На правах рукописи

**МИКОВ Дмитрий Александрович**

# УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ ДИСТАНЦИОННОГО МОНИТОРИНГА СОСТОЯНИЯ ОБЪЕКТА

Специальность: 05.13.01 – Системный анализ, управление и обработка информации (в технических системах)

**АВТОРЕФЕРАТ**

диссертации на соискание учёной степени
кандидата технических наук

Москва – 2018

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)».

| | |
|---|---|
| Научный руководитель: | доктор технических наук, профессор,<br>профессор кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана<br>Булдакова Татьяна Ивановна |
| Официальные оппоненты: | доктор технических наук, профессор,<br>профессор кафедры «Телематика» Санкт-Петербургского политехнического университета Петра Великого<br>Большаков Александр Афанасьевич |
| | доктор технических наук, профессор,<br>профессор кафедры «Автоматизированные системы управления тепловыми процессами» Национального исследовательского университета «Московский энергетический институт»<br>Проталинский Олег Мирославович |
| Ведущая организация: | федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный технический университет» |

Защита состоится 19 июня 2018 г. в 14:30 на заседании диссертационного совета Д 212.141.02 при МГТУ им. Н.Э. Баумана по адресу: 105005, Москва, Госпитальный пер., 10, ауд. 613м.

С диссертацией можно ознакомиться в библиотеке федерального государственного бюджетного образовательного учреждения высшего образования МГТУ им. Н.Э. Баумана и на сайте http://www.bmstu.ru

Автореферат разослан «__» _____ 2018 г.

Учёный секретарь
диссертационного совета,
к.т.н., доцент — Муратов Игорь Валентинович

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность темы.** В настоящее время в различных сферах (в телемедицине, нефтегазовой отрасли, теплоэнергетике и др.) всё большее распространение получают системы дистанционного мониторинга состояния объекта (СДМСО). Суть дистанционного мониторинга заключается в реализации процессов удалённого сбора, передачи, обработки, хранения данных о параметрах контролируемого объекта и выработки решения о его состоянии, что характерно для многих систем управления. Особенность рассматриваемого класса систем обусловливает повышенные требования к помехозащищённости протекающих в системе информационных процессов для обеспечения надёжного функционирования и выработки обоснованного решения. В отличие от других классов систем, СДМСО оказываются более уязвимыми к внешним (несанкционированным) воздействиям на информацию, которые могут носить и целенаправленный характер. В результате даже незначительные, на первый взгляд, нарушения любого из информационных процессов могут привести к тяжёлым последствиям – потере конфиденциальности, целостности и/или доступности информации в СДМСО, компрометации организации, подрыву доверия к ней, серьёзному ущербу как самой организации, так и её клиентам.

Сказанное обусловливает необходимость постоянного отслеживания уровня информационных рисков – потенциальной возможности искажения информации, а также выработки контрмер для их снижения, что составляет задачу управления рисками. Однако информационный риск зависит от многих условий функционирования СДМСО, а потому характеризуется неопределённостью. В связи с этим работа по созданию методов и моделей управления информационными рисками в СДМСО в условиях неопределённости и неполноты данных носит системный характер и является актуальной.

**Степень проработанности темы.** В настоящее большинство исследований направлено на решение отдельных задач, связанных с управлением информационными рисками. Многие отечественные и зарубежные ученые (Астахов А.М, Белов В.М., Белов Е.Б., Герасименко В.А., Домарев В.В., Карпеев Д.О., Лось В.П., Малюк А.А., Мещеряков Р.В., Нестеров С.А., Остапенко Г.А., Плетнёв П.В., Плотников Д.Г., Шелупанов А.А., Harris S., Petch J., Rodger C., Ryba M. и др.) посвятили свои работы исследованию статистических и экспертных методов оценки информационных рисков. В этих работах основное внимание уделяется вопросу оценки рисков и не рассматриваются такие важные этапы анализа, как выявление исходных данных для оценки, определение соотношения контрмер и возможного ущерба, отсутствуют рекомендации по реализации процессов управления рисками.

В работах других учёных (Абрамов М.А., Атаманов А.Н., Балашов П.А., Гильмуллин Т.М., Зикратов И.А., Лаврентьев В.С., Одегов С.В., Сидоров А.О., Тимонин М.В., Lee M.-C., Rot A. и др.) рассмотрены отдельные

методы интеллектуального моделирования в сфере информационных рисков, однако выбор методов не обосновывается. Сравнительный анализ эффективности применения интеллектуальных методов для управления рисками отсутствует.

**Целью работы** является повышение эффективности управления информационными рисками в СДМСО на основе системного подхода и предложенных критериев.

Для достижения поставленной цели были решены следующие **задачи**:

1) с позиций системного анализа выполнена декомпозиция рассматриваемой системы, выявлены и описаны основные внутренние и внешние элементы, участвующие в информационном процессе, создающие риски или подверженные им;

2) проведён сравнительный анализ эффективности существующих методов и средств управления информационными рисками;

3) предложены методы и модели для реализации различных этапов управления информационным риском с учётом критериев эффективности;

4) создана методика управления информационными рисками на основе разработанных методов и моделей;

5) проведена апробация созданной методики на примере системы дистанционного мониторинга состояния человека.

**Методы и средства исследований.** При выполнении работы были использованы методы системного анализа, теории принятия решений, комбинаторики и математической статистики, теории нечётких множеств, нейросетевого моделирования, теории игр.

**Научная новизна** диссертационной работы состоит в следующем:

1) формализована и поставлена задача управления информационными рисками в СДМСО и *впервые предложено решение на основе системного анализа*, что позволило представить её в виде взаимосвязанной иерархической совокупности задач меньшей трудоёмкости;

2) сформирована совокупность критериев эффективности, моделей описания потоков данных и процесса идентификации факторов риска в СДМСО, *что позволило реализовать* оптимальный выбор методов для разных этапов управления информационными рисками;

3) разработана нейронечёткая модель для оценки уровня информационных рисков в СДМСО, *отличающаяся учётом предложенных критериев эффективности*;

4) создана *оригинальная методика* управления информационными рисками, *позволяющая реализовать* оптимальный выбор методов и моделей на основе сформулированных критериев эффективности.

