

УДК 004.05

О. М. Романова (Князева), К.Н. Кургузкин

**РАЗРАБОТКА КОНЦЕПТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ  
ДЛЯ МЕТОДИКИ ОЦЕНКИ КАЧЕСТВА ИНФОРМАЦИОННЫХ  
СИСТЕМ «РЕВИЗОР»**

*ФГПУ ВПО Астраханский государственный университет,  
Астрахань, Россия*

*В статье рассмотрена проблема оценки качества информационных систем (ИС) организаций. Отмечено, что наиболее перспективными в области оценки и управления уровнем качества ИС являются подходы, основанные на использовании ISO 9000 в качестве методологической базы. К таким методикам можно отнести методику «Ревизор», разработанную И.М. Ажмухамедовым и О.М. Романовой. Для данной методики является актуальной задача разработки алгоритма и соответствующего программного обеспечения (ПО), реализующего сбор и обработку экспертных данных. Решению данной проблемы и посвящена статья. Для методики «Ревизор» были выделены этапы, на которых осуществляется сбор экспертных данных: определение функций ИС; определение подсистем ИС; определение элементов множеств концептов нечетких когнитивных моделей оценки качества ИС; определение связей между концептами нечетких когнитивных моделей оценки качества ИС; формирование базы знаний для оценки текущего уровня качества ИС, состоящей из нечетких продукционных правил, определяющих влияние каждого уровня повреждений иерархии повреждений на сервисы информационной безопасности; оценка состояния концептов нечетких когнитивных моделей оценки качества ИС, которые являются входными параметрами алгоритмов методики «Ревизор». Отмечено, что на этапах 4-6 необходимо использовать методы опроса, которые бы позволили исключить влияние остальных членов экспертной комиссии на мнение каждого из экспертов. В итоге для решения поставленной задачи был выбран метод онлайн-анкетирования. Систему сбора мнений экспертов было предложено разработать в формате веб-портала. Для него был разработан алгоритм работы, обозначены роли пользователей, определена структура анкет для опрашиваемых.*

**Ключевые слова:** информационная безопасность, оценка качества, инфраструктура, разработка программного обеспечения, информационная система, лицо принимающее решение, экспертная оценка.

**Введение.** Успешное функционирование организации зависит от эффективности и прозрачности управления ею. Успех, в том числе, достигается в результате внедрения и поддержания в рабочем состоянии информационных систем (ИС), эксплуатируемых в компании. Таким образом, вопрос использования «качественных» (удовлетворяющих требованиям лица, принимающего решения (ЛПР)) ИС является одним из важнейших для любой организации [1].

Поддержание ИС на должном уровне качества сводится к периодическому последовательному выполнению этапов:

1. Определение требуемого уровня качества ИС;

2. Оценка уровня качества ИС;
3. Выработка управляющих решений по выводу оцененного уровня качества ИС на требуемый (при несоответствии оцененного уровня качества ИС требуемому).

Наиболее перспективными в области оценки и управления уровнем качества ИС являются подходы, основанные на использовании ISO 9000 в качестве методологической базы. Это связано с общемировой тенденцией к стандартизации и сертификации в области управления качеством в целом, связанной с принятием данных стандартов, в которых не только приведено общее определение термина «Качество объекта», но и описаны классы показателей, влияющих на него.

К таким методикам оценки и управления качеством ИС можно отнести методику «Ревизор», изложенную в [2], к достоинствам которой можно отнести:

1. возможность применения методики, как на этапе внедрения, так и на этапе эксплуатации ИС;
2. возможность учета, как количественных, так и качественных показателей качества ИС, путем использования аппарата нечеткой логики и нечеткого когнитивного моделирования;
3. разделение уровня качества ИС на текущий (оцененный в текущий момент времени) и «событийно-прогнозный» (определяющий уровень качества системы при наступлении потенциальных угроз), что делает оценку более точной и пр.

Для сбора экспертных данных в методике предлагается использовать проведение совещаний. Достоинством такого метода является простота его реализации. Однако на совещании может быть принято ошибочное мнение одного из участников в силу его авторитета, служебного положения, настойчивости или ораторских способностей, что на некоторых этапах реализации методики оценки качества ИС совершенно неприемлемо. Также не было предложено отсутствуют решения по автоматизации сбора и обработки экспертных данных, что приводит к большим временным и финансовым затратам на реализацию данного этапа.

