УДК 004.056 DOI: 10.18698/0236-3933-2020-4-42-57

ЗАЩИТА ДАННЫХ ПРИ ДИСТАНЦИОННОМ МОНИТОРИНГЕ СОСТОЯНИЯ ЧЕЛОВЕКА

Т.И. Булдакова buldakova@bmstu.ru
Д.А. Миков mikov@bmstu.ru
А.В. Соколова aksinya.sokolova@yandex.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Рассмотрены телемедицинские системы мониторинга состояния здоровья человека и способы защиты передаваемых данных. Состояние здоровья человека оценивается с помощью биосигналов, которые регистрируются датчиками и передаются в облачную медицинскую информационную систему. На основе полученных данных принимается решение о состоянии человека. Поскольку система мониторинга работает с важной информацией ограниченного доступа, она должна быть надежно защищена. Выделены возможные угрозы информационной безопасности для всех компонентов телемедицинской системы. Проанализированы различные подходы к защите передаваемых данных в системах дистанционного мониторинга. Отмечено, что существующие методы являются недостаточными и требуются дополнительные способы защиты передаваемых данных. Предложено оценку защищенности данных выполнять с помощью методики управления информационными рисками

Ключевые слова

Защита информации, мониторинг, электронная медицинская карта, биосигналы, медицинские информационные системы

Поступила 29.10.2019
Принята 20.07.2020

Введение. В настоящее время в здравоохранении разных стран реализуются проекты по переходу на использование электронных медицинских карт (ЭМК), обеспечивающих обмен информацией между различными медицинскими организациями. К числу преимуществ использования ЭМК относится обеспечение пациентов и медицинских работников полной и точной медицинской информацией [1, 2]. Наиболее активно этот процесс реализуется в США и Германии. Например, в Германии создана Ассоциация ЭМК, включающая в себя основные больницы и клиники, а также локальные ассоциации и региональные сети здравоохранения [3]. Данный процесс облегчает переход к персонализированному здравоохранению и обес-

печивает доступность информации о состоянии пациента независимо от его нахождения [4]. Наиболее актуален такой подход для телемедицинских систем динамического наблюдения за состоянием пожилых людей и пациентов, страдающих тяжелыми хроническими заболеваниями [5, 6].

Цель настоящей работы — анализ особенностей дистанционного мониторинга состояния здоровья человека для выбора возможных способов защиты передаваемой информации.

Особенности телемедицинских систем мониторинга состояния здоровья человека. В общем случае в процессе мониторинга должны контролироваться различные факторы, влияющие на общественное здоровье людей. К ним следует отнести характер демографических процессов, уровень экономического развития, доходы социальных групп населения, ресурсы здравоохранения и качество деятельности социальных институтов здравоохранения, урбанизацию, динамику алкоголизации и наркотизации населения, стресс и характер производственной деятельности населения, условия труда, быта и питания, уровень образования и культуры населения.

Существует два основных способа измерения подобной информации. Первый способ наиболее распространен при диспансерных обследованиях населения. Он состоит в непосредственном измерении значимых показателей функций и адаптационных резервов организма человека, сравнении их с нормативами, субъективном оценочном интегрировании и оценке в виде «здоров», «практически здоров», «относится к группе риска», «нуждается в наблюдении и коррекции». Обычно по результатам такого подхода формируются статистические данные об общественном здоровье. Второй способ состоит в индивидуальном наблюдении и фиксации врачом физического состояния человека путем ввода медицинской информации о нем в электронную историю болезни.

Дистанционный мониторинг здоровья позволяет в режиме реального времени контролировать здоровье удаленных пациентов, находящихся вне медицинского учреждения. В телемедицинских системах при дистанционном мониторинге реализуются информационные процессы сбора, передачи, хранения и обработки данных, необходимых для формирования и принятия решений о состоянии здоровья человека (рис. 1).

Оценка состояния человека в подобных системах может выполняться различными способами: на основе анализа контролируемых параметров (норма–патология); под наблюдением лечащего врача; автоматизированно, по вычислительной модели человека (так называемой виртуальной физиологии), описывающей физиологическую активность подсистем человека [7–9]. При этом независимо от применяемого способа источника-

ми первичной информации выступают различные датчики, позволяющие регистрировать биосигналы (электрическую активность и сокращения сердца, пульсовой сигнал, электрическую активность мозга, функцию внешнего дыхания и т. д.).

