УДК 004.056

**Я. Н. Имамвердиев,** канд. техн. наук, зав. отделом, e-mail: yadigar@lan.ab.az,
Институт информационных технологий Национальной академии наук Азербайджана, г. Баку

# Нечеткая когнитивная модель стратегического управления информационной безопасностью электронного правительства

*Рассматриваются сущность и особенности применения нечеткого когнитивного моделирования в стратегическом управлении информационной безопасностью на уровне государства. Определены факторы стратегического управления информационной безопасностью, и на основе экспертного оценивания построена нечеткая когнитивная карта для управления информационной безопасностью электронного правительства. На основе разработанной когнитивной модели проанализированы результаты разных стратегий управления информационной безопасностью электронного правительства.*

***Ключевые слова:*** *информационная безопасность, управление информационной безопасностью, стратегия информационной безопасности, когнитивное моделирование, нечеткие когнитивные карты*

## Введение

В результате широкого внедрения информационных и коммуникационных технологий (ИКТ) в процессы государственного управления происходят фундаментальные преобразования в природе государства. Граждане широко участвуют в формировании и реализации государственной политики, формируется эффективная система взаимодействия и сотрудничества между государством, частным сектором и гражданским обществом. Этот феномен обозначается термином "электронное правительство" [1].

Следует подчеркнуть, что термин "electronic government" (e-government) часто переводится как "электронное правительство". Такой перевод сужает понятие и сводит вопрос только к государственному управлению, осуществляемому органами исполнительной власти. Но термин "e-government" подразумевает поддержку с помощью информационных и коммуникационных технологий деятельности во всех трех ветвях власти — законодательной, исполнительной и судебной. В работе [2] обсуждаются различные подходы к определению терминов "электронное правительство" и "электронное государство" и подчеркивается, что более правильным является использование термина "электронное государство", при этом многие источники допускают употребление двух этих терминов в качестве синонимов. Следуя устоявшейся терминологии в официальных документах, в данной статье используется термин "электронное правительство".

В условиях всесторонней глобализации, возрастающих рисков и неопределенностей общественных процессов информационная безопасность (ИБ) становится одной из основных функций самосохранения электронного правительства [2, 3]. Поэтому актуальным является управление системой обеспечения ИБ электронного правительства.

Управление ИБ электронного правительства является слабоструктурированной задачей [4, 5]: объект управления является сложной социотехнической системой, состоящей из автономных компонентов, каждый из которых действует целенаправленно. В системе происходят многочисленные процессы (социальные, политические, технологические), значительно взаимодействующие друг с другом. Эти процессы изменяются по времени, в них участвуют различные виды неопределенностей, но количественная информация о динамике процессов остается недоступной. Внешняя среда, окружающая электронное правительство, является потенциально "враждебной" средой. Как сами компоненты электронного правительства, так и внешняя среда являются источником многочисленных угроз, направленных на нарушение ИБ электронного правительства.

Для анализа и управления такого рода системами в настоящее время широко применяется когнитивный подход, который позволяет увидеть и осознать логику развития событий при большом числе взаимозависимых факторов [6, 7].

В этой работе на основе нечетких когнитивных карт предлагается когнитивная модель стратегического управления ИБ электронного правительства. Предлагаемый подход когнитивного моделирования перспективен в контексте создания интеллектуальных систем поддержки принятия решений, и его применение может существенно повысить эффективность стратегического управления и качество принимаемых решений в области обеспечения ИБ электронного правительства.

## Нечеткие когнитивные карты

Когнитивные карты (КК) впервые были предложены американским психологом Э. Толменом (E. Tolman) при изучении элементарных когнитивных процессов у крыс [8]. На основе экспериментов по обучению крыс в разных типах лабиринтов Толмен пришел к выводу, что в процессе взаимодействия с окружающей средой у животного формируется некая "когнитивная карта", или "мысленный план", всех характеристик лабиринта, которая совершенствуется при каждом следующем взаимодействии со средой.

Когнитивные карты являются робастными системами, которые могут моделировать очень сложные поведения. В своей работе Р. Аксельрод применил когнитивные карты при изучении структуры решений политических элит [9]. Он ввел понятия взвешенные КК и функциональные КК. Во взвешенных КК знак заменен положительным или отрицательным числом, которое показывает направление эффекта, а также его значение. В функциональных КК с каждой причинной связью ассоциируется функция, которая более точно показывает направление и значение эффекта. Эти два типа когнитивных карт дают больше гибкости, поскольку они могут обработать и предоставить более подробную информацию.

Нечеткие когнитивные карты (НКК) были предложены B. Kosko [10] как нечеткое расширение когнитивных карт. На самом деле НКК являются когнитивными картами, взвешенными с нечеткими весами. Обычно КК строятся путем сбора информации от экспертов, и эксперты, скорее всего, склонны выразить себя в качественных, а не в количественных терминах. С этой точки зрения более целесообразно использовать НКК, в которых концепции представляются лингвистически, с соответствующим нечетким множеством.

НКК комбинирует некоторые аспекты нечеткой логики и нейронных сетей в схеме представления эвристики и правила здравого смысла нечеткой логики с эвристикой обучения нейронных сетей. Эта структура представляется как взвешенный ориентированный граф, в котором вершины взаимно однозначно соответствуют факторам и в терминах которых описывается предметная область, а дуги отображают взаимовлияния между факторами (рис. 1).

Вес дуги между фактором $C_i$ и фактором $C_j$ может быть положительным, он означает, что увеличение значения фактора $C_i$ приводит к увеличению значения фактора $C_j$, в то же время уменьшение значения фактора $C_j$ приводит к уменьшению значения фактора $C_j$. Если вес дуги между фактором $C_i$ и фактором $C_j$ отрицательный, то увеличение значения фактора $C_i$ приводит к уменьшению значения фактора $C_j$, а уменьшение значения фактора $C_i$ приводит к увеличению значения фактора $C_j$.

