УДК 004.056

ОЦЕНКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ ДАННЫХ ОРГАНИЗАЦИИ В УСЛОВИЯХ ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья поступила в редакцию 02.07.2015, в окончательном варианте 16.09.2015.

Ажмухамедов Искандар Маратович, доктор технических наук, доцент, Астраханский государственный технический университет, 414025, Российская Федерация, г. Астрахань, ул. Татищева, 16, e-mail: aim_agtu@mail.ru

Князева Оксана Михайловна, аспирант Астраханского государственного технического университета, специалист по сопровождению 1С, ООО «АпГрейд», 414004, Российская Федерация, г. Астрахань, ул. Красная Набережная, 171, e-mail: chobitoksana@mail.ru

Для большинства организаций весьма актуальна задача оценки уровня информационной безопасности (ИБ) в случае реализации угроз их информационным ресурсам. Существующие методы оценки ИБ организаций во многих случаях не позволяют выработать обоснованного суждения о состоянии конфиденциальности, целостности и доступности имеющихся информационных ресурсов. Это затрудняет управление уровнем ИБ, в т.ч. принятие мер превентивного характера – особенно при наличии ресурсных и иных ограничений в отношении выполнения решений. Задача комплексной оценки уровня ИБ в силу ее особенностей является слабоформализуемой. В результате проведенных исследований авторами предложена методика оценки уровня ИБ организации на основе нечеткого когнитивного моделирования. Модель состоит из шести иерархических уровней. На самом нижнем (пятом) уровне когнитивного графа располагаются механизмы и средства защиты информации. На четвертом – угрозы и уязвимости ИБ. На третьем – атаки на информационные ресурсы. На втором – повреждения информационных ресурсов и средств защиты информации. На первом – свойства информации, характеризующие ее защищенность (конфиденциальность, целостность, доступность). На нулевом (высшем по иерархии) – интегральный показатель уровня ИБ организации. Входными данными модели являются лингвистические оценки текущего (либо планируемого в случае принятия решений по управлению уровнем ИБ) состояния средств защиты информации (множество значений: низкий; ниже среднего; средний; выше среднего; высокий). На основе этих оценок рассчитываются значения концептов на вышестоящих уровнях. Нечеткая когнитивная модель позволяет не только адекватно оценить уровень ИБ организации, но и выработать практические рекомендации по его повышению (с учетом взаимного влияния факторов). Предложенная методика реализована в виде программного комплекса «Нечеткое когнитивное моделирование системы комплексного обеспечения информационной безопасности». Методика и программное средство были апробированы в ООО «Центр обучения Пилот-информ». Полученная оценка ИБ организации послужила основанием для разработки практических рекомендаций по усилению мер, направленных на повышение уровня конфиденциальности информации в организации.

Ключевые слова: информационная безопасность, уязвимости, угрозы, повреждения информационных ресурсов, повреждения средств защиты информации, нечеткое когнитивное моделирование, лингвистическая переменная, нечеткие числа, нечеткий классификатор, поддержка принятия решений

ASSESSMENT OF STATUS FOR DATA SECURITY OF ORGANIZATION IN CONDITIONS OF REALIZATION POSSIBILITY FOR INFORMATION SECURITY THREATS

Azhmukhamedov Iskandar M., D.Sc. (Engineering), Associate Professor, Astrakhan State Technical University, 16 Tatishchev St., Astrakhan, 414025, Russian Federation, e-mail: aim_agtu@mail.ru

Knyazeva Oksana M., post-graduate student, Astrakhan State Technical University, specialist of supporting 1C, Ltd. «UpGrade», 171 Krasnaya Naberezhnaya St., Astrakhan, 414004, Russian Federation, e-mail: chobitoksana@mail.ru

For most organizations now exist urgent task of assessing the level of information security (IS) in case of IS threats implementations. Existing methods of assessing IS, in many cases do not allow generating enough informed judgments about the condition of information confidentiality, integrity and availability. Accordingly, it is difficult to take action to manage their levels, apply preventive measures – especially in the presence of resource and other limitations for decisions perfoming. The task of IS level assessing because of its features is weakly formalized. As a result of research made by authors, have been proposed a method of IS level assessing for organization, based on fuzzy cognitive modeling. The model has six hierarchical levels. The fifth level is the bottom of the hierarchy. At that level are located mechanisms and means of information protection. The fourth are the vulnerability and threats to IS. On the third are the attacks to the information resources of organization. On the second are the damage information assets and information protection means. At the first are the properties of information, describing its security (confidentiality, integrity, availability). On the zero level (the highest in the hierarchy) are an integral indicator of the organization IS. The inputs data to the model are the linguistic evaluations of current (or planned in case of decision-making, concerned with IS level management) status of information protection tools (a set of values: low, below average, average, above average, high). Based on these estimates are calculated value concepts at higher levels. Fuzzy cognitive model allows not only adequately assess the level of IS, but also develop recommendations for improving it (taking into account the mutual influence of factors). The proposed method has been implemented in software complex «Fuzzy cognitive modeling of integrated information security». Methods and software have been tested in the «Center of Training Pilot-Inform» by assessing the IS level of organization. This estimate served as the basis of developing recommendations for strengthening measures, aimed at confidentiality improving of information.

Keywords: security services, vulnerability, threat, damage of information resourses, damage of information security tools, fuzzy cognitive modeling, linguistic variable, fuzzy numbers, fuzzy classifier

Введение. В современных условиях деятельность большинства организаций в значительной степени автоматизирована. Электронный документооборот часто преобладает над бумажным; электронная почта, программы видеоконференцсвязи на сегодняшний день стали неотъемлемой частью делового общения; проведение платежей через банки в дистанционном режиме, начисление зарплаты сотрудникам на банковские карты, автоматизация учета материальных ценностей значительно снизили трудоемкость бухгалтерской деятельности, повысили ее качество. Компьютеризованные системы кадрового учета позволили улучшить эффективность работы кадровых служб организаций; участие в электронных торгах дает возможность юридическим лицам производить операции в режиме реального времени; архивы многих организаций все в большей степени переводятся из бумажной формы в электронную [6].

Однако с ростом уровня автоматизации деятельности организаций возрастает вероятность реализации угроз информационной безопасности (ИБ): кражи носителей информации; DDOS атак на сервера; несанкционированного изменения записей в базах данных и т.д. При реализации этих угроз организации обычно несут материальные, финансовые и репутационные потери. Следовательно, необходимо принятие соответствующих мер защиты, в т.ч. и превентивного характера. В связи с этим актуальной является задача оценки уровня ИБ в случае реализаций потенциальных угроз. Однако эти вопросы в существующей литературе отражены недостаточно полно – в том числе в отношении учета нечеткости условий оценки различных факторов; наличия их взаимосвязей, влияющих на уровни ИБ. Поэтому **цель** данной работы – разработка методики оценки уровня ИБ на основе нечеткого когнитивного моделирования (НКМ). Это позволяет преодолеть указанные трудности и эффективно управлять уровнем ИБ (свойствами конфиденциальности, целостности и доступности информации).

Постановка задачи. Существует несколько подходов к оценке уровня ИБ в условиях реализации потенциальных угроз: оценка рисков (например, методики CRAMM [14, 15, 19], FRAP [16], OCTAVE [17] и т.д.); определение актуальных угроз (например, «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК [13]). Эти направления обладают об-

щим недостатком – не позволяют выработать обоснованного суждения о состоянии конфиденциальности, целостности и доступности информации. Как следствие, это не дает возможности синтезировать управляющие решения по выводу данных показателей ИБ на требуемый (целевой) уровень.