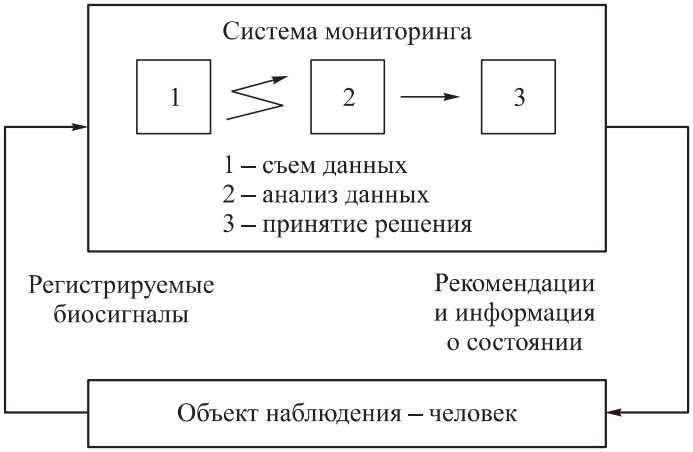

Рис. 1. Информационные процессы при мониторинге

В состав современной телемедицинской системы входят мощный компьютер, который легко сопрягается с разнообразным медицинским оборудованием, а также средства дальней и ближней беспроводной связи, средства IP-вещания и видеоконференции. При создании систем дистанционного мониторинга датчики биосигналов могут встраиваться в нательную одежду, мобильные телефоны, различные аксессуары [10, 11]. Зарегистрированные биосигналы передаются по каналам связи в медицинские центры мониторинга и обработки данных, где осуществляется углубленная оценка функционального состояния здоровья человека (рис. 2).

Одной из главных задач при создании телемедицинской системы является создание надежной и хорошо функционирующей системы для хранения информации о состоянии здоровья пациента. Информация, содержащаяся в ЭМК, должна быть доступна врачу для дистанционного консультирования пациента, а также медицинскому работнику, проводящему врачебные манипуляции, например, в условиях стационара или поликлиники. Обслуживающий персонал клиники, а также другие пользователи, авторизованные в телемедицинской системе, могут просматривать информацию о пациенте непосредственно из облачной медицинской информационной системы в режиме реального времени, а также принимать решения в соответствии с текущим функциональным состоянием человека.

Рис. 2. Компоненты телемедицинской системы

Учитывая возможный доступ, в том числе и несанкционированный, различных специалистов к информации, требуются методы и технологии для защиты персональных данных пациентов.

Проблема защиты данных в системах мониторинга. Решающее значение в системах дистанционного мониторинга имеет обеспечение безопасности личных медицинских данных [12, 13]. В результате анализа модели угроз для подобных систем выявлено, что существует проблема обеспечения информационной безопасности физиологических данных пациентов, передаваемых от датчика в хранилище — медицинскую информационную систему ЭМК (табл. 1). Отметим, что нарушение целостности и конфиденциальности информации, а также кража личных медицинских данных пациента могут привести не только к финансовым потерям, но и к нежелательным социальным последствиям, поскольку они наносят моральный ущерб человеку.

Таблица 1

Возможные угрозы информационной безопасности при мониторинге

Компоненты	Угрозы	Пояснения
Датчики	Доступ злоумышленника к датчику	Необходимо использовать надежные датчики, ограничивающие доступ
Коммуникации	Злоумышленники могут подслушивать все виды разговоров, а также искажать сигналы	Коммуникационная связь в системе ненадежна, необходимо шифровать сигналы
Облачная медицинская информационная система	Возможный доступ к данным в облаке	Только авторизованный врач может получить доступ к информации о пациенте
Медицинский персонал	Передача информации злоумышленнику	Предполагается, что медицинский персонал не откроет доступ к информации под влиянием злоумышленника
Пациент	Передача информации злоумышленнику	Предполагается, что пациент не откроет доступ к информации под влиянием злоумышленника
Тело пациента	Злоумышленник может иметь физический контакт с пациентом (например, пожать ему руку), поэтому биосигналы пациента могут быть искажены сигналами злоумышленника	Надежные датчики не позволяют злоумышленнику искажать сигналы. Кроме того, вся информация о состоянии здоровья пациента в прошлом неизвестна злоумышленнику

