УДК 004.056

УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ

Т.И. Булдакова
Московский государственный технический университет им. Н.Э. Баумана
Россия, 105005, Москва, 2-я Бауманская ул., 5/1
E-mail: buldakova@bmstu.ru

Д.А. Миков
Московский государственный технический университет им. Н.Э. Баумана
Россия, 105005, Москва, 2-я Бауманская ул., 5/1
E-mail: mikovda@yandex.ru

А.В. Соколова
Московский государственный технический университет им. Н.Э. Баумана
Россия, 105005, Москва, 2-я Бауманская ул., 5/1
E-mail: aksinya.sokolova@yandex.ru

Ключевые слова: защита информации, телемедицина, мониторинг состояния человека, модель угроз, управление рисками.

Аннотация: Рассмотрена проблема обеспечения защиты данных в телемедицинских системах мониторинга состояния человека. Выделены возможные угрозы информационной безопасности для мобильной измерительной системы, обеспечивающей непрерывный мониторинг состояния человека по регистрируемым биосигналам. Отмечены особенности управления информационными рисками при дистанционном мониторинге состояния человека, сформулированы основные проблемы и выделены составляющие управления рисками информационной безопасности. Указаны требования к процессу управления информационными рисками в телемедицинских системах дистанционного мониторинга состояния человека и описаны основные этапы предложенной методики. Приведены примеры реализации методики.

1. Введение

Процесс модернизации системы здравоохранения сопровождается созданием виртуальных инфраструктур здравоохранения, объединяющих на базе единого информационного пространства все составляющие элементы системы охраны здоровья населения. Внедрение информационно-коммуникационных технологий обеспечивает формирование каналов устойчивых коммуникаций между специалистами разных лечебно-профилактических учреждений, удаленный доступ к медицинским информационным системам, облегчение и ускорение записи пациентов на прием к врачам.

Примером развития виртуальных инфраструктур здравоохранения являются системы телемедицины, которые обеспечивают дистанционный мониторинг состояния пациентов [1].При этом источниками объективной информации о функциональном состоянии человека являются мобильные измерительные системы, выполненные по техноло-

гиям “sensor-on-a-chip” и “laboratory-on-a-chip” [2-4]. Зарегистрированные биосигналы передаются по каналам связи в медицинские центры мониторинга и обработки данных (рис. 1), где осуществляется углубленная оценка состояния человека.

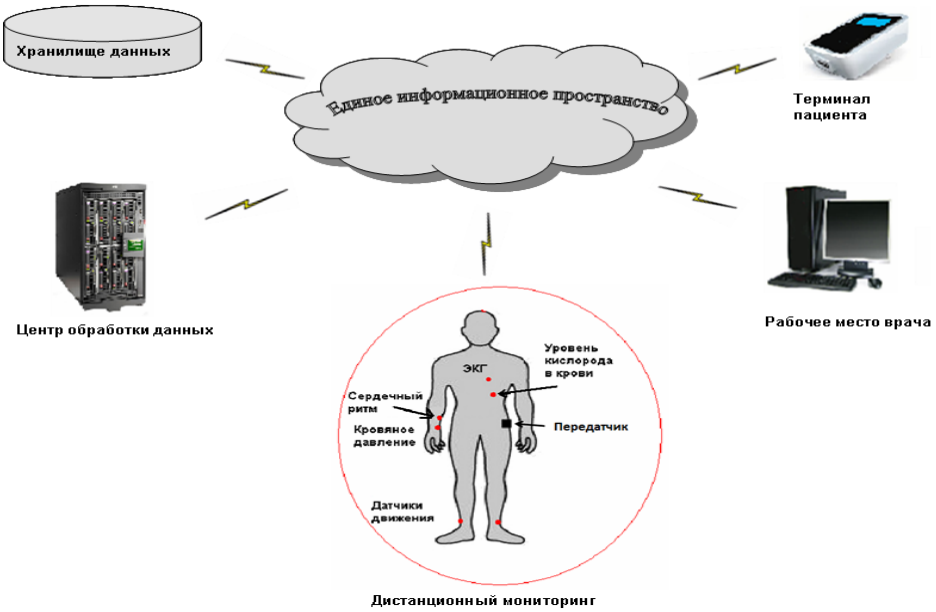

Рис. 1. Основные компоненты системы дистанционного мониторинга.

