УДК 004.23

ВЫЯВЛЕНИЕ ФАКТОРОВ ИНФОРМАЦИОННОГО РИСКА В ТЕЛЕМЕДИЦИНСКОЙ СИСТЕМЕ

Д.А. Миков mikov@bmstu.ru

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

Аннотация

Предложен метод исследования информационных потоков в автоматизированной системе на основе функционального моделирования с помощью методологии IDEF0. Проанализированы особенности выявления угроз информационной безопасности, потенциального ущерба, уязвимостей автоматизированной системы и выработки соответствующих контрмер. Разработана IDEF0-модель функционирования телемедицинской системы. На основе анализа разработанной модели выявлены факторы риска информационной безопасности в телемедицинской системе дистанционного мониторинга состояния человека, предложены контрмеры

Ключевые слова

Система дистанционного мониторинга состояния человека, IDEF0-модель, анализ информационных рисков, факторы риска, угрозы информационной безопасности, потенциальный ущерб, уязвимости автоматизированной системы, контрмеры

Поступила в редакцию 01.09.2016

Введение. Проблема защиты данных в автоматизированных системах любого профиля связана с анализом рисков информационной безопасности, который, в соответствии с требованиями ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью», является обязательной составляющей комплекса мероприятий по обеспечению информационной безопасности. Начальным этапом данного процесса является выявление факторов риска — угроз информационной безопасности, потенциально возможного ущерба, уязвимостей автоматизированной системы и выработка контрмер [1]. Решение этой задачи связано с построением модели автоматизированной системы и исследованием циркулирующих в ней информационных потоков.

Сравнительный анализ методологий ARIS, IDEF0, IDEF3 и UML показал, что IDEF0 наиболее полно учитывает и отображает необходимые для анализа потоков данных элементы автоматизированной системы. Отметим, что диаграммы IDEF0 менее наглядны, но и менее громоздки, по сравнению с ARIS и UML. Кроме того, для большего удобства визуального восприятия возможно использование дополнительных графических средств, представленных в работе [2, 3]. В этой связи цель настоящей работы выявить с помощью методологии IDEF0 факторы риска на примере телемедицинской системы дистанционного мониторинга состояния человека (СДМСЧ).

Принципы разработки IDEF0-модели автоматизированной системы. Для формирования перечня факторов информационного риска в автоматизирован-

ной системе с помощью IDEF0-модели, необходимо предварительно определить, каким группам факторов будут соответствовать входящие, исходящие и управляющие интерфейсные дуги и механизмы. Иначе говоря, сформировать принцип соответствия интерфейсных дуг группам факторов в зависимости от стороны функционального блока. Например, угрозы информационной безопасности соответствуют объектам, поступающим на вход процесса, потенциально возможный ущерб определяется состоянием объектов на выходе, а уязвимости автоматизированной системы зависят от механизмов реализации и управляющих воздействий на процесс. Организационно-правовые уязвимости выявляют через анализ управляющих дуг, все остальные — через анализ механизмов. Принцип расположения факторов риска в IDEF0-модели автоматизированной системы «как есть» показан на рис. 1.

