решения, которое должно использоваться при планировании действий силовых структур.

В целом, разработка и внедрение предлагаемой системы позволит повысить оперативность и объективность принимаемых решений по оценке оперативной обстановки, значительно сократить время реагирования на возникшие экстремальные ситуации, повысить уровень защищенности критически важных объектов территориальных объектов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Васильев В.И., Красько А.С., Матвеев П.В., Никитин А.А., Пестриков В.А.* О создании концепции безопасный город // Информационная безопасность: Материалы VIII Международной научно-практической конференции. Ч.1. – Таганрог: Изд-во ТРТУ, 2006. – С.28 – 30.

2. www.safetydynamics.net

3. *Андреев Н.Д., Дуленко В.А., Михайлов В.И., Пестриков В.А.* Методические рекомендации по разработке паспорта безопасности подразделения органов внутренних дел. – Уфа: Изд-во УЮИ МВД РФ, 2005. – 17 с.

4. *Дьяконов В.П.* Вейвлеты. От теории к практике – М.: Солон-Р, 2002. – 448 с.

5. *Бадамшин Р.А., Черняховская Л.Р., Ильясов Б.Г.* Проблемы управления сложными динамическими объектами в критических ситуациях на основе знаний. – М.: Машиностроение, 2003. – 240 с.

УДК 681.3

С.А. Радько, О.М. Лепешкин

РАЗВИТИЕ МЕТОДОЛОГИЧЕСКОГО ПОДХОДА РАЗРАБОТКИ ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННОЙ МОДЕЛИ ДОСТУПА СОЦИОТЕХНИЧЕСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

В результате объединения сложных социальных и технико-технологических систем в социотехническую перед современными системами управления стоит проблема решения организационно-управленческих задач распределения и контроля использования информационных ресурсов в реальном масштабе времени. Ввиду того, что данная задача связана с ключевыми понятиями «функции» и «ресурсы», актуальна тема разработки функционально-дискреционной модели доступа (ФДМД).

Подход реализации данной модели направлен на безопасность функционирования критических информационных систем обработки информации в органах управления. Причем в качестве объекта в СТИС рассматривается не вычислительная система как такова, а информационно-управляющая система, которой свойственны следующие особенности:

- работа в реальном масштабе времени;
- специфические требования по надежности и безопасности функционирования;
- эксплуатационные и инструментальные особенности;
- непрерывный режим функционирования;
- оператор часто отсутствует;
- нештатные ситуации должны корректно разрешаться самой вычислительной системой;

– специфические требования к проектированию и отладке.

Таким образом, основными областями для реализации ФДМД являются:

– обеспечение устойчивого процесса функционирования – функциональная безопасность (ФБ);
– защита от несанкционированного доступа использования ресурсов с учетом выполнения функций в реальном масштабе времени - информационная безопасность (ИБ).

Это связано с природой и особенностями функционирования изменяющейся социотехнической информационной системы (СТИС), которая на протяжении всего периода существования меняет цели, используемые ресурсы, решаемые задачи. Следовательно, защита такой системы также должна постоянно изменяться и модифицироваться [1].

Социотехническая информационная система – рабочая система, состоящая из технической подсистемы, подсистемы персонала, внутренней и внешней информационной среды, взаимодействующей с организацией. В настоящее время, понятие СТИС в аспектах информационной безопасности и безопасности функционирования при разработке моделей безопасности разграничения доступа данной системы, предпринимается переход от микроэргономического анализа к мидиэргономическому, то есть от анализа систем типа «человек-машина» к системам «коллектив-машина», «человек-сеть». В результате концептуально меняется подход к построению модели безопасности по принципу разграничения доступа, где требуется расширение вида управления системой в активности функционирования объектов, добавляя к жестко заданной логике адаптивный вид (рис. 1) [2].