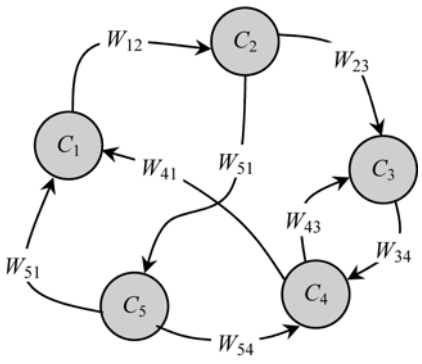


**Рис. 1. Пример нечеткой когнитивной карты**

В последнее десятилетие наблюдается повышенный интерес исследователей к построению нечетких когнитивных моделей во многих областях [11]. Методология НКК была успешно применена в представлении знаний [12], политических, социальных и социально-экономических исследованиях [13—15], стратегическом планировании [16] и принятии стратегических решений в нечеткой обстановке [17], бизнес-аналитике [18], экономическом прогнозировании [19], системах диспетчерского контроля [20], управлении ИТ-проектами [21], при оценке рисков качества программного обеспечения [22], в системах принятия решений в медицинской информатике [23], экологии [24, 25], интеллектуальном анализе данных [26] и т. д. Отметим, что в работе [27] когнитивная модель применена к моделированию и анализу состояния ИБ организации.

Для когнитивного моделирования управления ИБ электронного правительства необходимо:

- определить факторы, влияющие на состояние ИБ;
- построить матрицу взаимовлияний факторов;
- построить когнитивную модель управления ИБ;
- на разработанной модели отработать возможные стратегии управления ИБ электронного правительства.

## Факторы управления ИБ электронного правительства

НКК является одним из способов представления знаний. Для построения НКК должны использоваться знания и опыт экспертов в предметной области [28]. Эксперты определяют те факторы, которые лучше описывают предметную область. Факторами могут быть признаки, состояния или системные переменные. Эксперты идентифицируют, какие факторы являются центральными для моделирования системы, и выявляют, какие факторы влияют друг на друга, и для соответствующих факторов определяют позитивное или негативное влияние одного фактора на другое.

Для определения факторов, влияющих на управление ИБ электронного правительства, были проанализированы национальные стратегии кибербезопасности ряда стран [29], а также модельные стратегии международных организаций [30—33]. Эти стратегии разрабатывались с широким привлечением ведущих экспертов по ИБ и могут рассматриваться как достаточно хорошие источники аккумуляции знаний экспертов. В ходе анализа стратегий кибербезопасности был выделен ряд факторов, влияющих на управление ИБ электронного правительства, полный список которых представлен в табл. 1.

Рассмотрим краткое описание этих факторов.

***1. Правовые меры*** — для обеспечения ИБ необходимо создать адекватную нормативно-правовую базу. К нормативно-правовой базе относят планирование и разработку механизмов необходимой политики и регулирования, точное определение ролей, прав и обязанностей заинтересованных сторон, базовые мероприятия и инструкции действий по

Таблица 1

**Факторы, влияющие на управление ИБ электронного правительства**

| Факторы | Наименование фактора | Обозначение |
|---|---|---|
| $C_1$ | Правовые меры | *Legal* |
| $C_2$ | Организационные меры | *Org* |
| $C_3$ | Технические меры | *Tech* |
| $C_4$ | Развитие потенциала | *HR* |
| $C_5$ | Сотрудничество заинтересованных сторон | *Coop* |
| $C_6$ | Развитие угроз ИБ | *NewT* |
| $C_7$ | Уровень ИБ электронного правительства | *ISec* |

обеспечению ИБ и т. д. Предусматриваются также разработка основных механизмов реагирования на нарушения через расследование и судебное преследование за преступления и введение санкций за несоблюдение или нарушение закона.

Нормативно-правовые меры могут быть выработаны на основе правовой базы существующих правовых институтов и структур, занимающихся кибербезопасностью и киберпреступностью. Эта группа состоит из следующих показателей:

$C_{11}$. *Уголовное законодательство* — для предупреждения киберпреступности и присоединения к международной борьбе с киберопасностью необходимо развивать соответствующую правовую базу. Законодательство по киберпреступности может быть оценено по следующим уровням: отсутствует; разработано частично; является исчерпывающим.

$C_{12}$. *Регулирование и соответствие требованиям стандартов* — регулирование ИБ обозначает законы, касающиеся защиты данных, уведомлений о нарушении и требований сертификации/стандартизации. Законы также могут быть классифицированы по уровням: отсутствует; разработано частично; является исчерпывающим.

***2. Организационные меры*** — в стратегиях кибербезопасности предусматривается построение гибкой организационной структуры управления, направленной на обеспечение ИБ. Создание эффективных организационных структур необходимо для продвижения ИБ, борьбы с киберпреступностью и повышения роли мониторинга, предупреждения и реагирования на инциденты для обеспечения межведомственной, кросс-секториальной и трансграничной координации между новыми и существующими инициативами. Организационные меры можно оценить на основе существования и числа учреждений и стратегий, организующих развитие ИБ на национальном уровне. Подгруппа состоит из следующих показателей:

$C_{21}$. *Политика* — официально признанные национальные или по конкретным секторам стратегии ИБ.

$C_{22}$. *Дорожная карта для управления* — официально признанные национальные или по конкретным секторам планы управления для ИБ.

$C_{23}$. *Ответственный орган* — официально признанные национальные или по конкретным секторам агентства по ИБ.

$C_{24}$. *Национальный бенчмаркинг* — официально признанные национальные или по конкретным секторам упражнения бенчмаркинга, используемые для измерения уровня ИБ.

***3. Технические меры*** — технология является первой линией обороны против киберугроз и вредоносных Интернет-агентов. Без адекватных технических мер и потенциала для выявления и реагирования на кибератаки электронное правительство и его субъекты остаются уязвимыми для киберугроз. Поэтому электронное правительство должно быть способно развивать стратегии по установлению принятых минимальных критериев безопасности и схем аккредитации для программного обеспечения и информационных систем.