Анализ различных подходов к криптографической защите передаваемых данных выполнен в работе [14]. Показано, что традиционные подходы к обеспечению безопасности систем здравоохранения основываются на асимметричных криптосистемах. Асимметричное шифрование использует два разных ключа: для шифрования и дешифрования. Хотя данный подход достаточно надежен для обеспечения конфиденциальности и целостности передаваемых данных, однако он оказывается затратным для регулярного обмена информацией в режиме реального времени, поскольку требует больших затрат времени и ресурсов. Поэтому нецелесообразно использовать асимметричное шифрование в системах дистанционного мониторинга состояния здоровья человека.

Альтернативным подходом к шифрованию передаваемых данных является метод создания парных симметричных ключей для датчика и приемника, т. е. одного закрытого ключа. Такой подход реализуется в симметричных криптосистемах. Алгоритмы с закрытым ключом работают на три порядка быстрее алгоритмов с двумя (открытым и закрытым) ключами, что является определяющим для телемедицинских систем реального времени. Однако недостатком симметричных шифров является невозможность их использования для подтверждения авторства пользователя системы, так как ключ известен всем участникам процесса. Таким образом, в системах дистанционного мониторинга могут потребоваться дополнительные меры защиты передаваемых данных, в том числе для идентификации пациентов [15, 16]. Кроме того, для оценки защищенности данных в телемедицинских системах необходимо постоянно отслеживать уровень информационных рисков — потенциальной возможности искажения информации, а также вырабатывать контрмеры для их снижения, что составляет задачу управления рисками.

Методика управления информационными рисками. В отличие от систем других классов, системы дистанционного мониторинга оказываются более уязвимыми к внешним (несанкционированным) воздействиям на информацию, которые могут носить и целенаправленный характер (рис. 3).

Рис. 3. Процесс управления информационными рисками

Анализ существующих методов и средств управления информационными рисками позволил сформулировать основные проблемы и выделить составляющие управления информационными рисками (рис. 4).

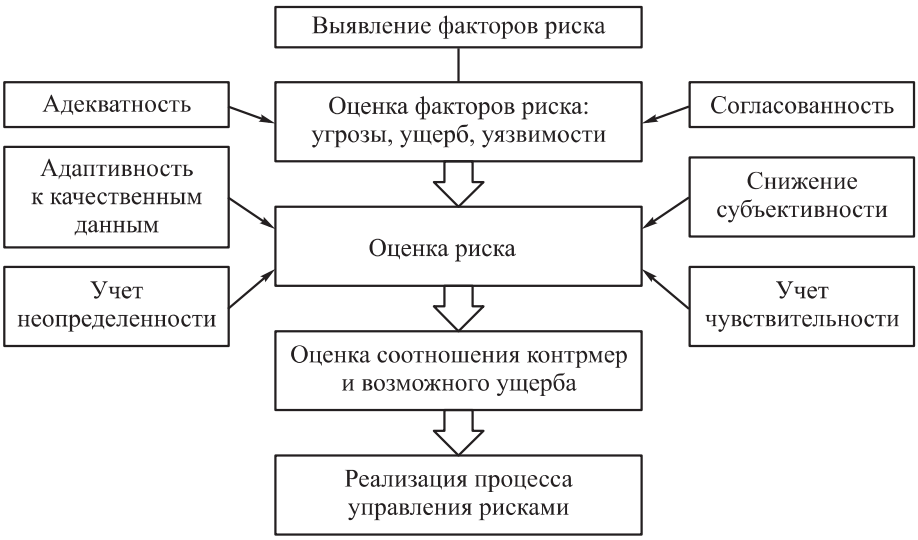

Рис. 4. Этапы управления информационными рисками

Из рис. 4 следует, что методика управления рисками информационной безопасности должна состоять из совокупности методов, используемых на различных этапах процесса и удовлетворяющих следующим показателям эффективности:

– наибольшая согласованность и адекватность оценок факторов риска;

– максимальная адаптивность к качественным данным;

– минимальная субъективность и неопределенность оценки риска;

– учет неодинаковой чувствительности риска к различным факторам.