**Практическая значимость** диссертации заключается в следующем:

1) определён способ обработки экспертных оценок факторов риска для последующей оценки его уровня на основе интеллектуальных моделей;

2) предложена стратегия выбора эффективных, способствующих снижению риска до приемлемого уровня, и экономически выгодных контрмер;

3) разработанная методика управления рисками внедрена в телемедицинскую систему медицинского центра «Столица» (г. Москва).

**Апробация работы.** Основные результаты работы докладывались и обсуждались на Всероссийских научно-технических конференциях «Безопасные информационные технологии» (Москва, 2011, 2012, 2013, 2017), Международной студенческой научно-технической конференции «Новые направления развития приборостроения» (Минск, 2013), Международной научно-практической конференции «Теоретические и прикладные аспекты современной науки» (Белгород, 2014), Международной научно-практической конференции «Современные тенденции развития науки и технологий» (Белгород, 2016), Всероссийском конкурсе-конференции студентов и аспирантов по информационной безопасности «SIBINFO-2015» (Томск, 2015); Международных научно-технических конференциях «Математические методы в технике и технологиях» (Рязань, 2015; Минск, 2017).

В 2016 году получен грант РФФИ на реализацию проекта «Математическое обеспечение и технология защиты данных в системах дистанционного мониторинга состояния человека» (№16-07-00878).

В 2017 году исследования поддержаны Государственным фондом содействия развитию малых форм предприятий в научно-технической сфере по программе «Участник молодёжного научно-инновационного конкурса У.М.Н.И.К.».

**Достоверность и обоснованность** результатов диссертационного исследования обеспечиваются согласованностью теоретических положений и выводов с результатами их экспериментальной проверки, успешным использованием полученных результатов в различных организациях, апробацией результатов на научных конференциях и публикацией в печати.

**Публикации.** По теме диссертации опубликовано 22 научные работы, в том числе 6 статей в научных журналах из Перечня ВАК РФ, 1 монография, 1 учебное пособие, 7 статей в других журналах, 7 докладов в трудах международных конференций.

**Личный вклад соискателя** состоит в разработке методов и моделей для реализации методики управления информационными рисками, получении исходных данных для построения функций принадлежности и формирования баз правил, апробации результатов исследования, участии автора в обработке и интерпретации экспериментальных данных, подготовке публикаций по выполненной работе.

**Положения, выносимые на защиту:**

1) метод идентификации факторов риска, основанный на структурно-функциональном моделировании информационных процессов в СДМСО;

2) метод экспертного опроса для оценки факторов риска, обеспечивающий их согласованность и адекватность;

3) нейронечёткая модель (структура и параметры функций принадлежности, база правил нечёткого вывода, метод обучения сети) для оценки уровня информационного риска;

4) метод выбора оптимальных и экономически целесообразных контрмер для снижения рисков, основанный на критериях теории игр;

5) оригинальная методика управления информационными рисками на основе разработанных методов и моделей, учитывающая предложенные критерии эффективности.

**Структура и объём работы.** Диссертационная работа состоит из введения, 4 глав, заключения, списка литературы и приложений. Работа изложена на 156 страницах, содержит 44 рисунка, 43 таблицы, библиографический список включает 127 наименований.

## СОДЕРЖАНИЕ РАБОТЫ

**Во введении** обоснована актуальность темы диссертационной работы, определена цель исследования, для достижения которой сформулированы задачи, указаны научная новизна и практическая значимость, приведены основные положения, выносимые на защиту. Описана структура диссертации, приведено её краткое содержание.

**В первой главе** рассмотрены особенности СДМСО, отмечена их уязвимость к несанкционированным воздействиям на информацию, в том числе и целенаправленного характера (Рис. 1). Отмечено, что даже незначительные, на первый взгляд, нарушения любого из протекающих в системе информационных процессов могут привести к тяжёлым последствиям – потере конфиденциальности, целостности и/или доступности информации в СДМСО, что обусловливает повышенные требования к помехозащищённости информационных процессов. Однако факторы риска искажения информации могут быть неизвестны, и требуется их идентификация. Поставлена задача управления информационными рисками, выделены основные этапы.

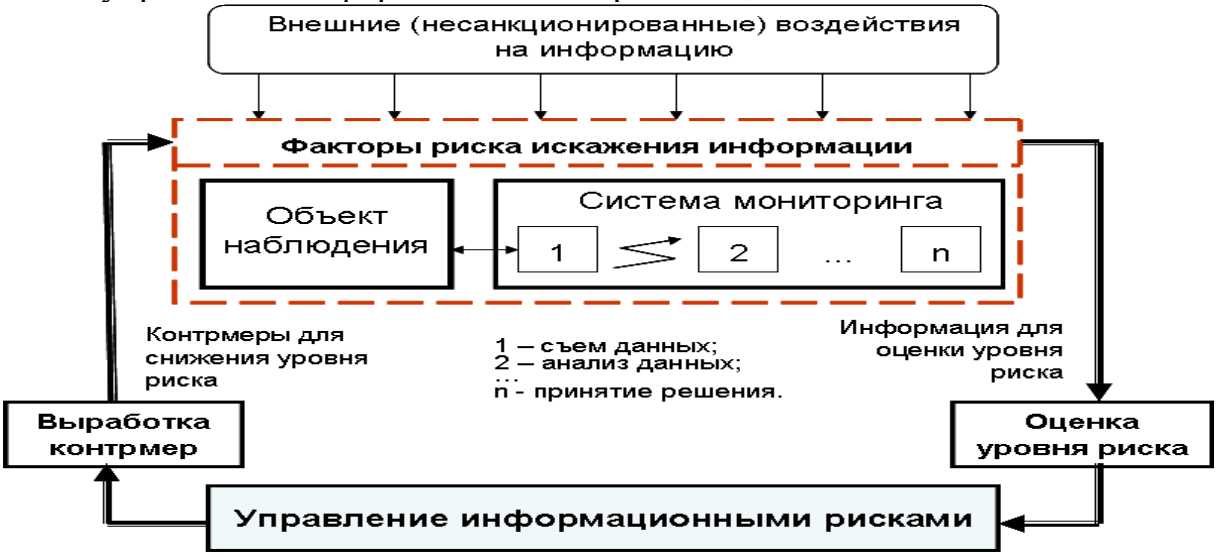


Рис. 1. Управление информационными рисками в СДМСО

Проведён анализ существующих методов и средств управления информационными рисками. Сформулированы выявленные проблемы, выделены составляющие управления рисками (Рис. 2).

