И. М. Ажмухамедов

МОДЕЛИРОВАНИЕ СИСТЕМ КОМПЛЕКСНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

Введение

В информационных системах (ИС) современного вуза хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Рост преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Создание эффективных механизмов управления информационными ресурсами системы высшего образования в современных условиях невозможно без научного обоснования и практической реализации сбалансированной политики информационной безопасности (ИБ) вуза, которая должна формироваться на основе разработки качественного и количественного (математического) описания процесса комплексного обеспечения ИБ, включающего:

- введение количественных индикаторов и критериев безопасности информационного обмена;
- разработку сценариев возможных нарушений основных сервисов безопасности информационных активов (конфиденциальность, целостность, доступность);
- определение значимости сервисов информационной безопасности при управлении различными информационными ресурсами вуза;
- выработку оптимальных решений, направленных на обеспечение ИБ.

При этом необходимо учесть, что системы комплексного обеспечения информационной безопасности (КОИБ) представляют собой яркий пример социотехнических систем (СТС): в них важнейшие управляющие решения принимает человек, и в то же время основная их часть направлена на уменьшение антропогенных угроз, источниками которых являются люди. Наличие антропогенного фактора превращает описание таких систем в плохо формализуемую (ПФ) проблему [1].

Для решения задачи обеспечения надежной защиты информации (ЗИ) ведущими отечественными и зарубежными исследователями в области теории информационной безопасности проводятся весьма интенсивные и крупномасштабные исследования.

Однако наличие антропогенного фактора, подверженность процессов ЗИ случайному влиянию, невозможность количественного измерения большинства параметров, сильная распределенность значительной части не имеющих четких границ СТС КОИБ (что влечет за собой их слабую структурированность (СС)) приводят к тому, что классические методы математического моделирования оказываются практически непригодными для описания такого рода социотехнических систем.

Возникает необходимость учета при формализации процессов, происходящих в СТС КОИБ, особенностей, связанных с поведением человека, как важнейшего элемента системы. При этом формальная модель должна опираться на методы, основанные на воспроизведении интеллектуальной деятельности лица, принимающего решения (ЛПР), что позволит снизить степень субъективности принимаемых им решений и, как следствие, повысит эффективность управления СТС, выведя ее на более высокий уровень.

Наиболее удобным математическим аппаратом для описания и исследования социотехнических систем, позволяющим реализовать указанные требования и объединить при моделировании аналитические, статистические, лингвистические описания различных подсистем, является нечеткое

когнитивное моделирование (НКМ) — одно из направлений современной теории поддержки принятия решений при управлении ПФ СС системами. Неоспоримыми достоинствами НКМ по сравнению с другими методами являются возможность формализации численно не измеримых факторов и использования неполной, нечеткой и даже противоречивой информации [2].

Модель системы комплексного обеспечения информационной безопасности вуза

Для построения НКМ оценки уровня ИБ вуза согласно методике, изложенной в [3–4], необходимо связать данные по составу угроз, уязвимостей, средств защиты между собой и рассмотреть влияние потенциально возможных атак на основные сервисы информационной безопасности.

Можно выделить следующие типы угроз информационным активам вуза:

- непреднамеренные субъективные угрозы (неумышленное повреждение или отключение оборудования; неумышленное удаление или искажение файлов с важной информацией; неумышленное удаление программ; порча носителей информации, ввод ошибочных данных и т. п.);

- преднамеренные субъективные угрозы (преднамеренное физическое разрушение системы; вывод из строя наиболее важных компонентов ИС, отключение подсистем обеспечения ИС, преднамеренное нарушение режимов эксплуатации устройств или режимов использования ПО, хищение носителей информации и т. п.);

- техногенные угрозы (сбой или отказ технических средств обработки информации, сбой или отказ вспомогательных технических средств, сбой или отказ систем электроснабжения, сбой или отказ систем климат-контроля и т. п.);

- стихийные угрозы (пожар, наводнение, землетрясение, пыльные бури экстремально высокая/низкая температура и т. п.).

