DOI: 10.24143/2072-9502-2017-2-69-79
УДК 004.05

О. М. Князева, Н. Н. Мустафаева

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА СИСТЕМ ОБРАБОТКИ ДАННЫХ ВУЗА

Предложено адаптировать и использовать разработанную ранее методику «Ревизор» для оценки уровня качества систем обработки данных вузов. Входящие в методику нечеткие когнитивные модели определения требуемого, оценки текущего и «прогнозного» уровней качества систем обработки данных, а также соответствующие им алгоритмы позволяют на основе экспертной информации проводить оценку на этапе проектирования и эксплуатации системы. Использование при этом комплексного критерия оценки качества позволяет повысить информативность оценки, что, в свою очередь, повышает эффективность управления качеством систем обработки данных. Адаптация методики под особенности функционирования вузов заключается в определении основных функций оцениваемых систем обработки данных; определении элементов множеств концептов нечетких когнитивных моделей, применяемых в методике; оценке наличия связей между концептами нечетких когнитивных моделей; заполнении базы знаний, необходимой для оценки текущего уровня информационной безопасности системы обработки данных. Методика была апробирована в одном из ведущих вузов Поволжья для оценки системы обработки данных «Деканат». Для адаптации методики и непосредственной оценки качества системы обработки данных была собрана экспертная комиссия, состоящая из сотрудников ИТ-отделов вуза, преподавателей профильных кафедр университета, работников деканата. Работа комиссии была организована путем проведения совещаний. Обсуждение каждого вопроса длилось до принятия экспертами согласованного решения. На основе данных, полученных в результате применения методики, были сформированы и реализованы меры по повышению качества системы «Деканат» до уровня «Выше среднего». По результатам апробации методика «Ревизор» рекомендуется для оценки качества систем обработки данных вузов.

Ключевые слова: системы обработки данных, качество систем, критерий оценки качества, надежность систем обработки данных, информационная безопасность, нечеткое когнитивное моделирование.

Введение

Системы обработки данных (СОД) стали неотъемлемой частью высших учебных заведений. Информатизация находит свое место и в управлении персоналом, и в сервисном облуживании: создаются локально-вычислительные сети, в которых циркулирует служебная информация, внедряются собственные почтовые, FTP-серверы, автоматизируется процесс приемки заявок отделами по техническому облуживанию, внедряются методы удаленного администрирования. Автоматизация работы структурных подразделений вуза позволяет сократить время, затрачиваемое на выполнение сопровождающих задач (создание ведомостей, учебных планов, рабочих программ, учет посещаемости, создание расписаний и т. д.), уменьшить количество ошибок, связанных с человеческим фактором, оптимизировать процесс принятия решений руководством вуза и др. [1–3]. При этом СОД должна отвечать различным и, в общем случае, противоречивым требованиям: быть надежной, обеспечивать защиту обрабатываемой информации, быть недорогой в эксплуатации и т. д. Согласно ГОСТ ISO 9000-2011, степень соответствия характеристик СОД тем требованиям, которые установило лицо, принимающее решения (ЛПР), образует качество системы. Однако оценка качества СОД осложняется наличием у вуза как объекта информатизации специфических особенностей:

– большое количество СОД, внедренных для решения различных задач, а также обрабатываемой информации, связанной не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками;

– территориальная разрозненность СОД, связанная с наличием в вузе филиалов и корпусов, между которыми должно быть настроено информационное взаимодействие;

– непостоянная аудитория (меняющийся контингент студентов, абитуриентов и других посетителей вуза).

Использование в высших учебных заведениях СОД несоответствующего, «низкого» качества, связанного в том числе с невыполнением требований по защите обрабатываемой информации, приводит к существенному снижению эффективности работы структурных подразделений вуза, снижению лояльности сотрудников, формированию негативного имиджа заведения и пр. В связи с этим оценка качества СОД для высших учебных заведений является актуальной задачей.

С учетом вышесказанного нами была сформулирована цель исследования: подобрать методику оценки качества СОД и адаптировать ее с учетом особенностей функционирования вузов.

Состояние проблемы

Исследованиям в области оценки и управления качеством СОД посвящено большое количество работ российских и зарубежных авторов. Разработаны общие принципы, методы и методологии оценки и управления качеством для отдельных видов систем (например, [4, 5]). Имеются исследования, посвященные разработке универсальных методик оценки качества (например, [6, 7]). Ряд работ посвящен отдельным составляющим показателя «Качество информационной системы»: информационной безопасности (например, [8, 9]); надежности (например, [10]); социально-экономическому эффекту (например, [11, 12]).

Однако существующие подходы не в полной мере учитывают слабую формализуемость процесса оценки. К их недостаткам относится также несоответствие мировой тенденции к стандартизации в области управления качеством в целом, связанной с принятием стандартов серии ISO 9000, в которых не только приведено общее определение термина «Качество объекта», но и описаны классы показателей, влияющих на него. Вводимые авторами работ [4–12] составляющие качества либо полностью не соответствуют данным классам, либо не охватывают особо значимые из них (например, связанные с информационной безопасностью, здоровьем персонала и пр.). Решения, полностью посвященные оценке отдельных показателей, также имеют свои недостатки. Например, существующие методики оценки уровня информационной безопасности не соответствуют ГОСТ Р ИСО/МЭК 27000 в части обеспечения непрерывности процесса управления информационной безопасностью. На основе информации, полученной в результате применения данных методик, затруднительно проводить целенаправленные мероприятия по повышению уровня информационной безопасности.