В связи с этим возникает необходимость в разработке методики, которая позволила бы адекватно оценивать и управлять уровнем ИБ организации в нечетких условиях. Анализ предметной области позволил построить онтологическую модель процесса оценки уровня ИБ организации при таких условиях (рис. 1).

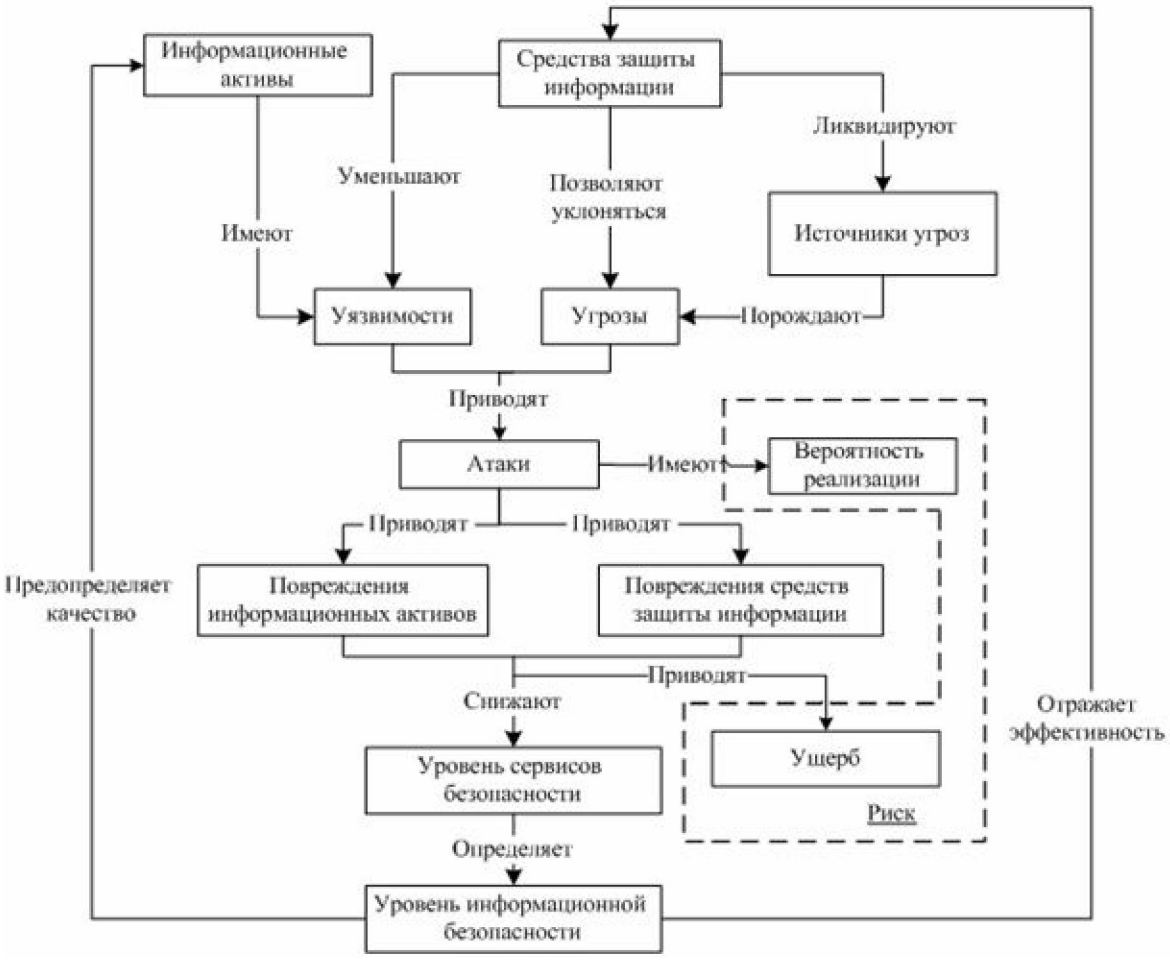

Рис. 1. Онтологическая модель процесса оценки уровня ИБ

Состояние ИБ зависит от прогнозного уровня повреждений информационных ресурсов (ИР) и средств защиты информации (СЗИ) при реализации угроз (атак). Под угрозой в соответствии с [7, 9] понимают совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. При этом согласно [8] угрозы, влияющие на ИБ, подразделяются по признаку отношения к природе их возникновения на объективные и субъективные; по отношению к объектам информационной системы – на внутренние и внешние. Внешние и внутренние угрозы ИБ могут носить как преднамеренный, так и непреднамеренный характер. Причиной их возникновения могут быть как сбои в техническом и программном обеспечении вследствие ошибок персонала, так и случайные нарушения в работе элементов информационной системы (например, из-за по-

ломки оборудования, сбоя в работе программного обеспечения, имеющего недостаточно высокую эксплуатационную надежность и т.д.). Для предотвращения возможности реализации угроз ИБ применяют средства и методы защиты информации, которые ликвидируют угрозы (предотвращают их реализацию); позволяют уклоняться от угроз; уменьшают уязвимости. В качестве специфического способа «защиты» от неблагоприятных последствий реализации угроз ИБ можно назвать также страхование рисков для ИР организации.

Процесс оценки уровня ИБ обладает рядом особенностей: неполнота и неопределенность исходной информации о составе и характере угроз; невозможность количественного измерения или статистической оценки большинства параметров процесса; необходимость учета большого числа частных показателей, а в ряде случаев и их взаимосвязей; необходимость учета особенностей поведения людей, которые не только принимают важные решения при управлении процессом обеспечения ИБ, но и сами являются объектом управления; затрудненность применения классических методов оптимизации [3, 10].

Наиболее полно учесть перечисленные особенности позволяет НКМ, неоспоримыми достоинствами которого являются возможность формализации численно неизмеримых факторов; возможности использования неполной, нечеткой и даже противоречивой информации [5, 12].

В качестве НКМ процесса оценки уровня ИБ (*PISL* – predicting of information security level) предлагается принять кортеж:

$$PISL = <G, QL, S, R, \Omega>, \quad (1)$$

где G – ориентированный граф, не содержащий горизонтальных ребер в пределах одного уровня иерархии (рис. 2); QL – набор качественных оценок уровней каждого фактора в графе; S – множество весов ребер графа G, отражающих степени влияния концептов на заданный элемент следующего (более высокого) уровня иерархии; R – набор правил для вычисления значений концептов на каждом из иерархических уровней G; Ω – индекс схожести, характеризующий степень соответствия значения фактора той или иной качественной оценке из терм-множества лингвистической переменной QL.