$C_{31}$. *Система раннего предупреждения* — предусматриваются повышение готовности к инцидентам, уменьшение времени реагирования, разработка плана восстановления после аварий и механизмов защиты критической информационной инфраструктуры (например, национальный план действий в особых условиях, правило поведения в киберпространстве, информирование о ситуации).

$C_{32}$. *Стандарты* — этот показатель определяет существование уполномоченной правительством структур(ы) для реализации международно признанных стандартов по ИБ в государственном секторе и в критических инфраструктурах.

$C_{33}$. *Сертификация* — этот показатель определяет существование утвержденной правительством структур(ы) для сертификации и аккредитации государственных учреждений и специалистов государственного сектора по международно признанным стандартам в области ИБ.

***4. Развитие потенциала*** — развитие человеческого и институционального потенциала существенно для первых трех факторов (правовые, технические и организационные). Понимание технологий, рисков и последствий может помочь в разработке более совершенного законодательства, более эффективных политик и стратегий, а также для лучшей организации различных ролей и обязанностей.

Подгруппа состоит из следующих показателей:

$C_{41}$. *Подготовка кадров* — указывается на необходимость новых образовательных программ, уделяющих внимание на образование IT-специалистов и профессионалов по кибербезопасности. В некоторых национальных стратегиях кибербезопасности ставится цель усовершенствования образовательных программ специалистов по кибербезопасности для надежного обеспечения кибербезопасности, а также сертификации специалистов по ИБ.

$C_{42}$. *Осведомленность населения* — программы осведомления, предусматривающие обучение пользователей новым моделям поведения и работы в киберпространстве.

$C_{43}$. *Научные исследования и инновации* — необходимо проведение комплексных научно-практических исследований, направленных на решение проблем безопасности и устойчивости как существующих, так и будущих систем и сервисов. В ряде стратегий предусматриваются определение ведущих центров в области исследований по кибербезопасности и обеспечение инвестициями.

$C_{44}$. *Разработка стандартов* — любые официально признанные национальные или по конкретным секторам программы/проекты исследования и разработка стандартов по ИБ, лучших практик и правил для применения в государственном и частном секторах.

$C_{45}$. *Сертификация государственных органов* — этот показатель можно измерить по числу государственных учреждений, сертифицированных в соответствии с международно признанными стандартами.

***5. Сотрудничество заинтересованных сторон*** — для управления ИБ требуется участие всех заинтересованных сторон, поэтому государственные структуры и частный сектор должны работать в тесном сотрудничестве. Международное сотрудничество является жизненно важным, поскольку все зависимы от одного киберпространства. Сотрудничество должно реализовываться путем обмена информацией и передовым опытом, знаниями на различных уровнях.

Национальное и международное сотрудничество может быть измерено на основе существования числа партнерств, совместных структур и сетей обмена информацией. Подгруппа состоит из следующих показателей:

$C_{51}$. *Внутригосударственное сотрудничество* — официально признанное национальное или по конкретным секторам партнерство для трансграничного совместного использования активов ИБ с другими государствами.

$C_{52}$. *Межведомственное сотрудничество* — любые официально признанные национальные или по конкретным секторам программы для обмена активами ИБ (люди, процессы, инструменты) в государственном секторе.

$C_{53}$. *Партнерство государственного и частного секторов* — официально признанные национальные или по конкретным секторам программы для обмена активами ИБ между государственным и частным секторами.

$C_{54}$. *Международне сотрудничество* — международное сотрудничество может охватывать законодательные меры, реагирование на инциденты, научные исследования, сертификацию аппаратного и программного обеспечения.

***6. Развитие угроз ИБ*** — в этой работе рассматриваются следующие показатели:

$C_{61}$. *Развитие акторов угроз* — динамика изменений в акторах угроз (инсайдеры, активисты/хактивисты, криминалы, стратегические конкуренты, враждебные государства).

$C_{62}$. *Появление новых типов атак* — разработка и осуществление хорошо скоординированных, целенаправленных атак [34], усовершенствование существующих методов атак, многошаговые, многовекторные атаки, атаки нулевого дня (0-дня), динамические, полиморфные вредные программы и т. д.

$C_{63}$. *Развитие целей атак* — развитие новых информационных технологий (критические инфраструктуры, мобильные, "облачные" вычисления, Интернет вещей и т. д.) и электронные услуги.

***7. Уровень ИБ электронного правительства*** — интегральная оценка уровня ИБ электронного правительства, определяется на основе основных показателей рисков ИБ электронного правительства. Рассматриваются следующие три уровня ИБ в зависимости от соответствующего уровня рисков [35]:

- высокий уровень ИБ — соответствует низкому уровню рисков;
- удовлетворительный уровень ИБ — соответствует приемлемому уровню рисков;
- низкий уровень ИБ — соответствует высокому уровню рисков.

### Построение матрицы взаимовлияний факторов

При построении НКК наиболее сложной задачей является назначение весов взаимовлияний факторов. В работе [20] приводятся два алгоритма вычисления матрицы взаимовлияний факторов.

В первом алгоритме каждый эксперт оценивает веса взаимовлияний как число из интервала $[-1, 1]$. Далее эти матрицы весов взаимовлияний агрегируются как осредненное значение суммы весов или применяется пороговая функция (например, сигмоидная функция). Так как опыт и знания экспертов об объекте оценки могут быть разными, то каждому эксперту можно назначить неотрицательный числовой вес доверия. С учетом весов доверия экспертов агрегированные значения весов взаимовлияний могут быть вычислены следующей формулой (учитываются только веса одинакового знака):

$$W_{ij} = \frac{\sum_{k=1}^{m} b_k w_{ij}^k}{m}, \qquad (1)$$

где $w_{ij}^k$ — оценка веса взаимовлияния между $C_i$ и $C_j$ $k$-м экспертом; $b_k$ — вес доверия $k$-го эксперта; $m$ — число экспертов. Если оценка эксперта отличается от оценок большинства экспертов, то он штрафуется — ему присваивают очень низкий или нулевой вес доверия. Для более детального ознакомления с описанием этого алгоритма читателям рекомендуется работа [20].