От указанных недостатков свободна методика оценки качества СОД, получившая название «Ревизор» [13–16]. Методика позволяет проводить оценку качества СОД на различных этапах ее жизненного цикла на основе экспертных данных и вырабатывать управляющие решения по повышению качества СОД.

Подход к оценке качества СОД на основе вычисления ключевых показателей качества системы по каждой функции СОД, предложенный в рамках методики «Ревизор» [13–16], а также выделение информационной безопасности в отдельную независимую функцию системы позволяют применять методику для оценки качества СОД в организациях различных отраслей. Однако для этого она должна быть адаптирована к их особенностям. Должны быть определены основные функции оцениваемой СОД (это необходимо для оценки валидности и надежности СОД); определены элементы множеств концептов нечетких когнитивных моделей (НКМ), применяемых в методике (например, перечень актуальных угроз для СОД, уязвимостей системы); оценены связи между концептами НКМ; заполнены базы знаний, необходимые для оценки текущего уровня информационной безопасности СОД.

Основные положения методики «Ревизор»

Для решения задачи оценки качества СОД в методике «Ревизор» использован аппарат нечеткого когнитивного моделирования. Для формализации оценок отдельных составляющих качества введена лингвистическая переменная «Уровень фактора» и терм-множество ее значений *QL*, состоящее из 9 элементов, принадлежащих отрицательной и положительной области 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 ($В^+$)}. В качестве семейства функций принадлежности для *QL* предложено использовать девятиуровневый классификатор, в котором функциями принадлежности нечетких чисел (НЧ), заданных на отрезке [–1, 1] ϵ *R*, являются трапеции:

$$\{B^-(-1; -1; -0{,}85; -0{,}75);\ BC^-(-0{,}85; -0{,}75; -0{,}65; -0{,}55);\ C^-(-0{,}65; -0{,}55; -0{,}45; -0{,}35);$$

$$H^-(-0{,}45; -0{,}35; -0{,}25; -0{,}15);\ «0»(-0{,}25; -0{,}15; 0{,}15; 0{,}25);\ H^+(0{,}15; 0{,}25; 0{,}35; 0{,}45);$$

$$C^+(0{,}35; 0{,}45; 0{,}55; 0{,}65);\ BC^+(0{,}55; 0{,}65; 0{,}75; 0{,}85);\ B^+(0{,}75; 0{,}85; 1)\},$$

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

В основу методики положен комплексный критерий оценки качества СОД, отражающий совокупное влияние различных групп показателей, которые соответствуют характеристикам качества, приведенным в стандартах серии ГОСТ ISO 9000 [17]:

$$Quality = \alpha_1 \cdot Safety + \alpha_2 \cdot Effect + \alpha_3 \cdot Inv(Cost) + \alpha_4 \cdot Sec + \alpha_5 \cdot Adap + \alpha_6 \cdot Int +$$
$$+ \alpha_7 \cdot Con + \alpha_8 \cdot Inv(Com) + \alpha_9 \cdot Str + \alpha_{10} \cdot Lab + \alpha_{11} \cdot Div + \alpha_{12} \cdot Suit + \alpha_{13} \cdot IS, \qquad (1)$$

где $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6, \alpha_7, \alpha_8, \alpha_9, \alpha_{10}, \alpha_{11}, \alpha_{12}, \alpha_{13}\ \hat{I}\ [0; 1]$ – соответственно коэффициенты влияния надежности (*Safety*), социально-экономического эффекта (*Effect*), затрат на владение (*Cost*), безопасности для персонала (*Sec*), адаптивности (*Adap*), интегрируемости (*Int*), целостности (*Con*), сложности (*Com*), структурированности (*Str*), лабильности (*Lab*), делимости (*Div*), валидности (*Suit*), информационной безопасности (*IS*) СОД на уровень качества (*Quality*).

Методика включает следующие шаги: формирование требуемого, оценка «прогнозного» и текущего уровня качества и информационной безопасности СОД. Каждая из перечисленных процедур преследует различные цели, проводится на различных этапах жизненного цикла СОД и предполагает использование разных входных данных.

На этапе проектирования/модернизации системы проводится формирование требуемого и оценка «прогнозного» уровня качества и информационной безопасности СОД. На этапе эксплуатации СОД проводится оценка «прогнозного» и текущего уровня качества СОД.

Структура НКМ, используемых для указанных оценок качества СОД, имеет вид $IS = <G, L, S, R, \Omega>$, где G – ориентированный граф, не содержащий горизонтальных ребер в пределах одного уровня иерархии (рис. 1); L – лингвистическая переменная, формализующая качественные (вербальные) оценки каждого фактора в графе; S – множество весов ребер графа G, отражающих степень влияния концептов на заданный элемент следующего уровня иерархии; R – набор правил для вычисления значений концептов на каждом из уровней иерархии G; Ω – индекс схожести [18], позволяющий распознавать лингвистические значения концептов.