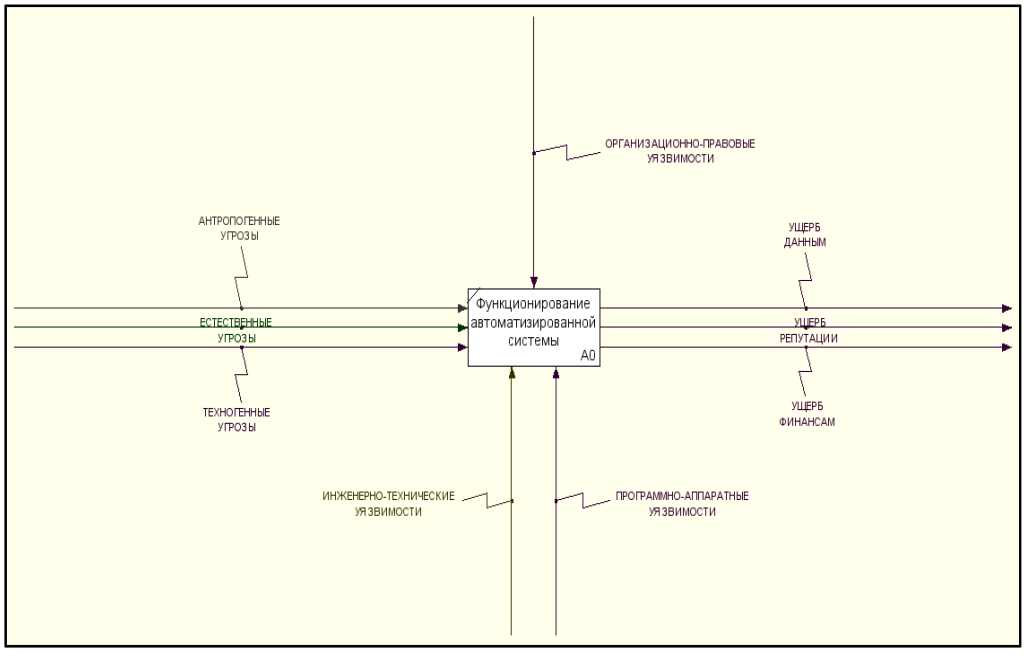

Рис. 1. Факторы риска в IDEF0-модели «как есть»

Факторы риска целесообразно расположить в модели «как есть», а контрмеры, необходимые и достаточные для снижения или устранения выявленных факторов — в модели «как должно быть» (рис. 2). Контрмеры призваны воздействовать на процессы автоматизированной системы, нейтрализуя или снижая угрозы (активные контрмеры) и уязвимости (пассивные контрмеры). Но вне зависимости от вида контрмер, они всегда являются либо управляющим воздействием на процесс, либо дополнительным механизмом, защищающим его реализацию. Поэтому в IDEF0-модели их следует обозначать через интерфейсные дуги управления и механизмов. Иногда добавление контрмер приводит к формированию новых процессов, тогда в модель «как должно быть» необходимо добавить соответствующие функциональные блоки.

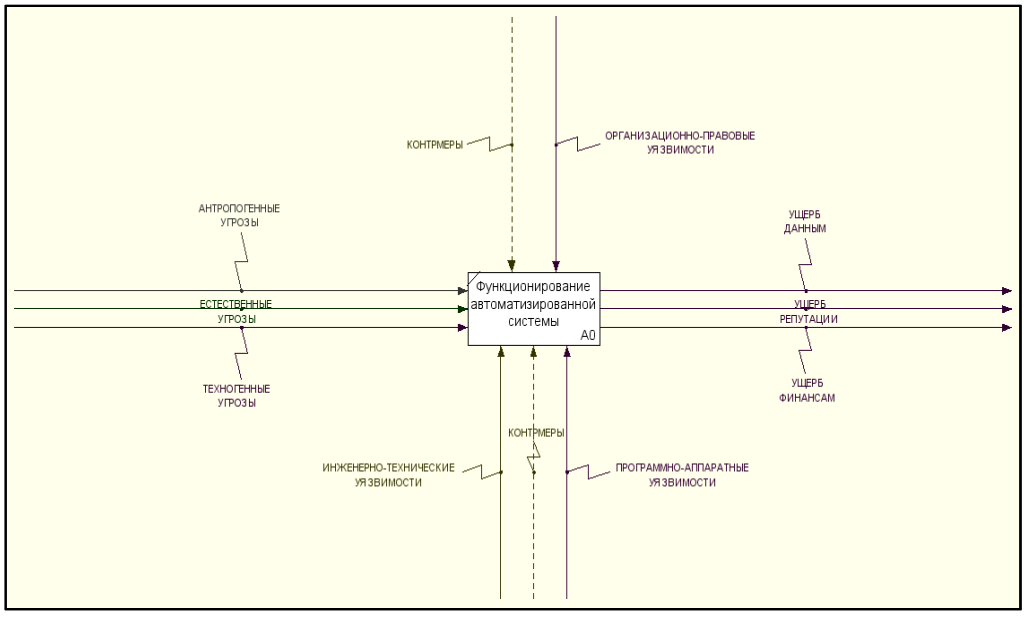

Рис. 2. Факторы риска и контрмеры в модели «как должно быть»

На основе анализа представленных данных, обозначим принципы, в соответствии с которыми необходимо разрабатывать IDEF0-модель функционирования автоматизированной системы для выявления факторов риска (табл. 1).