Второй алгоритм для построения матрицы взаимовлияний факторов НКК использует нечеткую логику. Эксперты описывают каузальность между факторами с помощью лингвистических переменных. Каждый эксперт определяет влияние одного фактора на другой фактор как "негативное" или "позитивное" и после этого описывает степень влияния

с помощью лингвистических переменных типа "сильный", "слабый" и т. д. [36]. Преимуществом этой методологии является то, что экспертам не нужно присваивать числовые веса каузальным связям, они описывают степень каузальных связей между факторами привычными терминами.

Следуя этой методологии, влияние одного фактора на другой можно интерпретировать как лингвистическая переменная, которая принимает значения в универсальном множестве [−1, 1]. Ее множество термов может быть следующим [11]:

$T$(влияние) = {негативно очень сильное, негативно сильное, негативно среднее, негативно слабое, негативно нулевое, позитивно слабое, позитивно среднее, позитивно сильное, позитивно очень сильное}.

Ниже определяется семантическое правило, и эти термы характеризуются нечеткими множествами, функции принадлежности которых показаны на рис. 2.

- $T$(негативно очень сильное) = нечеткое множество для "влияние ниже −75 %" с функцией принадлежности $\mu_{nvs}$;
- $T$(негативно сильное) = нечеткое множество для "влияние близко к −75 %" с функцией принадлежности $\mu_{ns}$;
- $T$(негативно среднее) = нечеткое множество для "влияние близко к −50 %" с функцией принадлежности $\mu_{nm}$;
- $T$(негативно слабое) = нечеткое множество для "влияние близко к −25 %" с функцией принадлежности $\mu_{nw}$;
- $T$(негативно нулевое) = нечеткое множество для "влияние близко к 0" с функцией принадлежности $\mu_z$;

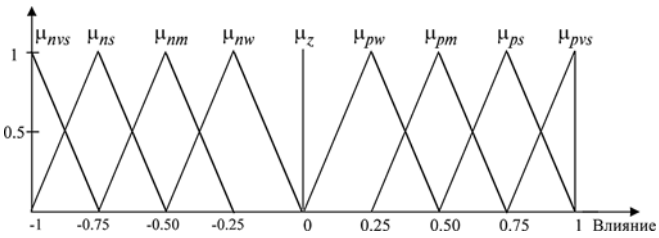


**Рис. 2. Термы лингвистической переменной "Влияние"**

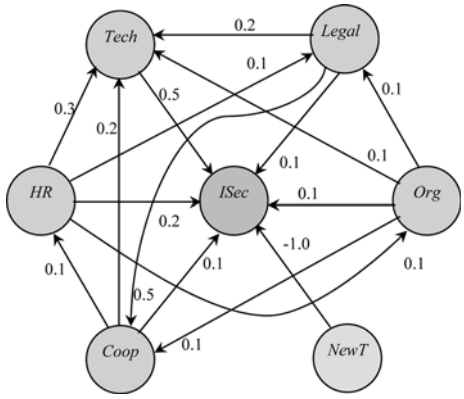


**Рис. 3. НКК модель управления ИБ "электронного государства" в виде графа**

- $T$(позитивно слабое) = нечеткое множество для "влияние близко к 25 %" с функцией принадлежности $\mu_{pw}$;
- $T$(позитивно среднее) = нечеткое множество для "влияние близко к 50 %" с функцией принадлежности $\mu_{pm}$;
- $T$(позитивно сильное) = нечеткое множество для "влияние близко к 75 %" с функцией принадлежности $\mu_{ps}$;
- $T$(позитивно очень сильное) = нечеткое множество для "влияние выше 75 %" с функцией принадлежности $\mu_{pvs}$.

Лингвистические переменные, которые описывают все взаимодействия факторов, агрегируются, и общая лингвистическая переменная преобразуется в интервал [−1, 1] с помощью дефаззификации. В этой работе использовался метод центра тяжести для дефаззификации [37].

НКК имеют те же основные недостатки, что и другие нечеткие системы: они не в состоянии обучаться самостоятельно. При доступности соответствующих данных веса взаимовлияний факторов можно улучшить, используя механизмы обучения нейронных сетей. Большинство таких подходов основано на методе обучения Хебба (см., например, [38, 39]), но существуют также подходы с использованием эволюционных вычислений [40].

Для вычисления матрицы взаимовлияний факторов в модели НКК для стратегического управления электронным правительством были привлечены пять экспертов по управлению ИБ. Эксперты оценивали влияние факторов друг на друга в вышеопределенных лингвистических переменных, и полученный результат после агрегации и дефаззификации приведен на рис. 3.

## Моделирование динамики НКК

Процессы вывода НКК включают вектор состояний $A_{1\times n}$, который состоит из $n$ значений факторов, и весовую матрицу $W_{n\times n}$, которая отражает веса $w_{ij}$ взаимовлияния между $n$-факторами. На значение каждого фактора оказывают влияние значения связанных с ним факторов и их предыдущее значение. Значение активации для каждого фактора вычисляется итеративно следующим правилом:

$$A_i^{(t+1)} = f\left(\sum_{j=1}^{n} w_{ij}A_i^{(t)}\right),\ i \neq j, \qquad (2)$$

где $t$ — текущее время; $A$ — уровень активации фактора $C_i$; $A_j$ — уровень активации фактора $C_j$; $w_{ij}$ — вес взаимовлияния между $C_i$ и $C_j$; $f$ — пороговая функция.

