Тел.: 8 (917) 0996858.
Студент.

Kamanin Maksim Alekseevich
Astrakhan State Technical University.
E-mail: astradox@yandex.ru.
App. 53, 16, Kosmonavtov str., Astrakhan, 414057, Russia.
Phone: 8 (917) 0996858.
Student.

УДК 681.3

О.М. Лепешкин

МЕТОДИКА РЕАЛИЗАЦИИ ФУНКЦИОНАЛЬНО-ДИСКРЕЦИОННОЙ МОДЕЛИ НА ОСНОВЕ СРЕДЫ РАДИКАЛОВ

Рассмотрен подход по разработке функционально-дискреционной модели, представлен принцип формирования нормализации проблемной области организации доступа на основе среды радикалов.

Информационная система; социотехническая система; функциональная безопасность; радикал; дискреционное управление доступом.

O.M. Lepeshkin

METHOD OF FUNCTIONAL-DISCRETIONARY MODEL REALIZATION ON THE BASIS OF RADICALS

In the paper the approach of functional-discretionary model developing is considered, the problem area normalisation formation principle of the access organisation on the basis of radicals is presented.

Information system; sociotehnical system; functional safety; the radical; discretionary access control

Понятие *информационно-системной безопасности* (ИСБ) сложной системы [1] является главной ее характеристикой. ИСБ включает в себя две составляющих – информационную безопасность и системную безопасность сложной системы.

Информационная безопасность является особого рода функциональной устойчивостью сложной системы, когда обеспечивается безусловное решение задач жизненного цикла системы вне зависимости от формы (от языка) представления входной информации и от полноты этой информации. Обеспечение информационной безопасности сложной системы реализуется, главным образом, путем постоянного использования символьного моделирования проблемной области системы и методов логического вывода. В терминах математической информатики это означает переход от операторов к ультраоператорам [2, 3].

Системная безопасность сложной системы – это безусловное сохранение ядра системы при решении любой частной задачи жизненного цикла. Другими словами, это сохранение системообразующих (жизненных) составляющих системы и тех связей, которые обеспечивают полноценное функционирование сложной системы, ее системную целостность. Системная безопасность сложной системы – это постоянный учет и устранение конфликтов между ее составляющими и их связями, ко-

торые появляются при решении задач жизненного цикла системы, а также конфликтов между самой сложной системой и внешними к ней системами. Системная безопасность требует реализации системного подхода ко всей проблемной области сложной системы [1, 3, 4].

Разрушительные последствия нарушения функционирования сложных систем и человеческий фактор приводят зачастую к непредсказуемым последствиям для такой системы – это и многое другое говорят, что чем сложнее система, тем важнее для нее проблема обеспечения ИСБ в течение ее жизненного цикла.

Основной подход к обеспечению ИСБ сложной системы – это интеллектуализация такой системы. Интеллектуализация любой системы подразумевает ситуационное представление ее проблемной области и на основе этого оснащение отдельных составляющих системы и ее подсистем элементами искусственного интеллекта. Такое оснащение должно обеспечивать постоянную адаптацию сложной системы к изменяющимся внутренним и внешним условиям, возможность проводить диагностику, контроль, анализ и синтез отдельных составляющих системы и функционирования системы в целом с учетом последствий этого функционирования с целью обеспечения ИСБ на протяжении всего жизненного цикла системы.

Таким образом, интеллектуализация сложной системы означает создание интеллектуальной надстройки, сложной системы, включающей:

1) создание символьной модели всей проблемной области сложной системы, то есть картины мира системы, включающей саму систему, ее окружение и все проблемы жизненного цикла системы;

2) создание специального информационно-программного оснащения этой модели (картины мира) средствами обеспечения ИСБ сложной системы. Целью такого оснащения является обеспечение ИСБ сложной системы при решении задач ее жизненного цикла путем моделирования, анализа и синтеза проблемной области системы, включая окружение системы, ее отдельных составляющих, ее характеристик, адаптацию и прогнозирование поведения системы и многое другое.

Термином “интеллектуализация” подчеркивается свойство такой надстройки развиваться и расширять круг решаемых ею штатных задач ИСБ за счет обучения решению некоторых нештатных для нее задач. Чем больше разнообразных и более трудных нештатных задач может решать такая интеллектуальная система, тем более она интеллектуальная.

Основным способом обеспечения информационно-системной безопасности в условиях воздействия угроз и дестабилизирующих факторов является организация управления доступом к информационным ресурсам.

Из существующих в настоящее время подсистем управления доступом к информационным ресурсам [4] наибольшее распространение получили модели, построенные на основе матрицы доступа, в которой каждому субъекту S_i, $S_i \in S=\{S_1,\ldots S_i\}$ пользователю, по определенным правилам предоставляется доступ к объектам O_i, $O_i \in O=\{ O_1,\ldots O_i \}$.

В подсистемах управления доступа на основе матрицы с фиксированными полномочиями при определении их полномочий для того, чтобы учесть динамику изменения состояния информационной системы, следует ориентироваться на пессимистический вариант развития событий, что приводит к существенному завышению требований к организации доступа и соответствующему снижению целевого функционирования, что ведет к уменьшению функциональной безопасности системы, так как усложняет семантическое взаимодействие задач и функций.