Таким образом, разработка алгоритма и соответствующего программного обеспечения (ПО), реализующего сбор и обработку экспертных данных в рамках методики «Ревизор», является актуальной задачей, решению которой и посвящена данная работа.

**Решение задачи.** Сбор экспертных данных осуществляется на следующих этапах методики оценки качества ИС:

1. Определение функций ИС.
2. Определение подсистем ИС.
3. Определение элементов множеств концептов нечетких когнитивных моделей оценки качества ИС (Рисунок 1):

- a. средства защиты ИС (СЗИ) -  $Z_{\{1,2,3,\dots\}}$
  - b. угрозы ИС  $UG_{\{1,2,3,\dots\}}$
  - c. уязвимости ИС  $UZ_{\{1,2,3,\dots\}}$
  - d. атаки на ИС  $A_{\{1,2,3,\dots\}}$
  - e. повреждения элементов системы  $Des_{\{1,2,3,\dots\}}$
4. Определение связей между концептами нечетких когнитивных моделей оценки качества ИС.
  5. Формирование базы знаний для оценки текущего уровня качества ИС, состоящей из нечетких продукционных правил, определяющих влияние каждого уровня повреждений иерархии повреждений (Рисунок 2) на сервисы информационной безопасности.
  6. Оценка состояния концептов нечетких когнитивных моделей оценки качества ИС, которые являются входными параметрами алгоритмов методики «Ревизор» [3].

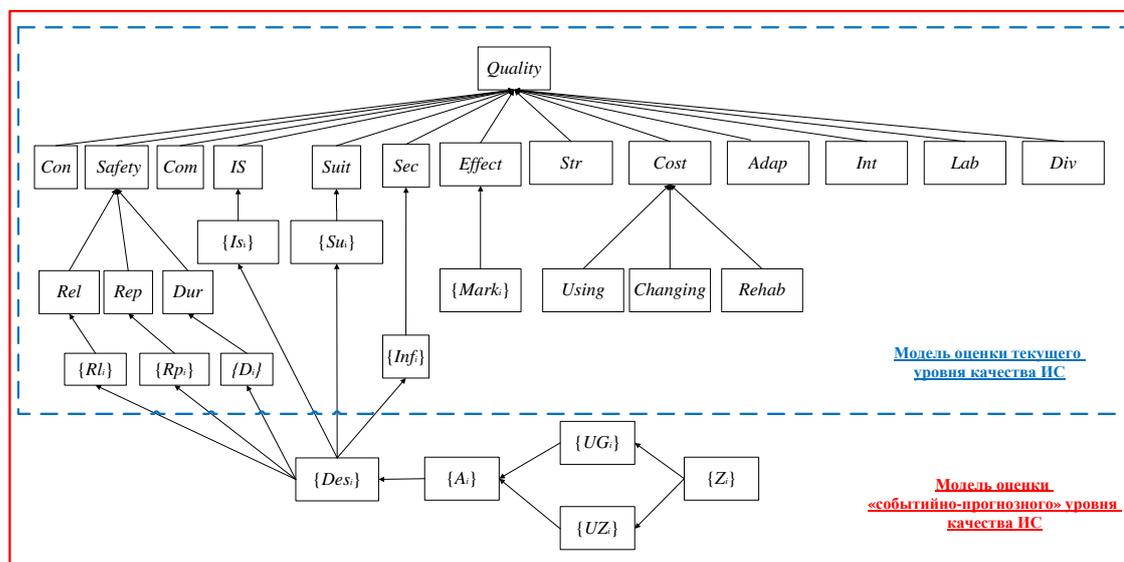


Рисунок 1 - Нечеткие когнитивные модели оценки качества ИС

На этапах 1-3 целесообразно использовать стандартные коллективные методы сбора экспертных данных, такие как «проведение совещания» или «мозговой штурм», поскольку в них необходимо лишь составить списки элементов (множество концептов, функций ИС, подсистем ИС). Этапы же 4-6 более сложные: на них необходимо вербально оценить влияние показателей друг на друга.