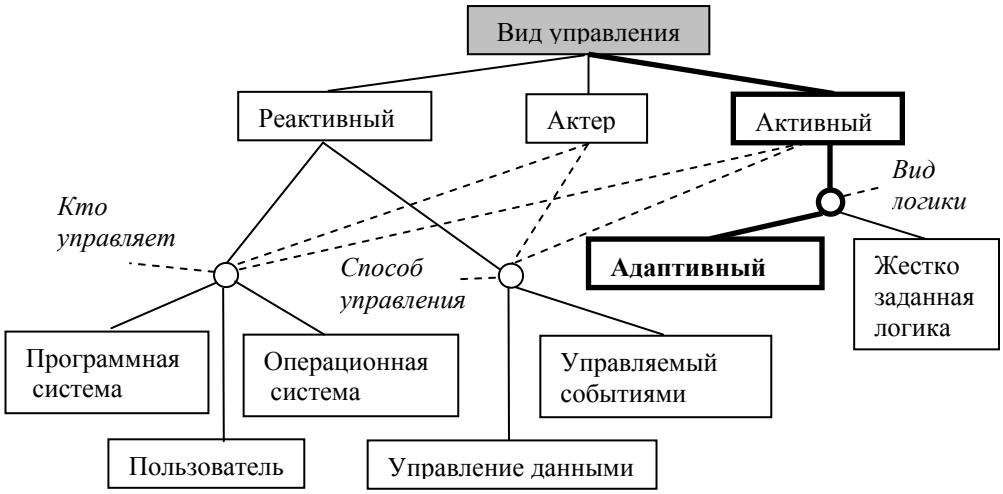

Рис. 1. Вид управления в информационной среде

В результате требуется расширение области информационной безопасности (ИБ) до информационно-системной безопасности (ИСБ). Информационно-системная безопасность включает ФБ и ИБ, причем данные две области рассматриваются системно через функциональную устойчивость (ФУ) (рис. 2). Этот подход следует из особенности природы современных информационных систем, которые включают информатизацию большей части деятельности человека, что вле-

чет к переходу, к организации нового типа, основой которой является единая информационная среда.

Ввиду того, что проблема обеспечения функциональной безопасности СТИС связана с динамикой устойчивых безопасных состояний системы, необходимо рассмотреть картеж параметров (m, R, Z), где m – информационные ресурсы, R – отношения, Z – виды композиций [1].

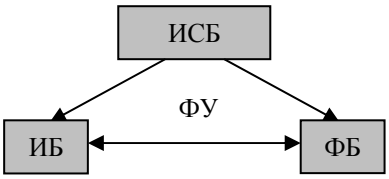

Рис. 2. Схема обеспечения ИСБ СТИС

Обеспечение ИБ информационных систем рассматривается в аспекте функциональной стабильности, где четко расписаны связи (R) доступа к тем или иным информационным ресурсам по принципу выполнения функций (Z). Но так как СТИС по природе своей не может рассматриваться как функционально стабильная система, то картеж (m, R, Z) является по сути динамическим. В результате для обеспечения ИБ появляется необходимость системного рассмотрения изоморфных преобразований отношений использования информационных ресурсов и их композиций согласно функциональности СТИС в реальном масштабе времени. В результате данные изоморфные переходы должны основываться на методах многосвязного регулирования и оптимального управления.

Ввиду данных методологий, предлагается объединить основные подходы описания систем управления (процессный, ситуационный, научный и системный) на основе ключевых понятий СТИС (функции, ресурсы и полномочия, логические схемы), где нормализованная среда радикалов [3] является основой решения. На основе этого, разработана следующая структурная схема методологического способа обеспечения ИБ и ФБ СТИС (рис.3) [4].

Вытекающие методы многосвязного регулирования и оптимального управления приводят к условию интеллектуализации системы управления сложной системы СТИС на основе предлагаемой среды радикалов, где сама технология среды радикалов является инструментом регулирования процессов функционирования в данной системе с учетом эксплуатационных особенностей.

В силу определения слова «радикал» [5] и на основе этого понятия разработанных технологий [3], нормализованная среда радикалов позволяет:

- решать конфликты использования общих ресурсов в процессе функционирования, при этом учитывая возможные каналы утечки информации;
- реализовать построение динамических матриц доступа на основе функциональности СТИС, фиксирующие взаимодействие ресурсов и полномочий их использования как внутри функции, так и на межфункциональном уровне в реальном масштабе времени;
- минимизировать ущербы от внешних и внутренних дестабилизирующих факторов;
- схематически строить график взаимодействия информационных ресурсов и целевых функций в реальном масштабе времени.

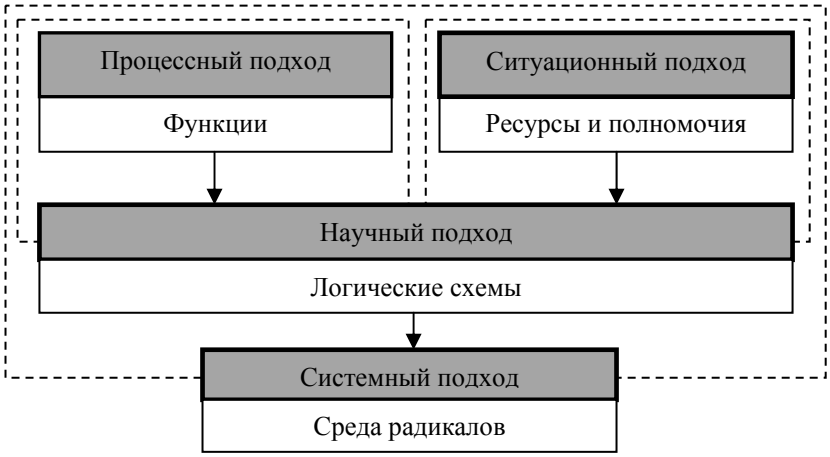

Рис 3. Схема методологического способа обеспечения ИБ и ФБ для СТС с применением нормализованной среды радикалов

Схематический язык описания информационных ресурсов (m) и их отношения (R) в системе уже разработан на языке радикалов (рис. 4).

