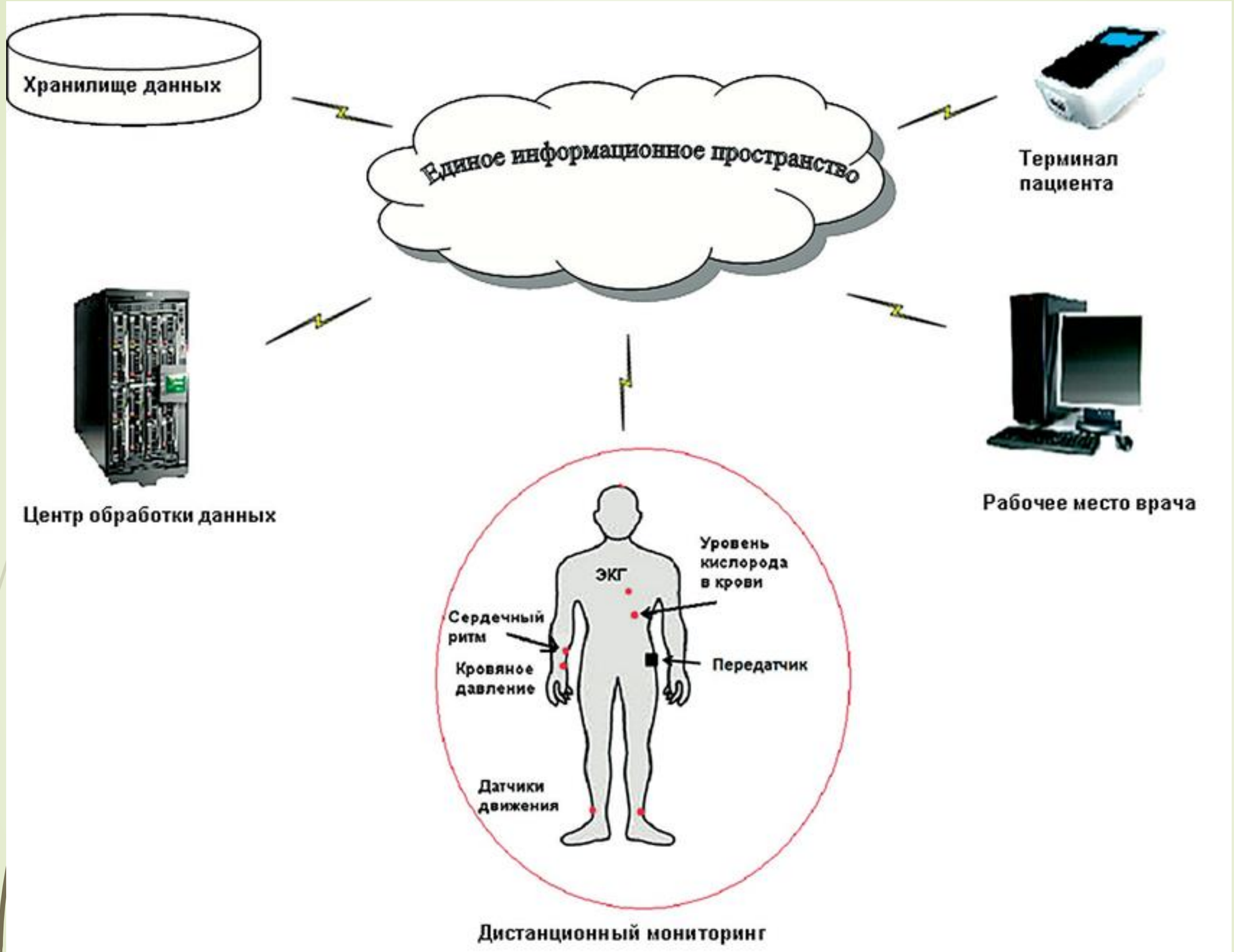

Рис. 1. *Дистанционный мониторинг состояния человека на основе ЕИП*

Хранение, вычисление и визуализация огромного количества данных, собранных системой мониторинга, требует значительных вычислительных ресурсов, предоставляемых виртуальной инфраструктурой с помощью облачных технологий. Датчики могут отправлять данные на облако напрямую, либо через промежуточные базовые станции. Обслуживающий персонал и пользователь могут просматривать собранную медицинскую информацию непосредственно из облака с помощью смартфона или через Интернет в режиме реального времени и принимать решения в соответствии с текущим функциональным состоянием человека (рис. 2).