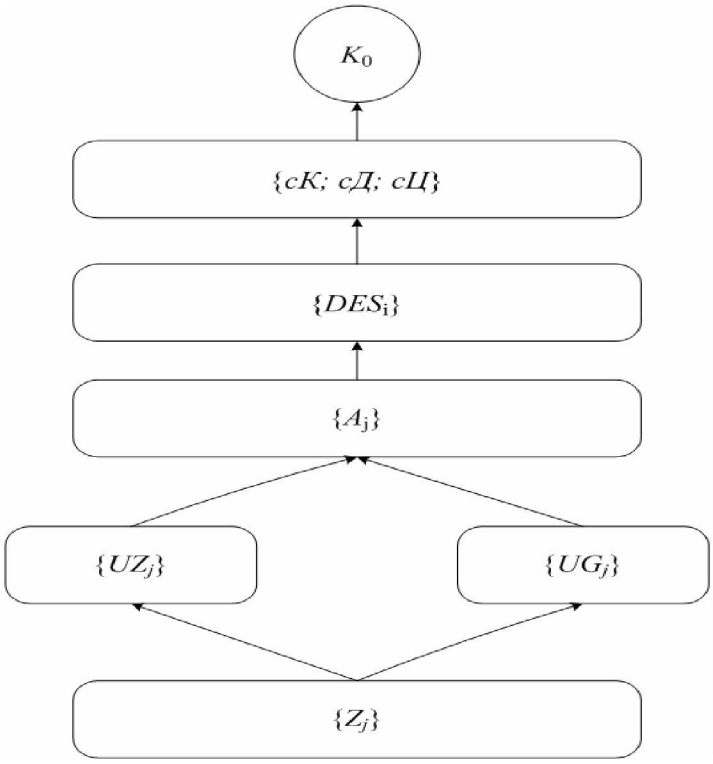

Рис. 2. Граф G, отражающий процесс оценки уровня ИБ

Индекс схожести Ω двух нечетких чисел $A(a_1, a_2, a_3, a_4)$ и $B(b_1, b_2, b_3, b_4)$ с соответствующими функциями принадлежности $\mu_A(x)$ и $\mu_B(x)$ находится по формулам (2) и (3) [3]:

$$\Omega = (1 + \tilde{\rho})/2, \quad (2)$$

$$\tilde{\rho} = (\rho_{in} - \rho_{out})/(\rho_{in} + \rho_{out}), \quad (3)$$

где $\rho_{in} = \int_{a_1}^{a_4} \min[\mu_A(x); \mu_B(x)]dx$; $\rho_{out} = \left| \int_{b_1}^{b_4} [\mu_B(x)]dx - \rho_{in} \right|$

В последней формуле ρ_{out} представляет собой площадь нечеткого числа $B(b_1, b_2, b_3, b_4)$, лежащую вне эталонного нечеткого числа $A(a_1, a_2, a_3, a_4)$; ρ_{in} – площадь, лежащая внутри этого же нечеткого числа.

Вершины графа G на нижнем (пятом) уровне отражают механизмы и средства защиты информации $Z_{\{1,2,3,\ldots\}}$, обеспечивающие реализацию 3-ех стратегий: ликвидация источников угроз; уклонение от угроз $UG_{\{1,2,3,\ldots\}}$ (4-ый уровень); уменьшение уязвимостей $UZ_{\{1,2,3,\ldots\}}$ (4-ый уровень).

С целью унификации подходов к рассмотрению процесса обеспечения ИБ будем считать, что уровень уязвимостей на объекте информатизации (ОИ) всегда наивысший, и он может быть снижен только с помощью применения СЗИ.

Большинство угроз являются внешними по отношению к ОИ. В связи с этим обычно невозможно вынести обоснованного суждения об уровне их опасности (под этим уровнем будем понимать степень разрушительности угроз в отношении ИР).

Поэтому при нахождении нижней границы оценки состояния ИБ на ОИ целесообразно считать начальный уровень опасности угроз (до применения СЗИ) наивысшим.

На третьем иерархическом уровне расположены концепты, соответствующие атакам на информационные системы (ИС) – $A_{\{1,2,3,\ldots\}}$ организации. Под ИС авторы понимают совокупность содержащейся в базах данных информации и информационных технологий, а также технических средств, обеспечивающих их обработку. Таким образом, ИС может быть как автоматизированной, так и неавтоматизированной.

Второй иерархический уровень представлен повреждениями элементов ИС и СЗИ $Des_{\{1,2,3,\ldots\}}$, которые образуются (возникают) в результате атак на ИР.

Первый иерархический уровень образуют частные показатели ИБ (свойства информации): *сК* – конфиденциальность; *сЦ*– целостность; *сД* – доступность.

Доступность, целостность и конфиденциальность как свойства информации возникают (существуют) при ее представлении, обработке, хранении, передаче и т.д. При этом целостность и доступность – свойства, порождаемые технологиями обработки информации. Они обеспечиваются соответствующими элементами ИС. Конфиденциальность же, в отличие от целостности и доступности, не является имманентным свойством технологии обработки данных. Она возникает в результате применения правил, методов, средств ограничения доступа к информации. Иными словами конфиденциальность порождается использованием элементов СЗИ.

Вершина нулевого уровня K_0 графа G соответствует интегральному критерию ИБ ОИ в целом.

Множество концептов НКМ. Комплексный подход к защите информации предусматривает согласованное применение правовых, организационных и программно-технических мер, представленных в виде следующего списка.

Z_1 – процедура защиты документов при их хранении, включающая в себя следующее: регламент защиты документов при их хранении; контроль защиты документов при их хранении; Z_2 – процедура контроля за работой пользователей ИС и обслуживающего персонала, содержащая организационные и технические средства контроля; Z_3 – использование сертифицированного в отношении ИБ лицензионного программного обеспечения (ПО); Z_4 – процедура разграничения доступа к ИР, состоящая из организационных, технических и программно-аппаратных мер, обеспечивающих разграничение возможностей доступа для различных пользователей; Z_5 – тех-

ническая поддержка аппаратных средств; Z_6 – поддержка программных средств; Z_7 – техническая поддержка средств жизнеобеспечения ОИ (электропитание, водоснабжение, канализация); Z_8 – обучение сотрудников основам ИБ; Z_9 – работа с персоналом, включающая в себя институциональное, мотивационное и информационное управление; Z_{10} – использование физических барьеров (оградительных конструкций) для защиты ОИ и его периметра; Z_{11} – организация пропускного режима и охраны; Z_{12} – организация противопожарной защиты, включающая в себя следующее: систему обнаружения очагов возгорания; средства автоматического и / или ручного пожаротушения; Z_{13} – контроль выполнения мер по защите информации (ЗИ); Z_{14} – процедура аудита, анализа и управления инцидентами ИБ, содержащая следующее: средства проведения аудита инцидентов ИБ; регламент аудита; Z_{15} – применение специальных технических средств защиты информации и контроля обстановки на ОИ; Z_{16} – применение алгоритмов криптографической ЗИ; Z_{17} – использование средств межсетевого экранирования; Z_{18} – применение средств антивирусной защиты (антивирусное ПО и регламент его использования); Z_{19} – использование средств контентного анализа сетевого трафика; Z_{20} – применение средств защиты от спама; Z_{21} – заземление основного и вспомогательного оборудования, используемого при обработке информации; Z_{22} – использование средств защиты от наводнений и ливневых осадков большой интенсивности, в том числе применение водостойких строительных материалов, водонепроницаемых барьеров, специальных водоотводящих каналов; Z_{23} – использование сейсмоустойчивых фундаментов; Z_{24} – применение громоотводов (молниеводов); Z_{25} – использование средств защиты помещений на ОИ от пыли; Z_{26} – применение средств климат-контроля в помещениях ОИ; Z_{27} – использование средств защиты локальной вычислительной сети организации от несанкционированного доступа (НСД) из общедоступных сетей: организация демилитаризованной зоны (DMZ); организация виртуальных частных сетей (VPN); Z_{28} – использование закрытого бумажного документооборота; Z_{29} – выявление и увольнение «рассеянных» сотрудников (лиц с недостаточной концентрацией внимания); Z_{30} – выявление и увольнение сотрудников, не выполняющих требования ИБ; Z_{31} – размещение ОИ на территории с низкой вероятностью возникновения пожаров на близлежащих объектах; Z_{32} – расположение ОИ на территории с низкой вероятностью наводнения или обильных ливневых осадков; Z_{33} – расположение ОИ на территории с низкой вероятностью землетрясения со значительной магнитудой; Z_{34} – расположение объекта на территории с низкой вероятностью возникновения урагана или смерча; Z_{35} – расположение объекта на территории с низкой грозовой активностью; Z_{36} – расположение объекта на труднодоступной для посторонних лиц территории; Z_{37} – расположение объекта на территории с низкой вероятностью возникновения пыльной бури; Z_{38} – расположение объекта на территории с умеренным климатом (отсутствием температурных аномалий). С точки зрения авторов статьи, приведенный перечень обладает свойствами «необходимости и достаточности». Приоритетность этих мер зависит от условий деятельности конкретной организации и может не соответствовать приведенному списку.