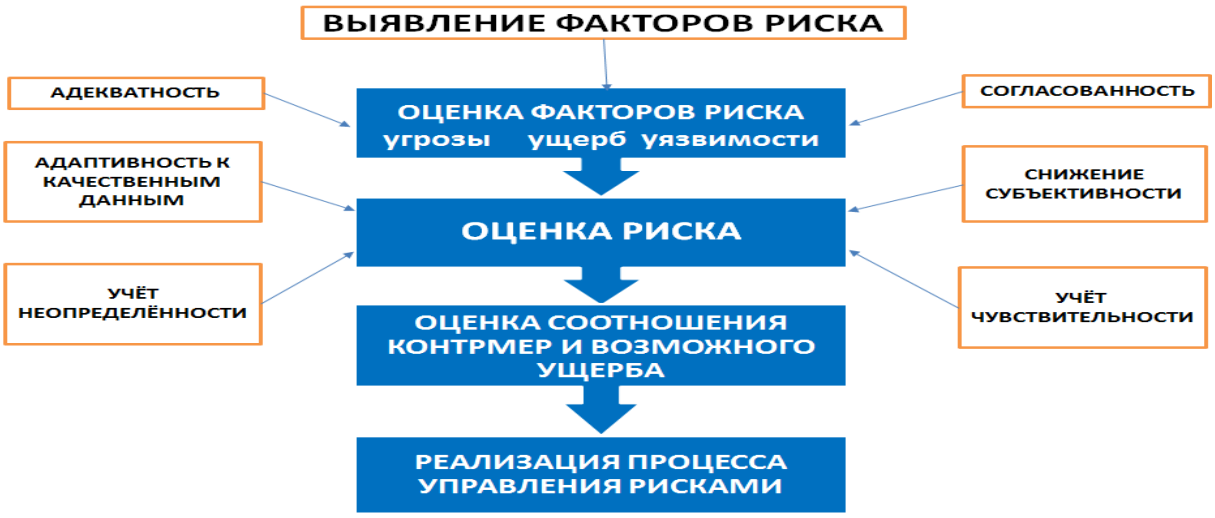


Рис. 2. Этапы управления рисками

Введены обозначения: $R = f(x)$ – риск; $x = \{x_1, x_2, x_3, x_4\}$ – множество факторов риска; $x_1 = \{x_{11}, x_{12}, x_{13}\}$ – множество угроз ($x_{11}$ – антропогенные, $x_{12}$ – естественные, $x_{13}$ – техногенные); $x_2 = \{x_{21}, x_{22}, x_{23}\}$ – множество видов ущерба ($x_{21}$ – информационный, $x_{22}$ – репутационный, $x_{23}$ – финансовый); $x_3 = \{x_{31}, x_{32}, x_{33}\}$ – множество уязвимостей ($x_{31}$ – инженерно-технические, $x_{32}$ – организационно-правовые, $x_{33}$ – программно-аппаратные); $x_4 = \{x_{41}, x_{42}, x_{43}\}$ – множество контрмер ($x_{41}$ – существующие контрмеры, $x_{42}$ – необходимые контрмеры (снижающие риск до минимума), $x_{43}$ – достаточные контрмеры (снижающие риск до приемлемого уровня)). Множество методов управления риском обозначено как $Y = \{y_1, y_2, \dots, y_n\}$.

Предложен вектор критериев для выбора методов: $a(y_k) = [0,1]$ – согласованность оценок факторов риска по методу $y_k$; $b(y_k) = [0,1]$ – адекватность оценок факторов риска по методу $y_k$; $c(y_k) = [0,1]$ – адаптивность метода $y_k$ к качественным данным; $d(y_k) = [0,1]$ – субъективность оценки риска по методу $y_k$; $e(y_k) = [0,1]$ – неопределённость оценки риска по методу $y_k$; $k = 1, \dots, n$; $F = \begin{bmatrix} f_{11} & f_{12} & f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \\ f_{41} & f_{42} & f_{43} \end{bmatrix}$ – чувствительность риска, $f_{ij} = [0,1], i = \{1,2,3,4\}, j = \{1,2,3\}$ – показатели чувствительности риска.

Сформирована совокупность требований для выбора оптимальных методов управления информационными рисками:

$$\begin{cases} \sum_{i=1}^{4}\sum_{j=1}^{3} f_{ij} \times a(y_k) \times b(y_k) \times c(y_k) \to max, \\ \sum_{i=1}^{4}\sum_{j=1}^{3} f_{ij} \times d(y_k) \times e(y_k) \to min\,. \end{cases}$$

Показано, что соответствие методов критериям эффективности необходимо проверять на каждом этапе процесса управления информационными рисками. В результате получим $Y^* \epsilon Y$ – множество (набор) методов, используемых на разных этапах управления информационными рисками и удовлетворяющих соответствующим критериям.

Поставленная задача является слабоструктурированной, для её решения применён системный подход. В результате сформулированная задача представлена в виде взаимосвязанной совокупности задач меньшей трудоёмкости, которые решены в последующих главах диссертации.

