Журнал правовых и экономических исследований.
Journal of Legal and Economic Studies, 2016, 4: 196–201

УДК (621.39:346.548):330.4

V.P. Fomchenkov, B.V. Okunev, A.N. Rudometkin

PROBLEM-GOAL-BASED COGNITIVE MODELING OF AN ENTITY TELECOMMUNICATION INFRASTRUCTURE SECURITY MANAGEMENT SYSTEM

The study has been financially supported by the Russian Foundation for Basic Research (project № №16-01-00293-a)

Vladimir Fomchenkov – Associate Professor at the Department of Management and Information Technologies in Economy, Smolensk branch of National Research University "Moscow Power Engineering Institute", PhD in Technical Sciences, Associate Professor, Smolensk; **e-mail: ok-bmv@rambler.ru**.
Boris Okunev – Associate Professor at the Department of Management and Information Technologies in Economy , Smolensk branch of National Research University "Moscow Power Engineering Institute", PhD in Technical Sciences, Associate Professor, Smolensk; **e-mail: ok-bmv@rambler.ru**.
Andrey Rudometkin – A PhD student at the Department of Management and Information Technologies in Economy , Smolensk branch of National Research University "Moscow Power Engineering Institute", Smolensk; **e-mail: tatjank@yandex.ru**.

The article deals with cognitive modeling of an entity telecommunication infrastructure security management system to wit achieving a basic problem-goal-based model of a security management system on the basis of a fuzzy cause-effect network.

The authors are of the opinion that working out sound recommendations as to the need for updating the model parameters in the context of variability of the system operation goals and changeability of its functions should be considered a particular scientific problem and that it might be further studied.

Keywords: *organizational and technical system; socio-technical system; cognitive modeling; problem-goal-based model; fuzzy cause-effect network; information security; telecommunications infrastructure.*

В.П. Фомченков, Б.В. Окунев, А.Н. Рудометкин

ПРОБЛЕМНО-ЦЕЛЕВОЕ КОГНИТИВНОЕ МОДЕЛИРОВАНИЕ СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ТЕЛЕКОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНИЗАЦИИ

Работа выполнена при финансовой поддержке гранта Российского фонда фундаментальных исследований №16-01-00293-а

Владимир Петрович Фомченков – доцент кафедры менеджмента и информационных технологий в экономике, филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ» в г. Смоленске, кандидат технических наук, доцент, г. Смоленск; **e-mail: ok-bmv@rambler.ru**.
Борис Васильевич Окунев – доцент кафедры менеджмента и информационных технологий в экономике, филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ» в г. Смоленске, кандидат технических наук, доцент, г. Смоленск; **e-mail: ok-bmv@rambler.ru**.
Андрей Николаевич Рудометкин – аспирант кафедры менеджмента и информационных технологий в экономике, филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Национальный исследовательский университет «МЭИ» в г. Смоленске, г. Смоленск; **e-mail: tatjank@yandex.ru**.

В статье рассмотрены вопросы когнитивного моделирования системы управления безопасностью телекоммуникационной инфраструктуры организации, а именно: построение базовой проблемно-целевой модели системы управления безопасностью на основе нечеткой причинно-следственной сети. Авторы считают, что задача выработки обоснованных рекомендаций о необходимости корректировки параметров модели в условиях изменчивости целей функционирования системы и выполняемых ею функций является отдельной научной проблемой и может стать предметом дальнейших исследований.

Ключевые слова: *организационно-техническая система; социально-техническая система; когнитивное моделирование; проблемно-целевая модель; нечеткая причинно-следственная сеть; информационная безопасность; телекоммуникационная инфраструктура.*

Системы управления информационно-телекоммуникационной инфраструктурой организации по ряду признаков могут быть отнесены к классу сложных организационно-технических систем (ОТС), под которыми понимают искусственную, самоорганизующуюся, динамическую, организационно-техническую совокупность взаимосвязанных элементов, предназначенных для производства товарной продукции, предоставления услуг или иной деятельности, осуществляемой человеком [6; 7].

Среди наиболее важных признаков вышеуказанных систем управления можно отметить:

- наличие подсистем, например, сетевой инфраструктуры, защиты информации, автоматизированных систем управления и др. [4];
- непостоянство во времени структуры системы управления;
- изменчивость целей функционирования системы и выполняемых ею функций [3; 9];
- наряду с аппаратным и программным обеспечением важным фактором функционирования системы является субъективная деятельность человека;
- наличие качественных показателей, которые не могут быть описаны количественно.