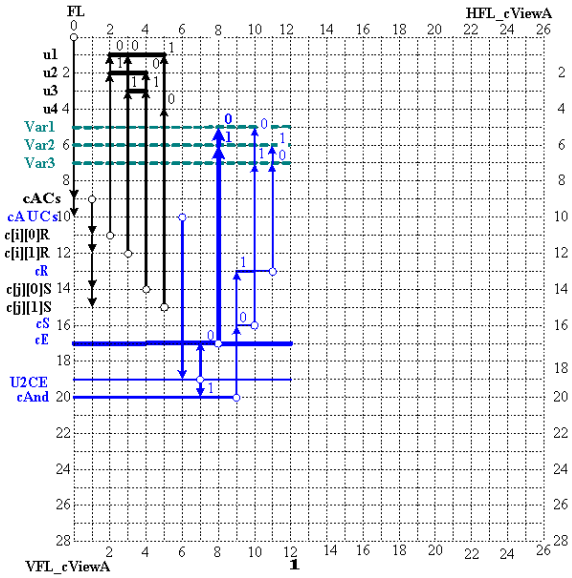

Рис. 4. Схематический язык описания информационных ресурсов и их отношения в СТИС

Предполагается разработка языка управления доступа к использованию информационных ресурсов для выполнения целевых функций СТИС в реальном масштабе времени на основе среды радикалов. Данный язык отвечает за решения следующих поставленных задач функционально-дискреционной модели:

- обеспечение нормального функционирования СТИС в информационной среде;
- выявление и локализацию конфликтных областей СТИС в технологическом процессе использования информационных ресурсов;
- ликвидацию инцидентов конфликтной области.

Первая задача рассматривает проблему выполнения целевых функций. Решение данной задачи основывается на изоморфном перераспределении использования информационных ресурсов в аспекте ИБ и на реорганизации выполнения целевых функций в аспекте ФБ. Вторая задача, ввиду масштабности деятельности в информационной среде СТИС, выявляет конфликтные области за счет логических схем и рассматриваемого языка управления. Третья задача направлена на стратегическое планирование реорганизации СТИС для минимизации возникновения дальнейших конфликтов как на краткосрочный, так и на долгосрочный период функционирования.

В результате данный методологический подход реализации ФДМД на основе особенностей природы функционирования СТИС и среды радикалов направлен на обеспечение информационно-системной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Волобуев С.В.* Философия безопасности социотехнических систем: информационные аспекты. – М.: Вузовская книга, 2004. – 360 с.

2. *Тарасов В.А.* Развитие внутренней структуры базовых логических элементов объектно-ориентированных программных систем. ВІСНИК Донбаської державної машинобудівної академії № 1Е (6), 2006.

3. *Пирогов М.В., Чечкин А.В.* Технология решения задач в нормализованной среде радикалов. Конференция "Интеллектуальные системы и компьютерные науки". – М.: МГУ, 23-27 октября 2006.

4. *Лепешкин О.М., Радько С.А.* Применение теории радикалов как методологического способа обеспечения функциональной и информационной безопасности социотехнических систем управления. Конференция «Управление региональными системами». – Волгоград, Центр прикладных научных исследований, 19 февраля 2008.

5. *Т.С. Соболева, А.В. Чечкин* Дискретная математика с элементами математической информатики [Текст] / под ред. Чечкина А.В. – М.: Учебное пособие для вузов РВСН, 2005. – С. 14.

УДК 004.322.067

М. Б. Гузаиров, И. В. Машкина, Т. Х. Тухватшин

РАЗРАБОТКА МОДЕЛЕЙ ПРИНЯТИЯ РЕШЕНИЙ ПО ОПЕРАТИВНОМУ УПРАВЛЕНИЮ ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ ЧИСЛЕННОЙ ОЦЕНКИ ВЕРОЯТНОСТИ АТАКИ

Любая информационная система функционирует в условиях воздействия угроз, на которые необходимо адекватно реагировать. Современные средства обнаружения вторжений, основанные на сигнатурном анализе, не могут противостоять всему разнообразию атак из-за постоянного их обновления. Средства, основанные на отслеживании аномального поведения, в свою очередь, наоборот, производят большое число ложных срабатываний, что снижает их эффективность. К тому же основная часть присутствующих на рынке средств, имеющих наилучшие показа-