Каждая из перечисленных угроз UG_j имеет априорную вероятность возникновения, зависящую от привлекательности информационного актива для злоумышленника, уровня его квалификации, состояния внешней инфраструктуры, окружающей объект информатизации, климатических условий, месторасположения объекта и т. д. Любая из угроз множества $UG = \{UG_j\}$ может реализоваться в виде атаки на информационные активы при наличии соответствующей уязвимости.

К основным уязвимостям UZ_k информационных систем образовательных учреждений можно отнести: отсутствие утвержденной концепции ИБ, наличие ПЭМИН, ошибки в ПО, несоблюдение режима охраны на ОИ, нештатные режимы эксплуатации ТС, нештатные режимы использования ПО, несоблюдение мер обеспечения ИБ, низкую надежность ТСОИ, низкую надежность вспомогательных ТС, старение и размагничивание носителей информации, низкую надежность ПО и т. д.

Средства защиты информации (организация процедуры хранения документов, разработка процедуры оперативного реагирования на инциденты, административные и технические средства контроля за работой пользователей, использование только сертифицированного лицензионного ПО, разграничение доступа к ПО, резервное копирование, обучение сотрудников основам ИБ, формирование корпоративной культуры и т. д.) образуют множество мер противодействия $Z = \{ Z_i \}$.

Таким образом, на нижнем уровне иерархии G при построении НКМ КОИБ вуза располагаются средства и механизмы защиты Z, действия которых уменьшают вероятность возникновения угроз UG и ослабляют степень уязвимостей UZ, расположенных на уровень выше. Угрозы и уязвимости, в свою очередь, предопределяют вероятность возникновения атак A, которые негативно влияют на сервисы безопасности SRV.

В качестве наиболее значимых для вуза сервисов безопасности выберем конфиденциальность, целостность и доступность. Эти сервисы в совокупности определяют интегральный показатель комплексной информационной безопасности учебного заведения K_0 и влияют на рейтинговые

показатели вуза: репутацию, материально-техническое состояние, финансовую устойчивость, качество образовательного процесса и т. п.

Таким образом, в качестве модели социотехнической системы КОИБ вуза выступает кортеж:

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

где G — ориентированный граф, имеющий одну корневую вершину и не содержащий горизонтальных ребер в пределах одного уровня иерархии; QL — набор качественных оценок уровней каждого фактора в иерархии (лингвистическая переменная); S — множество весов ребер графа G, отражающих степень влияния концептов на элементы следующего уровня иерархии; R — набор правил для вычисления значений концептов на каждом из уровней иерархии G; Ω — индекс схожести, позволяющий распознавать лингвистические значения концептов. В свою очередь, G также представляет собой кортеж:

$$G = <\{GF_i\}; \{GD_{ij}\}>, \quad (2)$$

где $\{GF_i\}$ — множество вершин графа (факторов или концептов в терминологии НКМ); $\{GD_{ij}\}$ — множество дуг, соединяющих i-ю и j-ю вершины (множество причинно-следственных связей между концептами); $GF_0 = K_0$ — корневая вершина, отвечающая цели функционирования системы КОИБ в целом (целевой концепт).

Далее необходимо в каждой из информационных систем вуза (АСУ «Деканат», АСУ «Учебный процесс», АСУ «Бухгалтерия», АСУ «Абитуриент» и т. д.) выделить и проранжировать по степени значимости информационные активы, которые могут быть подвержены атакам.

Из множеств UG и UZ нужно отобрать угрозы и уязвимости, характерные для каждого из активов. Затем необходимо составить перечень имеющихся в вузе средств обеспечения ИБ и проанализировать влияние этих средств на угрозы и уязвимости, выявленные на предыдущем этапе.