В качестве пороговых функций использовались бинарные, тривалентные и сигмоидные функции [41]. В этой работе в качестве пороговой функции для НКК используется сигмоидная функция

$$f(x) = \frac{1}{1+\mathbf{e}^{-\lambda x}}, \qquad (3)$$

где $\lambda > 0$. Эта функция непрерывна, и ее областью значений является отрезок [0, 1].

Мы предполагаем, что состояния факторов могут быть определены как нечеткие переменные, состоящие из трех нечетких множеств: высокое (high), среднее (medium) и низкое (low).

### Результаты вычислительных экспериментов

Отметим, что каждая из концепций $C_j$ может принимать значения в интервале [0, 1], который также называется "уровнем активации". Уровень активации можно интерпретировать как относительное число [25]. Более строго уровень активации может представлять членство в нечетком множестве, описывающем лингвистические меры относительной численности (например, низкий, средний, высокий) [10].

Процесс моделирования НКК инициализируется присвоением значения из интервала [0, 1] уровням активации каждого узла НКК на основе мнений специалистов/заинтересованных сторон для текущего состояния. Значение 0 говорит о том, что данный фактор не присутствует в системе в определенной итерации, в то время как значение 1 указывает, что данный фактор присутствует в максимальной степени. Другие значения соответствуют промежуточным уровням активации.

Рассмотрим моделирование следующих сценариев управления ИБ.

***Сценарий A:*** *саморазвитие ситуации* A(0) = (1.0, 1.0, 1.0, 1.0, 1.0, 1.0, 0.0).

***Сценарий B:*** *использование только технических мер* A(0) = (0.0, 0.0, 1.0, 0.0, 0.0, 0.0, 0.0).

***Сценарий C:*** *сильная активация фактора "развитие угроз ИБ"* A(0) = (0.0, 0.0, 0.0, 0.0, 0.0, 1.0, 0.0).

***Сценарий D:*** *сильная активация факторов "Развитие потенциала" и "Развитие угроз ИБ"* A(0) = = (0.0, 0.0, 0.0, 1.0, 0.0, 1.0, 0.0).

В вычислительных экспериментах мы использовали сигмоидную функцию с параметром $\lambda = 1$. Как правило, вычисления по формуле (2) сходились менее чем за пять временных шагов моделирования. Все модели закончились в стабильном состоянии, но теоретически они могли бы также перейти в предельный цикл или в хаотический аттрактор [6]. Промежуточные значения факторов при вычислениях по сценарию *A* приведены в табл. 2.

Как видно из табл. 2, сохранение существующих тенденций факторов приведет к ухудшению уровня информационной безопасности.

Из табл. 3 можно заключить, что использование только технических мер не дает существенного улучшения состояния ИБ (разность между стабильными состояниями сценариев *A* и *B* составляет 0,0424).

Табл. 4 показывает, что при активации фактора "Развитие угроз ИБ" состояние ИБ ухудшается значительно, также можно отметить ухудшение начальной тенденции фактора "Технические меры".

Табл. 5 показывает, что при развитии угроз ИБ не удается обеспечить приемлемый уровень ИБ

Таблица 2

**Вычисление стабильного состояния для НКК (сценарий *A*)**

| Факторы итерации | *Legal* | *Org* | *Tech* | *HR* | *Coop* | *NewT* | *ISec* |
|---|---|---|---|---|---|---|---|
| 0 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 |
| 1 | 0,5498 | 0,5250 | 0,6457 | 0,5987 | 0,5498 | 0,5000 | 0,5987 |
| 2 | 0,5281 | 0,5150 | 0,5871 | 0,5619 | 0,5292 | 0,5000 | 0,5721 |
| 3 | 0,5269 | 0,5140 | 0,5821 | 0,5570 | 0,5275 | 0,5000 | 0,5633 |
| 4 | 0,5268 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,0000 | 0,5624 |
| 5 | 0,5267 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,5000 | 0,5624 |
| 6 | 0,5267 | 0,5139 | 0,5816 | 0,5566 | 0,5274 | 0,5000 | 0,5624 |

Таблица 3

**Конечные результаты вычислений по сценарию *B***

| Факторы | Начальные значения — сценарий *B* | Конечные значения — сценарий *B* | Разность между стабильными состояниями сценариев *A* и *B* |
|---|---|---|---|
| Правовые меры | 0,00 | 0,5275 | 0,0008 |
| Организационные меры | 0,00 | 0,5147 | 0,0008 |
| Технические меры | 1,00 | 1,00 | 0,4184 |
| Развитие потенциала | 0,00 | 0,5875 | 0,0309 |
| Сотрудничество заинтересованных сторон | 0,00 | 0,5378 | 0,0104 |
| Развитие угроз ИБ | 0,00 | 0,5000 | 0 |
| Уровень ИБ | 0,00 | 0,6048 | 0,0424 |

Таблица 4

**Конечные результаты вычислений по сценарию *C***

| Факторы | Начальные значения — сценарий *C* | Конечные значения — сценарий *C* | Разность между стабильными состояниями сценариев *A* и *C* |
|---|---|---|---|
| Правовые меры | 0,00 | 0,5267 | 0,00 |
| Организационные меры | 0,00 | 0,5139 | 0,00 |
| Технические меры | 0,00 | 0,5569 | −0,0247 |
| Развитие потенциала | 0,00 | 0,5547 | −0,0019 |
| Сотрудничество заинтересованных сторон | 0,00 | 0,5267 | −0,0007 |
| Развитие угроз ИБ | 1,00 | 1,00 | 0,5 |
| Уровень ИБ | 0,00 | 0,4976 | −0,0648 |

Таблица 5

**Конечные результаты вычислений по сценарию *D***

| Факторы | Начальные значения — сценарий *D* | Конечные значения — сценарий *D* | Разность между стабильными состояниями сценариев *A* и *D* |
|---|---|---|---|
| Правовые меры | 0,00 | 0,5381 | 0,0114 |
| Организационные меры | 0,00 | 0,5250 | 0,0111 |
| Технические меры | 0,00 | 0,5904 | 0,0088 |
| Развитие потенциала | 0,00 | 1,0000 | 0,4434 |
| Сотрудничество заинтересованных сторон | 0,00 | 0,5279 | 0,0005 |
| Развитие угроз ИБ | 1,00 | 1,00 | 0,5 |
| Уровень ИБ | 0,00 | 0,5238 | −0,0386 |

только за счет развития потенциала; наряду с развитием соответствующего потенциала требуется найти оптимальное сочетание правовых, технических, организационных мер по информационной безопасности при эффективном сотрудничестве всех заинтересованных сторон.