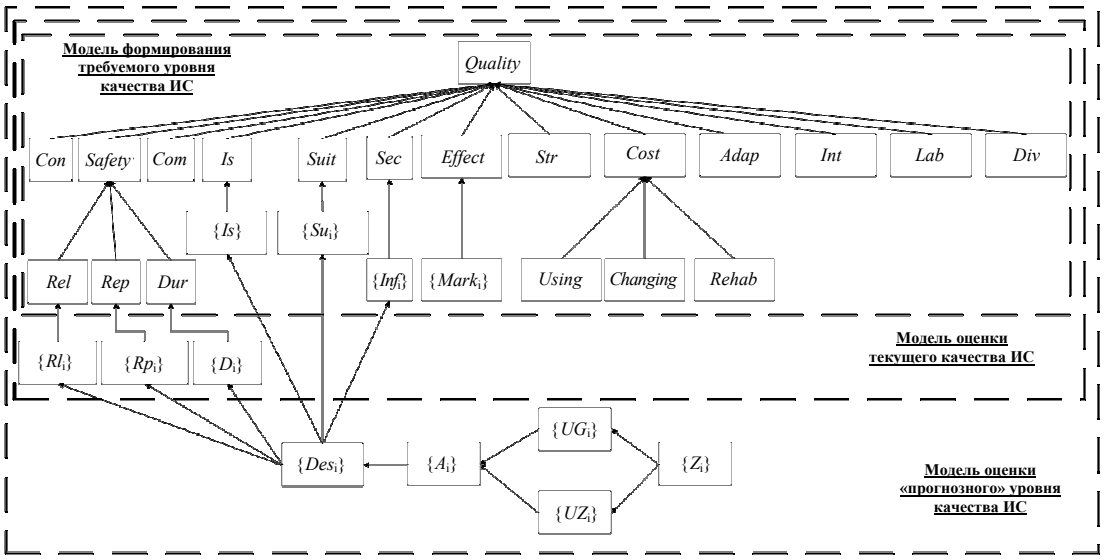

Рис. 1. Граф G: ИС – информационная система

На самом высоком (нулевом) слое графа G находится показатель *Quality* – качество СОД, на первом – показатели, образующие комплексный критерий оценки качества, приведенные в формуле (1). Валидность системы определяется по каждой функции СОД $Su_{\{1,\,2,\,3\,\ldots\}}$. Социально-экономический эффект (уровень 1) СОД определяется через финансовые, организационные, социальные и другие показатели эксплуатации СОД.

Затраты на владение СОД включают в себя эксплуатационные затраты – *Using*; затраты на восстановление/ремонт – *Rehab*; затраты на модификацию – *Changing*. Уровень надежности определяется через показатели безотказности – *Rel,* ремонтопригодности – *Rep* и долговечности – *Dur* системы. Уровень безотказности и ремонтопригодности определяется для каждой функции СОД $Rl_{\{1,\,2,\,3,\,\ldots\}}$, $Rp_{\{1,\,2,\,3,\,\ldots\}}$. Долговечность СОД определяется по среднему сроку службы каждой подсистемы СОД $\{D_i\}$. Безопасность СОД для персонала определяется возможными негативными воздействиями «поврежденной» СОД на психическое и (или) физическое здоровье сотрудников – $Inf_{\{1,\,2,\,3,\,\ldots\}}$. Информационная безопасность определяется способностью СОД обеспечивать сервисы информационной безопасности $Is_{\{1,\,2,\,3,\,\ldots\}}$. Четвертый слой графа G представлен повреждениями элементов системы $Des_{\{1,\,2,\,3,\,\ldots\}}$, которые образуются в результате атак на информационные активы $A_{\{1,\,2,\,3,\,\ldots\}}$. Атаки являются результатом реализации угроз СОД $UG_{\{1,\,2,\,3,\,\ldots\}}$ через уязвимости СОД $UZ_{\{1,\,2,\,3,\,\ldots\}}$ (6-й слой графа G). Седьмой слой графа G представлен средствами защиты информации (СЗИ) $Z_{\{1,\,2,\,3,\,\ldots\}}$.

Для формирования требуемого уровня качества СОД предложен следующий алгоритм.

1. Задать требуемый уровень показателей безотказности, ремонтопригодности, долговечности для каждой функции СОД, нормировать их к интервалу [0; 1] и вычислить результирующие значения данных показателей для системы в целом. Например, уровень безотказности вычисляется по формуле

$$Rel = \sum_{i=1}^{n} \alpha_i \cdot Rl_i, \tag{2}$$

где Rl_i – уровень безотказности СОД по i-й функции, представляющий собой аддитивную свертку частных показателей безотказности, приведенных к интервалу [0; 1]; α_i – коэффициент влияния Rl_i на Rel.

2. Вычислить уровень надежности СОД как аддитивную свертку частных критериев.

3. Задать требуемый уровень информационной безопасности, валидности, безопасности СОД для персонала в терминах лингвистической переменной «Уровень фактора».

4. Вычислить требуемый уровень социально-экономического эффекта от эксплуатации СОД на основе заданных значений его составляющих.

5. Рассчитать допустимый уровень затрат на владение СОД.

6. Задать требуемый уровень адаптивности, интегрируемости, лабильности, делимости СОД, общесистемных показателей СОД.

7. Вычислить требуемый уровень качества СОД.

Для оценки «прогнозного» уровня качества СОД необходимо:

1. Оценить состояние СЗИ.