При этом все оценки задаются с помощью лингвистической переменной «Уровень фактора» с терм-множеством:

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

В качестве семейства функций принадлежности выступает стандартный пятиуровневый 01-классификатор [5], где функции принадлежности μ_F — трапециевидные нечеткие числа (НЧ):

Н (0; 0; 0,15; 0,25); НС (0,15; 0,25; 0,35; 0,45); С (0,35; 0,45; 0,55; 0,65); ВС (0,55; 0,65; 0,75; 0,85); В (0,75; 0,85; 1; 1).

Суть данного нечеткого классификатора в том, что если о факторе неизвестно ничего, кроме того, что он может принимать любые значения в пределах [0;1] (принцип равнопредпочтительности), и надо провести ассоциацию между качественной и количественной оценками фактора, то предложенный классификатор делает это с максимальной достоверностью. При этом сумма всех функций принадлежности для любого $x \in [0;1]$ равна единице, что указывает на его непротиворечивость.

Применение классификатора позволяет перейти от качественного описания уровня параметра к стандартному количественному виду соответствующей функции принадлежности μ_F из множества нечетких трапециевидных чисел. При этом в рамках такого представления четкие значения после их нормирования и приведения к интервалу [0;1] рассматриваются как частный случай, что позволяет совместно использовать в рамках одной модели *количественную и качественную* информацию.

Значения весов $s_{ij} \in [-1;1]$ из множества S могут быть получены экспертным путем. При этом необходимо учесть, что «мягкие» качественные измерения типа сравнения, отнесения к классу, упорядочения гораздо более надежны, чем назначение субъективных вероятностей, количественных оценок важности критериев, «весов» полезностей и т. п. [6, 7]. Кроме того, для эксперта в большинстве случаев затруднительно дать непосредственные численные оценки.

Поэтому предпочтительнее ранговые методы, при реализации которых требуется лишь упорядочить критерии.

Для оценки *силы нечетких связей между концептами* в [3] был предложен модифицированный метод нестрогого ранжирования, в соответствии с которым экспертом производится нумерация всех критериев по возрастанию степени их значимости. Причем допускается, что эксперту не удастся различить между собой некоторые критерии. В этом случае при ранжировании он помещает их рядом в произвольном порядке. Затем проранжированные критерии последовательно нумеруются. Оценка (ранг) критерия определяется его номером. Если на одном месте находятся несколько неразличимых между собой критериев, то за ранг каждого из них принимается номер всей группы как целого объекта в упорядочении.

Найденные предложенным способом оценки представляют собой обобщение системы весов Фишберна для случая смешанного распределения предпочтений, когда наряду с предпочтениями в систему входят и отношения безразличия. Веса Фишберна отражают тот факт, что системе убывающего предпочтения N альтернатив наилучшим образом отвечает система снижающихся по правилу арифметической прогрессии весов: предпочтение по Фишберну выражается в убывании на единицу числителя рациональной дроби весового коэффициента более слабой альтернативы.

Таким образом, при использовании метода нестрогого ранжирования на граф G необходимо наложить систему отношений предпочтения:

$$E = \{GF_i(e)GF_j \mid e \in (\succ; \approx)\}, \tag{3}$$

где GF_i и GF_j — факторы одного уровня иерархии G; $\succ$ — отношение предпочтения; $\approx$ — отношение безразличия.

Такая система позволяет определить обобщенные на случай предпочтения/безразличия факторов по отношению друг к другу веса Фишберна для каждой дуги GD_{ij} (веса связей).