## Заключение

В работе представлен метод построения когнитивной модели для стратегического управления информационной безопасностью электронного правительства. Выделены основные управляющие факторы, и на основе математического аппарата нечетких когнитивных карт построена когнитивная карта, отображающая взаимовлияние факторов. Определены начальные тенденции изменения факторов и проанализированы различные стратегические сценарии развития системы управления информационной безопасностью электронного правительства. Предлагаемое когнитивное моделирование позволяет при первом приближении оценить степень достижимости поставленных стратегических целей по ИБ.

### Список литературы


1. **Grönlund A., Horan T. A.** Introducing e-gov: history, definitions, and issues // Communications of the Association for Information Systems. 2004. V. 15. P. 713—729.
2. **Имамвердиев Я. Н.** Модель ситуационного управления информационной безопасностью электронного правительства // Информационные технологии. 2014. № 8. С. 24—32.
3. **Wimmer M., von Bredow B.** E-government: aspects of security on different layers // Proc. of the 12th International Workshop on Database and Expert Systems Applications. 2001. P. 350—355.
4. **Chen Y.-S., Chong P. P., Zhang B.** Gyber security management and e-government // Electronic Government. 2004. V. 1, N. 3. P. 316—327.
5. **Алгулиев Р. М., Имамвердиев Я. Н.** Информационная безопасность э-государства: актуальные направления исследований // Проблемы информационного общества. 2010. № 1. С. 3—13.
6. **Glykas M.** Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications. Studies in Fuzziness and Soft Computing. Springer, 2010. V. 247.
7. **Максимов В. И., Корноушенко Е. К.** Аналитические основы применения когнитивного подхода при решении слабоструктурированных задач // Труды ИПУ РАН, 199. Т. 2. С. 95—109.
8. **Tolman E.** Cognitive maps in rats and men // Psychological Review. 1948. N. 55. P. 189—208.
9. **Axelrod R.** Structure of decision: The cognitive maps of political elites. New Jersey: Princetown University Press, 1976.
10. **Kosko B.** Fuzzy cognitive maps // International Journal of Man-Machine Studies. 1986. V. 24, N 1. P. 65—75.
11. **Papageorgiou E. I.** Review study of fuzzy cognitive maps and their applications during the last decade // Studies in Computational Intelligence: Business Process Management. 2013. V. 444. P. 281—298.
12. **Taber W. R.** Knowledge processing with fuzzy cognitive maps // Expert Systems with Applications. 1991. V. 2, N. 1. P. 83—87.
13. **Andreou A. S., Mateou N. H., Zombanakis G. A.** Soft computing for crisis management and political decision making: the use of genetically evolved fuzzy cognitive maps // Soft Computing Journal. 2005.V. 9, N. 3. P. 194—210.
14. **Carvalho J. P.** On the semantics and the use of Fuzzy Cognitive Maps in social sciences // Proc. of the IEEE World Congress on Computational Intelligence (WCCI). 2010. N 5584033.
15. **Максимов В. И.** Структурно-целевой анализ развития социально-экономических ситуаций // Проблемы управления. 2005. № 3. С. 30—38.
16. **Tsadiras A., Margaritis K., Mertzios B.** Strategic planning using extended Fuzzy Cognitive Maps // Studies in Informatics and Control. 1995. V. 4, N. 3. P. 237—345.
17. **Силов В. Б.** Принятие стратегических решений в нечеткой обстановке. М.: ИНПРО-РЕС, 1995. 228 с.
18. **Xirogiannis G., Glykas M.** Fuzzy Cognitive Maps in business analysis and performance-driven change // IEEE Transactions on Engineering Management. 2004. V. 51, N. 3. P. 334—351.
19. **Song H., Miao C., Rael W., Shen Z., Catthoor F.** Implementation of fuzzy cognitive maps based on fuzzy neural network and application in prediction of time series // IEEE Transactions on Fuzzy Systems. 2010. V. 18, N. 2. P. 233—250.
20. **Stylios C. D., Groumpos P. P.** Fuzzy cognitive map in modeling supervisory control systems // Journal of Intelligent & Fuzzy Systems. Application in Engineering and Technology. 2000. V. 8, N. 2. P. 83—98.
21. **Rodriguez-Repiso L., Setchi R., Salmeron J. L.** Modelling IT Projects success with Fuzzy Cognitive Maps // Expert Systems with Applications. 2007. V. 32, N. 2. P. 543—559.
22. **Bhatia N., Kapoor N.** Fuzzy Cognitive Map based approach for software quality risk analysis // ACM SIGSOFT Software Engineering Notes. 2011. V. 36, N. 6. P. 1—9.
23. **Papageorgion E. I.** A new methodology for decisions in Medical Informatics using Fuzzy Cognitive Maps based on fuzzy rule-extraction techniques // Applied Soft Computing. 2011. V. 11, N. 1. P. 500—513.
24. **Özesmi U., Özesmi S. L.** Ecological models based on people's knowledge: a multi-step fuzzy cognitive mapping approach // Ecological Modelling. 2004. V. 176, N. 1—2. P. 43—64.
25. **Hobbs B. F., Ludsin S. A., Knight R. L., Ryan P. A., Biberhofer J., Ciborowski J. J. H.** Fuzzy cognitive mapping as a tool to define management objectives for complex ecosystems // Ecological Applications. 2002. V. 12. P. 1548—1565.
26. **Hong T., Han I.** Knowledge-based data mining of news information on the Internet using cognitive maps and neural networks // Expert Systems with Applications. 2002. V. 23, N. 1. P. 1—8.
27. **Камаев В. А., Натров В. В.** Моделирование и анализ состояния информационной безопасности организации // Известия ТулГУ. Технические науки. 2011. № 3. С. 148—155.
28. **Schneider M., Shnaider E., Kandel A., Chew G.** Automatic construction of FCMs // Fuzzy Sets and Systems. 1998. V. 93, N. 2. P. 161—172.
29. **Luiijf H., Besseling K., Spoelstra M., de Graaf P.** Ten National Gyber Security Strategies: a comparison // Proc. 6th International Conference on Critical Information Infrastructures Security (CRITIS 2011). September 2011.
30. **ENISA:** National Gyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace. May 2012. 15 p.
31. **The ITU** National Cybersecurity Strategy Guide. Geneva, 2012. 122 p.
32. **OECD:** Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies. OECD Digital Economy Papers. OECD Publishing. 2012. N. 212.
33. **Klimburg A.** (Ed.) National Cyber Security Framework Manual, Tallinn: NATO CCD COE Publication, 2012. 235 p.
34. **Sood A. K., Enbody R. J.** Targeted Cyberattacks: A Superset of Advanced Persistent Threats // IEEE Security & Privacy. 2013. V. 11, N. 1. P. 54—61.
35. **Brotby W. K.** Information security management metrics; A definitive guide to effective security monitoring and measurement. CRC Press. 2012. 200 p.
36. **Kosko B.** Neural networks and fuzzy systems. Englewood Cliffs. N. J.: Prentice-Hall, 1992.
37. **Runkler T. A.** Selection of appropriate defuzzification methods using application specific properties // IEEE Transactions on Fuzzy Systems. 1997. V. 5, N. 1. P. 72—79.
38. **Papakostas G. A., Polydoras A. S., Koulouriotis D. E., Tourassis V. D.** Training Fuzzy Cognitive Maps by using Hebbian learning algorithms: A comparative study // IEEE International Conference on Fuzzy Systems (FUZZ). 2011. P. 851—858.
39. **Papageorgiou E. I., Stylios C. D., Groumpos P. P.** Active Hebbian learning algorithm to train fuzzy cognitive maps // International Journal of Approximate Reasoning. 2001. V. 37, N. 3. P. 219—249.
40. **Papageorgiou E. I., Parsopoulos K. E., Stylios C. D., Groumpos P. P., Vrahatis M. N.** Fuzzy Cognitive Maps learning using Particle Swarm Optimization // International Journal of Intelligent Information Systems. 2005. V. 25, N. 1. P. 95—121.
41. **Tsadiras A. K.** Comparing the inference capabilities of binary, trivalent and sigmoid fuzzy cognitive maps // Information Sciences. 2008. V. 178, N. 20. P. 3880—3894.