Если Z_i представляет собой комплекс отдельных мер, то ЛПР задает лингвистическую оценку z_j^i, входящих в Z_i. Состояние Z_i в этом случае определяется на основе следующих правил:

$$\begin{cases} Z_i = \min\limits_j \{z_j^i\}, \text{ если } \{z_j^i\} \text{ действуют одновременно (параллельно)}, \\ Z_i = \prod\limits_{j=1}^{M} \{z_j^i\}^{\alpha_i}, \text{ если } \{z_j^i\} \text{ действуют последовательно, образуя рубежи защиты}, \end{cases}$$

где Z_i – текущее значение, отражающее состояние i-й «*комплексной*» меры; z_j^i – j-я мера, входящая в i-ю «*комплексную*» меру; M – количество z_j^i, образующих Z_i; $\alpha_j \in [0;\,1]$ – коэффициент влияния z_j на Z_i.

Если же Z_i не представляется возможным рассматривать как совокупность отдельных мер, то ЛПР задает лингвистическую оценку непосредственно Z_i.

2. Вычислить уровни опасности угроз, уязвимостей, «разрушительности» атак, повреждений элементов СОД и СЗИ и уровня информационной безопасности в целом.

3. Вычислить уровень безотказности, ремонтопригодности, долговечности и надежности СОД по формуле (2) с заменой требуемых значений показателей на фактические.

4. Вычислить уровень валидности и безопасности СОД для персонала.

5. Вычислить показатели социально-экономического эффекта от эксплуатации СОД и уровня затрат на владение СОД.

6. Оценить уровень адаптивности и интегрируемости СОД.

7. Вычислить «прогнозный» уровень качества СОД.

После оценки «прогнозного» уровня качества СОД ЛПР принимает решение о целесообразности его повышения. Решение формируется на основе расчета величины абсолютного отклонения Δ:

$$\Delta = Quality_p - Quality,$$

где $Quality$ – оцененный уровень качества СОД; $Quality_p$ – требуемый уровень.

Величина Δ является нечетким числом. Чтобы привести ее к количественному виду $\Delta_д$, необходимо провести процедуру дефаззификации. Для этого предлагается использовать метод центра тяжести, который заключается в расчете центроида трапеции: $\Delta_д = s_1 / s_2$, где $s_1 = \int_{a_1}^{a_4} x\mu(x)dx$, $s_2 = \int_{a_1}^{a_4} \mu(x)dx$; $\Delta_д$ – результат дефаззификации; a_1 и a_4 – абсциссы нижнего основания НЧ; $\mu(x)$ – его функция принадлежности. Если величина отклонения находится в недопустимых, по мнению ЛПР, пределах, то принимается решение по повышению качества СОД. Управляющие воздействия вырабатываются путем имитационного моделирования, в процессе которого управляемые концепты модели подбираются таким образом, чтобы обеспечить достижение целевого уровня качества системы.

Оценка текущего уровня качества СОД включает в себя оценку текущего уровня информационной безопасности, валидности, надежности системы; оценку текущего уровня затрат на владение и вычисление текущего уровня социально-экономического эффекта от эксплуатации СОД; вычисление текущего уровня безопасности для персонала; оценку текущего уровня адаптивности, интегрируемости, лабильности, делимости, общесистемных показателей; вычисление текущего уровня качества СОД.

Следует отметить, что значения показателей вычисляются аналогично соответствующим параметрам алгоритма оценки «прогнозного» уровня качества системы. Решение о соответствии текущего уровня качества требуемому, так же как и «прогнозного», принимается на основе расчета величины абсолютного отклонения.

Адаптация методики «Ревизор» для оценки качества систем обработки данных вуза

В вузах можно выделить значительное количество СОД, предназначенных для автоматизации рабочих мест сотрудников структурных подразделений: приемная комиссия; деканаты; кафедры; учебно-методический отдел; бухгалтерия; отдел кадров; профсоюзный комитет и пр. [19]. Поскольку, как было сказано ранее, данные системы выполняют различные функции, часто территориально распределены и имеют свой специфический набор программного обеспечения, необходимо проводить оценку качества для каждой из них по отдельности.

Рассмотрим адаптацию методики «Ревизор» на примере СОД «Деканат» одного из ведущих вузов Поволжья.

Деканат является одним из важнейших структурных подразделений вуза. Для применения методики «Ревизор» прежде всего были разработаны рекомендации по формированию и работе экспертной комиссии:

1. Формирование экспертной группы.

Экспертная группа должна иметь минимально необходимую с практической точки зрения численность для быстрого и эффективного использования ресурсов (как временных, так и материальных). В качестве экспертов рекомендуется привлекать специалистов, деятельность которых связана с обработкой информации в системе, а также специалистов, имеющих квалификацию и опыт работы в области применения информационных технологий и (или) в области защиты информации. Для оценки финансовых и экономических показателей функционирования СОД в экспертную группу могут быть включены представители таких подразделений, как бухгалтерия и (или) экономический отдел.

При привлечении в качестве экспертов специалистов от подразделений по защите информации и обслуживанию ИТ-инфраструктуры организации рекомендуется отдавать предпочтение лицам, имеющим высшее образование или имеющим не менее трех лет стажа практической работы в сфере своей деятельности.

Если информационную систему организации обслуживает аутсорсинговая компания, необходимо в экспертную комиссию включить тех ее специалистов, которые оказывали ИТ-услуги организации в течение последнего года.

Эксперты должны обладать независимостью, основанной на отсутствии коммерческого и финансового интереса или другого давления, которое может оказать влияние на принимаемые решения. Не рекомендуется формировать экспертную группу из участников, находящихся в прямом подчинении, т. к. это может негативным образом повлиять на результат определения угроз безопасности информации.

2. Проведение экспертной оценки.