Угрозы ИБ различного типа на практике, как правило, тесно взаимосвязаны. Вследствие этого уязвимость элементов ИС или СЗИ по отношению к какому-либо одному типу (виду) угроз может приводить к возможности (или повышению вероятности) реализации угроз других типов – одной или их совокупности.

При этом деструктивное воздействие на ИР часто осуществляется через несанкционированный доступ, т. е. доступ к элементам ИС, выходящий за рамки полномочий, разрешённых для конкретных пользователей. Актуальными могут быть и угрозы, связанные с психологическим воздействием на персонал организации: шантаж, угрозы расправы, подкуп, моральное давление (в т.ч. и на родственников) и т.д. Эти угрозы достаточно часто реализуются на практике, поэтому необходимо уделять им серьёзное внимание как с теоретических, так и практических позиций [2].

Таким образом, множество угроз ИС может быть представлено в виде следующего перечня. UG_1 – неумышленные повреждения оборудования; UG_2 – неправомерные отключения оборудования; UG_3 – неумышленные удаления файлов с важной информацией; UG_4 – неумышленные искажения файлов с важной информацией; UG_5 – неумышленные удаления программ; UG_6 – неумышленные внесения изменений в программы; UG_7 – неправомерные изменения режимов работы устройств, связанных доступом к ИР, их обработкой и т.д; UG_8 – неправомерные изменения режимов работы программ; UG_9 – неумышленная порча носителей информации; UG_{10} – некомпетентный запуск (применение) технологических / сервисных программ; UG_{11} – заражения компьютера вирусами (вредоносными программами); UG_{12} – хищения носителей информации; UG_{13} – несанкционированное копирования информации; UG_{14} – хищения черновиков и временных копий документов; UG_{15} – чтение информации из оперативной памяти (ОП) компьютеров и микроконтроллеров; UG_{16} – чтение «остаточной» информации после выполнения стирания данных на снятых с эксплуатации жестких дисках, внешних запоминающих устройствах (ВЗУ); UG_{17} – вскрытие шифров криптозащиты информации; UG_{18} – навязывание ложных сообщений (фальсификация); UG_{19} – несанкционированные модификации потока данных; UG_{20} – отказ (сбой) технических средств обработки информации (ТСОИ); UG_{21} – поломки на ОИ бытовых электроприборов, используемых в рамках технологических процессов работы с ИР; UG_{22} – сбои системы электроснабжения на ОИ; UG_{23} – сбои системы климат-контроля на ОИ; UG_{24} – сбои внешних информационных каналов коммуникации; UG_{25} – отказ систем водоснабжения и канализации на ОИ; UG_{26} – пожары на ОИ или вблизи него; UG_{27} – наводнения; UG_{28} – землетрясения; UG_{29} – поражения молнией зданий с ОИ; UG_{30} – возникновение урагана; UG_{31} – пыльные бури; UG_{32} – воздействия экстремальных температур; UG_{33} – подкуп персонала; UG_{34} – шантаж персонала или иные средства оказания на него морального давления.

Угрозы как потенциальная возможность совершения какого-либо действия (или реализации какого-то события), в том числе специально направленного против объекта защиты, реализуются через уязвимости и могут приводить к повреждениям элементов ИС и СЗИ на ОИ. Уязвимости присущи ОИ, неотделимы от них и обуславливаются недостатками процесса обеспечения функционирования ИС, свойствами ее архитектуры, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой ИС, условиями ее эксплуатации (включая места размещения оборудования) и др. Типовые уязвимости ИС могут быть представлены элементами следующего списка: UZ_1 – ненадежность оборудования; UZ_2 – некомпетентность (или недостаточная компетентность) персонала в вопросах эксплуатации элементов ИС; UZ_3 – некомпетентность персонала и пользователей в вопросах защиты информации (ЗИ); UZ_4 – ненадежность носителей информации; UZ_5– эксплуатация технических средств (ТС) в нештатных режимах; UZ_6 – возможность использования ПО в нештатных режимах; UZ_7– наличие неиспользуемых потенциально опасных служб операционной системы, недокументированных возможностей программных средств; UZ_8 – мотивированность отдельных лиц из состава персонала на совершение деструктивных действий; UZ_9 – возможности хищения носителей информации; UZ_{10} – возможность несанкционированного копирования информации; UZ_{11} – наличие неучтенных копий и черновиков документов; UZ_{12} – возможность несанкционированного доступа к ОП ЭВМ во время обработки информации; UZ_{13} – некомпетентность вспомогательного обслуживающего персонала; UZ_{14} – недостаточная стойкость систем криптозащиты; UZ_{15} – ненадежность протоколов взаимной аутентификации компьютеров в локальной сети; UZ_{16} – ненадёжность технических средств обработки информации (ТСОИ); UZ_{17} – ненадёжность бытовых электроприборов, используемых на ОИ; UZ_{18} – ненадежность внутренней системы электроснабжения на ОИ; UZ_{19} – ненадежность внешних сетей электроснабжения; UZ_{20} – ненадёжность внешних коммуникационных каналов; UZ_{21} – ненадежность внутренних коммуникационных каналов;

UZ_{22} – ненадежность систем водоснабжения и канализации на ОИ; UZ_{23} – несоблюдение мер пожарной безопасности; UZ_{24} – возможность сбоя (или выхода из строя) элементов ИС при превышении допустимого уровня влажности; UZ_{25} – возможность повреждения (уничтожения) ОИ в случае землетрясения; UZ_{26} – возможность сбоя элементов ИС при выходе значений силы тока и напряжения за рамки допустимого диапазона; UZ_{27} – возможность повреждения элементов ИС в случае механического удара; UZ_{28} – возможность сбоя элементов ИС при превышении предельной допустимой концентрации (ПДК) частиц пыли в воздухе помещений ОИ; UZ_{29} – возможность сбоя элементов ИС при нарушениях температурного режима эксплуатации; UZ_{30} – возможность несанкционированного физического доступа на ОИ; UZ_{31} – наличие побочных электромагнитных наводок и излучений; UZ_{32} – ошибки в программном обеспечении.