Для этого в методике «Ревизор» введена лингвистическая переменная «Уровень фактора» и терм-множество ее значений QL. Оно состоит из 9 элементов, принадлежащих отрицательной и положительной областям оценок: QL = {Высокий отрицательный (В-); Выше среднего отрицательный (ВС-); Средний отрицательный (С-); Низкий

отрицательный (Н-); Нулевой (0); Низкий положительный (Н+); Средний положительный (С+); Выше среднего положительный (ВС+); Высокий положительный (В+)}.



Рисунок 2 - Иерархия повреждений

В качестве семейства функций принадлежности для QL предложено использовать девятиуровневый классификатор, в котором функциями принадлежности нечетких чисел (НЧ), заданных на отрезке  $[-1,1]$  (обозначаемым как R), являются трапеции:

$$\{B^-( -1; -1; -0,85; -0,75 ); BC^-( -0,85; -0,75; -0,65; -0,55 ); C^-( -0,65; -0,55; -0,45; -0,35 ); H^-( -0,45; -0,35; -0,25; -0,15 ); \langle 0 \rangle ( -0,25; -0,15; 0,15; 0,25 ); H^+( 0,15; 0,25; 0,35; 0,45 ); C^+( 0,35; 0,45; 0,55; 0,65 ); BC^+( 0,55; 0,65; 0,75; 0,85 ); B^+( 0,75; 0,85; 1 )\}, \quad (1)$$

где в нечётком числе (НЧ)  $(a_1, a_2, a_3, a_4)$   $a_1$  и  $a_4$  – абсциссы нижнего основания,  $a_2$  и  $a_3$  – абсциссы верхнего основания трапеции. В случае четкого числа  $a_1=a_2=a_3=a_4$ . Отрицательная часть классификатора используется для нахождения отклонений полученных оценок от требуемых.

Используемый классификатор осуществляет проекцию нечеткого лингвистического описания на отрезок  $[-1; 1]$ , при этом делает это непротиворечивым способом, симметрично располагая узлы

классификации. В этих узлах значение соответствующей функции принадлежности равно единице, а всех остальных функций – нулю. Неуверенность эксперта в классификации убывает (возрастает) линейно с удалением от узла (с приближением к узлу, соответственно). Применение классификатора позволяет перейти от качественного описания уровня параметра к стандартному количественному виду соответствующей функции принадлежности из множества нечетких трапецеидальных чисел.

Таким образом, на этапах 4-6 необходимо использовать методы опроса, которые бы позволили исключить влияние остальных членов экспертной комиссии на мнение каждого из экспертов.

Для решения поставленной задачи целесообразно использовать метод онлайн-анкетирования, который обладает следующими преимуществами:

1. Возможность получения информации от большого количества людей за короткий промежуток времени.
2. Отсутствие влияния на мнение эксперта других членов группы.
3. Возможность для эксперта обдумывать вопрос необходимое для него время.
4. Возможность вернуться к предыдущим вопросам и изменить свой ответ на них.
5. Возможность осуществления компьютерной обработки информации и пр.

Систему сбора мнений экспертов было предложено разработать в формате веб-портала. Для работы с Интернет-ресурсом предусматривается два вида ролей пользователей: эксперт и лицо, принимающее решение (ЛПР). Вход в систему будет происходить с помощью процедур идентификации и аутентификации. В качестве идентификатора используется уникальный логин пользователя, а в качестве аутентификатора - пароль. При этом в системе настраивается процедура аудита над основными событиями, такими как вход или выход из системы, добавление (удаление, изменение) записей в таблицах и т.п.

Общий алгоритм работы с порталом будет выглядеть следующим образом:

Предварительный этап оценки качества ИС:

1. ЛПР заполняет множества концептов нечетких когнитивных моделей оценки качества ИС; определяет какие множества могут влиять друг на друга (например, что множество  $\{Uz_i\}$  влияет на  $\{UG_i\}$ ).
2. ЛПР вносит данные об элементах иерархии повреждений (наименование повреждения, уровень (ступень) иерархии которому принадлежит повреждение, критический уровень «узлового повреждения»). Данная информация будет

использована для формирования базы знаний для оценки текущего уровня информационной безопасности ИС (подробное описание методики оценки текущего уровня качества изложено в [4]).