Практические исследования по созданию наиболее эффективной методики управления информационными рисками позволили сделать вывод [17, 18], что заданные требования достигаются путем комбинации методов структурно-функционального анализа на этапе составления перечня факторов риска, экспертных опросов с последующей математической обработкой на этапе оценки факторов риска, методов нечеткого моделирования на этапе оценки риска, а также методов теории игр на этапе выбора контрмер.

Разработанная методика управления информационными рисками [19] основана на совместном использовании и взаимодействии IDEF0-модели, экспертного опроса, нейронечеткой сети, методов теории игр и позволяет максимально эффективно реализовать составление перечня факторов рис-

ка, их оценку, вычисление уровня риска и выбор контрмер. Исследования показали, что применение предложенной методики управления информационными рисками в телемедицинских системах позволяет снизить на 10…15 % уровень риска.

Апробация методики. Апробация методики управления информационными рисками выполнена для системы дистанционного мониторинга состояния человека (СДМСЧ). Для указанной телемедицинской системы с помощью IDEF0-модели сформирован перечень факторов информационного риска, которые оценены группой экспертов, куда входят аналитик службы безопасности, программист службы автоматизации, группа внедрения и сопровождения программного обеспечения (три эксперта), группа обслуживания и ремонта технических средств (три эксперта), администратор штатных средств и администратор дополнительных средств защиты.

Перечень факторов риска состоит из следующих 14 позиций.

Угрозы:

1) несанкционированный доступ злоумышленника к ресурсам СДМСЧ;

2) нарушение конфиденциальности/целостности данных при передаче с телемедицинских датчиков в облачное хранилище;

3) нарушение доступности/целостности информации, находящейся в облачном хранилище;

4) перегрузка трафика при передаче данных.

Ущерб:

5) телемедицинские датчики пациента;

6) компьютер/смартфон пациента;

7) коммуникации между телемедицинскими датчиками/компьютером/смартфоном пациента и облачным хранилищем;

8) информационные ресурсы СДМСЧ.

Уязвимости:

9) нарушение работоспособности клиентской части при временном отсутствии связи с сервером;

10) отсутствие письменного согласия пациента на сбор и обработку персональных данных;

11) отсутствие распределенной, комплексной политики контроля и разграничения доступа к данным;

12) возможность информационной несовместимости при обмене данными;

13) отсутствие возможности отслеживания действий клиентов в произвольный момент времени;

14) несвоевременная установка обновлений, исправлений клиентских модулей.

Разработанная методика управления информационными рисками включает в себя отсеивание несогласованных экспертных оценок с помощью вычисления коэффициента конкордации по шкалам Марголина и Харрингтона [19]. В результате получена сводная табл. 2 экспертных оценок по шкале от 1 до 10, обеспечивающая требуемый уровень согласованности.

Таблица 2

Сводная таблица экспертных оценок

Номер фактора	Оценки экспертов (пустые ячейки — отсеянные оценки)									
	1	2	3	4	5	6	7	8	9	10
Угрозы										
1		6			7		6	8		6
2	8	8		8		9			8	
3						9	10	9	9	10
4				8	9		9		8	10
Ущерб										
5		3		2			1	3		1
6			6	9			8	9	7	
7	5			1	3		2	1		
8	6	5					6		6	4
Уязвимости										
9	10	8			10		8		10	
10	8		7		6	8				
11	9			8			10		8	10
12	2		2	1	1	5				
13		10		9		8		10		8
14		6	6	7		6	8			

В результате обработки приведенных экспертных оценок факторов риска в соответствии с симплекс-методом [19] получены три входных значения для нейронечеткой системы (ННС): угроза — 8,3 (очень высокая); потенциально возможный ущерб — 6,3 (высокий); уязвимость — 4,3 (средняя).

После подачи этих значений на вход ННС на выходе получен уровень риска — 0,627 (выше среднего), это указывает на то, что система монито-

ринга может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее. Другими словами, полученный уровень риска информационной безопасности отобразил слабую защищенность информационных потоков, поэтому должны быть приняты соответствующие меры по защите данных в СДМСЧ.