Вычисления значений факторов в иерархии G производится по следующим формулам:

$$\overline{UZ}_j^{mn} = UZ_j^{mn} \cdot \prod_i Inv(Z_i^{mn})^{r_i^{mn}}; \tag{4}$$

$$\overline{UZ}^{mn} = Inv\left[\prod_j Inv(\overline{UZ}_j^{mn})^{s_j^{mn}}\right]; \tag{5}$$

$$\overline{UG}_n^m = UG_n^m \cdot \prod_i Inv(Z_i^{mn})^{v_i^{mn}}, \tag{6}$$

где $Inv(F) = 1 - \mu_F$ — инверсия фактора F; $\overline{UZ}_j^{mn}$ — остаточный (после применения средств защиты) уровень j-й уязвимости m-го актива относительно n-й угрозы; UZ_j^{mn} — исходный (до применения средств защиты) уровень j-й уязвимости m-го актива относительно n-й угрозы; Z_i^{mn} — уровень i-й защитной меры по отношению к n-й угрозе m-му активу; r_i^{mn} — весовой коэффициент, отражающий «вклад» i-й защитной меры в снижение уровня n-й угрозы m-у активу; $\overline{UZ}^{mn}$ — интегральный уровень уязвимости m-го актива по отношению к n-й угрозе; s_j^{mn} — весовой коэффициент, отражающий «вклад» $\overline{UZ}_j^{mn}$ в $\overline{UZ}^{mn}$; $\overline{UG}_n^m$ — остаточная вероятность существования n-й угрозы для m-го актива после применения совокупности средств защиты Z_i^{mn}; UG_n^m — исходная вероятность существования n-й угрозы m-му активу; v_i^{mn} — весовой коэффициент, отражающий «вклад» элемента защиты Z_i^{mn} в уменьшение угрозы UG_n^m.

При нахождении сверток векторного критерия в иерархии G под суммой или произведением лингвистических значений факторов понимается сумма или произведение соответствующих им нечетких чисел. В этом случае результат также является нечетким числом, которое необходимо лингвистически распознать, чтобы выработать суждение о качественном уровне показателей. Для этого вычисляется индекс схожести Ω, характеризующий степень соответствия значения фактора той или иной качественной оценке из терм-множества лингвистической переменной QL.

Индекс схожести Ω находится следующим образом:

$$\Omega = (1 + \tilde{\rho})/2; \quad (7)$$

$$\tilde{\rho} = (\rho_{in} - \rho_{out})/(\rho_{in} + \rho_{out}), \quad (8)$$

где $\rho_{in} = \int_{a_1}^{a_4} min[\mu_1(x); \mu_2(x)]dx$; $\rho_{out} = \left| \int_{b_1}^{b_4} [\mu_2(x)]dx - \rho_{in} \right|$; ($\rho_{out}$ — представляет собой площадь НЧ $B(b_1, b_2, b_3, b_4)$, характеризующего результат, лежащую вне эталонного НЧ $A(a_1, a_2, a_3, a_4)$, а ρ_{in} — площадь, лежащую внутри этого же эталонного НЧ).

Определенный таким образом индекс схожести, изменяясь от 0 до 1, характеризует близость найденной свертки к тому или иному нечеткому числу, которое, в свою очередь, соответствует элементу эталонного терм-множества. При этом обеспечивается семантическое соответствие: чем больше индекс схожести, тем выше степень соответствия вычисленного значения одному из элементов терм-множества QL.

Разница индексов схожести качественных оценок, полученных экспериментальным и теоретическим путями, может быть использована в *качестве метрической характеристики степени адекватности нечеткой когнитивной модели*.

Значения концептов НКМ в общем случае являются функциями времени t. При проведении динамических расчетов необходимо задать их начальные значения при $t = 0$. Тогда значение произвольного концепта K_j в дискретные моменты времени $t = 1, 2, 3, \ldots$ находится по формуле:

$$K_j(t) = K_j(t-1) + H(\Delta U_i, KBS, t), \quad (9)$$

где $H(\Delta U_i, KBS, t)$ — заданная кортежем KBS обобщенная функция влияния приращений ΔU_i, воздействующих на K_j концептов, на выходное значение K_j.