Эффективным средством описания сложных ОТС является проблемно-целевое когнитивное моделирование, что послужило причиной проведения активных научных исследований в данном направлении [1; 2; 5; 8;]. Сильной стороной проблемно-целевого анализа является его ориентация на выбор обоснованных мероприятий, направленных на решение проблемных ситуаций, возникающих в организации, с целью достижения ее целевых показателей. Один из возможных подходов к проблемно-целевому анализу сложных ОТС с использованием когнитивного математического аппарата, интегрирующий различные методы и технологии решения разнотипных эвристических и аналитических задач, возникающих при проблемно-целевом анализе, предложен В.В. Борисовым, И.А. Бычковым, А.В. Дементьевым, А.П. Соколовым, А.С. Федуловым [1].

В данном случае проблемно-целевая модель представляет собой нечеткую причинно-следственную сеть. Узлами сети являются элементы множества концептов $E = \{e_1, e_2, ..., e_p\}$, которые определены относительно целевых функций решаемой проблемы. Типовое состояние концептов e_i характеризуется лингвистическими переменными с набором терм-множеств $T_i = \{T_1^i, T_2^i, ..., T_{m_i}^i\}$. Связи между узлами сети характеризуются множеством отношений причинности между каждой парой концептов $W = \{w(e_i, e_j)\}$. Связи $w(e_i, e_j)$ между типовыми состояниями каждой пары концептов характеризуются лингвистическими переменными с набором терм-множеств $T_{w(e_i, e_j)} = \{T_{11}^{w(e_i, e_j)}, ..., T_{kl}^{w(e_i, e_j)}\}$.

Отметим особенности базовой модели:

- множества концептов E и отношений причинности W не являются значимыми и согласованными;
- терм-множества T_i и $T_{w(e_i, e_j)}$ не определены;
- базовая модель не учитывает специфики организации системы управления

безопасностью телекоммуникационной инфраструктуры конкретных организаций.

При проектировании базовой модели множества E и W задаются в наиболее общем виде. Основой для их определения является анализ агрегированной информации и проблемно-целевых информационно-аналитических ресурсов: законодательных, уставных, нормативных, отчетных, финансово-экономических, технических и аналитических документов.

Поставим задачу построения базовой проблемно-целевой когнитивной модели системы управления безопасностью телекоммуникационной инфраструктуры организации. Причем, с целью уменьшения количества концептов ограничимся организациями. В качестве источников информации для определения элементов множеств концептов $E = \{e_1, e_2, ..., e_p\}$ и отношений причинности между каждой парой концептов $W = \{w(e_i, e_j)\}$ использовались Федеральное законодательство Российской Федерации в сфере информационной безопасности, международные стандарты управления информационной безопасностью, а также сложившаяся практика обеспечения информационной безопасности в организациях.

В результате проведенных исследований было определено следующее основное множество концептов $E = \{e_1, e_2, ..., e_p\}$ базовой проблемно-целевой когнитивной модели системы управления безопасностью телекоммуникационной инфраструктуры организации:

- (e_1) – информирование и обучение персонала организации, вовлеченного в информационно-телекоммуникационную сферу;
- (e_2) – привлечение к ответственности нарушителей политики безопасности организации;
- (e_3) – правильная организация рабочих мест персонала организации, вовлеченного в информационно-телекоммуникационную сферу;
- (e_4) – разработка правил доступа пользователей к ресурсам корпоративной информационной системы (разработка политики безопасности);
- (e_5) – организация охраны и пропускного режима;
- (e_6) – организация видеонаблюдения за работой сотрудников организации;
- (e_7) – организация специального делопроизводства, порядка хранения, перевозки носителей коммерческой тайны;
- (e_8) – минимизация числа лиц в организации, допускаемых к коммерческой тайне;
- (e_9) – обеспечение выполнения требований по информационной безопасности в процессе производства, сбыта изделий, рекламы, подписания контрактов и т.п.;
- (e_{10}) – организация плановости разработки и осуществления мер по защите коммерческой тайны, систематический контроль за эффективностью принимаемых мер;
- (e_{11}) – обеспечение персонала нормативно-правовыми актами в области защиты информации;
- (e_{12}) – методическая помощь в организации изучения нормативно-правовых актов;
- (e_{13}) – специальный подбор и проверка персонала, который планируется использовать в сфере информационных технологий;
- (e_{14}) – управление доступом к информационным ресурсам организации;
- (e_{15}) – распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.п.) среди сотрудников организации, вовлеченных в информационно-телекоммуникационную сферу;
- (e_{16}) – использование передового опыта, современных технических и программных средств защиты информации;
- (e_{17}) – техническое совершенствование (с точки зрения информационной безопасности) корпоративных информационных систем;
- (e_{18}) – организация системы мониторинга телекоммуникационных сетей;
- (e_{19}) – использование шифрования и электронной цифровой подписи при хранении и передаче информации;
- (e_{20}) – организация системы резерв-