3. Эксперты определяют коэффициенты влияния концептов нечетких моделей друг на друга.
4. Эксперты заполняют базу знаний для оценки текущего уровня информационной безопасности ИС (формируют правые части нечетких продукционных правил).
5. Собранные экспертные данные обрабатываются: определяется степень согласованности мнений экспертов; формируется итоговое значение оцениваемых показателей и параметров.

Этапы агрегирования данных о требуемом уровне качества ИС и оценки качества ИС:

1. Лица, принимающие решения, оценивают состояния концептов нечетких когнитивных моделей, которые являются входными параметрами алгоритмов методики «Ревизор».
2. Собранные данные обрабатываются: определяется степень согласованности мнений ЛПР; формируется итоговое значение оцениваемых показателей и параметров.

При оценке влияния концептов нечетких когнитивных моделей друг на друга экспертам предлагается ответить на вопросы вида:

1. Заполните в таблице коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) частных мер и средств защиты информации «Мера<sub>1</sub>», «Мера<sub>2</sub>» ... на комплексное средство защиты информации «Комплексное средство защиты информации» (Таблица 1).

Таблица 1 – Комплексное средство защиты информации

	Мера <sub>1</sub>	Мера <sub>2</sub>	...
Комплексное средство защиты информации			

2. Выберите из списка какие меры и средства защиты информации влияют на угрозу «Угроза<sub>1</sub>». Расставьте коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) каждой меры и средства защиты информации на угрозу (Таблица 2).

Таблица 2 – Комплексное средство защиты информации

Средства и меры защиты информации	Коэффициенты влияния на «Угроза <sub>1</sub> »
СЗИ <sub>1</sub>	
СЗИ <sub>2</sub>	
СЗИ <sub>3</sub>	
СЗИ <sub>n</sub>	

3. Выберите из списка какие меры и средства защиты информации влияют уязвимость «Уязвимость<sub>1</sub>». Расставьте коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) каждой меры и средства защиты информации на уязвимость (Таблица 3).

Таблица 3 – Влияние на уязвимость

Средства и меры защиты информации	Коэффициенты влияния на «Уязвимость <sub>1</sub> »
СЗИ <sub>1</sub>	
СЗИ <sub>2</sub>	
СЗИ <sub>3</sub>	
СЗИ <sub>n</sub>	

4. Выберите из списка через какие уязвимости может реализовываться угроза «Угроза<sub>1</sub>» (Таблица 4).

5. Выберите из списка какие атаки приводят к повреждению «Повреждение<sub>1</sub>». Оцените степень влияния  $pwr_i \in QL$  атак на «Повреждение<sub>1</sub>» (Таблица 5).

Таблица 4 – Возможность реализации угрозы

Уязвимости	Возможность реализации угрозы «Угроза <sub>1</sub> »
Уязвимость <sub>1</sub>	
Уязвимость <sub>2</sub>	
Уязвимость <sub>3</sub>	
Уязвимость <sub>n</sub>	

Таблица 5 – Возможность появления повреждения

Атаки	Возможность появления повреждения «Повреждение <sub>1</sub> »
Атака <sub>1</sub>	
Атака <sub>2</sub>	
Атака <sub>3</sub>	
Атака <sub>n</sub>	

6. Выберите из списка какие повреждения влияют на сервис информационной безопасности «Сервис<sub>1</sub>». Оцените степень влияния  $int_i \in QL$  повреждений на «Сервис<sub>1</sub>» (Таблица 6).

Таблица 6 – Влияние повреждения на сервис

Повреждения	Влияние повреждения на «Сервис <sub>1</sub> »
Повреждение <sub>1</sub>	
Повреждение <sub>2</sub>	
Повреждение <sub>3</sub>	
Повреждение <sub>n</sub>	

7. Выберите из списка какие повреждения влияют на уровень безотказности ИС по функции «Функция<sub>1</sub>». Оцените степень влияния  $int_i \in QI$  повреждений на уровень безотказности ИС по функции «Функция<sub>1</sub>» (Таблица 7).

8. Выберите из списка какие повреждения влияют на уровень долговечности ИС по подсистеме «Подсистема<sub>1</sub>». Оцените степень влияния  $int_i \in QI$  повреждений на уровень долговечности ИС по подсистеме «Подсистема<sub>1</sub>» (Таблица 8).