Алгоритм нахождения начальных значений концептов зависит от того, к какому типу процессов они относятся. В случае объективных процессов, вызванных техногенными или природными источниками, для этого используются методы статистического анализа, в результате применения которых после нормирования каждому фактору ставится в соответствие некоторая функция принадлежности на [0;1]. В случае же субъективного фактора для определения значения концепта необходимо построить «модель нарушителя» — НКМ более низкого уровня иерархии. При этом учитываются: уровень прав субъекта в системе; уровень мотивированности его действий, зависящий от степени лояльности, от его психологического портрета, преследуемых субъектом целей и т. п.; психофизические возможности нарушителя; его компетентность (уровень знаний и навыков); техническая оснащенность (используемые методы и средства) и т. д.

Реализация n-й угрозы m-му активу $\overline{UG}_n^m$ через оставшиеся уязвимости $\overline{UZ}^{mn}$ порождает атаку A_n^m, вероятность возникновения которой может быть оценена по формуле:

$$A_n^m = \overline{UG}_n^m \cdot \overline{UZ}^{mn}. \quad (10)$$

Если данная величина отлична от нуля, то есть, несмотря на предпринятые защитные мероприятия, в некоторый момент времени t^{mn} атака A_n^m все же возникла, необходимо задействовать меры Z_j^{mn} по снижению уровня таких нарушений безопасности (инцидентов).

Данные меры могут быть активизированы не сразу, а спустя некоторое время $(t_j^{mn})_{нач}$, необходимое для идентификации атаки и принятия решения о реагировании на нее. При достижении времени $(t_j^{mn})_{кон}$ действие этих мер прекращается либо в связи с окончанием инцидента, либо в связи с исчерпанностью ресурсов, обеспечивающих сдерживание атаки.

Во время действия данных мер остаточный уровень n-й атаки на m-й ресурс $\overline{A}_n^m$ может быть найден по формуле:

$$\overline{A}_n^m = A_n^m \cdot \prod_j Inv(Z_j^{mn})^{v_i^{mn}}, \quad (11)$$

где υ_j^{mn} — весовой коэффициент, отражающий вклад меры Z_j^{mn} в снижение уровня n-го инцидента (атаки) по отношению к m-му активу.

Инциденты безопасности при условии, что их уровень выше некоторого критического порога $(\overline{A}_n^m)_{крит}$ и продолжительность больше некоторого критического интервала времени $(t_j^{mn})_{крит}$, могут порождать новые или усиливать уже имеющиеся уязвимости системы, что должно найти отражение при оценке их уровня на следующем шаге по времени:

$$UZ_j^{mn}(t+1) = UZ_j^{mn}(t) \cdot Inv\left[\prod_n Inv(\overline{A}_n^m)^{\delta_j^{mn}}\right]. \quad (12)$$

Совокупность атак на m-й актив, в свою очередь, предопределяет уровень обеспеченности сервисов безопасности данного актива SRV_k^m:

$$SRV_k^m = \prod_n Inv(\overline{A}_n^m)^{w_n^{mk}}. \quad (13)$$

Если уровень какого-либо сервиса падает ниже критического значения, необходимо предпринять меры по его восстановлению, то есть реализовать мероприятия «блока ликвидации последствий» [4]. Результат действий на этом шаге можно формализовать с помощью следующей формулы:

$$\overline{SRV}_k^m = SRV_k^m Inv\left[\prod_j Inv(Z_j^{mk})^{\theta_j^{mk}}\right], \quad (14)$$

где $\overline{SRV}_k^m$ — уровень k-го сервиса m-го актива после реализации мер ликвидации последствий Z_j^{mk}; θ_j^{mk} — весовой коэффициент, отражающий вклад меры Z_j^{mk} в повышение уровня k-го сервиса безопасности m-го актива.

Так же как и в случае с мерами по снижению уровня инцидентов, до активизации данных мер проходит некоторое время $(t_j^{mk})_{нач}$, требующееся для идентификации уровня сервисов безопасности и принятия решения о необходимости их повышения. Действие этих мер прекращается в некоторый момент времени $(t_j^{mk})_{кон}$ либо в связи с достижением нужного уровня сервиса безопасности, либо в связи с исчерпанностью ресурсов для его повышения.