Эксперты привлекаются для решения следующих задач:

– определение множества концептов НКМ и связей между ними;

– оценка текущих уровней показателей качества (состояния СЗИ, повреждений информационной системы, текущих затрат на содержание системы и пр.).

Сбор данных рекомендуется осуществлять путем проведения совещания. Обсуждение каждого вопроса должно длиться до принятия экспертами по нему согласованного решения. Группе должен быть предоставлен раздаточный материал с вопросами, на которые им предстоит ответить. Вопросы должны быть четкими, однозначно трактуемыми и должны предполагать однозначные ответы. Вопросы, которые предполагают оценку связей между концептами НКМ, целесообразно представлять в виде таблиц (рис. 2, 3).

Условное обозначение меры защиты	**Наименование меры защиты**	**Условное обозначение уязвимости**		
		UZ_1	…	UZ_m
		Наименование уязвимости	…	**Наименование уязвимости**
Z_1	Наименование	Ранг влияния	…	Ранг влияния
…	…	…	…	…
Z_n	Наименование	Ранг влияния	…	Ранг влияния

Рис. 2. Структура таблицы, отражающей влияние $\{Z_i\}$ на $\{UZ_j\}$

Условное обозначение меры защиты	**Наименование меры защиты**	**Номер угрозы**		
		UG_1	…	UG_m
		Наименование угрозы	…	**Наименование угрозы**
Z_1	Наименование	Ранг влияния	…	Ранг влияния
…	…	…	…	…
Z_n	Наименование	Ранг влияния	…	Ранг влияния

Рис. 3. Структура таблицы, отражающей влияние $\{Z_i\}$ на $\{UG_j\}$

С учетом данных рекомендаций в состав комиссии вошли сотрудники ИТ-отделов вуза, преподаватели профильных кафедр университета, работники деканата. Основные задачи, которые были поставлены перед комиссией: определение состава НКМ, заполнение базы знаний, формирование входных данных для методики «Ревизор».

Обсуждение каждого вопроса длилось до принятия экспертами согласованного решения.

В частности, комиссия выявила основные функции системы «Деканат»: планирование учебного процесса (формирование и учет учебных планов и рабочих учебных планов; создание, хранение и обработка графиков учебного процесса и пр.); расчет и распределение нагрузки; хра-

нение и обработка сведений о контингенте студентов вуза; учет успеваемости и посещаемости. Эксперты установили, что все функции одинаково важны для работы подразделения.

Наиболее сложной задачей было определение множества угроз и уязвимостей. При ее решении эксперты опирались на банк данных угроз и уязвимостей безопасности информации, разработанный Федеральным автономным учреждением «Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю» (ФАУ «ГНИИИ ПТЗИ ФСТЭК России»).

В перечень угроз и уязвимостей, характерных для СОД «Деканат», вошли:

а) угрозы:

– угроза внедрения вредоносного кода или данных;

– угроза воздействия на программы с высокими привилегиями;

– угроза восстановления аутентификационной информации;

– угроза доступа к защищаемым файлам с использованием обходного пути;

– угроза доступа/перехвата/изменения HTTP-cookies;

– угроза заражения DNS-кеша;

– угроза изменения компонентов системы;

– угроза изменения режимов работы аппаратных элементов компьютера;

– угроза некорректного использования функционала программного обеспечения;

– угроза неправомерных действий в каналах связи;

– угроза несанкционированного доступа к аутентификационной информации;

– угроза несанкционированного копирования защищаемой информации;

– угроза несанкционированного создания учётной записи пользователя;

– угроза несанкционированного удаления защищаемой информации;

– угроза определения топологии вычислительной сети;

– угроза подмены доверенного пользователя;

– угроза несанкционированной модификации защищаемой информации;

– угроза подмены программного обеспечения;

б) уязвимости:

– использование серверными процессами ragent.exe, rmngr.exe, rhost.exe одного и того же модуля rtrsrvc.dll для работы с TCP-соединением;

– использование серверными процессами ragent.exe, rmngr.exe, rhost.exe одного и тот же модуля core82.dll;

– ненадежность декодера Fast Infoset библиотеки для работы с XML-документами (xml2.dll);

– уязвимость браузера Opera, позволяющая злоумышленнику выполнить произвольный код при двойном нажатии на всплывающее окно;

– уязвимость браузера Firefox, позволяющая злоумышленнику выполнить межсайтовый скриптинг;

– уязвимость текстового редактора Microsoft Word, которая появляется при преобразовании документов в бинарный формат в конвертере форматов файла;

– уязвимость текстового редактора Microsoft Word, связанная с переполнением буфера обмена;

– уязвимость библиотеки sxs.dll браузера Google Chrome;

– передача незашифрованных данных по протоколу telnet в операционной системе Windows и пр.

Далее экспертами была произведена непосредственно оценка качества СОД «Деканат».