Включение мобильной измерительной системы в единое информационное пространство позволяет осуществить непрерывный мониторинг состояния человека независимо от его местоположения. Однако при этом возникает проблема с обеспечением целостности, конфиденциальности и доступности данных пациента.

2. Анализ угроз информационной безопасности

В системах дистанционного мониторинга решающее значение имеет обеспечение безопасности личных медицинских данных. Однако, несмотря на растущий поток исследований в области защиты информации, очень мало исследований направлено на изучение рисков информационной безопасности в сфере здравоохранения, которая в значительной степени регулируется и использует бизнес-модели, отличающееся от моделей других отраслей промышленности [5]. Нарушение целостности и конфиденциальности информации, кража личных медицинских данных приводят не только к финансовым потерям, но и к нежелательным социальным последствиям, наносят моральный ущерб пациенту.

Результаты анализа возможных угроз информационной безопасности применительно к компонентам системы мониторинга приведены в таблице 1. Анализ модели угроз показал [6], что мобильные измерительные системы, когда регистрируемые данные передаются через открытый коммуникационный канал от датчиков к облачному хранилищу (медицинской базе данных) являются наиболее уязвимыми. Это обусловливает необходимость шифрования передаваемых данных, а также предъявляет повышенные требования к помехозащищенности информационных процессов системы мониторинга, которые влияют на принятие обоснованного решения о состоянии пациента.

Таблица 1. Возможные угрозы информационной безопасности

Компоненты	Угрозы	Комментарии
Датчики	Доступ злоумышленника к датчику	Необходимо использовать надежные датчики, ограничивающие доступ
Коммуникации	Злоумышленники могут подслушивать все виды разговоров, а также исказить сигналы	Коммуникационная связь в системе является ненадежной, поэтому необходимо шифрование сигналов
Хранилище данных в облаке	Возможный доступ к данным в облаке	Только после успешной авторизации врач сможет получить доступ к информации о пациенте
Медицинский персонал	Передача информации злоумышленнику	Предполагается, что медицинский персонал не откроет доступ к информации под влиянием злоумышленников
Пациент	Передача информации злоумышленнику	Предполагается, что пациент не откроет доступ к информации под влиянием злоумышленников
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

Таким образом, в системах дистанционного мониторинга необходимо постоянно отслеживать уровень информационных рисков – потенциальной возможности искажения информации, а также вырабатывать контрмеры для их снижения, что составляет задачу управления рисками.

3. Особенности управления информационными рисками

В отличие от других классов систем, системы дистанционного мониторинга оказываются более уязвимыми к внешним (несанкционированным) воздействиям на информацию, которые могут носить и целенаправленный характер (рис. 2).

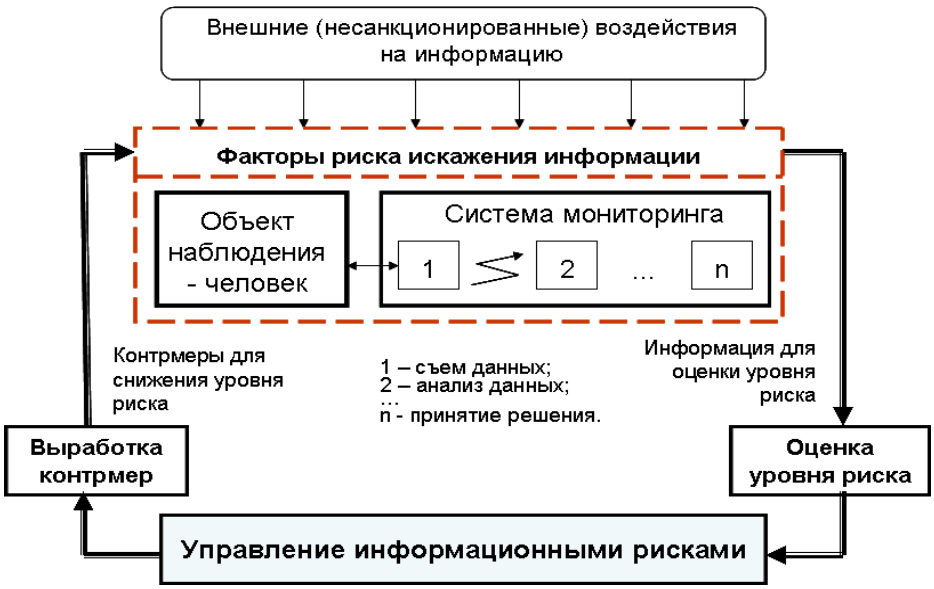

Рис. 2. Управление информационными рисками.