Разработанная телемедицинская система, для которой выполнена оценка информационных рисков, представляет собой распределенную сеть серверов, где хранятся пользовательские файлы, внутренняя структура и организация данной сети скрыта. Для обеспечения полноценной работы, а также сохранения врачебной тайны приняты дополнительные меры по защите данных, в частности, особое внимание уделено вопросу разграничения прав доступа [20]. Работа с функционалом системы приходится на веб-приложение, авторизовавшись в котором пользователь открывает весь функционал, предусмотренный для его роли.

Сервис авторизации и проксирования обеспечивает контроль доступа к системе. С помощью сравнения хеш-пароля, полученного от пользователя, и пароля из базы данных определяется будущий ответ системы. Если пароли совпадают, то пользователю открывается доступ к тому функционалу, который предназначается ему, исходя из роли.

Важно разграничить права пользователей, поскольку доступ к определенным документам, файлам и данным для работы в системе не должен принадлежать всем пользователям. Разграничение прав реализуется модулем, который предоставляет пользователям различные права доступа к объектам и осуществляется как по категориям, так и по паролям. Применение категорий пользователей позволяет упростить процедуры назначения прав пользователей за счет применения групповых политик безопасности. В зависимости от роли пользователя ему будет доступен тот или иной функционал системы, например, врач — просмотр и редактирование медицинских карт пациентов, пациент — только просмотр собственной медицинской карты (рис. 5).

В результате повторной оценки факторов риска с учетом внедрения выбранных контрмер получены три входных значения для оценки остаточного риска с помощью ННС: угроза — 1,68 (очень низкая); потенциально возможный ущерб — 1,7 (очень низкий); уязвимость — 0,68 (очень низкая).

После подачи новых значений на вход ННС на выходе получен уровень остаточного риска — 0,165 (очень низкий), что означает высокую степень защиты данных. Тем самым продемонстрирована эффективность предложенной методики управления информационными рисками.