Безотказность было решено определять средней наработкой СОД до отказа. Ее текущее значение для всех функций СОД составило 11 месяцев. Путем нормирования данного значения по величине максимально приемлемой наработки системы до отказа (12 месяцев) были вычислены значения $Rl_1 = Rl_2 = Rl_3 = Rl_4$ = НЧ(0,92; 0,92; 0,92; 0,92). Поскольку все функции СОД являются равнозначными, то безотказность *Rel* = НЧ(0,92; 0,92; 0,92; 0,92). Для оценки ремонтопригодности было рассчитано среднее время восстановления способности СОД после отказа для выполнения ее функций – 8 часов. Путем нормирования данного значения по максимально допустимому времени ремонта информационной системы (24 часа) были вычислены значения $Rp_1 = Rp_2 = Rp_3 = Rp_4$ = НЧ(0,33; 0,33; 0,33; 0,33). Таким образом, уровень ремонтопригодности *Rep* = НЧ(0,33; 0,33; 0,33; 0,33). Средний срок службы информационной системы составляет 7 лет. Путем нормирования данного значения по максимальному сроку службы информационной системы (10 лет) был вычислен уровень долговечности *Dur* = НЧ(0,75; 0,75; 0,75; 0,75). Поскольку для компании безот-

казность, ремонтопригодность, долговечность одинаково важны, то значения их весовых коэффициентов влияния на показатель надежности равны и составляют 1/3. Таким образом, текущий уровень *Safety* составил 1/3 · 0,93 + 1/3 · 0,33 + 1/3 · 0,75 = НЧ(0,67; 0,67; 0,67; 0,67).

Далее экспертами были вербально оценены как «Средние» текущие уровни валидности, адаптивности, интегрируемости, лабильности, делимости. Затраты на владение информационной системой были оценены как НЧ(0,3; 0,3; 0,3; 0,3) (отношение текущих затрат к максимальным затратам, которые может позволить себе компания – 0,3), социально-экономический эффект от эксплуатации – как НЧ(0,5; 0,5; 0,5; 0,5), безопасность для персонала – «Выше среднего», значения общесистемных показателей – как «Средние». На основе экспертных данных о состоянии текущих повреждений информационной системы был вычислен текущий уровень информационной безопасности – «Выше среднего».

В результате текущий уровень качества СОД, вычисленный по формуле (1), оказался равным НЧ, которое можно отнести к категории «Средний» с индексом схожести $\Omega = 0,63$ и к категории «Выше среднего» с $\Omega = 0,39$. Значение «прогнозного» уровня качества оказалось равным НЧ, которое можно отнести к категории «Средний» с индексом схожести $\Omega = 0,8$. Данный результат определила недостаточная квалификация персонала учебного заведения в вопросах информационной безопасности и устаревший регламент управления инцидентами в СОД.

Для повышения уровня качества в системе «Деканат» были предложены меры по улучшению общесистемных показателей СОД, а также ее валидности, адаптивности, интегрируемости, лабильности, делимости (удаление неиспользуемого, нецелевого, устаревшего программного обеспечения; создание общих каталогов для пользователей СОД, обновление специализированного программного обеспечения до актуальных версий и пр.), а также по улучшению системы защиты информации (формирование нового регламента управления инцидентами в СОД, проведение тренингов для сотрудников деканата по вопросам защиты информации).

Реализация этих мер позволила повысить «прогнозные» и текущие уровни качества (в том числе и информационной безопасности) до значений «Выше среднего».

Выводы

Таким образом, результаты апробации методики «Ревизор» в отдельно взятом университете показали ее применимость для оценки качества СОД вузов. В дальнейшем планируется разработать программное обеспечение для автоматизации процесса оценки, а также хранения баз знаний, необходимых для использования методики.

СПИСОК ЛИТЕРАТУРЫ

1. *Ажмухамедов И. М.* Моделирование систем комплексного обеспечения информационной безопасности высших учебных заведений // Безопасность информационных технологий. 2013. № 2. С. 10–17.

2. *Ажмухамедов И. М., Проталинский О. М.* Информационная безопасность вуза // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2009. № 1. С. 18–23.

3. *Брумштейн Ю. М., Бондарев А. А.* Системный анализ вопросов информационной безопасности вузовских сайтов // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2014. № 2. С. 138–147.

4. *Глухова Л. В.* Методология оценки и управления качеством функционирования информационных систем // Вестн. Казан. технол. ун-та. 2008. № 4. С. 174–181.

5. *Сигов А. С., Анцыферов Е. С., Голубь С. С., Анцыферов С. С.* Системные принципы управления качеством проектирования адаптивных информационно-распознающих систем // Изв. ЮФУ. Технические науки. 2005. № 10. С. 167–174.

6. *Исаев Г. Н.* О синтезе систем управления качеством информационных систем // Вестн. ассоциации вузов туризма и сервиса. 2009. № 4. С. 89–94.

7. *Гусарова Н. Ф., Маятин А. В.* Координационные методы управления качеством в информационных системах // Науч.-техн. вестн. информационных технологий, механики и оптики. 2006. № 33. С. 241–249.

8. *Домарев В. В.* Защита информации и безопасность компьютерных систем. Киев: Диасофт, 2006. 480 с.

9. *Исхаков С. Ю., Шелупанов А. А., Исхаков А. Ю.* Имитационная модель комплексной сети систем безопасности // Докл. Томск. гос. ун-та систем управления и радиоэлектроники. 2014. № 2. С. 82–86.

10. *Матуско В. Н., Лебедев Н. С.* Надежность информационных систем: учеб. пособие. Новосибирск: СГГА, 2006. 129 с.

11. *Никитская Е. Ф., Гаранина Г. Г.* Оценка эффективности организационно-управленческих инноваций как результата внедрения системы электронного документооборота // Интернет-журнал «Науковедение». 2015. Т. 7, № 2. URL: http://naukovedenie.ru/PDF/86EVN215.pdf (дата обращения: 19.03.2017).

12. *Бунова Е. В., Буслаева О. С.* Оценка эффективности внедрения информационных систем // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2012. № 1 С. 158–164.