ного копирования данных;

● (e_{21}) – обеспечение информационно-телекоммуникационной инфраструктуры предприятия системами бесперебойного питания (источники бесперебойного питания, автономные генераторы напряжения и т.п.);

● (e_{22}) – организация работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению её защиты;

● (e_{23}) – поддержка контактов с правоохранительными органами и службами безопасности контрагентов в интересах изучения криминогенной обстановки в сфере защиты информации;

● (e_{24}) – разработка основополагающих документов (устава, коллективного договора, правил внутреннего трудового распорядка, должностных инструкций и т.п.) с целью закрепления в них требований обеспечения безопасности и защиты коммерческой тайны;

● (e_{25}) – соблюдение персоналом трудовой и технологической дисциплины, обеспечивающей высокий уровень информационной безопасности;

● (e_{26}) – сохранение работоспособности информационно-телекоммуникационной инфраструктуры предприятия;

● (e_{27}) – выявление внутренних и внешних угроз конфиденциальной информации;

● (e_{28}) – выработка мер по обеспечению защиты конфиденциальной информации;

● (e_{29}) – соответствие профессиональных качеств сотрудников уровню их допуска к конфиденциальной информации;

● (e_{30}) – надежное хранение и использование документов и носителей информации (определение правил выдачи, ведение журналов выдачи и т.п.);

● (e_{31}) – выполнение требований Федерального законодательства в области защиты персональных данных и информационной безопасности;

● (e_{32}) – формирование позитивного внутреннего и внешнего имиджа;

● (e_{33}) – минимизация недополученной прибыли от реализованных нарушений информационной безопасности;

● (e_{34}) – минимизация финансовых потерь от судебных издержек, штрафов и т.д., связанных с нарушениями требований Федерального законодательства в области защиты персональных данных и информационной безопасности;

● (e_{35}) – получение прибыли.

Множество концептов модели можно разделить на следующие группы:

- ($e_1 – e_{23}$) – концепты-мероприятия по организации системы управления безопасностью;

- ($e_{24} – e_{31}$) – концепты-результаты проводимых мероприятий по организации системы управления безопасностью;

- ($e_{32} – e_{35}$) – целевые концепты.

Множества отношений причинности $W= \{w(e_i, e_j)\}$ определялись на основе предварительного экспертного анализа и представления положительно-отрицательных нечетких связей (отношений сходства).

Разработанная базовая проблемно-целевая модель системы управления безопасностью телекоммуникационной инфраструктуры организации представлена на рисунке.

Данная модель является основой для разработки проблемно-целевых моделей, учитывающих специфику организации системы управления работой по защите информации на конкретных предприятиях. Недостатком предложенного подхода является статический характер модели. Совершенно очевидно, что такая предметная область как информационная безопасность телекоммуникационной инфраструктуры характеризуется высокой степенью изменчивости. В результате изменения внешнего окружения организации, внутренних условий изменяются цели функционирования системы, выполняемые ею функции, что приводит к необходимости периодической корректировки элементов множеств концептов $E = \{e_1, e_2 , \ldots, e_p\}$ и отношений причинности между каждой парой концептов $W= \{w(e_i, e_j)\}$.

Разработка и корректировка проблемно-целевой модели в виде нечеткой причинно-следственной сети конкретной организации требует серьезных организаци-