Поскольку атака – это попытка реализации угрозы через какую-либо уязвимость, то названия атак целесообразно определить исходя из наименований угроз: A_1 – неумышленное повреждение оборудования; A_2 – неправомерное отключение оборудования; A_3 – неумышленное удаление файлов с важной информацией; A_4 – неумышленное искажение файлов с важной информацией; A_5 – неумышленное удаление программ; A_6 – неумышленное внесение изменений в программы; A_7 – неправомерное изменение режимов работы устройств; A_8 – неправомерное изменение режимов работы программ; A_9 – неумышленная порча носителей информации; A_{10} – некомпетентный запуск технологических (сервисных) программ; A_{11} – заражение компьютера вирусами или иными вредоносными программами; A_{12} – хищение носителей информации; A_{13} – несанкционированное копирование информации; A_{14} – хищение черновиков, временных и промежуточных документов; A_{15} – несанкционированное чтение информации из ОП; A_{16} – чтение остаточной информации с внешних ЗУ, выведенных из эксплуатации жестких дисков; A_{17} – вскрытие шифров криптозащиты информации; A_{18} – навязывание ложных сообщений (фальсификация) в каналах связи компьютерной сети; A_{19} – несанкционированная модификация потока данных; A_{20} – отказ (сбой) ТСОИ; A_{21} – поломка (выход из строя) бытовых электроприборов на ОИ; A_{22} – сбой системы электроснабжения; A_{23} – сбой системы климат-контроля; A_{24} – сбой внешних информационных каналов коммуникаций; A_{25} – отказ систем водоснабжения и/или канализации на ОИ; A_{26} – пожар; A_{27} – наводнение; A_{28} – землетрясение; A_{29} – поражение здания с ОИ молнией; A_{30} – ураган; A_{31} – пыльная буря; A_{32} – экстремальные температуры; A_{33} – подкуп персонала; A_{34} – шантаж персонала.

При рассмотрении процесса обеспечения ИБ необходимо оценить уровень (степень) повреждений, возникающих в результате реализации атак. Совокупность типичных повреждений может относиться к следующим объектам: DES_1 – коммуникационное оборудование и кабели передачи данных; DES_2 – бумажные носители данных; DES_3 – аппаратные средства серверов; DES_4 – аппаратные средства рабочих станций; DES_5 – аппаратные части накопителей данных (запоминающих устройств); DES_6 – инженерно-технические средства (меры) защиты информации; DES_7 – операционные системы (ОС) серверов; DES_8 – ОС рабочих станций; DES_9 – серверные части пользовательского ПО; DES_{10} – клиентские части пользовательского ПО; DES_{11} – локальное ПО рабочих станций; DES_{12} – программы криптографической защиты; DES_{13} – программы резервного копирования данных; DES_{14} – программы мониторинга и аудита ИБ; DES_{15} – программы защиты от НСД; DES_{16} – файлы на серверах; DES_{17} – файлы на рабочих станциях; DES_{18} - системы защиты документов при их хранении; DES_{19} - (нарушения) систем организации пропускного режима и охраны; DES_{20} – системы противопожарной защиты; DES_{21} – системы аудита, анализа и управления инцидентами ИБ; DES_{22} – специальные технические средства ЗИ; DES_{23} – средства межсетевого экранирования; DES_{24} – средства антивирусной защиты; DES_{25} – средств контентного анализа сетевого трафика; DES_{26} – средства защиты от спама; DES_{27} – заземления основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС); DES_{28} – средства за-

щиты от наводнения; DES_{29} – сейсмостойкие фундаменты; DES_{30} – громоотводы; DES_{31} – средства защиты от пыли (в первую очередь – помещений, где расположены сервера); DES_{32} – средства климат-контроля помещений ОИ.

Приведенный перечень важен с позиций обеспечения полноты учета факторов (и их совокупностей) при принятии решений, связанных с обеспечением ИБ.

Вычисление значений концептов на каждом уровне НКМ. Для описания состояния концептов графа G определим лингвистическую переменную «Уровень фактора» и терм-множество ее значений QL, состоящее из пяти элементов:

QL = {Низкий (Н), Ниже среднего (НС), Средний (С),
Выше среднего (ВС), Высокий (В)}. (4)

В качестве семейства функций принадлежности для QL используем пятиуровневый классификатор, в котором функциями принадлежности нечетких чисел (НЧ), заданных на отрезке $[0,1] \in R$, являются трапеции:

$$\{XX(a_1, a_2, a_3, a_4)\}, \quad (5)$$

где a_1 и a_4 – абсциссы нижнего, a_2 и a_3 – абсциссы верхнего основания трапеции [11, 18].

Применение классификатора позволяет перейти от качественного описания уровня параметра к стандартному количественному виду соответствующей функции принадлежности из множества нечетких трапециевидных чисел. Вычисление текущих значений факторов графа G предлагается производить по приведенным ниже формулам (6) … (12):

$$\overline{UZ_j} = UZ_j \cdot \prod_{i=1}^{N} \left(Inv\left(Z_i\right)\right)^{\alpha_i}, \quad (6)$$

где $\overline{UZ_j}$ – остаточный (после применения мер защиты Z_i) уровень j-ой уязвимости; UZ_j – исходный (до применения средств защиты) уровень j-ой уязвимости; $UZ_j = 1$, в случае наличия уязвимости, $UZ_j = 0$, в случае отсутствия уязвимости; N – количество мер защиты Z_i, влияющих на j-ую уязвимость; Z_i – уровень i-ой защитной меры, влияющей на j-ую уязвимость; $\alpha_i \in [0;1]$ – коэффициент снижения уровня j-ой угрозы в результате применения i-ой защитной меры Z_i.

Для нахождения инверсии (противоположного значения) приращения фактора F в приводимых ниже формулах предлагается использовать выражение [3]:

$$Inv(F) = (1 - \mu(F)), \quad (7)$$

где $\mu(F)$ – функция принадлежности нечеткого числа, соответствующего лингвистическому значению QL_F приращения фактора F.

$$\overline{UG_j} = UG_j \cdot \prod_{i=1}^{L} \left(Inv\left(Z_i\right)\right)^{\beta_i}, \quad (8)$$

где $\overline{UG_j}$ – остаточный (после применения мер защиты Z_i) уровень j-ой угрозы; UG_j – исходный (до применения средств защиты) уровень j-ой угрозы; $UG_j = 1$ в случае наличия угрозы, $UG_j = 0$ в случае отсутствия угрозы; L – количество применяемых (или планируемых) мер защиты Z_i, влияющих уровень j-ой угрозы; Z_i – уровень i-ой защитной меры, влияющей на j-ую угрозу; $\beta_i \in [0;1]$ – коэффициент снижения уровня опасности j-ой угрозы в результате применения i-ой защитной меры Z_i.

$$A_j = \max_{\{i|\delta_j^i \neq 0\}} \{UG_j \cdot UZ_i\}, \quad (9)$$

где A_j – уровень опасности j-ой атаки; UZ_i – уровень i-ой уязвимости,

$$\delta_j^i = \begin{cases} 0 - \text{если для реалиизации уугроз } UG_j \textit{ не требуется } \text{наличие уязвимости } UZ_i \\ 1 - \text{если для реалиизации уугроз } UG_j \textit{ требуется } \text{наличие уязвимости } UZ_i \end{cases}.$$

$$Des_j = \max_i \{A_i \cdot pwr_i\}, \quad (10)$$

где Des_j – уровень j-го повреждения; $pwr_i \in QL$ – интенсивность (сила) влияния i-ой атаки на j-ое повреждение.

$$K_j = Inv(\max_i \{Des_i \cdot \text{int}_i\}), \quad (11)$$

где K_j – уровень j-го частного показателя безопасности; Des_j – уровень i-го повреждения, влияющего на j-ый показатель безопасности; $\text{int}_i \in QL$ интенсивность (сила) влияния i-го повреждения на j-ый показатель безопасности.

$$K_0 = \prod_{j=1}^{3} (K_j)^{\alpha_j}, \quad (12)$$

где K_0 – уровень комплексной ИБ ИС; K_j – уровень j-го частного показателя безопасности; $\alpha_j \in [0;1]$ – коэффициент влияния K_j на обобщенный показатель ИБ ОИ; $\sum_{j=1}^{3} \alpha_j = 1$. Коэффициент α_j отражает приоритетность соответствующих свойств ИБ для конкретной организации.