Таблица 7 – Влияние повреждения на уровень безотказности

Повреждения	Влияние повреждения на уровень безотказности ИС по функции «Функция <sub>1</sub> »
Повреждение <sub>1</sub>	
Повреждение <sub>2</sub>	
Повреждение <sub>3</sub>	
Повреждение <sub>n</sub>	

Таблица 8 – Влияние повреждения на уровень ремонтпригодности

Повреждения	Влияние повреждения на уровень ремонтпригодности ИС по подсистеме «Подсистема <sub>1</sub> »
Повреждение <sub>1</sub>	
Повреждение <sub>2</sub>	
Повреждение <sub>3</sub>	
Повреждение <sub>n</sub>	

9. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) показателей безотказности по каждой функции ИС, на безотказности ИС в целом (Таблица 9).

Таблица 9 – Влияние повреждения на безотказность ИС в целом

	Безотказность по функции 1	Безотказность по функции 2	...
Безотказность			

10. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) показателей ремонтпригодности по каждой функции ИС, на ремонтпригодность ИС в целом (Таблица 10).

11. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) показателей долговечности по каждой подсистеме ИС, на долговечность ИС в целом (Таблица 11).

Таблица 10 – Влияние на ремонтпригодность ИС в целом

	Ремонтпригодность по функции 1	Ремонтпригодность по функции 2	...
Ремонтпригодность			

Таблица 11 – Влияние на долговечность ИС в целом

	Долговечность по подсистеме 1	Долговечность по подсистеме 2	...
Долговечность			

12. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) ремонтпригодности, долговечности, безотказности на надежность ИС (Таблица 12).

Таблица 12 – Влияние на надежность ИС

	Ремонтпригодность	Долговечность	Безотказность
Надежность ИС			

13. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) сервисов ИБ на уровень информационной безопасности ИС (Таблица 13).

Таблица 13 – Влияние на ИБ

	«Сервис <sub>1</sub> »	«Сервис <sub>2</sub> »	...
Уровень информационной безопасности ИС			

14. Выберите из списка какие повреждения влияют на уровень валидности ИС по функции «Функция<sub>1</sub>». Оцените степень влияния  $int_i \in QI$  повреждений на уровень валидности ИС по функции «Функция<sub>1</sub>».

15. Определите коэффициенты влияния  $\alpha_i$  ( $\alpha_i \in [0; 1]$ ;  $\sum \alpha_i = 1$ ) показателей валидности по каждой функции ИС, на валидность ИС в целом (Таблица 15).

Таблица 14 – Влияние повреждений на уровень валидности

Повреждения	Влияние повреждения на уровень валидности ИС по функции «Функция <sub>1</sub> »
Повреждение 1	
Повреждение 2	
Повреждение 3	
Повреждение n	

Таблица 15 – Влияние на валидность ИС в целом

	Валидность по функции 1	Валидность по функции 2	...
Валидность			

16. Определите коэффициенты влияния  $\alpha_i$  показателей социально-экономического эффекта от эксплуатации ИС «Показатель<sub>1</sub>», «Показатель<sub>2</sub>», ... на общий социально-экономический эффект от эксплуатации ИС (Таблица 16).

17. Определите коэффициенты влияния  $int_i \in QI$  негативных воздействий на здоровье персонала, эксплуатирующих ИС «Показатель<sub>1</sub>», «Показатель<sub>2</sub>», ... на уровень безопасности ИС для персонала (Таблица 17).

Таблица 16 – Влияние на общий социально-экономический эффект

	«Показатель <sub>1</sub> »	«Показатель <sub>2</sub> »	...
Социально-экономический эффект от эксплуатации ИС			

Таблица 17 – Влияние на уровень безопасности персонала

	«Показатель <sub>1</sub> »	«Показатель <sub>2</sub> »	...
Уровень безопасности ИС для персонала			

18. Выберите из списка какие повреждения влияют на негативное воздействие на здоровье персонала, эксплуатирующих ИС «Негативное воздействие<sub>1</sub>». Оцените степень влияния  $int_i \in QI$  повреждений на «Негативное воздействие<sub>1</sub>» (Таблица 18).