Даже незначительные (на первый взгляд) нарушения любого из протекающих в системе информационных процессов могут привести к тяжелым последствиям – потере конфиденциальности, целостности и/или доступности информации. Однако факторы риска искажения информации могут быть неизвестны, и требуется их идентификация [7]. Проведенный анализ существующих методов и средств управления информационными рисками позволил сформулировать основные проблемы и выделить составляющие управления информационными рисками (рис. 3).

Рис. 3. Этапы управления информационными рисками.

Сделан вывод, что методика управления рисками информационной безопасности должна состоять из множества (набора) методов, используемых на различных этапах процесса и удовлетворяющих следующим показателям эффективности:

a) наибольшая согласованность и адекватность оценок факторов риска;
b) максимальная адаптивность к качественным данным;
c) минимальная субъективность и неопределенность оценки риска;
d) учет неодинаковой чувствительности риска к различным факторам.

Реализация методики связана с рядом сложностей. Во-первых, необходим метод, позволяющий составить наиболее полный перечень факторов риска, что связано с задачей создания модели автоматизированной системы и анализа ее информационных потоков. Во-вторых, необходимо проанализировать множество существующих методов управления рисками информационной безопасности. В-третьих, необходимо для каждого метода или группы методов корректно оценить показатели эффективности и способность учитывать чувствительность риска.

Практические исследования по созданию наиболее эффективной методики управления информационными рисками позволили сделать вывод [8, 9], 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;
- методов теории игр на этапе выбора контрмер.

В работе [10] приведены результаты реализации методики оценки информационных рисков. Показано, что применение предложенной методики управления информационными рисками в телемедицинских системах позволит снизить уровень риска на 10-15%.

4. Заключение

В данной работе рассмотрены особенности мобильных измерительных систем и проанализированы возможные способы защиты данных в системах дистанционного мониторинга состояния человека. Показано, что создание технологии защиты данных для оценки состояния человека, которые передаются через открытый коммуникационный канал от датчиков к облачному хранилищу (медицинской базе данных) остается актуальной задачей и требует разработки новых математических методов, моделей и алгоритмов для обеспечения целостности, доступности и конфиденциальности информации.

Методика управления информационными рисками должна объединять наиболее эффективные методы для каждого этапа этого процесса. Ее применение существенно расширяет возможности интегрирования различных методов, используя их сильные стороны и обеспечивая гибкий и плавный переход от одного метода к другому, а также обеспечивает качество входной информации и надежность (степень доверия) источников данных.

Список литературы

1. 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.
2. Булдакова Т.И., Коблов А.В., Суятинов С.И. Информационно-измерительный комплекс совместной регистрации и обработки биосигналов // Приборы и системы. Управление, контроль, диагностика. 2008. № 6. С. 41-46.
3. Paradiso R., Loriga G., Taccini N. A Wearable Health Care System Based on Knitted Integrated Sensors // IEEE Transactions on Information Technology in Biomedicine. 2005. Vol. 9, No. 3. P. 337-344.
4. A Multiparameter Wearable Physiologic Monitoring System for Space and Terrestrial Applications / C.W. Mundt, K.N. Montgomery, U.E. Udoh, V.N. Barker // IEEE Transaction on Information Technology in Biomedicine. 2005. Vol. 9, No. 3. P. 382-391.
5. Appari A., Johnson M. E. Information Security and Privacy in Healthcare: Current State of Research // International Journal of Internet and Enterprise Management. 2010. Vol. 6, No 4. P. 279-314.
6. Булдакова Т.И., Кривошеева Д.А. Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. № 5 (13). С. 45-50.
7. Булдакова Т.И., Суятинов С.И., Миков Д.А. Анализ информационных рисков виртуальных инфраструктур здравоохранения // Информационное общество. 2013. № 4. С. 6.
8. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечеткой модели // Наука и образование: научное издание МГТУ им. Н.Э. Баумана. 2013. № 11. С. 295-310.
9. Lee M.-C. Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method // International Journal of Computer Science & Information Technology (IJCSIT). 2014. Vol 6, No. 1. P. 29-45.
10. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. № 4 (12). С. 53-61.