В качестве примера, иллюстрирующего приведенные выше рассуждения, можно рассмотреть следующую ситуацию. Предположим, что, несмотря на предпринятые превентивные меры, на объекте информатизации возник пожар. В этом случае для уменьшения последствий инцидента включится система пожаротушения. Возникновение пожара резко увеличит уровень других уязвимостей системы и создаст уязвимости, отсутствовавшие при штатной работе ОИ. Система пожаротушения отработает положенное время и отключится. Если за это время пожар не будет локализован и потушен, с высокой долей вероятности доступность информационных ресурсов будет нарушена. Возникнет необходимость ее восстановления, например, путем подключения к резервному (удаленному) серверу. Однако ресурсов резервного сервера и каналов связи с ним может оказаться недостаточно, чтобы длительное время поддерживать доступность ИС на нужном уровне. Следовательно, необходимо предусмотреть варианты полного восстановления сервисов за время, не превышающее время работы по резервному каналу.

Основываясь на значениях сервисов безопасности SRV_k^m для m-го актива, можно определить интегральный уровень безопасности K^m:

$$K^m = \prod_k (\overline{SRV}_k^m)^{\alpha_k^m}, \quad (15)$$

где α_k^m — весовой коэффициент, отражающий «вклад» k-го сервиса в интегральную оценку уровня безопасности m-го актива.

Интегральный показатель K_0 комплексной безопасности всего учебного заведения может быть найден по формуле:

$$K_0 = \prod_m (K^m)^{\beta_m}, \quad (16)$$

где β_m — весовой коэффициент, отражающий значимость m-го информационного актива в интегральной оценке комплексного уровня безопасности образовательного учреждения.

Для выработки суждений о качественном уровне показателей безопасности необходимо лингвистически распознать значения концептов, получаемые в иерархии G и представляющие собой НЧ. Для этого согласно формулам (7)—(8) вычисляется индекс схожести Ω, характеризующий степень соответствия значения фактора той или иной качественной оценке из терм-множества лингвистической переменной QL.

Таким образом, построенная динамическая нечеткая когнитивная модель дает возможность, последовательно пройдя все уровни ее иерархии и применяя формулы (4)—(16), моделировать процесс КОИБ во времени, оценивать уровень безопасности информационных активов вуза и вырабатывать рекомендации по его повышению.

Предложенный в работе подход был применен для решения задачи комплексного обеспечения информационной безопасности ФГБОУ ВПО «Астраханский государственный технический университет (АГТУ)».

Для оценки уровня ИБ в рамках НКМ были объединены данные по составу угроз, уязвимостей, средств защиты и рассмотрено влияние потенциально возможных атак на основные сервисы безопасности информационных активов (ИА) учебного заведения. При имеющихся в АГТУ средствах ЗИ интегральный уровень ИБ K_0 был оценен с помощь построенной НКМ как «средний» с Ω = 0,78.

С целью проверки адекватности полученной оценки были выбраны 13 угроз, направленных на основные сервисы безопасности ИС вуза, для каждой из отобранных угроз были определены пороговые уровни необходимых для их реализации компетенций «злоумышленника» и была сформирована команда для имитации этих угроз.

Формирование команды было осуществлено с помощью процедуры, предусматривающей два этапа [8]. На первом — оценивался уровень компетенций каждого из претендентов. На втором — на основе полученных данных отбирался наиболее подходящий состав исполнителей.

Была сформирована команда из 8 участников, которая в течение 3 месяцев тестировала систему КОИБ АГТУ. В результате из 53 попыток реализации антропогенных угроз 14 оказались успешными. Кроме того, была проанализирована статистика по имевшимся инцидентам, связанным с техногенными и природными угрозами ИБ, за 2009—2012 г.