Таблица 1

Принципы разработки IDEF0-модели для выявления факторов риска

Элементы моделирования	Особенности реализации
Цель разработки	Выявление факторов риска
Точка зрения на модель	Риск-менеджер информационной безопасности
Степень детализации	Возможность выявления и описания всех факторов риска и выработка соответствующих контрмер
Выявление угроз информационной безопасности	Анализ входящих интерфейсных дуг (модель «как есть»)
Выявление потенциально возможного ущерба	Анализ исходящих интерфейсных дуг (модель «как есть»)
Выявление организационно-правовых уязвимостей	Анализ управляющих интерфейсных дуг (модель «как есть»)
Выявление инженерно-технических и программно-аппаратных уязвимостей	Анализ механизмов (модель «как есть»)
Отображение существующих контрмер	Интерфейсные дуги управления и механизмов (модель «как есть»)
Отображение необходимых и достаточных контрмер	Интерфейсные дуги управления и механизмов, при необходимости — новые функциональные блоки (модель «как должно быть»)

При выборе необходимых и достаточных контрмер и добавлении их в модель «как должно быть» следует понимать, что сначала их перечень будет предварительным, так как выявленные факторы риска еще не подверглись оценке экспертной группой, следовательно, нельзя сделать однозначный вывод о степени их влияния на выявление угрозы и уязвимости.

После оценки факторов риска и последующего расчета уровня риска (после преобразования всех величин в числовые значения) перечень необходимых и достаточных контрмер может быть подвергнут корректировке. Вследствие этого, неизбежны изменения в модели «как должно быть» после реализации дальнейших этапов анализа.

Построение IDEF0-модели. Процесс моделирования начинается с определения субъекта моделирования, цели моделирования и точки зрения на модель. В рамках данного исследования субъектом моделирования является система дистанционного мониторинга состояния человека, целью моделирования — составление перечня факторов риска, точкой зрения на модель — риск-менеджер информационной безопасности. Сначала строится модель «как есть». Контекстная диаграмма этой модели представлена на рис. 3.

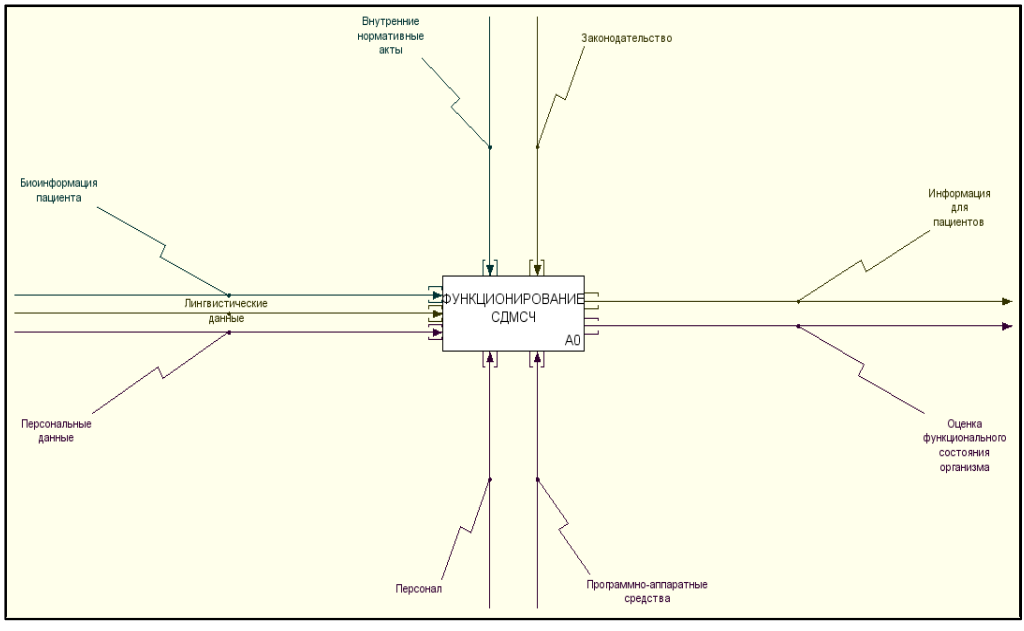

Рис. 3. Контекстная диаграмма IDEF0-модели «как есть»

Далее необходимо провести функциональную декомпозицию контекстной диаграммы. Для этого проводят разделение контекстной диаграммы на основные функциональные блоки, из которых состоит функционирование СДМСЧ. При этом все интерфейсные дуги с внешних сторон диаграмм декомпозиции нижних уровней должны соответствовать интерфейсным дугам диаграммы декомпозиции верхнего уровня. Диаграмма декомпозиции первого уровня представлена на рис. 4.