Состояния (эффективности) мер защиты Z_i, входящих в систему комплексного обеспечения ИБ, определяет лицо, принимающее решение (ЛПР). В случае если Z_i не представляется возможным рассматривать как совокупность отдельных мер защиты информации (такие Z_i назовем «*атомарными*»), то ЛПР задает лингвистическую оценку непосредственно Z_i. «*Атомарными*» мерами защиты являются, например, Z_3, Z_5, Z_6 и т.д.

В случае если Z_i представляет собой комплекс отдельных мер защиты информации z_j^i (такие меры защиты назовем «*молекулярными*»), то ЛПР задает лингвистическую оценку z_j^i, входящих в Z_i. Состояние Z_i в этом случае определяется на основе правил:

$$\begin{cases} Z_i = \min_j \{z_j^i\} \text{ если } \{z_j^i\} \text{действуют одновременно (}\textit{параллельно}\text{)} \\ Z_i = \prod_{j=1}^{M} (z_j^i)^{\alpha_j}, \text{если } \{z_j^i\} \text{действуют последовательно, образуя ребежи защиты} \end{cases},$$

где Z_i – текущее значение, отражающее состояние i-ой «*молекулярной*» меры защиты; z_j^i – j-ая мера защиты, входящая в i-ую «*молекулярную*» меру защиты; M – количество z_j^i образующих Z_i; $\alpha_j \in [0;1]$ – коэффициент влияния z_j^i на Z_i.

Так, например, организационные средства контроля за работой пользователей ИС и обслуживающего персонала (z_1^2), технические средства контроля за работой пользователей ИС и обслуживающего персонала (z_2^2), входящие в процедуру контроля за работой пользователей ИС и обслуживающего персонала (Z_2), действуют параллельно. Таким образом, значение Z_2 будет вычисляться как $\min(z_1^2; z_2^2)$.

Напротив, система обнаружения очагов возгорания (z_1^{12}), средства автоматического пожаротушения (z_2^{12}), средства ручного пожаротушения (z_3^{12}), входящие в средство защиты «Организация противопожарной защиты» (Z_{12}), действуют последовательно, образуя рубежи защиты. Таким образом, значение Z_{12} будет вычисляться как мультипликативная свертка ($z_1^{12}; z_2^{12}; z_3^{12}$).

Определение весов влияния концептов в иерархии. Для применения НКМ оценки уровня ИБ на практике необходимо определить множество весов ребер S графа G, отражающих степень влияния концептов друг на друга.

Для апробации подхода, предназначенного для решения этой задачи, было проведено исследование, основанное на методе экспертных оценок (методе «Дельфи»). В качестве экспертов были привлечены сотрудники сервисной службы ООО «Центр обучения Пилотинформ», специалисты по защите информации ООО «АпГрейд», а также преподаватели профильных кафедр Астраханского государственного технического университета (АГТУ) – всего 3 группы экспертов (9 человек).

Опрос проводился в 4 итерации, пока группы экспертов не пришли к единому мнению.

Каждой группе предлагалось заполнить следующее: таблицы, отражающие влияние $\{Z_i\}$ на $\{UZ_j\}$ и на $\{UG_j\}$; таблицу, описывающую взаимодействие $\{UZ_i\}$ и $\{UG_j\}$; таблицы, отражающие влияние $\{A_i\}$ на $\{DES_j\}$, и зависимость основных показателей безопасности $\{cK, cЦ, cД\}$ от $\{DES_i\}$; влияние $\{cK, cЦ, cД\}$ на K_0.

Влияние $\{Z_i\}$ на $\{UZ_j\}$ и на $\{UG_j\}$ представлено в таблицах 1 и 2. Для оценки силы нечетких связей между концептами экспертам было предложено использовать модифицированный метод нестрогого ранжирования [1, 2], в соответствии с которым производится нумерация критериев по возрастанию степени значимости их влияния. Причем допускается, что группе экспертов не удастся различить между собой некоторые критерии по важности. В этом случае при ранжировании эксперты помещают их рядом в произвольном порядке. Затем проранжированные критерии последовательно нумеруются. Оценка (ранг) критерия определяется его номером. Если на одном месте находится несколько неразличимых между собой по важности критериев, то за ранг каждого из них принимается номер всей группы – как целого объекта в упорядочении. При этом если Z_i не оказывает влияния на UZ_j (или на UG_j), то ранг влияния принимает значение «0» и не учитывается в дальнейших расчетах.

Таблица 1

Влияние $\{Z_i\}$ на $\{UZ_j\}$

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

Таблица 2

Влияние $\{Z_i\}$ на $\{UG_j\}$

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

Взаимодействие $\{UZ_i\}$ и $\{UG_j\}$ представлено в таблице 3. Для оценки наличия связей между концептами экспертам предлагалось поставить в ячейке (i, j) «+», если для реализа-

ции угрозы UG_j требуется наличие уязвимости UZ_i, или «–», если для реализации угрозы UG_j не требуется наличие уязвимости UZ_i .

Таблица 3

Взаимодействие $\{UZ_i\}$ и $\{UG_j\}$

Условное обозначение уязвимости	**Наименование уязвимости**	**Номер угрозы**		
		UZ_1	…	UZ_m
		Наименование угрозы	…	**Наименование угрозы**
UZ_1	Наименование	«+» или «–»	…	«+» или «–»
…	…	…	…	…
UZ_n	Наименование	«+» или «–»	…	«+» или «–»

Влияние $\{A_i\}$ на $\{DES_j\}$ представлено в таблице 4. Для оценки силы нечетких связей между концептами $\{A_i\}$ и $\{DES_j\}$ экспертам необходимо было занести в ячейку $(i; j)$ лингвистическое значение из терм-множества (2): QL = {Н, НС, С, ВС, В}, отражающее интенсивность (силу) влияния i-ой атаки на j-ое повреждение.

Таблица 4

Влияние $\{A_i\}$ на $\{DES_j\}$

Условное обозначение атаки	**Наименование атаки**	**Номер повреждения**		
		DES_1	…	DES_m
		Наименование повреждения	…	**Наименование повреждения**
A_1	Наименование	Интенсивность влияния	…	Интенсивность влияния
…	…	…	…	…
A_n	Наименование	Интенсивность влияния	…	Интенсивность влияния

Зависимость основных сервисов безопасности $\{cK, cЦ, cД\}$ от $\{DES_i\}$ представлена в таблице 5. Для оценки силы нечетких связей между концептами $\{cK, cЦ, cД\}$ и $\{DES_i\}$ каждой группе экспертов необходимо было занести в ячейку $(i; j)$ лингвистическое значение из терм-множества (2): QL = {Н, НС, С, ВС, В}, отражающее интенсивность влияния i-го повреждения на j-ый сервис безопасности.