Оценка уровня повреждений сервисов безопасности после реализации совокупности техногенных, природных и антропогенных угроз была произведена по методике, изложенной в [9]. Данные по оценке уровня сервисов ИБ вместе с полученными с помощью предложенной модели теоретическими значениями приведены в табл. 1.

Таблица 1.

Сервис безопасности	Эксперимент. оценка / Ω	Расчет. оценка / Ω	Отклон. Ω
Конфиденциальность	ВС / 1	ВС / 0,79	0,21
Целостность	С / 1	С / 0,81	0,19
Доступность	НС / 1	НС / 0,94	0,06

Отклоненияе индексов схожести теоретически рассчитанных и экспериментальных результатов не превышает 0,21, что для данного типа моделей, формализующих ПФ СС процессы, можно считать вполне допустимым. Это, в свою очередь, позволяет сделать вывод о достаточной адекватности предложенной модели.

В результате проведенного анализа были предложены дополнительные меры обеспечения ИБ АГТУ, включающие в себя, в том числе, и новые технические решения, которые позволили увеличить оценку уровня сервисов «целостность» и «доступность» до значения ВС (с Ω = 0,84 и 0,91 соответственно), а также повысить степень соответствия значению ВС для сервиса «конфиденциальность» до значения 0,86.

Выводы

Таким образом, предложенный подход к моделированию систем КОИБ позволяет учесть все их основные особенности: нечеткая когнитивная модель отражает нечеткость структуры системы в целом; нечеткие связи эффективно оцениваются с помощью весов Фишберна; «размытость» значений элементов системы и целей ее функционирования учитывается путем введения лингвистических переменных и соответствующих их терм-множеству нечетких классификаторов, многокритериальность — с помощью использования различных сверток векторного критерия.

Построенная НКМ адекватно отражает процесс обеспечения ИБ вуза, позволяет унифицировать подходы к управлению комплексной безопасностью и приступить к разработке соответствующих вычислительных процедур и модулей, которые могут быть в дальнейшем использованы в системах поддержки принятия решений.

СПИСОК ЛИТЕРАТУРЫ:

1. *Проталинский О. М., Ажмухамедов И. М.* Системный анализ и моделирование слабо структурированных и плохо формализуемых процессов в социотехнических системах // Инженерный вестник Дона. Электронный научно-инновационный журнал. 2012. № 3. URL: http://www.ivdon.ru/magazine/ archive/n3y2012/916/ (дата обращения: 26.06.2013).
2. *Максимов В. И., Корноушенко Е. К.* Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач // Труды ИПУ РАН. 1999. Т. 2. С. 95–109.
3. *Ажмухамедов И. М.* Анализ и управление комплексной безопасностью на основе когнитивного моделирования // Управление большими системами. Вып. 29. М.: ИПУ РАН, 2010. С. 5–15.
4. *Ажмухамедов И. М.* Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. № 2. С. 68–72.
5. *Недосекин А. О.* Нечеткий финансовый менеджмент. М.: Аудит и финансовый анализ, 2003.
6. *Асанов А. А., Ларичев О. И.* Влияние надежности человеческой информации на результаты применения методов принятия решений // Автоматика и телемеханика. 1999. № 5. С. 20–31.
7. *Ларичев О. И., Мошкович Е. М.* Качественные методы принятия решений. Вербальный анализ решения. М.: Наука, 2006.
8. *Ажмухамедов И. М., Ажмухамедов А. И.* Методика формирования команды для реализации IT-проектов на основе нечеткой когнитивной модели оценки компетенций // Прикладная информатика. 2011. № 4 (34). С. 70–76.
9. *Ажмухамедов И. М.* Оценка повреждений безопасности информационной системы на основе нечетко-когнитивного подхода // Проблемы информационной безопасности. Компьютерные системы. 2012. № 1. С. 7–11.