**Во второй главе** разработана методика управления информационными рисками в СДМСО. Проведён сравнительный анализ эффективности структурно-функциональных и объектно-ориентированных методов исследования информационных потоков для идентификации факторов риска.

Сделан вывод о наибольшей эффективности (с точки зрения управления информационными рисками СДМСО) IDEF0-методологии структурно-функционального анализа, позволяющей разрабатывать 2 типа моделей: AS-IS («как есть» – для идентификации угроз, активов и уязвимостей) и TO-BE («как должно быть» – для идентификации контрмер).

Проанализирована структура факторов риска и выявлены подлежащие оценке составляющие: вероятностные компоненты реализации факторов риска предложено оценивать по статистическим данным, а силовые компоненты негативного воздействия – по созданной вербально-числовой шкале.

Разработан метод экспертного опроса, который соответствует трём критериям эффективности: согласованность оценок ($a(y_k)$), адекватность оценок ($b(y_k)$), чувствительность риска к различным факторам ($F$).

Оценка факторов риска выполняется следующим образом:

$$x_{ij1} = k_{ij1} \times p_{ij1} \times f_{ij1}; x_{ij2} = k_{ij2} \times p_{ij2} \times f_{ij2}; x_{ij3} = k_{ij3} \times p_{ij3} \times f_{ij3};$$

где $x_{ij1}$ – оценка угрозы, $k_{ij1} \in [0, 10]$ – мощность угрозы, $p_{ij1} \in [0, 1]$ – вероятность реализации угрозы, $f_{ij1} \in [0, 1]$ – чувствительность риска к оценке угрозы, $x_{ij2}$ – оценка потенциально возможного ущерба, $k_{ij2} \in [0, 10]$ – стоимость актива, $p_{ij2} \in [0, 1]$ – вероятность нанесения активу наивысшего ущерба, $f_{ij2} \in [0, 1]$ – чувствительность риска к оценке возможного ущерба, $x_{ij3}$ – оценка уязвимости, $k_{ij3} \in [0, 10]$ – степень уязвимости, $p_{ij3} \in [0, 1]$ – вероятность использования уязвимости, $f_{ij3} \in [0, 1]$ – чувствительность риска к оценке уязвимости, $i = \{1, 2, \dots, m\}$ – эксперты, выполняющие оценку, $j = \{1, 2, \dots, n\}$ – факторы из перечня.

Для обеспечения согласованности экспертных мнений разработан гибридный алгоритм отсеивания оценок с использованием коэффициента конкордации, основанный на вербально-числовых шкалах Марголина и Харрингтона. Вычисление итоговых значений угрозы ($x_1$), потенциально возможного ущерба ($x_2$) и уязвимости ($x_3$) на основе обработки оставшихся

после отсеивания экспертных оценок выполняется путём максимизации функции $F(x) = x_1 + x_2 + x_3 \rightarrow max$ с учётом ограничений в виде влияния всех факторов на уровень риска.

Выполнение требования адекватности оценок обеспечивается построением избыточной системы неравенств:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \leq b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \leq b_2 \ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + a_{m3}x_3 \leq b_m \end{cases}$$

где $x_1, x_2, x_3 \in [0, 10]$ – итоговые оценки уровня угрозы, ущерба и уязвимости, $a_{i1}, a_{i2}, a_{i3} \in \{0, 1, \ldots, m\}$ – число оставшихся у $i$-го эксперта оценок угроз, ущерба и уязвимостей, $b_i$ – сумма всех оценок $i$-го эксперта.

Обосновано сочетание нечёткой логики с нейросетевой технологией и предложена методика управления информационными рисками (Рис. 3).