Таблица 5

Зависимость основных сервисов безопасности $\{cK, cЦ, cД\}$ от $\{DES_i\}$

Условное обозначение повреждения	**Наименование повреждения**	**Наименование сервиса**		
		Конфиденциальность	**Целостность**	**Доступность**
DES_1	Наименование	Интенсивность влияния	Интенсивность влияния	Интенсивность влияния
…	Наименование	Интенсивность влияния	Интенсивность влияния	Интенсивность влияния
DES_n	Наименование	Интенсивность влияния	Интенсивность влияния	Интенсивность влияния

Влияние $\{cK, cЦ, cД\}$ на K_0 представлен таблице 6. Для оценки силы нечетких связей между данными концептами экспертам предлагалось использовать модифицированный метод нестрогого ранжирования, описанный выше.

Таблица 6

Влияние {*сК*, *сЦ*, *сД* } на K_0

Наименование сервиса	Ранг влияния на интегральный критерий безопасности ОИ
Конфиденциальность	Ранг влияния
Целостность	Ранг влияния
Доступность	Ранг влияния

Несмотря на трудоемкость и больш*и*е временные затраты на проведение опроса, метод «Дельфи» показал свою эффективность для решения поставленной задачи.

На основе описанной выше методики на языке высокого уровня C# был разработан программный комплекс «Нечеткое когнитивное моделирование системы комплексного обеспечения информационной безопасности». При помощи этого комплекса ЛПР может оценивать уровень ИБ организации в условиях возможности реализации угроз ИБ и на основе таких оценок принимать обоснованные решения по управлению этим уровнем. Входными данными программного продукта являются лингвистические оценки состояния средств защиты информации. Выходными данными – лингвистические оценки уровня конфиденциальности, целостности и доступности информации [4].

Применение разработанной методики на практике. Описанный подход был применен для оценки уровня ИБ в ООО «Центр обучения Пилот-Информ» (г. Астрахань).

Ответственный за ИБ сотрудник ООО «Центр обучения Пилот-Информ» оценил состояние СЗИ, используемых в организации, следующим образом:

- регламент защиты документов при их хранении – «Высокий»;
- контроль защиты документов при их хранении – «Средний»;
- организационные средства контроля за работой пользователей ИС и обслуживающего персонала – «Средний»;
- технические средства контроля за работой пользователей ИС и обслуживающего персонала – «Средний»;
- использование сертифицированного лицензионного ПО – «Высокий»;
- организационные меры разграничения доступа к ИА – «Выше среднего»;
- технические меры разграничения доступа к ИА – «Выше среднего»;
- программно-аппаратные меры разграничения доступа к ИА – «Выше среднего» и т.д.

Объективность этих оценок обуславливалась следующими факторами: компетентностью специалиста, осуществлявшего оценивание, в отношении вопросов ИБ; наличием у него опыта работы в организации; отсутствием у него личной заинтересованности в искажении оценок.

С использованием программного комплекса, реализующего описанную выше методику, на основании полученной от ЛПР информации была проведена оценка состояния основных показателей ИБ (свойств «Конфиденциальность», «Целостность», «Доступность») ООО «Центр обучения Пилот-Информ». Эта оценка дала следующие результаты:

- уровень конфиденциальности – «Средний» ($\Omega = 1{,}0$);
- уровень целостности – «Ниже среднего» ($\Omega = 0{,}75$);
- уровень доступности – «Ниже среднего» ($\Omega = 0{,}75$).

Полученная оценка послужила основанием для разработки рекомендаций по усилению мер обеспечения уровня конфиденциальности информации: усиление контроля над работой сотрудников; доработка регламента аудита за инцидентами ИБ; проведение для сотрудников тренингов, посвященных вопросам обеспечения ИБ и т.д. Реализация этих мер в организации позволила обеспечить следующее: повысить уровень конфиденциальности до состояния «Выше среднего» с индексом схожести (степенью принадлежности итогового уровня конфиденциальности к значению «Выше среднего») 0,8; для целостности и доступности информации повысить индекс схожести до значений 1,0 и 0,9 соответственно.

Заключение. Разработанная методика оценки уровня ИБ в условиях возможности реализации угроз ИБ позволяет учесть нечеткий характер суждений ЛПР о состоянии СЗИ, а также нечеткость связей между концептами в рамках предложенной НКМ.

Программная реализация изложенной методики была осуществлена на языке C#. Созданный программный продукт позволяет ЛПР не только оперативно оценивать уровень основных показателей ИБ (конфиденциальность, целостность, доступность), но и вырабатывать обоснованное суждение о необходимости синтеза управляющих решений для вывода указанных показателей на необходимый целевой уровень.

Список литературы

1. Ажмухамедов А. И. Мотивационное, институциональное и информационное управление персоналом коммерческого банка / А. И. Ажмухамедов, Т. А. Копытина // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 2. – С. 10–20.

2. Ажмухамедов И. М. Информационная безопасность. Системный анализ и нечеткое когнитивное моделирование : монография / И. М. Ажмухамедов. – Москва : LAP LAMBERT Academic Publishing GmbH & Co. KG, 2012. – 385 с.

3. Ажмухамедов И. М. Методология моделирования плохо формализуемых слабо структурированных социотехнических систем / И. М. Ажмухамедов, О. М. Проталинский // Вестник Астраханского государственного технического университета. Сер. Управление, вычислительная техника и информатика. – 2013. – № 1. – С. 144–154.

4. Ажмухамедов И. М. Нечеткое когнитивное моделирование системы комплексного обеспечения информационной безопасности / И. М. Ажмухамедов, О. М. Князева, Ф. В. Романов // Свидетельство о гос. регистрации программы для ЭВМ № 2015615682. – Заявка № 2015611005 зарегистр. в реестре программ для ЭВМ 22 мая 2015 г.

5. Борисов В. В. Нечеткие модели и сети / В. В. Борисов, В. В. Круглов, А. С. Федулов. – Москва : Горячая линия-Телеком, 2012. – 284 с.

6. Брумштейн Ю. М. ИКТ-компетентность стран, регионов, организаций и физических лиц: системный анализ целей, направлений и методов оценки / Ю. М. Брумштейн, А. Б. Кузьмина // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 2. –С. 47–63.

7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Взамен ГОСТ 50922–96 ; введен 2008–02–01. – Москва : Национальный стандарт Российской Федерации, 2008. – 12 с.

8. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – Взамен ГОСТ 51275–99 ; введен 2008–02–01. – Москва : Национальный стандарт Российской Федерации, 2008. – 12 с.

9. ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – Введен 2009–10–01. – Москва : Национальный стандарт Российской Федерации, 2009. – 20 с.

10. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – Киев : Диасофт, 2004. – 992 с.

11. Копылов А. В. Модель принятия решения задачи определения параметров стратегического потенциала предприятия в условиях неопределенности / А. В. Копылов, Б. Х. Санжапов // Интернет-Вестник Волгоградского государственного архитектурно-строительного университета. – Режим доступа: http://vestnik.vgasu.ru/attachments/KopylovSanzhapov1-2013_10(30).pdf (дата обращения: 01.09.2015), свободный. – Заглавие с экрана. – Яз. рус.