13. *Князева О. М.* Управление качеством информационных систем на основе процессного подхода // Прикаспийский журнал: управление и высокие технологии. 2016. № 2. С. 36–47.

14. *Князева О. М.* Нечеткая когнитивная модель процесса оценки качества информационных систем // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: сб. ст. II Всерос. науч.-техн. конф. молодых ученых, аспирантов и студентов. Таганрог: Изд-во Южн. фед. ун-та. 2016. С. 21–24.

15. *Князева О. М.* Комплексная оценка качества информационных систем на основе нечеткого когнитивного моделирования // Математические методы в технике и технологиях – ММТТ-29: сб. тр. XXIX Междунар. науч. конф. Саратов, 2016. Т. 1. С. 117–123.

16. *Ажмухамедов И. М., Князева О. М.* Унификация подходов к управлению уровнем информационной безопасности в организациях различного профиля // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2015. № 1. С. 66–77.

17. *ГОСТ ISO 9000-2011.* Системы менеджмента качества. Основные положения и словарь. URL: http://docs.cntd.ru/document/1200093424 (дата обращения: 19.03.2017).

18. *Ажмухамедов И. М., Проталинский О. М.* Методология моделирования плохоформализуемых слабоструктурированных социотехнических систем // Вестн. Астрахан. гос. техн. ун-та. Сер.: Управление, вычислительная техника и информатика. 2013. № 1. С. 144–154.

19. *Петров С. А., Крепков И. М., Федоров А. Б., Овсянникова М. Р.* Автоматизация кадрового учёта как составная часть автоматизации управления вузом // Информатизация инженерного образования. Труды Междунар. науч.-практ. конф. – ИНФОРИНО-2016. М.: МЭИ, 2016. С. 186–189.

Статья поступила в редакцию 28.03.2017

ИНФОРМАЦИЯ ОБ АВТОРАХ

Князева Оксана Михайловна – Россия, 414056, Астрахань; Астраханский государственный технический университет; аспирант кафедры автоматизированных систем обработки информации и управления; chobitoksana@mail.ru.

Мустафаева Нелля Нагимовна – Россия, 414056, Астрахань; Астраханский государственный технический университет; студентка, специальность «Информационная безопасность автоматизированных систем»; nellya.mustafaeva@mail.ru.

O. M. Knyazeva, N. N. Mustafaeva

THE TECHNIQUES OF ASSESSMENT OF QUALITY OF UNIVERSITY DATA PROCESSING SYSTEMS

Abstract. The article presents the method "Inspector" to be adapted for assessment of the levels of quality of data processing systems in universities. Included into the methodology fuzzy cognitive models of determining the required, estimating the current and "forecasted" levels of quality of data processing systems, as well as corresponding algorithms allow evaluating the system at the design stage and operation stage on the basis of expert information. Using the complex criterion of quality assessment makes it possible to increase the informativeness of the assessment, which, in turn, increases the efficiency of quality of data processing systems. Adapting methodology to the peculiarities of functioning of universities includes defining the main functions of the evaluated data processing systems; defining the elements of the sets of concepts of fuzzy cognitive models used in the methodology; verifying the existence of links between concepts of fuzzy cognitive models; filling the knowledge base necessary to assess the current level of information security of the data processing system. The methodology was approved in one of the leading higher educational institutions of the Volga region for assessment of the data processing system "Deccan". To adapt the methodology and directly assess the quality and information security of the data processing system, an expert commission was assembled, consisting of IT staff of the university, professors of profile de-

partments of the university, employees of the dean's office. The work of the commission was organized through meetings. Discussion of each issue lasted until the experts made an agreed decision. According to the data obtained after application of the methodology, there were taken measures to elevate quality of the Deccan system to the level "above average". Approbation of the method "Inspector" showed its applicability for assessing the quality of data processing systems of universities.

Key words: data processing systems, quality of systems, quality assessment criterion, reliability of data processing systems, information security, fuzzy cognitive modeling.

REFERENCES

1. Azhmukhamedov I. M. Modelirovanie sistem kompleksnogo obespecheniia informatsionnoi bezopasnosti vysshikh uchebnykh zavedenii [Simulating complex systems of information security management in higher educational universities]. *Bezopasnost' informatsionnykh tekhnologii*, 2013, no. 2, pp. 10-17.

2. Azhmukhamedov I. M., Protalinskii O. M. Informatsionnaia bezopasnost' vuza [Information security in higher educational institutions]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2009, no. 1, pp. 18-23.

3. Brumshtein Iu. M., Bondarev A. A. Sistemnyi analiz voprosov informatsionnoi bezopasnosti vuzovskikh saitov [System analysis of information security of university websites]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2014, no. 2, pp. 138-147.

4. Glukhova L. V. Metodologiia otsenki i upravleniia kachestvom funktsionirovaniia informatsionnykh sistem [Methodology of quality assessment and management of information system functioning]. *Vestnik Kazanskogo tekhnologicheskogo universiteta*, 2008, no. 4, pp. 174-181.

5. Sigov A. S., Antsyferov E. S., Golub' S. S., Antsyferov S. S. Sistemnye printsipy upravleniia kachestvom proektirovaniia adaptivnykh informatsionno-raspoznaiushchikh sistem [System concepts of managing quality design of adaptive information-recognizing systems]. *Izvestiia Iuzhnogo federal'nogo universiteta. Tekhnicheskie nauki*, 2005, no. 10, pp. 167-174.