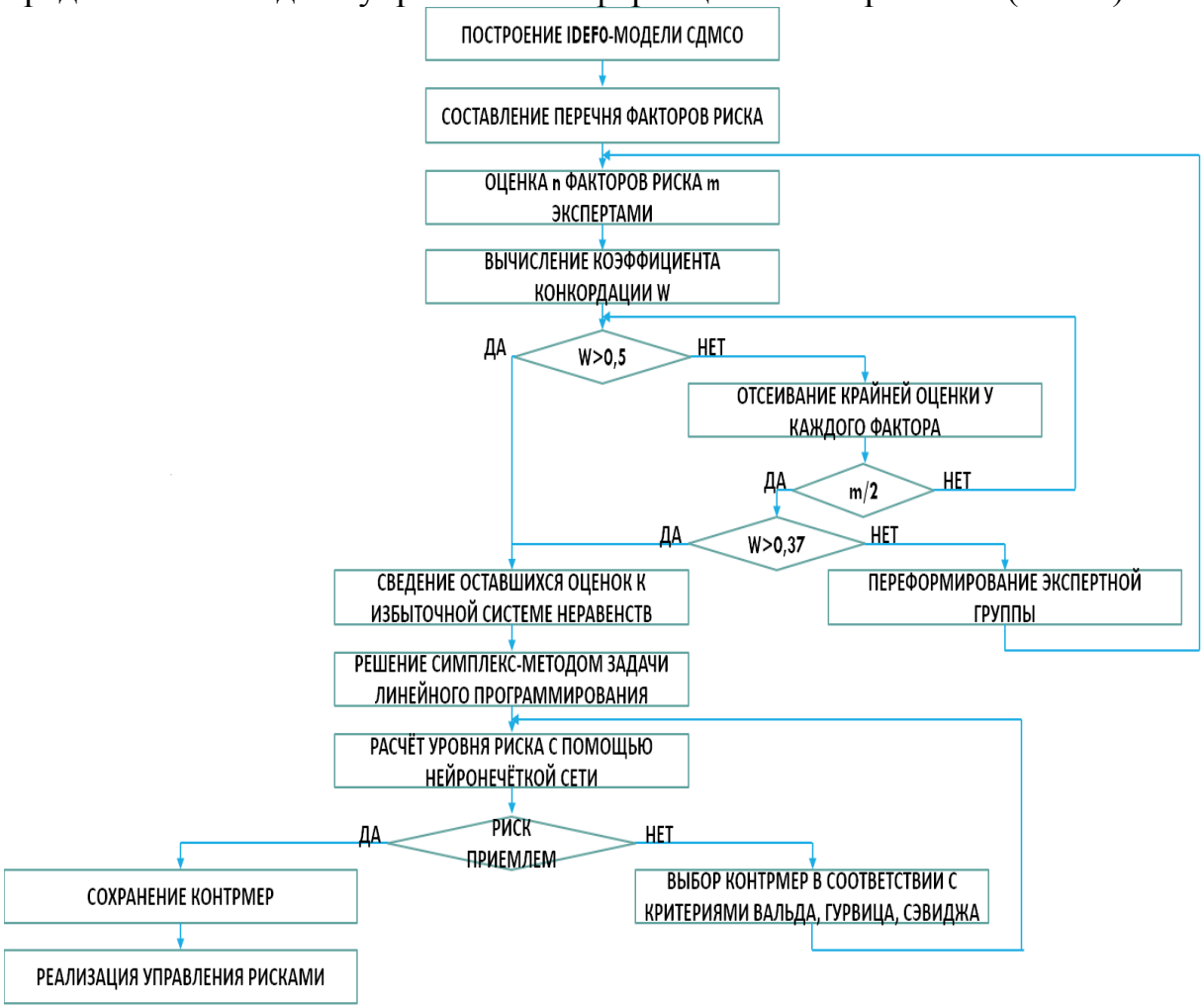


Рис. 3. Методика управления информационными рисками

**В третьей главе** разработаны методы и модели для реализации методики управления рисками, и обоснована их эффективность.

Сформирована совокупность принципов, в соответствии с которыми необходимо разрабатывать IDEF0-модель функционирования СДМСО для идентификации факторов риска и соответствующих контрмер.

Для оценки информационных рисков разработана нейронечёткая модель на основе нейронечеткой сети (ННС) со следующей конфигурацией:

1) структура – пятислойная ННС (фаззификация, агрегирование, активизация, аккумуляция, дефаззификация);

2) тип нечёткой модели – модель Такаги-Сугено-Канга (ТСК);

3) три входные переменные (угроза, ущерб, уязвимость), значения которых получены по разработанной методике экспертного опроса;

4) пять нечётких множеств входных переменных;

5) одна выходная переменная (**y**) – уровень риска;

6) девять значений выходной переменной;

7) конъюнкция: $T(A \wedge B) = T(A) \times T(B)$;

8) дизъюнкция: $T(A \vee B) = \mathrm{T(A)} + \mathrm{T(B)} - \mathrm{T(A)} \times \mathrm{T(B)}$;

9) дефаззификация – метод взвешенного среднего.

Обучение ННС (Рис. 4) основывается на минимизации целевой функции, которая вычисляется с применением евклидовой нормы:

$$E = \frac{1}{2}\sum_{k=1}^{p}(y(x^k) - d^k)^2,$$

где $d$ – значение риска в обучающих данных.

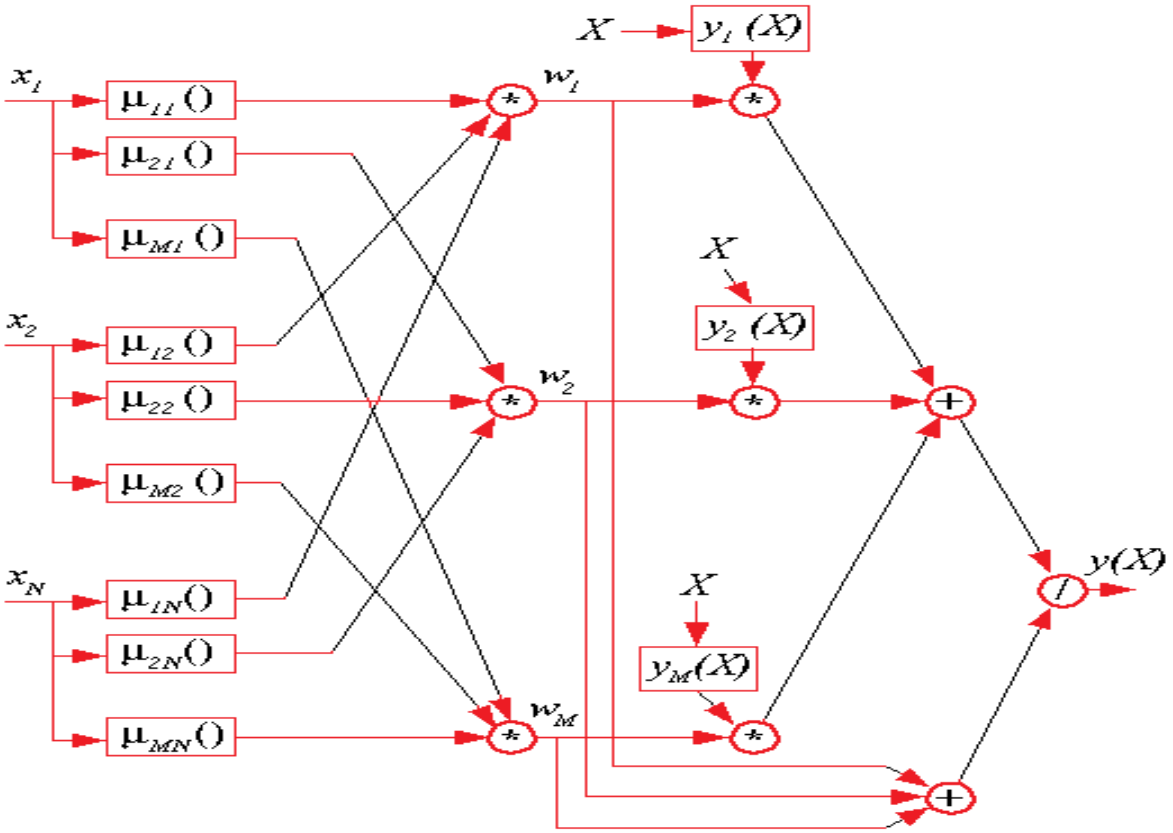


Рис. 4. Архитектура нейронечёткой сети

Для обучения использован двухэтапный (в соответствии с первым и третьим параметрическими слоями) алгоритм обратного распространения ошибки, вычисляемой по методу наименьших квадратов.