12. Максимов В. ИАналитические основы применения когнитивного подхода при решении слабоструктурированных задач / В. И. Максимов, Е. К. Корноушенко // Труды Института проблем управления Российской академии наук. – 1999. – Т. 2. – С. 95–109.

13. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных // ФСТЭК России. – Режим доступа: http://fstec.ru/component/attachments/download/290 (дата обращения: 01.09.2015), свободный. – Заглавие с экрана. – Яз. рус.

14. Обзор методик анализа рисков информационной безопасности информационной системы предприятия // CYBERLENINKA. – Режим доступа: http://cyberleninka.ru/article/n/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya (дата обращения: 01.09.2015), свободный. – Заглавие с экрана. – Яз. рус.

15. Charitoudi K. A Socio-Technical Approach to Cyber Risk Management and Impact Assessment / K. Charitoudi, A. Blyth // Journal of Information Security. – 2013. – № 3. – P. 33–41.

16. Facilitated risk analysis PROCESS (FRAP) // IT Today. – Available at: http://www.itto-day.info/AIMS/DSM/85-01-21.pdf (acessed: 01.09.2015).

17. OCTAVE // CERT. – Available at: http://www.cert.org/resilience/products-services/octave/index.cfm (accessed: 01.09.2015).

18. Rao P. Ranking generalized fuzzy numbers using area, mode, spreads and weight / P. Rao, N. Shankar // International Journal of Applied Science and Engineering. – 2012. – № 10, vol. 1. – P. 41–57.

19. Shahri A. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS / A. Shahri, Z. Ismail // Journal of Information Security. – 2012. – № 3. – P. 169–176.

References

1. Azhmukhamedov A. I., Kopytina T. A. Motivatsionnoe, institutsionalnoe i informatsionnoe upravlenie personalom kommercheskogo banka [Motivational, institutional and information management personnel of a commercial bank]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 2, pp. 10–20.

2. Azhmukhamedov I. M. *Informatsionnaya bezopasnost. Sistemnyy analiz i nechetkoe kognitivnoe modelirovanie* [Information Security. System analysis and fuzzy cognitive modeling], Moscow, LAP LAMBERT Academic Publishing GmbH & Co. KG Publ. House, 2012. 385 p.

3. Azhmukhamedov I. M., Protalinskiy O. M. Metodologiya modelirovaniya plokho formalizuemykh slabo strukturirovannykh sotsiotekhnicheskikh system [Modelling methodology bad formalizable poorly structured social engineering systems]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya. Upravlenie, vychislitelnaya tekhnika i informatika* [Bulletin of the Astrakhan State Technical University. Series: Management, Computer Facilities and Informatics], 2013, no. 1, pp. 144–154.

4. Azhmukhamedov I. M., Knyazeva O. M., Romanov F. V. Nechetkoe kognitivnoe modelirovanie sistemy kompleksnogo obespecheniya informatsionnoy bezopasnosti [Fuzzy cognitive modeling of integrated information security]. *The Certificate of Registration of Computer Programms no. 2015615682. The application №2015611005 registered in the registry of the computer programs May 22, 2015.*

5. Borisov V. V., Kruglov V. V., Fedulov A. S. *Nechetkie modeli i seti* [Fuzzy models and networks], Moscow, Goryachaya liniya-Telekom Publ., 2012. 284 p.

6. Brumshteyn Yu. M., Kuzmina A. B. IKT-kompetentnost stran, regionov, organizatsiy i fizicheskikh lits: sistemnyy analiz tseley, napravleniy i metodov otsenki [ICT competence of countries, regions, organizations and individuals: systematic analysis of the objectives, directions and methods of assessment]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 2, pp. 47–63.

7. GOST R 50922-2006. Data protection. Basic terms and definitions. Instead of GOST 50922–96, introduced 2008–02–01. Moscow, National Standard of the Russian Federation Publ. House, 2008. 12 p.

8. GOST R 51275-2006. Data protection. Object information. Factors influencing the information. General. Instead of GOST 51275–99, introduced 2008–02–01. Moscow, National Standard of the Russian Federation Publ. House, 2008. 12 p.

9. GOST R 53114-2008. Data protection. Ensuring information security in the organization. Basic terms and definitions. Introduced 2009–10–01. Moscow, National Standard of the Russian Federation Publ. House, 2009. 20 p.

10. Domarev V. V. *Bezopasnost informactsionnykh tekhnologiy. Sistemnyy podkhod* [Safety of information technology. Systems approach], Kiev, Diasoft Publ., 2004. 992 p.

11. Kopylov A. V, Sanzhapov B. Kh. Model prinyatiya resheniya zadachi opredeleniya parametrov strategicheskogo potentsiala predpriyatiya v usloviyakh neopredelennosti [Model the decision problem of determining the parameters of the strategic potential of the enterprise in the face of uncertainty]. *Internet-Vestnik Volgogradskogo gosudarstvennogo arkhitekturno-stroitelnogo universiteta* [Internet Bulletin of the

Volgograd State University of Architecture and Civil Engineering]. Available at: http://vestnik.vgasu.ru/attachments/KuvalkinKuvalkinSanzhapovSereda1-2013_10(30).pdf. (accessed: 01.09.2015).

12. Maksimov V. I., Kornoushenko Ye. K. Analiticheskie osnovy primeneniya kognitivnogo podkhoda pri reshenii slabostrukturirovannykh zadach [Analytical basis for the use of the cognitive approach in solving semistructured problems]. *Trudy Instituta problem upravleniya Rossiyskoy akademii nauk* [Proceedings of the Institute of Control Sciences of Russian Academy of Sciences], 1999, no. 2, pp. 95–109.

13. Metodika opredeleniya aktualnykh ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh [Methods of determining the actual threat of personal data security at their processing within the information systems of personal data]. *FSTEK Rossii* [The Federal Service for Technical and Export Control of Russia]. Available at: http://fstec.ru/component/attachments/download/290 (accessed: 01.09.2015).

14. Obzor metodik analiza riskov informatsionnoy bezopasnosti informatsionnoy sistemy predpriyatiya. Tekst nauchnoystati po spetsialnosti «Ekonomika i ekonomicheskie nauki» [Review of methods of information security risk analysis of enterprise information system. The text of scientific articles on «Economics and economic sciences»]. *CYBERLENINKA*. Available at: http://cyberleninka.ru/article/n/obzor-metodik-analiza-riskov-informatsionnoy-bezopasnosti-informatsionnoy-sistemy-predpriyatiya (accessed: 01.09.2015).

15. Charitoudi K., Blyth A. A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. *Journal of Information Security*, 2013, no. 3, pp. 33–41.

16. Facilitated risk analysis PROCESS (FRAP). *IT Today*. Available at: http://www.ittoday.info/AIMS/DSM/85-01-21.pdf (acessed: 01.09.2015).

17. OCTAVE. *CERT*. Available at: http://www.cert.org/resilience/products-services/octave/index.cfm (accessed: 01.09.2015).

18. Rao P., Shankar N. Ranking generalized fuzzy numbers using area, mode, spreads and weight. *International Journal of Applied Science and Engineering*, 2012, no. 10, vol. 1, pp. 41–57.

19. Shahri A., Ismail Z. A Tree Model for Identification of Threats as the First Stage of Risk Assessment in HIS. *Journal of Information Security*, 2012, no. 3. , pp. 169–176.