При формировании базы знаний для оценки текущего уровня информационной безопасности ИС экспертам необходимо ответить на вопросы вида [5]:

1. Заполните правую часть нечеткого продукционного правила:  
 Если («Повреждение<sub>1</sub>» = «Уровень повреждения») То («Степень уверенности эксперта» (Сервис ИБ «Сервис<sub>1</sub>» = «Уровень сервиса»)
2. Оцените критические уровни узловых повреждений иерархии повреждений (Таблица 19).

Таблица 18 – Влияние повреждения на негативные воздействия

Повреждения	Влияние повреждения на «Негативное воздействие <sub>1</sub> »
Повреждение <sub>1</sub>	
Повреждение <sub>2</sub>	
Повреждение <sub>3</sub>	
Повреждение <sub>n</sub>	

Таблица 19 - Критические уровни иерархии повреждений

Повреждение	Критический уровень
Повреждения ОС рабочих станций	
Повреждение локальных программ рабочих станций	
Повреждения серверной части пользовательского ПО	
Повреждения элементов обработки данных серверов	
Повреждения жестких дисков серверов	

Таблица 29 - Критические уровни иерархии повреждений

Повреждение	Критический уровень
Повреждения жестких дисков рабочих станций	

Таблица 39 - Продолжение

Повреждение	Критический уровень
Повреждения ОС серверов	
Повреждения элементов обработки данных рабочих станций	
Повреждение клиентской части пользовательского ПО	

При оценке состояния концептов нечетких когнитивных моделей, которые являются входными параметрами алгоритмов методики «Ревизор», экспертам задаются вопросы вида:

1. Оцените уровень концептов из множества «Множество<sub>1</sub>» (Таблица 20):

Таблица 20 – Уровень концептов

Концепты	Уровень концепта
Концепт1	
Концепт2	
Концепт3	
Концепт <sub>n</sub>	

2. Оцените уровень текущих повреждений ИС.

Таблица 21 - Нулевой уровень иерархии повреждений

Повреждение	Уровень
Повреждения инженерно-технических средств (мер) защиты информации	
Повреждение аппаратных средств (мер) защиты информации	
Повреждение организационно-правовых средств (мер) защиты информации	
Повреждение носителей с резервными копиями данных	
Повреждения элементов обработки данных серверов	
Повреждение каналов передачи данных	
Повреждения жестких дисков серверов	
Повреждения жестких дисков рабочих станций	
Повреждения элементов обработки данных рабочих станций	

Таблица 22 - Первый уровень иерархии повреждений

Повреждение	Уровень
Повреждения ОС рабочих станций	
Повреждения ОС серверов	

Таблица 23 - Второй уровень иерархии повреждений

Повреждение	Уровень
Повреждение локальных программ рабочих станций	
Повреждения серверной части пользовательского ПО	
Повреждение программ резервного копирования, установленных на серверах	

Таблица 23 - Продолжение

Повреждение	Уровень
Повреждение программ мониторинга и аудита, установленных на рабочих станциях	
Повреждения криптографических программ, установленных на рабочих станциях	
Повреждение программ защиты от НСД, установленных на серверах	
Повреждение программ мониторинга и аудита, установленных на серверах	
Повреждение программ защиты от НСД, установленных на рабочих станциях	
Повреждение криптографических программ, установленных на серверах	
Повреждение программ резервного копирования данных, установленных на рабочих станциях	
Повреждение клиентской части пользовательского ПО	

Таблица 24 - Третий уровень иерархии повреждений

Повреждение	Уровень
Повреждение файлов на рабочих станциях	
Повреждение файлов на серверах	

При этом должны быть исключены из рассмотрения повреждения, оценка которых невозможна из-за влияния узловых повреждений, уровень которых выше критического.

**Заключение.** Таким образом, для методики оценки качества ИС «Ревизор» были подобраны следующие методы сбора экспертной информации:

1. для этапов определения функций, подсистем ИС; формирования множеств концептов НКМ – методы проведения совещаний и мозгового штурма;
2. для этапов определения связей между концептами НКМ, формирования базы знаний для оценки текущего уровня качества ИС, оценки состояния концептов нечетких когнитивных моделей оценки качества ИС – метод «онлайн-анкетирование».