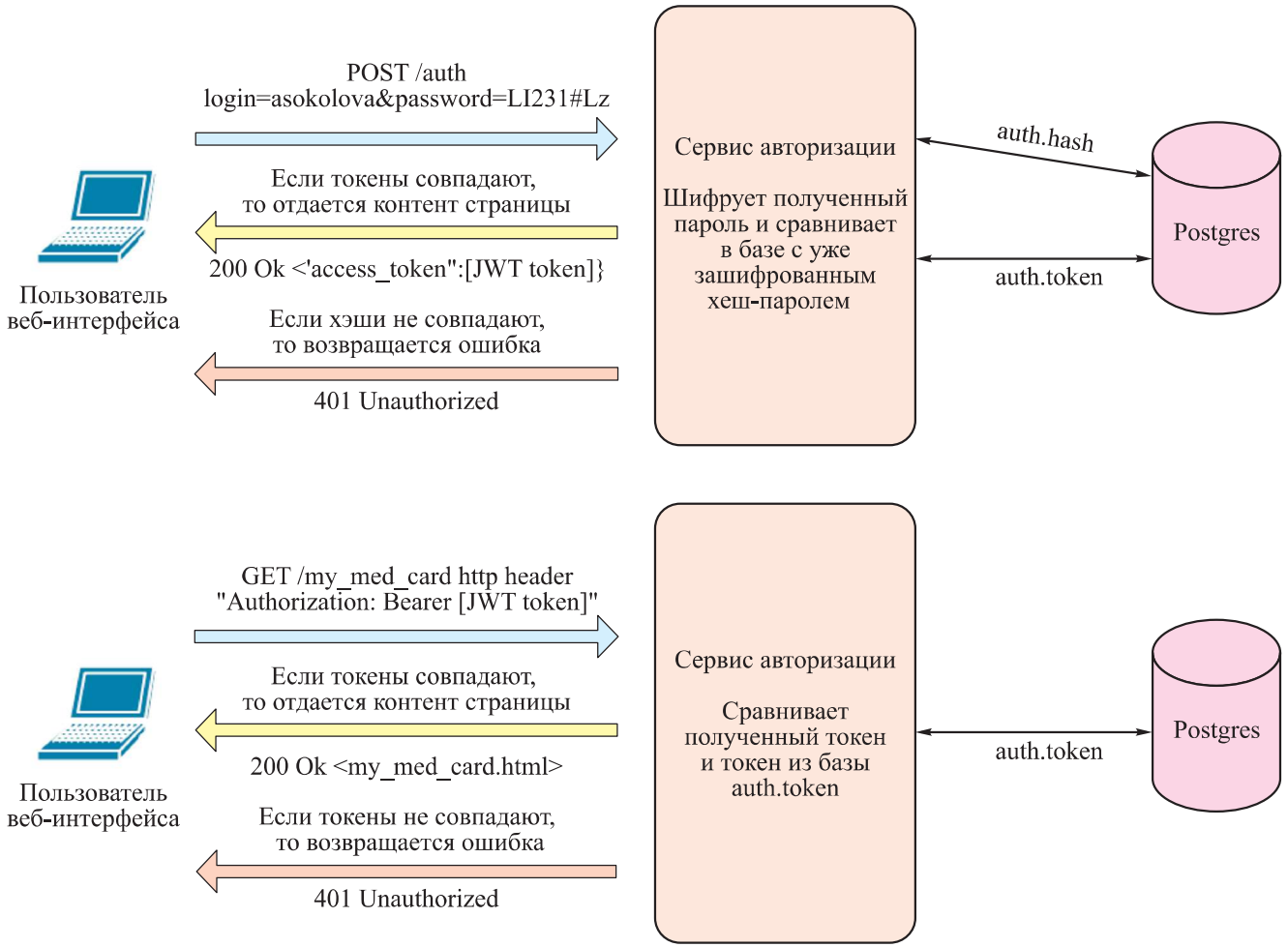

Рис. 5. Схема алгоритма разграничения прав доступа

Заключение. Рассмотрены особенности телемедицинских систем мониторинга состояния здоровья человека и отмечена актуальность проблемы обеспечения информационной безопасности. Показано, что создание технологии защиты данных для оценки состояния здоровья человека, которые передаются через открытый коммуникационный канал от датчиков к облачному хранилищу (медицинской информационной системе), остается важной задачей и требует разработки новых математических методов и моделей для обеспечения целостности, доступности и конфиденциальности информации.

Оценка защищенности данных в телемедицинских системах может быть выполнена с помощью предложенной методики управления информационными рисками.

ЛИТЕРАТУРА

[1] Bashi N., Karunanithi M., Fatehi F., et al. Remote monitoring of patients with heart failure: an overview of systematic reviews. *J. Med. Internet Res.*, 2017, vol. 19, no. 1, art. e18. DOI: https://doi.org/10.2196/jmir.6571

[2] 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.

[3] 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: https://doi.org/10.1109/MC.2012.294

[4] Shevchuk B., Geraimchuk M., Ivakhiv O., et al. Remote monitoring of the person physiological state. *IDAACS*, 2017, pp. 707–711.
DOI: https://doi.org/10.1109/IDAACS.2017.8095182

[5] Анищенко В.С., Булдакова Т.И., Довгалевский П.Я. и др. Концептуальная модель виртуального центра охраны здоровья населения. *Информационные технологии*, 2009, № 12, с. 59–64.

[6] Karavaev A.S., Ishbulatov Y.M., Kiselev A.R., et al. A model of human cardiovascular system containing a loop for the autonomic control of mean blood pressure. *Hum. Physiol.*, 2017, vol. 43, no. 1, pp. 61–70.
DOI: https://doi.org/10.1134/S0362119716060098

[7] Булдакова Т.И., Игнатьева Е.В., Ляпина Н.С. и др. Оценка состояния человека и выделение групп риска развития хронических заболеваний. *Системный анализ и управление в биомедицинских системах*, 2011, т. 10, № 2, с. 391–395.