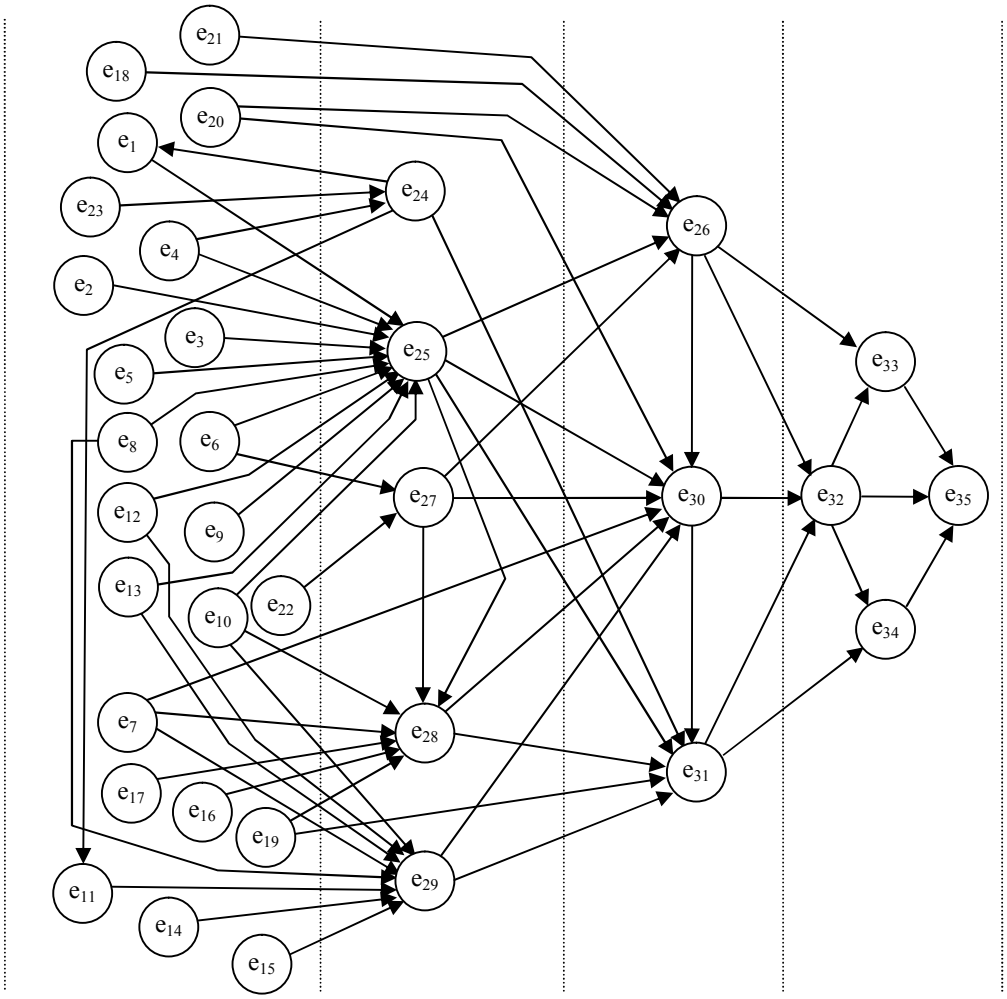

Рис. Когнитивная модель системы управления безопасностью телекоммуникационной инфраструктуры организации

онных и финансовых затрат, так как в этот процесс в качестве экспертов должны быть вовлечены и сотрудники организации.

Поэтому задача выработки обоснованных рекомендаций о необходимости корректировки параметров модели в условиях изменчивости целей функционирования системы и выполняемых ею функций является отдельной научной проблемой и может стать предметом дальнейших исследований.

ЛИТЕРАТУРА

1. *Борисов В.В., Бычков И.А., Дементьев А.В., Соловьев А.П., Федулов А.С.* Компьютерная поддержка сложных организационно-технических систем. М.: Горячая линия – Телеком, 2002. 154 с.

2. *Бояринов Ю.Г., Борисов В.В., Дли М.И.* Методы построения и использования нечетких полумарковских моделей для анализа сложных систем // Информационные технологии моделирования и управления. 2011. № 1 (66). С. 43–55.

3. *Бояринов Ю.Г., Стоянова О.В., Дли М.И.* Применение нейро-нечеткого метода группового учета аргументов для построения моделей социально-экономических систем // Программные продукты и системы. 2006. № 3. С. 7.

4. *Дли М.И., Какатунова Т.В.* Применение аппарата когнитивного моделирования для анализа сложных систем // Транспортное дело России. 2013. № 4. С. 193–195.

5. *Дли М.И., Какатунова Т.В., Петрушко И.Н.* Оценка инновационного потенциала предприятия: эксергетический подход // Интеграл. 2010. № 6. С. 46–47.

6. *Кудж С.А.* Администрирование информационных систем. М.: УПП «Репрография» МИИГАиК, 2009. 72 с.

7. *Мешалкин В.П., Какатунова Т.В., Дли М.И.* Влияние рисков информатизации на инновационную деятельность в региональных промышленных комплексах // Транспортное дело России. 2011. № 4. С. 66–68.

8. *Окунев Б.В., Фомченков В.П.* Когнитивное моделирование подсистем управления предприятий железнодорожного транспорта // Проблемы безопасности российского общества. 2014. № 2. С. 184–189.

9. *Палюх Б.В., Какатунова Т.В., Дли М.И., Багузова О.В.* Интеллектуальная система поддержки принятия решений по управлению сложными объектами с использованием динамических нечетких когнитивных карт // Программные продукты и системы. 2013. № 4. С. 155.