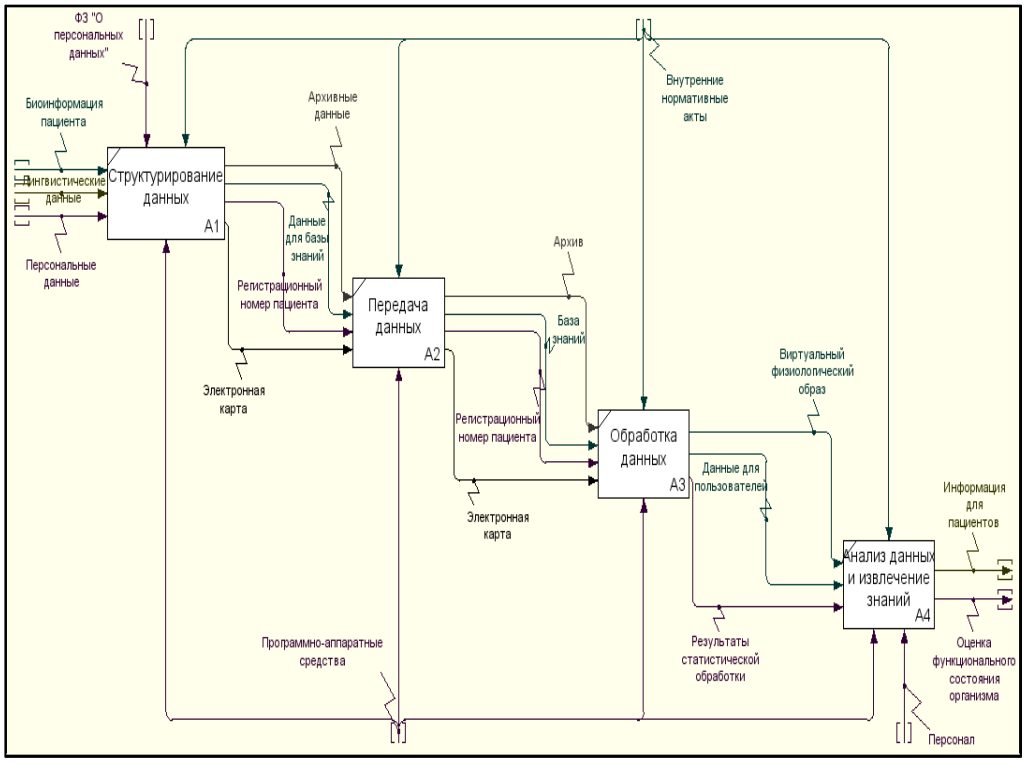

Рис. 4. Диаграмма декомпозиции первого уровня

Следующий этап — построение диаграмм декомпозиции второго уровня по каждому из функциональных блоков (подсистем) СДМСЧ.

Блок 1. Структурирование проводят в несколько этапов:

1) сбор и первичная обработка данных;
2) формирование структуры моделей;
3) формирование и ведение базы данных;
4) формирование и ведение базы знаний;
5) формирование и ведение базы электронных карт;
6) ведение архива.

Блок 2. Процесс передачи данных строится следующим образом:

1) передача сигналов;
2) обнаружение сигналов;
3) фильтрация сигналов;
4) оценка параметров;
5) преобразование сигналов в данные.

Блок 3. Обработка данных включает:

1) статистическую обработку данных;
2) выбор структуры модели;
3) формирование виртуального физиологического образа (ВФО);
4) формирование отчетов;
5) организацию доступа к данным;
6) обмен данными с клиентами.

Блок 4. Анализ данных и извлечение знаний подразумевает следующие действия:

1) формирование эталонов типовых ВФО;

2) моделирование и визуализацию состояния системы «сердце–сосуды–легкие»;

3) сопоставление модели с эталонами;

4) диагностику и прогнозирование;

5) выработку рекомендаций;

6) информирование пациента о функциональном состоянии организма.

Таким образом, IDEF0-модель «как есть» можно считать завершенной. Достигнутый уровень детализации является достаточным для анализа системы.

Составление перечня факторов риска и выработка контрмер. На этапе сбора и первичной обработки данных необходимо проверить выполнение требований относительно обработки персональных данных, представленных в Федеральном законе «О персональных данных» от 27.07.2006 N 152-ФЗ. В соответствии со статьей 6 данного закона, обработка персональных данных осуществляется с согласия субъекта. Статья 10 названного указывает, что обработка данных, касающихся состояния здоровья, не допустима без письменного согласия субъекта. Согласно статье 9 обозначенного закона, согласие в форме электронного документа, подписанного электронной подписью, признается равнозначным.