[8] Prado M., Roa L., Reina-Tosina J. Virtual center for renal support: technological approach to patient physiological image. *IEEE Trans. Biomed. Eng.*, 2002, vol. 49, no. 12, pp. 1420–1430. DOI: https://doi.org/10.1109/TBME.2002.805454

[9] Suyatinov S.I. Criteria and method for assessing the functional state of a human operator in a complex organizational and technical system. *GloSIC*, 2018.
DOI: https://doi.org/10.1109/GloSIC.2018.8570088

[10] Lamonaca F., Barbe K., Polimeni G., et al. Health parameters monitoring by smartphone for quality of life improvement. *Measurement*, 2015, vol. 73, no. 28, pp. 82–94. DOI: https://doi.org/10.1016/j.measurement.2015.04.017

[11] Paradiso R., Loriga G., Taccini N. A wearable health care system based on knitted integrated sensors. *IEEE Trans. Inform. Tech. Biomed.*, 2005, vol. 9, no. 3, pp. 337–344. DOI: https://doi.org/10.1016/j.measurement.2015.04.017

[12] Булдакова Т.И., Суятинов С.И., Миков Д.А. Анализ информационных рисков виртуальных инфраструктур здравоохранения. *Информационное общество*, 2013, № 4, с. 6.

[13] Shevchuk B., Ivakhiv O., Geraimchuk M., et al. Efficient encoding and transmission of monitoring data in information-efficient wireless networks. *IDAACS-SWS*, 2016, pp. 138–143. DOI: https://doi.org/10.1109/IDAACS-SWS.2016.7805803

[14] Булдакова Т.И., Суятинов С.И., Кривошеева Д.А. Обеспечение информационной безопасности в телемедицинских системах на основе модельного подхода. *Вопросы кибербезопасности*, 2014, № 5, с. 21–29.

[15] Banerjee A., Gupta S.K.S., Venkatasubramanian K.K. PEES: physiology-based end-to-end security for mHealth. *Proc. 4th Conf. Wireless Health*, 2013, art. 2.

DOI: https://doi.org/10.1145/2534088.2534109

[16] 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: http://dx.doi.org/10.18698/0236-3933-2017-3-95-106

[17] Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейронечеткой модели. *Наука и образование: научное издание МГТУ им. Н.Э. Баумана*, 2013, № 11, с. 295–310.
DOI: 10.7463/1113.0645489

[18] Lee M.-C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *IJCSIT*, 2014, vol. 6, no. 1, pp. 29–45.
DOI: http://dx.doi.org/10.5121/ijcsit.2014.6103

[19] Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB. *Вопросы кибербезопасности*, 2015, № 4, с. 53–61.

[20] Соколова А.В. Разработка телемедицинской системы мониторинга состояния здоровья человека. *ММТТ*, 2019, т. 3, с. 86–89.

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

Миков Дмитрий Александрович — канд. техн. наук, доцент кафедры «Компьютерные системы и сети» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Соколова Аксинья Владимировна — аспирантка кафедры «Компьютерные системы и сети» 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., Миков Д.А., Соколова А.В. Защита данных при дистанционном мониторинге состояния человека. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2020, № 4, с. 42–57.
DOI: https://doi.org/10.18698/0236-3933-2020-4-42-57

DATA SECURITY AT REMOTE MONITORING OF HUMAN STATE

T.I. Buldakova buldakova@bmstu.ru
D.A. Mikov mikov@bmstu.ru
A.V. Sokolova aksinya.sokolova@yandex.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper focuses on telemedicine systems for monitoring the human state and methods of protecting the transmitted data. To assess the state, biosignals are used, which are recorded by sensors and transmitted to a cloud medical information system. Based on the data obtained, a decision is made about the human state. Since the monitoring system works with restricted access information, it must be reliably protected. The study places an emphasis on possible information security threats for all components of the telemedicine system, analyzes various approaches to the protection of transmitted data in remote monitoring systems. It is noted that the existing methods are insufficient and additional methods of protecting the transmitted data are required. It is proposed to assess data security using the information risk management methods

Keywords

Data security, monitoring, electronic medical records, biosignals, medical information systems

Received 29.10.2019
Accepted 20.07.2020

REFERENCES

[1] Bashi N., Karunanithi M., Fatehi F., et al. Remote monitoring of patients with heart failure: an overview of systematic reviews. *J. Med. Internet Res.*, 2017, vol. 19, no. 1, art. e18. DOI: https://doi.org/10.2196/jmir.6571

[2] 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.).