**Y. N. Imamverdiyev,** Head of Laboratory, e-mail: yadigar@lan.ab.az,
Institute of Information Technology of Azerbaijan National Academy of Sciences

# A Fuzzy Cognitive Model for the Strategic Management of Information Security of E-Government

*The article studies the nature and application of cognitive modeling in the strategic management of information security of e-government. Factors of strategic management of information security are defined and the fuzzy cognitive map for strategic management of e-government information security is built on the basis of expert assessments. Based on the developed cognitive model results of different strategies for e-government information security management are analyzed.*

***Keywords:*** *information security, information security management, information security strategy, cognitive modeling, fuzzy cognitive maps*

### References

1. **Grönlund A., Horan T. A.** Introducing e-gov: history, definitions, and issues. *Communications of the Association for Information Systems.* 2004. V. 15. P. 713—729.
2. **Imamverdiyev Ya. N.** Model' situacionnogo upravlenija informacionnoj bezopasnost'ju je-gosudarstva. *Informacionnye tehnologii.* 2014. N. 8. P. 24—32.
3. **Wimmer M., von Bredow B.** E-government: aspects of security on different layers. *Proc. of the 12th International Workshop on Database and Expert Systems Applications.* 2001. P. 350—355.
4. **Chen Y.-S., Chong P. P., Zhang B.** Gyber security management and e-government. *Electronic Government.* 2004. V. 1, N. 3. P. 316—327.
5. **Alguliyev R. M., Imamverdiyev Yu. N.** Informacionnaya bezopasnost' e-gosudarstva: aktual'nye napravleniya issledovanii. *Problemy informacionnogo obshestva*. 2010. N. 1. P. 3—13.
6. **Glykas M.** *Fuzzy Cognitive Maps: Advances in Theory, Methodologies, Tools and Applications. Studies in Fuzziness and Soft Computing.* Springer. 2010. V. 247.
7. **Maksimov V. I., Kornoushenko E. K.** Analitiheskie osnovy primenenija kognitivnogo podhoda pri reshenii slabostrukturirovannyh zadach. *Trudy IPU RAN.* 1999. V. 2. P. 95—109.
8. **Tolman E.** Cognitive maps in rats and men. *Psychological Review.* 1948. N. 55. P. 189—208.
9. **Axelrod R.** Structure of decision: The cognitive maps of political elites. New Jersey: Princetown University Press, 1976.
10. **Kosko B.** Fuzzy cognitive maps. *International Journal of Man-Machine Studies.* 1986. V. 24, N. 1. P. 65—75.
11. **Papageorgiou E. I.** Review study of fuzzy cognitive maps and their applications during the last decade. *Studies in Computational Intelligence: Business process Management.* 2013. V. 444. P. 281—298.
12. **Taber W. R.** Knowledge processing with fuzzy cognitive maps. *Expert Systems with Applications.* 1991. V. 2, N. 1. P. 83—87.
13. **Andreou A. S., Mateou N. H., Zombanakis G. A.** Soft computing for crisis management and political decision making: the use of genetically evolved fuzzy cognitive maps. *Soft Computing Journal.* 2005. V. 9, N. 3. P. 194—210.
14. **Carvalho J. P.** On the semantics and the use of Fuzzy Cognitive Maps in social sciences. *Proc. of the IEEE World Congress on Computational Intelligence (WCCI).* 2010. N 5584033.
15. **Maksimov V. I.** Strukturno-celevoj analiz razvitija social'no-jekonomicheskih situacij. *Problemy upravlenija*. 2005. N 3. P. 30—38.
16. **Tsadiras A., Margaritis K., Mertzios B.** Strategic planning using extended Fuzzy Cognitive Maps. *Studies in Informatics and Control.* 1995. V. 4, N 3. P. 237—345.
17. **Silov V. B.** *Prinjatie strategicheskih reshenij v nechetkoj obstanovke.* M.: INPRO-RES, 1995. 228 p.
18. **Xirogiannis G., Glykas M.** Fuzzy Cognitive Maps in business analysis and performance-driven change. *IEEE Transactions on Engineering Management.* 2004. V. 51, N. 3. P. 334—351.
19. **Song H., Miao C., Rael W., Shen Z., Catthoor F.** Implementation of fuzzy cognitive maps based on fuzzy neural network and application in prediction of time series. *IEEE Transactions on Fuzzy Systems.* 2010. V. 18, N. 2. P. 233—250.