Следующей проблемой в подсистеме структурирования данных является управление базой данных, базой знаний, базой электронных карт и архивом с помощью единой СУБД, т. е. обеспечение совместимости при организации информационного обмена и гарантии проверки целостности, резервного копирования и восстановления данных. Решением может быть использование CALS-технологий и языка XML для представления, хранения и использования биотехнических и физиологических данных. Кроме того, форматы описания данных (в частности, биосигналов), принятые в медицине, сходны со структурой передаваемого пакета данных, предписанной стандартом MIL 1840.

В подсистеме передачи данных главная опасность заключается в нарушении конфиденциальности при передаче с телемедицинских датчиков в облачную медицинскую базу данных. Для решения этой проблемы можно использовать регистрируемые датчиками биосигналы, отражающие физиологические особенности пациента, для шифрования информации по некоторым морфологическим особенностям биосигналов, которые являются уникальными для каждого человека и мало изменяются с течением времени, получая своеобразную «физиологическую» подпись индивидуума [4].

В подсистеме обработки данных нарушение безопасности может привести к необратимым последствиям для заинтересованных лиц. В то же время существует необходимость в полном доступе ко всей информации, относящейся к пациентам, а статистику необходимо передавать в Министерство здравоохранения Российской

Федерации. Самым сложным аспектом является определение полномочий (ограничений), предоставленных пациентам. Возможность указания степени ограничения доступа к их медицинским данным, ведет к сложному контролю доступа, основанному на ролевой модели (RBAC) [5–7]. Еще одной проблемой подсистемы обработки данных является большой объем архивной информации, передаваемой Web-сервером серверу обработки в целях статистической обработки и формирования отчетности. Решить проблему можно с помощью «сжатия» данных.

В подсистеме анализа данных и извлечения знаний в процессе взаимодействия сервера обработки с клиентскими приложениями при обмене информацией о ВФО присутствуют «слабые места». Протокол взаимодействия «клиент–сервер» позволит отследить действия каждого клиента в произвольный момент, а также выявить пользователя, действия которого привели к порче данных либо к возникновению спорных ситуаций при ошибочно введенных данных. Автоматическое обновление клиентских модулей обеспечит своевременную установку обновлений и исправлений, значительно упрощая работу, связанную с администрированием. Автономная работа при потере связи с сервером позволит сохранить работоспособность клиентской части. Перечень факторов риска и предлагаемые контрмеры представлены в табл. 2.

Таблица 2

Перечень факторов риска и предлагаемые контрмеры

Факторы риска	Предлагаемые контрмеры
Письменное согласие пациента на обработку персональных данных	Применение цифрового документа и электронной подписи
Информационная совместимость при обмене данными	Хранение информации в формате XML и применение CALS-технологий
Единое управление и обеспечение целостности хранимой информации	Применение XML-СУБД Sedna, обладающей собственной политикой безопасности
Нарушение конфиденциальности данных при передаче с датчиков в облачное хранилище	Шифрование данных на основе морфологических особенностей биосигналов пациента
Обеспечение контроля доступа к данным без нанесения ущерба доступности	Распределение прав доступа к данным и синхронизация доступа на основе RBAC
Большой объем архивных данных, передаваемых Web-сервером серверу обработки	«Сжатие» архивных данных для снижения расхода дисковой памяти, сетевого трафика
Отслеживание действий клиентов в произвольный момент для выявления нарушителя	Ведение открытого сетевого протокола взаимодействия Sedna Client-Server Protocol
Установка обновлений и исправлений клиентских модулей	Автоматическое обновление с помощью модуля XUpdate
Сохранение работоспособности клиентской части при временном отсутствии связи с сервером	Использование 64-разрядного диспетчера памяти, адресации и подкачки

Отметим, что одной из наиболее сложных задач является защита передаваемых данных. Решению этой задачи планируется посвятить дальнейшие исследования [4, 8].

Выводы. Для составления перечня факторов риска целесообразно использовать методологию IDEF0 и построить две модели автоматизированной системы. Модель «как есть» необходима для составления перечня угроз информационной безопасности, активов (процессов и ресурсов), подлежащих защите (которым может быть нанесен ущерб) и уязвимостей автоматизированной системы. Модель «как должно быть» позволит составить перечень контрмер, необходимых и достаточных для снижения или устранения выявленных факторов. Также необходимо отметить, что построение IDEF0-модели является не конечным результатом, а только средством составления перечня факторов риска. Поэтому эффективность анализа информационных рисков зависит от осознания того, что именно должно быть проанализировано, какие стороны работы автоматизированной системы необходимо рассмотреть.