На первом этапе нелинейные характеристики известны. Выходной сигнал рассчитывается по формулам:

$$y(x) = \sum_{i=1}^{m} w'(p_{i0} + \sum_{j=1}^{n} p_{ij}x_j),$$

$$w' = v_i = \prod_{j=1}^{n} \frac{mu_{ij}(x_j)}{\sum_{l=1}^{m} \prod_{j=1}^{n} mu_{lj}(x_j)} = const.$$

Для $k$ выборок $< x^k, d^k >$ получается система $k$ линейных уравнений:

$$A \times P = D,$$

где $P = [p_{10}, p_{11}, \dots, p_{1n}, \dots, p_{m0}, p_{m1}, \dots, p_{mn}]^T$ – весовой вектор третьего слоя, $D = [d^1, d^2, \dots, d^k]^T$ – вектор, полученный на основе $k$ выборок.

Матрица $A$ выглядит следующим образом:

$$A = \begin{bmatrix} v_1^1\ v_1^1 \times x_1^1 \cdots v_1^1 \times x_n^1 & \cdots & v_m^1\ v_m^1 \times x_1^1 \cdots v_m^1 \times x_n^1 \\ \vdots & \ddots & \vdots \\ v_1^k\ v_1^k \times x_1^k \cdots v_1^k \times x_n^k & \cdots & v_m^k\ v_m^k \times x_1^k \cdots v_m^k \times x_n^k \end{bmatrix}$$

Решение этой системы линейных алгебраических уравнений может быть получено за один шаг следующим образом:

$$P = A^+ \times D,$$

где $A^+$ – псевдообратная матрица по отношению к матрице $A$.

На втором этапе известны показатели линейных характеристик третьего слоя и производится корректирование нелинейных характеристик первого слоя классическим методом убывания обратного градиента:

$$a_{ij}^{k+1} = a_{ij}^k - nu_a \frac{\partial E^k}{\partial a_{ij}^k},$$

$$b_{ij}^{k+1} = b_{ij}^k - nu_b \frac{\partial E^k}{\partial b_{ij}^k},$$

$$c_{ij}^{k+1} = c_{ij}^k - nu_c \frac{\partial E^k}{\partial c_{ij}^k},$$

где $k$ – цикл обучения, равный порядку выборки в онлайн-режиме.

На основе девяти изначально заданных значений выходной переменной разработана вербально-числовая шкала оценки риска, позволяющая интерпретировать уровень риска, получаемый на выходе ННС в виде числового показателя.

Разработан метод экспертного опроса по выбору контрмер для снижения риска на основе критериев теории игр – Вальда, Гурвица и Сэвиджа.

Каждому эксперту необходимо заполнить два экземпляра таблиц оценок влияния контрмер, предложенных в IDEF0-модели TO-BE, на факторы риска – для активных контрмер, влияющих на угрозы и ущерб, и для пассивных, влияющих на уязвимости и ущерб (Таблица 1).

Таблица 1.

Оценка влияния контрмер на факторы риска: матрица стратегий

| **Стоимость контрмер** | $b_1$ | $b_2$ | … | $b_n$ |
|---|---|---|---|---|
| $a_1 = v_1$ | $c_{11}$ | $c_{12}$ | … | $c_{1n}$ |
| $a_2 = v_2$ | $c_{21}$ | $c_{22}$ | … | $c_{2n}$ |
| … | … | … | … | … |
| $a_m = v_m$ | $c_{m1}$ | $c_{m2}$ | … | $c_{mn}$ |

Здесь $a_i$ – предложенные контрмеры, $b_j$ – факторы риска, $c_{ij} \in [0; 10]$ – влияние $i$-ой контрмеры на $j$-ый фактор, $v_i$ – стоимость $i$-ой контрмеры; $i = \{1, \dots, m\}$; $j = \{1, \dots, n\}$.

После выбора контрмеры $a_i$ в соответствии с любым из трёх критериев, в зависимости от экономической стратегии, $i$-ая строка удаляется из матрицы стратегий, после чего необходимо провести новый цикл. Контрмеры среди оставшихся выбираются до тех пор, пока их суммарная стоимость не превысит величину потенциально возможного ущерба: $\sum v \leq v_{\text{у}}$, где $\sum v$ – суммарная стоимость выбранных контрмер, $v_{\text{у}}$ – величина потенциально возможного ущерба (бюджет на реализацию контрмер).

Для пересчёта уровня остаточного риска с учётом выбранных контрмер, каждому эксперту необходимо вычесть свои оценки влияния контрмер на факторы риска из полученных им ранее оценок:

$$x^*_{ij1} = x_{ij1} - c_{ija},$$
$$x^*_{ij2} = x_{ij2} - c_{ija} - c_{ijp},$$
$$x^*_{ij3} = x_{ij3} - c_{ijp},$$

где $x^*_{ij1}$ – новая оценка угрозы; $x_{ij1}$ – старая оценка угрозы; $x^*_{ij2}$ – новая оценка ущерба; $x_{ij2}$ – старая оценка ущерба; $x^*_{ij3}$ – новая оценка уязвимости; $x_{ij3}$ – старая оценка уязвимости; $c_{ija}$ – оценка влияния активной контрмеры; $c_{ijp}$ – оценка влияния пассивной контрмеры.

Обновлённые оценки обрабатываются, как и первоначальные оценки, а три итоговых значения (обновлённого уровня угрозы, потенциально возможного ущерба и уязвимости) вновь подаются на вход ННС, которая вычисляет уровень остаточного риска. Если остаточный риск выше приемлемого, то необходимо добавлять/заменять контрмеры, повторяя цикл до тех пор, пока риск не станет допустимым.