«Онлайн-анкетирование» предложено организовать при помощи создания веб-ресурса, для успешного функционирования которого в работе предложен общий алгоритм и форматы вопросов для экспертов.

Это позволяет после разработки методов оценки согласованности мнений экспертов, учитывающих нечеткость производимых оценок, приступить к созданию веб-приложения по сбору и обработке экспертной информации для методики «Ревизор».

## ЛИТЕРАТУРА

1. Князева О.М. Управление качеством информационных систем на основе процессного подхода // Прикаспийский журнал: управление и высокие технологии. 2016, № 2, С. 36-47.
2. О. М. Князева, Н. Н. Мустафаева. Методика оценки качества систем обработки данных вуза // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2018, С. 69-79.
3. Ажмухамедов И.М., Князева О.М. Комплексный критерий оценки качества информационных систем // Актуальные проблемы гуманитарных и естественных наук. 2017, № 4-6, С. 14-17.
4. Ажмухамедов И.М., Князева О.М., Большакова Л.В. Оценка уровня информационной безопасности финансовых учреждений // Современные проблемы науки и образования. 2015, №1.
5. Ажмухамедов И.М., Князева О.М. Унификация подходов к управлению уровнем информационной безопасности в организациях различного профиля // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. 2015, №1, С. 66-77.

O. M. Romanova (Knyazeva), K.N. Kurguzkin

## DEVELOPMENT OF THE SOFTWARE CONCEPT OF THE TECHNIQUE OF ASSESSMENT OF QUALITY OF INFORMATION SYSTEMS "INSPECTOR"

*FSBEI HO Astrakhan State University, Astrakhan, Russia*

*The article considers the problem of assessing the quality of information systems (IS) of organizations. It was observed, that the most promising approaches in the field of IS quality assessment and management based on ISO 9000. The method "Inspector" which was developed by I.M. Azhmukhamedov and O.M. Romanova refers to such methods. The task of developing an algorithm and software that collects and processes expert data is actual. The article is devoted to the solution of this problem. The stages were identified in which experts data are collected for the "Inspector": definition of IS functions; definition of IS subsystems; definition of elements of sets of concepts of fuzzy cognitive models of IS quality assessment; identification of links between the concepts of fuzzy cognitive models of IS quality assessment; formation of a knowledge base for assessing the current level of IS quality, consisting of fuzzy logic rules that determine the impact of each damage's level of the damage hierarchy on information security services; condition assessment of concepts of fuzzy cognitive models of an estimation of quality of IS, which are input parameters of algorithms of a method "Inspector". It is noted that at stage four-six it is necessary to use methods that excludes the influence of other experts on the opinion of one expert. As a result, the method of online questioning was chosen to solve the problem. It was suggested that the system is required in the form of a web portal. The algorithm of work was developed. The roles of portal users were identified. The structure of the portal form was defined.*

**Keywords:** information security, quality assessment, infrastructure, software development, information system, decision maker, expert evaluation.

### REFERENCES

1. Knyazeva O.M. Upravlenie kachestvom informacionnyh sistem na osnove processnogo podhoda // Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii. 2016, № 2, S. 36-47.
2. O. M. Knyazeva, N. N. Mustafaeva. Metodika ocenki kachestva sistem obrabotki dannyh vuza // Vestnik Astrahanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika. 2018, S. 69-79.
3. Azhmuhamedov I.M., Knyazeva O.M. Kompleksnyj kriterij ocenki kachestva informacionnyh sistem // Aktual'nye problemy gumanitarnyh i estestvennyh nauk. 2017, № 4-6, S. 14-17.
4. Azhmuhamedov I.M., Knyazeva O.M., Bol'shakova L.V. Ocenka urovnya informacionnoj bezopasnosti finansovyh uchrezhdenij // Sovremennye problemy nauki i obrazovaniya. 2015, №1.
5. Azhmuhamedov I.M., Knyazeva O.M. Unifikaciya podhodov k upravleniyu urovnem informacionnoj bezopasnosti v organizacijah razlichnogo profilya // Vestnik AGTU. Ser.: Upravlenie, vychislitel'naya tekhnika i informatika. 2015, №1, S. 66-77