Работа выполнена при финансовой поддержке РФФИ, проект №16-07-00878.

Литература

1. *Миков Д.А.* Анализ методов и средств, используемых на различных этапах оценки рисков информационной безопасности // Вопросы кибербезопасности. 2014. № 4 (7). С. 49–54.

2. *Миков Д.А.* Анализ методов изучения потоков данных для оценки рисков информационной безопасности // Ежемесячный научный журнал «Prospero». 2014. № 7. С. 28–33.

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

4. *Булдакова Т.И., Кривошеева Д.А.* Угрозы безопасности в системах дистанционного мониторинга // Вопросы кибербезопасности. 2015. № 5 (13). С. 45–50.

5. *Eyers D.M., Bacon J., Moody K.* Oasis role-based access control for electronic health records // IEE Proceedings — Software. 2006. Vol. 153. No. 1. P. 16–23. DOI: 10.1049/ip-sen:20045038

6. *Ferraiolo D.F., Kuhn D.R.* Role based access control // 15th National Computer Security Conference. October 1992. P. 554–563.

7. *Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E.* Role-based access control models // IEEE Computer. 1996. Vol .29. No. 2. P. 38–47. DOI: 10.1109/2.485845

8. *Булдакова Т.И., Джалолов А.Ш.* Анализ информационных процессов и выбор технологий обработки и защиты данных в ситуационных центрах // Научно-техническая информация. Сер. 1. 2012. № 6. С. 16–22.

Миков Дмитрий Александрович — аспирант, ассистент кафедры «Информационная безопасность», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

DETECTING INFORMATION TECHNOLOGY RISK FACTORS IN A TELEMEDICINE SYSTEM

D.A. Mikov mikov@bmstu.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

We suggest a method for researching information flows in an automated system based on function modelling employing the IDEF0 methodology. We analyse the specifics of detecting information security threats, potential damage, vulnerabilities of the automated system, and developing corresponding countermeasures. We developed an IDEF0 model of the operation of a telemedicine system. By analysing the model developed, we detected information security risk factors in a telemedicine system for remote health condition monitoring and suggested countermeasures

Keywords

Remote health condition monitoring system, IDEF model, information technology risk analysis, risk factors, information security threats, potential damage, vulnerabilities of an automated system, countermeasures

References

[1] Mikov D.A. Analysis of methods and tools which are used in the various stages of information security risk assessment. *Voprosy kiberbezopasnosti,* 2014, no. 4 (7), pp. 49–54 (in Russ.).

[2] Mikov D.A. Analysis of data stream research methods for information security risk assessment. *Ezhemesyachnyy nauchnyy zhurnal "Prospero",* 2014, no. 7, pp. 28–33 (in Russ.).

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

[4] Buldakova T.I., Krivosheeva D.A. Security threats in systems of the remote monitoring. *Voprosy kiberbezopasnosti*, 2015, no. 5(13), pp. 45–50 (in Russ.).

[5] Eyers D.M., Bacon J., Moody K. Oasis role-based access control for electronic health records. *IEE Proceedings — Software*, 2006, vol. 153, no. 1, pp. 16–23. DOI: 10.1049/ip-sen: 20045038

[6] Ferraiolo D.F., Kuhn D.R. Role based access control. 15th National Computer Security Conference, 1992, pp. 554–563.

[7] Sandhu R., Coyne E.J., Feinstein H.L., Youman C.E. Role-based access control models. *IEEE Computer*, 1996, vol. 29, no. 2, pp. 38–47. DOI: 10.1109/2.485845

[8] Buldakova T.I., Dzhalolov A.Sh. Analysis of data processes and choices of data-processing and security technologies in situation centers. *Nauchno-tekhnicheskaya informatsiya*. Ser. 1, 2012, no. 6, pp. 16–22. (Eng. version of journal: Scientific and Technical Information Processing, 2012, vol. 39, no. 2, pp. 127–132. DOI: 10.3103/S0147688212020116)

Mikov D.A. — post-graduate student, Assist. Lecturer of Information Security Department, Bauman Moscow State Technical University, Moscow, Russian Federation.