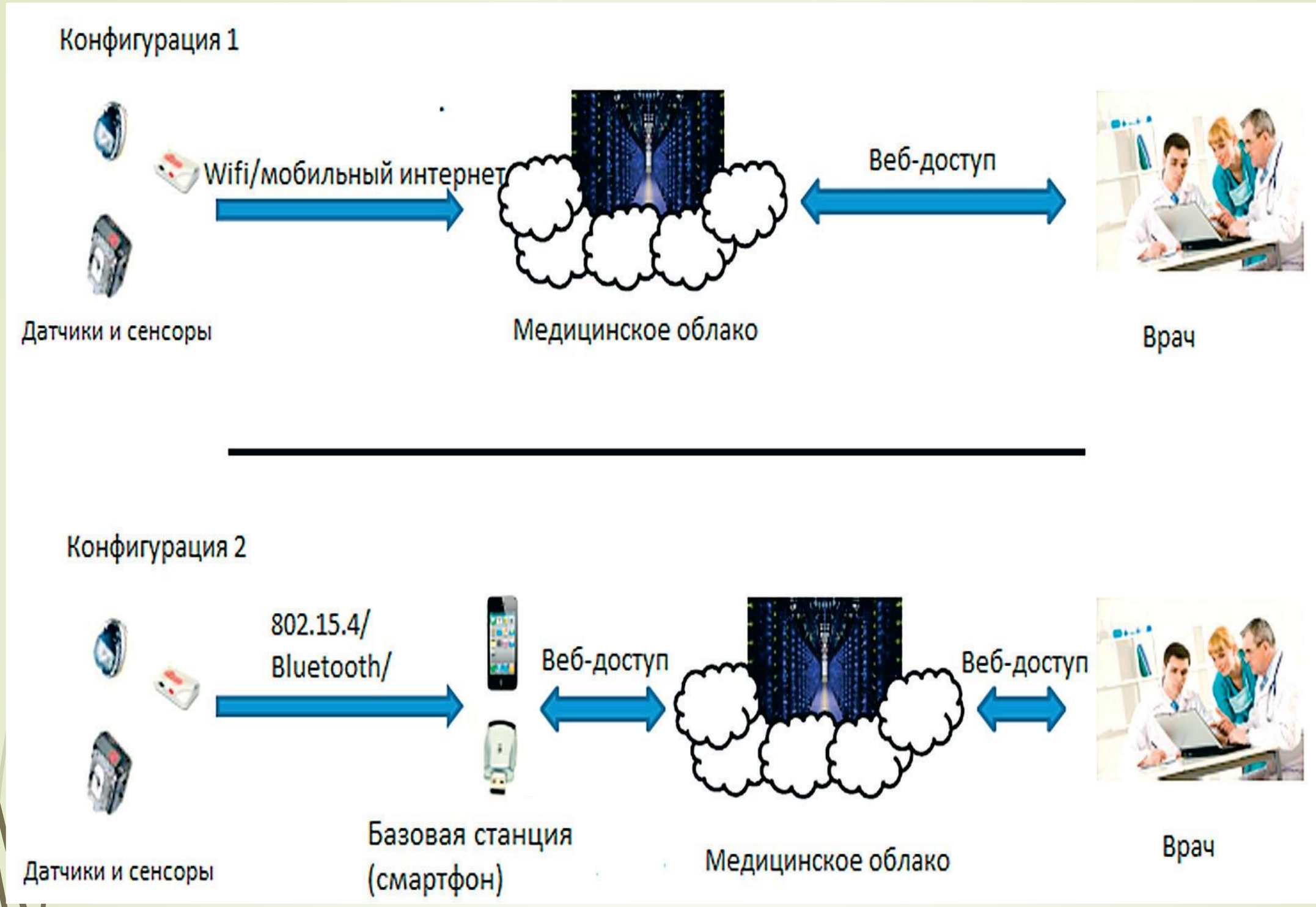

Рис. 2. *Конфигурации мобильной системы дистанционного мониторинга*

Рассмотрим возможные угрозы информационной безопасности применительно ко всем составляющим системы мониторинга:

- датчики: все датчики в системе изначально должны быть надежны, тогда злоумышленник не сможет получить доступ к датчику и остаться незамеченным;
- коммуникации: коммуникационная связь в системе является ненадежной. Злоумышленники могут подслушивать все виды разговоров и могут исказить сигналы. Однако не должно быть никаких помех и отказов в обслуживании и взаимодействии авторизованных устройств;

- базовая станция: даже если злоумышленник не может физически воздействовать на датчик, он может повлиять на базовую станцию. Например, если базовая станция установлена на смартфоне, то злоумышленники могут взломать приложение на нем;
- облако: предполагается, что медицинское облако является надежным. Обслуживающий персонал может получить доступ к информации о пациенте только после успешной авторизации;
- обслуживающий персонал или пациент: предполагается, что они не откроют доступ к информации под влиянием злоумышленников;

- тело пациента: предполагается, что злоумышленник может иметь физический контакт с пользователем мобильной системы (например, пожать руку пациента), поэтому электрические сигналы пользователя могут быть искажены сигналами злоумышленника.
Однако злоумышленник не может внедрить вредоносные датчики в систему.
Кроме того, предполагается, что информация о состоянии здоровья пациента в прошлом неизвестна злоумышленнику.

Традиционные подходы к обеспечению безопасности систем здравоохранения

С точки зрения защиты информации наиболее уязвимым является канал связи «датчик-облако». Часто используемый в таких случаях протокол защиты *E2E (end-to-end)* работает путем задания и последующего распределения криптографических ключей между датчиками и облаком. Этот протокол обеспечивает скрытность и целостность данных. В дальнейшем ключ также можно использовать для взаимной проверки подлинности сообщения. Основная проблема здесь заключается в возможности конфиденциального распределения (доставки) ключей их пользователям. Для пациента эта процедура должна быть понятна и не обременительна. В наиболее благоприятном случае пациент вообще не должен заботиться о ключе.

Традиционные подходы к обеспечению безопасности систем здравоохранения основываются на асимметричных криптосистемах.
Асимметричное шифрование использует два разных ключа: один для шифрования (который также называется открытым), другой для дешифрования (называется закрытым или секретным). Такой подход является достаточно надежным для обеспечения конфиденциальности и целостности передаваемых данных, но оказывается дорогим для регулярного обмена данными в системе реального времени, поскольку требует больших затрат ресурсов и времени.

Кроме того, асимметричная криптография плохо противостоит некоторым видам атак и для ее использования необходимы дополнительные механизмы аутентификации. Поэтому в системах дистанционного мониторинга нецелесообразно использовать асимметричное шифрование. Альтернативным является подход к защите передаваемых данных путем создания парных симметричных ключей для датчика и приемника.

В симметричной криптосистеме для шифрования и дешифрования применяется один и тот же криптографический ключ, который должен сохраняться в секрете обеими сторонами. В результате алгоритмы с закрытым ключом работают на три порядка быстрее алгоритмов с открытым ключом, что очень важно для телемедицинских систем реального времени. Однако недостатком симметричных шифров является невозможность их использования для подтверждения авторства, так как ключ известен каждой стороне.

Для повышения надежности симметричных криптографических ключей и уменьшения нагрузки на пациента в ряде работ предложено использовать регистрируемые датчиками биосигналы, которые отражают физиологические особенности пациента и могут использоваться для сокрытия информации.

Отмеченные свойства биосигналов позволяют использовать их для создания ключей.

Необходимая информация (морфологические особенности биосигналов конкретного человека) извлекается при первой регистрации сигналов.