[3] 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: https://doi.org/10.1109/MC.2012.294

[4] Shevchuk B., Geraimchuk M., Ivakhiv O., et al. Remote monitoring of the person physiological state. *IDAACS*, 2017, pp. 707–711. DOI: https://doi.org/10.1109/IDAACS.2017.8095182

[5] Anishchenko V.S., Buldakova T.I., Dovgalevskiy P.Ya., et al. Conceptual model of virtual centre of public health services. *Informatsionnye tekhnologii* [Information Technologies], 2009, no. 12, pp. 59–64 (in Russ.).

[6] Karavaev A.S., Ishbulatov Y.M., Kiselev A.R., et al. A model of human cardiovascular system containing a loop for the autonomic control of mean blood pressure. *Hum. Physiol.*, 2017, vol. 43, no. 1, pp. 61–70. DOI: https://doi.org/10.1134/S0362119716060098

[7] Buldakova T.I., Ignat'yeva E.V., Lyapina N.S., et al. Evaluation of the human states and allocation of risk groups of chronic diseases developing. *Sistemnyy analiz i upravlenie v biomeditsinskikh sistemakh*, 2011, vol. 10, no. 2, pp. 391–395 (in Russ.).

[8] Prado M., Roa L., Reina-Tosina J. Virtual center for renal support: technological approach to patient physiological image. *IEEE Trans. Biomed. Eng.*, 2002, vol. 49, no. 12, pp. 1420–1430. DOI: https://doi.org/10.1109/TBME.2002.805454

[9] Suyatinov S.I. Criteria and method for assessing the functional state of a human operator in a complex organizational and technical system. *GloSIC*, 2018. DOI: https://doi.org/10.1109/GloSIC.2018.8570088

[10] Lamonaca F., Barbe K., Polimeni G., et al. Health parameters monitoring by smartphone for quality of life improvement. *Measurement*, 2015, vol. 73, no. 28, pp. 82–94. DOI: https://doi.org/10.1016/j.measurement.2015.04.017

[11] Paradiso R., Loriga G., Taccini N. A wearable health care system based on knitted integrated sensors. *IEEE Trans. Inform. Tech. Biomed.*, 2005, vol. 9, no. 3, pp. 337–344. DOI: https://doi.org/10.1016/j.measurement.2015.04.017

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

[13] Shevchuk B., Ivakhiv O., Geraimchuk M., et al. Efficient encoding and transmission of monitoring data in information-efficient wireless networks. *IDAACS-SWS*, 2016, pp. 138–143. DOI: https://doi.org/10.1109/IDAACS-SWS.2016.7805803

[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, pp. 21–29 (in Russ.).

[15] Banerjee A., Gupta S.K.S., Venkatasubramanian K.K. PEES: physiology-based end-to-end security for mHealth. *Proc. 4th Conf. Wireless Health*, 2013, art. 2. DOI: https://doi.org/10.1145/2534088.2534109

[16] Buldakova T.I., Lantsberg A.V., Smolyaninova K.A. Secure access to information using smart card art. *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 (in Russ.). DOI: http://dx.doi.org/10.18698/0236-3933-2017-3-95-106

[17] Buldakova T.I., Mikov D.A. Estimating information risks in computer-aided systems using a neuro-fuzzy model. *Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana* [Science and Education: Scientific Publication], 2013, no. 11, pp. 295–310 (in Russ.). DOI: 10.7463/1113.0645489

[18] Lee M.-C. Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *IJCSIT*, 2014, vol. 6, no. 1, pp. 29–45. DOI: http://dx.doi.org/10.5121/ijcsit.2014.6103

[19] Buldakova T.I., Mikov D.A. Implement of information security risk assessment technique in MATLAB. *Voprosy kiberbezopasnosti*, 2015, no. 4, pp. 53–61 (in Russ.).

[20] Sokolova A.V. Development of a telemedicine system for monitoring of human health. *MMTT*, 2019, vol. 3, pp. 86–89 (in Russ.).

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

Mikov D.A. — Cand. Sc. (Eng.), Assoc. Professor, Department of Computers Systems and Networks, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Sokolova A.V. — Post-Graduate Student, Department of Computers Systems and Networks, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Buldakova T.I., Mikov D.A., Sokolova A.V. Data security at remote monitoring of human state. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2020, no. 4, pp. 42–57 (in Russ.).
DOI: https://doi.org/10.18698/0236-3933-2020-4-42-57