6. Isaev G. N. O sinteze sistem upravleniia kachestvom informatsionnykh sistem [On the synthesis of quality control systems of information systems]. *Vestnik assotsiatsii vuzov turizma i servisa*, 2009, no. 4, pp. 89-94.

7. Gusarova N. F., Maiatin A. V. Koordinatsionnye metody upravleniia kachestvom v informatsionnykh sistemakh [Coordinating methods of quality control in information systems]. *Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki*, 2006, no. 33, pp. 241-249.

8. Domarev V. V. *Zashchita informatsii i bezopasnost' komp'iuternykh sistem* [Data protection and computer system security]. Kiev, Diasoft Publ., 2006. 480 p.

9. Iskhakov S. Iu., Shelupanov A. A., Iskhakov A. Iu. Imitatsionnaia model' kompleksnoi seti sistem bezopasnosti [Simulation model of the complex system of security systems]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki*, 2014, no. 2, pp. 82-86.

10. Matusko V. N., Lebedev N. S. *Nadezhnost' informatsionnykh sistem* [Reliability of information systems]. Novosibirsk, SGGA, 2006. 129 p.

11. Nikitskaia E. F., Garanina G. G. Otsenka effektivnosti organizatsionno-upravlencheskikh innovatsii kak rezul'tata vnedreniia sistemy elektronnogo dokumentooborota [Efficiency assessment of organizational and managerial innovations as a result of implementation of the system of electronic data interchange]. *Internet-zhurnal «Naukovedenie», 2015, no. 7.* Available at: http://naukovedenie.ru/PDF/86EVN215.pdf (accessed: 19.03.2017).

12. Bunova E. V., Buslaeva O. S. Otsenka effektivnosti vnedreniia informatsionnykh sistem [Efficiency assessment of implementing information systems]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2012, no. 1, pp. 158-164.

13. Kniazeva O. M. Upravlenie kachestvom informatsionnykh sistem na osnove protsessnogo podkhoda [Quality control of information systems in terms of process approach]. *Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii*, 2016, no. 2, pp. 36-47.

14. Kniazeva O. M. Nechetkaia kognitivnaia model' protsessa otsenki kachestva informatsionnykh sistem [Fuzzy cognitive model of the process of information system quality control]. *Fundamental'nye i prikladnye aspekty komp'iuternykh tekhnologii i informatsionnoi bezopasnosti: sbornik statei II Vserossiiskoi nauchno-tekhnicheskoi konferentsii molodykh uchenykh, aspirantov i studentov* [Fundamental and applied aspects of computer technologies and information security: collected papers of II all-Russian scientific-technical conference of young scientists, postgraduates and students]. Taganrog, Izd-vo Iuzhnogo federal'nogo universiteta, 2016. P. 21-24.

15. Kniazeva O. M. Kompleksnaia otsenka kachestva informatsionnykh sistem na osnove nechetkogo kognitivnogo modelirovaniia [The comprehensive assessment of information system quality based on the concept of fuzzy cognitive modelling]. *Matematicheskie metody v tekhnike i tekhnologiiakh – MMTT-29: sbornik trudov XXIX Mezhdunarodnoi nauchnoi konferentsii* [Mathematical methods in technics and technologies – MMTT-29: proceedings of the XXIX International scientific conference]. Saratov, 2016, vol. 1, pp. 117-123.

16. Azhmukhamedov I. M., Kniazeva O. M. Unifikatsiia podkhodov k upravleniiu urovnem informatsionnoi bezopasnosti v organizatsiiakh razlichnogo profilia [Unification of approaches to information security control in enterprises of different specializations]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2015, no. 1, pp. 66-77.

17. *GOST ISO 9000-2011. Sistemy menedzhmenta kachestva. Osnovnye polozheniia i slovar'* [GOST ISO 9000-2011. Quality management systems. General regulations and a dictionary]. Available at: http://docs.cntd.ru/document/1200093424 (accessed: 19.03.2017).

18. Azhmukhamedov I. M., Protalinskii O. M. Metodologiia modelirovaniia plokhoformalizuemykh slabostrukturirovannykh sotsiotekhnicheskikh sistem [Methodology of modelling difficult to formalize and poor structured socio-technical systems]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriia: Upravlenie, vychislitel'naia tekhnika i informatika*, 2013, no. 1, pp. 144-154.

19. Petrov S. A., Krepkov I. M., Fedorov A. B., Ovsiannikova M. R. Avtomatizatsiia kadrovogo ucheta kak sostavnaia chast' avtomatizatsii upravleniia vuzom [Automation of personnel records as a part of automation of University management]. *Informatizatsiia inzhenernogo obrazovaniia. Trudy Mezhdunarodnoi nauchno-prakticheskoi konferentsii – INFORINO-2016* [Informatization of engineering education. Proceedings of the International scientific-practical conference – INFORINO-2016]. Moscow, MEI, 2016. P. 186-189.

The article submitted to the editors 28.03.2017

INFORMATION ABOUT THE AUTHORS

Knyazeva Oksana Mikhailovna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Postgraduate Student of the Department of Automated Systems of Information Processing and Management; chobitoksana@mail.ru.

Mustafaeva Nellya Nagimovna – Russia, 414056, Astrakhan; Astrakhan State Technical University; Student, Specialty "Information Security of Automated Systems"; nellya.mustafaeva@mail.ru.