**В четвёртой главе** разработанная методика апробирована на примере системы дистанционного мониторинга состояния человека (СДМСЧ).

Построена IDEF0-модель функционирования СДМСЧ, в которой выделены подсистемы структурирования данных, передачи данных, обработки данных, анализа данных и извлечения знаний.

В результате дальнейшей декомпозиции и анализа диаграмм IDEF0-модели AS-IS составлен перечень факторов риска (Таблица 2), оценённых в соответствии с разработанной методикой экспертного опроса.

Таблица 2.

Перечень факторов риска

| **УГРОЗЫ ИНФОРМАЦИИ** |
|---|
| 1. Несанкционированный доступ злоумышленника к информационным ресурсам СДМСЧ |
| 2. Нарушение конфиденциальности/целостности данных при их передаче с телемедицинских датчиков в облачное хранилище |
| 3. Нарушение доступности/целостности информации, находящейся в облачном хранилище |
| 4. Перегрузка трафика при передаче данных от web-сервера на сервер обработки |
| **ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ПОДВЕРЖЕННЫЕ УЩЕРБУ** |
| 5. Телемедицинские датчики пациента |
| 6. Компьютер/смартфон пациента |
| 7. Коммуникации между телемедицинскими датчиками/компьютером/смартфоном пациента и хранилищем |
| 8. Информационные ресурсы (подсистемы структурирования, обработки, анализа данных и извлечения знаний) |
| **УЯЗВИМОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ** |
| 9. Нарушение работоспособности клиентской части при временном отсутствии связи с сервером |
| 10. Отсутствие письменного согласия пациента на сбор и обработку его персональных данных |
| 11. Отсутствие распределённой, 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. Несвоевременность установки обновлений и исправлений клиентских модулей |

Сформированы 125 правил нечёткого вывода ЕСЛИ...ТО и в программном комплексе MATLAB реализована и обучена ННС, для которой обоснован вид входных функций принадлежности. Проведённый сравнительный анализ показал более высокую эффективность трапецеидальных функций, которые сохраняют локальные неровности в поверхности вывода, обеспечивая реакцию на крайние значения входных переменных, в отличие от колокола Гаусса, где абсолютно гладкая, монотонная и плоская поверхность

вывода приводит к вычислению риска как усреднённого значения входных переменных с учётом снижения порядка.

В результате обработки экспертных оценок факторов риска получены три входных значения для ННС: 1) угроза – 8,3 (очень высокая); 2) потенциально возможный ущерб – 6,3 (высокий); 3) уязвимость – 4,3 (средняя).

После подачи этих значений на вход ННС на выходе получен уровень риска – 0,627 (выше среднего): система может продолжать работу, но корректирующий план действий необходимо применить как можно быстрее.

В результате анализа диаграмм IDEF0-модели TO-BE составлен перечень контрмер (Таблица 3), оценённых в соответствии с разработанным методом на основе критериев теории игр.

Таблица 3.

Перечень контрмер

| |
|---|
| 1. Использование надёжных телемедицинских датчиков, ограничивающих доступ злоумышленника к ещё не зашифрованным данным и защищающих информацию от случайных искажений при физических контактах пациента с другими лицами |
| 2. Шифрование данных, передаваемых с телемедицинских датчиков пациента в облачное хранилище, на основе морфологических особенностей биосигналов пациента |
| 3. Получение согласия пациента на сбор и обработку его персональных данных с помощью цифрового документа, подписанного электронной подписью |
| 4. Хранение информации в формате XML и применение CALS-технологий для информационной совместимости при обмене данными |
| 5. Применение XML-СУБД Sedna, обладающей собственной политикой безопасности, для единого управления и обеспечения целостности хранимой информации |
| 6. Распределение прав и синхронизация доступа к данным на основе RBAC – ролевой модели разграничения и управления правами пользователей |
| 7. Сжатие архивных данных для снижения расхода дисковой памяти и сетевого трафика |
| 8. Ведение открытого протокола взаимодействия Sedna Client-Server Protocol с целью отслеживания действий клиентов в произвольный момент времени для выявления потенциальных нарушителей |
| 9. Автоматическая установка обновлений и исправлений клиентской части с помощью модуля XUpdate |
| 10. Использование 64-разрядного диспетчера памяти, адресации и подкачки для сохранения работоспособности клиентской части в случае временной потери связи с сервером |

В результате оценки факторов риска с учётом внедрения выбранных контрмер получены три входных значения для оценки остаточного риска с

помощью ННС: 1) угроза – 1,68 (очень низкая); 2) потенциально возможный ущерб – 1,7 (очень низкий); 3) уязвимость – 0,68 (очень низкая).

После подачи новых значений на вход ННС на выходе получен уровень остаточного риска – 0,165 (очень низкий).

**В заключении** диссертации сформулированы основные результаты, полученные при выполнении работы.

## ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В работе предложены, разработаны и успешно апробированы методы и модели для управления рисками, повышающие эффективность в соответствии с заданными критериями. Получены следующие результаты:

1. Впервые с позиций системного анализа дано формализованное описание и поставлена задача управления информационными рисками в СДМСО;

2. Сформулирован вектор критериев эффективности для обоснования методов и моделей управления информационными рисками в СДМСО: согласованность, адекватность оценок, адаптивность к качественным данным, снижение субъективности, неопределённость и чувствительность риска;

3. Разработан метод идентификации факторов риска на основе построения IDEF0-модели анализируемой системы. Перечень угроз, активов, которым может быть нанесён ущерб, и уязвимостей составляется с помощью модели AS-IS, перечень контрмер – с помощью модели TO-BE;

4. Разработан метод экспертного опроса для оценки факторов риска с применением гибридного отсеивания оценок, основанного на вычислении коэффициента конкордации и вербально-числовых шкалах Марголина и Харрингтона, для повышения согласованности экспертных мнений, с последующим сведением оценок к задаче линейного программирования, решаемой симплекс-методом, для повышения адекватности оценок;