20. **Stylios C. D., Groumpos P. P.** Fuzzy cognitive map in modeling supervisory control systems. *Journal of Intelligent & Fuzzy Systems. Application in Engineering and Technology.* 2000. V. 8, N. 2. P. 83—98.
21. **Rodriguez-Repiso L., Setchi R., Salmeron J. L.** Modelling IT Projects success with Fuzzy Cognitive Maps. *Expert Systems with Applications.* 2007. V. 32, N. 2. P. 543—559.
22. **Bhatia N., Kapoor N.** Fuzzy Cognitive Map based approach for software quality risk analysis. *ACM SIGSOFT Software Engineering Notes.* 2011. V. 36, N. 6. P. 1—9.
23. **Papageorgion E. I.** A new methodology for decisions in Medical Informatics using Fuzzy Cognitive Maps based on fuzzy rule-extraction techniques. *Applied Soft Computing.* 2011. V. 11, N. 1. P. 500—513.
24. **Özesmi U., Özesmi S. L.** Ecological models based on people's knowledge: a multi-step fuzzy cognitive mapping approach. *Ecological Modelling.* 2004. V. 176, N. 1—2. P. 43—64.
25. **Hobbs B. F., Ludsin S. A., Knight R. L., Ryan P. A., Biberhofer J., Ciborowski J. J. H.** Fuzzy cognitive mapping as a tool to define management objectives for complex ecosystems. *Ecological Applications.* 2002. V. 12. P. 1548—1565.
26. **Hong T., Han I.** Knowledge-based data mining of news information on the Internet using cognitive maps and neural networks. *Expert Systems with Applications.* 2002. V. 23, N. 1. P. 1—8.
27. **Kamaev V. A., Natrov V. V.** Modelirovanie i analiz sostojanija informacionnoj bezopasnosti organizacii. *Izvestija TulGU. Tehnicheskie nauki.* 2011. N. 3. P. 148—155.
28. **Schneider M., Shnaider E., Kandel A., Chew G.** Automatic construction of FCMs. *Fuzzy Sets and Systems.* 1998. V. 93, N. 2. P. 161—172.
29. **Luiijf H., Besseling K., Spoelstra M., de Graaf P.** Ten National Gyber Security Strategies: a comparison. Proc. *6th International Conference on Critical Information Infrastructures Security (CRITIS 2011).* September 2011.
30. **ENISA:** *National Gyber Security Strategies: Setting the course for national efforts to strengthen security in cyberspace.* May 2012. 15 p.
31. **The ITU** *National Cybersecurity Strategy Guide.* Geneva. 2012. 122 p.
32. **OECD:** Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies. *OECD Digital Economy Papers.* OECD Publishing. 2012. N. 212.
33. **Klimburg A.** (Ed.) *National Cyber Security Framework Manual,* Tallinn: NATO CCD COE Publication, 2012. 235 p.
34. **Sood A. K., Enbody R. J.** Targeted Cyberattacks: A Superset of Advanced Persistent Threats. *IEEE Security & Privacy.* 2013. V. 11, N. 1. P. 54—61.
35. **Brotby W. K.** *Information security management metrics; A definitive guide to effective security monitoring and measurement.* CRC Press. 2012. 200 p.
36. **Kosko B.** *Neural networks and fuzzy systems. Englewood Cliffs.* N. J.: Prentice-Hall, 1992.
37. **Runkler T. A.** Selection of appropriate defuzzification methods using application specific properties. *IEEE Transactions on Fuzzy Systems.* 1997. V. 5, N. 1. P. 72—79.
38. **Papakostas G. A., Polydoras A. S., Koulouriotis D. E., Tourassis V. D.** Training Fuzzy Cognitive Maps by using Hebbian learning algorithms: A comparative study. *IEEE International Conference on Fuzzy Systems (FUZZ).* 2011. P. 851—858.
39. **Papageorgiou E. I., Stylios C. D., Groumpos P. P.** Active Hebbian learning algorithm to train fuzzy cognitive maps. *International Journal of Approximate Reasoning.* 2001. V. 37, N. 3. P. 219—249.
40. **Papageorgiou E. I., Parsopoulos K. E., Stylios C. D., Groumpos P. P., Vrahatis M. N.** Fuzzy Cognitive Maps learning using Particle Swarm Optimization. *International Journal of Intelligent Information Systems.* 2005. V. 25, N. 1. P. 95—121.
41. **Tsadiras A. K.** Comparing the inference capabilities of binary, trivalent and sigmoid fuzzy cognitive maps. *Information Sciences.* 2008. V. 178, N. 20. P. 3880—3894.