5. Проведён сравнительный анализ методов машинного обучения, мягких вычислений и гибридных моделей по четырём оставшимся критериям эффективности. Сделан вывод о наибольшей эффективности нейронечётких сетей для оценки риска по значениям его факторов;

6. Проведён сравнительный анализ функций принадлежности в виде трапеций и колокола Гаусса, который показал более высокую эффективность трапецеидальных функций, где локальные неровности поверхности вывода обеспечивают реакцию на крайние значения входных переменных, в отличие от колокола Гаусса, где гладкая поверхность вывода приводит к вычислению риска как усреднённого значения входных переменных;

7. Разработана и реализована в среде MATLAB пятислойная нейронечёткая сеть на основе ТСК-модели с трапецеидальными входными функциями принадлежности, рассчитывающая уровень риска по трём входным переменным – угроза, потенциально возможный ущерб, уязвимость;

8. Разработан метод обеспечения экономической эффективности внедрения контрмер для снижения уровня риска на основе выбора стратегии принятия решения в соответствии с критериями теории игр;

9. Создана оригинальная методика управления информационными рисками в СДМСО, обеспечивающая оптимальный выбор методов и моделей на основе сформулированных критериев эффективности;

10. Выполнена апробация предложенной методики управления информационными рисками для системы дистанционного мониторинга состояния человека в медицинском центре «Столица» (г. Москва).

## ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ


1. Булдакова Т.И., Миков Д.А. Обеспечение согласованности и адекватности оценки факторов информационного риска // Вопросы кибербезопасности. 2017. №3 (21). С. 8-15.

2. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде MATLAB // Вопросы кибербезопасности. 2015. №4 (12). С. 53-61.

3. Булдакова Т.И., Миков Д.А. Методика анализа информационных рисков с применением нейро-нечёткой сети // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2015. №4. С. 13-17.

4. Булдакова Т.И., Миков Д.А. Анализ информационных процессов виртуального центра охраны здоровья // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2014. №2. С. 10-20.

5. Булдакова Т.И., Миков Д.А. Оценка информационных рисков в автоматизированных системах с помощью нейро-нечёткой модели // Наука и образование: электронное научно-техническое издание. 2013. №11. С. 295-310.

6. Булдакова Т.И., Суятинов С.И., Миков Д.А. Анализ информационных рисков виртуальных инфраструктур здравоохранения // Информационное общество. 2013. №4. С. 6.

7. Булдакова Т.И., Миков Д.А. Исследование сложных процессов и систем. – М.: Изд-во МГТУ имени Н.Э. Баумана, 2018. 48 с.

8. Миков Д.А. Выявление факторов информационного риска в телемедицинской системе // Политехнический молодёжный журнал. 2016. №3. С. 3.

9. Миков Д.А. Способы повышения эффективности анализа рисков информационной безопасности // Современные тенденции развития науки и технологий. 2016. №1-1. С. 75-79.

10. Миков Д.А. Применение нейронечётких моделей в области анализа рисков информационной безопасности // Математические методы в технике и технологиях – ММТТ. 2015. №7. С. 169-174.

11. Миков Д.А. Анализ методов изучения потоков данных для оценки рисков информационной безопасности // Ежемесячный научный журнал Prospero. 2014. №7. С. 28-33.

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

13. Миков Д.А. Основные этапы оценки информационных рисков и способы их реализации // Теоретические и прикладные аспекты современной науки. 2014. №5-3. С. 103-106.

14. Миков Д.А. Разработка нейронечёткой сети для анализа информационных рисков // Молодёжный научно-технический вестник. 2014. №10. С. 28.

15. Миков Д.А. Управление информационными рисками с использованием экспертного опроса. Германия, Саарбрюккен: LAP LAMBERT Academic Publishing, 2013. 83 с.

16. Миков Д.А. Нейронечёткий подход к оценке рисков информационной безопасности в виртуальном здравоохранении // Безопасные информационные технологии: Труды Всероссийской конференции. МГТУ им. Н.Э. Баумана. 2013. С. 99-102.

17. Миков Д.А. Риск-менеджмент информационной безопасности // Молодёжный научно-технический вестник. 2013. №12. С. 40.

18. Миков Д.А. Построение IDEF0-модели виртуального центра охраны здоровья // Молодёжный научно-технический вестник. 2013. №9. С. 37.

19. Миков Д.А. Применение IDEF0-методики для анализа информационных потоков // Новые направления развития приборостроения: Материалы 6-й Международной научно-технической конференции. Минск. 2013. С. 344.

20. Миков Д.А. Вопросы информационной безопасности в концепции виртуального здравоохранения // Безопасные информационные технологии: Труды Всероссийской конференции. МГТУ им. Н.Э. Баумана. 2012. С. 120-122.

21. Булдакова Т.И., Миков Д.А. Метод повышения адекватности оценок информационных рисков // Инженерный журнал: наука и инновации. 2012. №3 (3). С. 36.

22. Булдакова Т.И., Миков Д.А. Анализ методов оценки информационных рисков // Безопасные информационные технологии: Труды Всероссийской конференции. МГТУ им. Н.Э. Баумана. 2011. С. 120-122.

МИКОВ ДМИТРИЙ АЛЕКСАНДРОВИЧ

**УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ РИСКАМИ В СИСТЕМАХ ДИСТАНЦИОННОГО МОНИТОРИНГА СОСТОЯНИЯ ОБЪЕКТА**

Автореферат
Корректор

Подписано в печать _____ Формат 60x84 1/16

Бум. офсет. Усл. печ. л. 1.0 Уч.-изд. л. 1.0

Тираж 100 экз. Заказ 200 Бесплатно

Московский государственный технический университет имени Н.Э. Баумана
105005, г. Москва, ул. 2-я Бауманская, 5

Отпечатано в Издательстве МГТУ им. Н.Э. Баумана, 105005, г. Москва, ул. 2-я Бауманская, д. 5