Внедрение процессного подхода на основе среды радикалов в системы безопасности требует пересмотра реализации моделей доступа, внедрение системного

принципа позволяет организовать доступ с учетом состояния и возможности реализации функций и задач системой.

Понятие радикала является главным понятием математической информатики [2] и, по-видимому, всей дискретной математики [3].

Под радикалом понимается любая функциональная система, имеющая два доступных извне состояния: активное и пассивное. Активный радикал функционирует согласно своему предназначению, а пассивный радикал нет. Он как бы выключен. Множество радикалов со связями между собой является средой радикалов.

Информационно-системная безопасность сложной системы обеспечивается нормализацией среды радикалов проблемной области. Нормализация проводится в три этапа. Первый этап нормализации состоит в разделении радикалов на два вида: уникумы и контейнеры.

Имя уникума начинается с символа ‘u’ (от слова «unicum») и содержит три индекса: u[1:*][2:*][3:*]smthunicum;. С помощью первого индекса идентифицируется тип уникального радикала, например: целое число; конечная десятичная дробь; истинностное значение; единица измерения длины; составляющая сложной системы; составляющая некоторой проблемной области. С помощью второго индекса идентифицируется экземпляр уникума определенного типа. С помощью третьего индекса идентифицируется модификация уникума. Допускается сокращенная запись вида usmthunicum;, usu;.

Определение: Уникум доступа *uD* определяется в системе как активный или пассивный элемент, имеющий функциональное предназначение *F* в виде определенного набора задач a_n: $uD=F(a_n)$.

При организации процессного подхода обеспечение безопасности доступа основывается на нормализации в среде радикалов. Тогда среда доступна для уникума и записывается как $u_n \rightarrow uD_n\{u_1, u_2, \ldots, u_n\}$, где $u_1 \rightarrow u_2 = uD_1 \rightarrow uD_2$ при $D_1 = D_2$.

С помощью понятия контейнера реализуется идея топологической фильтрации уникумов в среде радикалов. Если уникумы соответствуют компонентам проблемной области сложной системы, то контейнеры отвечают за их свойства. Контейнер может содержать только те уникумы (компоненты системы), которые обладают выделенным свойством. В математической информатике контейнеру соответствует многоместное отношение или понятие, или многоместный предикатный символ.

Имя контейнера начинается с символа ‘C’ (от слова «container») и содержит три индекса: c[1:*][2:*][3:*]smthcontainer (допускается сокращенная запись: csmthcontainer;, csc;). Индексы контейнеров определяются аналогично индексам уникумов. Всякий контейнер, соответствующий многоместному отношению (предикатному символу), обязательно связан со схемой радикалов, раскрывающей это отношение. Контейнер – способ задания связи определенного типа между радикалами.

Определение: Контейнер доступа *CD* определяется в системе функциональным предназначением *F* в виде определенного набора разрешенных к взаимодействию контейнеров C_n: $CD=F(C_n)$. На основе данного выражения можно описать среду доступа и для контейнера C, $C_n \rightarrow CD_n\{C_1, C_2, \ldots, C_n\}$, где $C_1 \rightarrow C_2 = CD_1 \rightarrow CD_2$ при $D_1 = D_2$.

Второй этап нормализации состоит в ультраоснащении среды радикалов. В среде радикалов вводятся три взаимосвязанных части: опорная среда, ультрасреда и терминальная среда. Опорная среда образуется из опорных радикалов – это уникумы и контейнеры возможных и присутствующих сущностей проблемной

области, например, составляющих сложной системы. Ультрасреда образуется из ультрарадикалов. Это системы анализа и синтеза, предназначенные для ИСБ-решения задач жизненного цикла системы. Ультрарадикалы – это продукции базы знаний проблемной области. Терминальная среда образуется из радикалов-исполнителей и радикалов-датчиков, осуществляющих связь между опорными радикалами и ультрарадикалами. Ультрасреда вместе с терминальной средой определяют так называемое ультраоснащение среды радикалов, предназначенное для ИСБ-решения задач жизненного цикла сложной системы, выявления и снятия конфликтов и системных нарушений целостности системы.

Для построения ультрасред будем использовать схемы специального вида, определяемые ультраконтейнерами двух типов 1 и 2.

Ультраконтейнеры типа 1 используются при поиске схем в среде опорных радикалов, а также для добавления новых схем к этой среде. Ультраконтейнеры типа 2 имеют, в отличие от ультраконтейнеров типа 1, непустую посылку. Ультраконтейнер типа 2 – это схема-продукция с непустой посылкой. Схемы, связываемые ультраконтейнером типа 2, могут содержать как уникумы, так и звенья-переменные.

Определение: Ультраконтейнер доступа U*D* определяется в системе функциональным предназначением *F* в виде определенного набора разрешенных к взаимодействию ультраконтейнеров U_n: $UD=F(U_n)$.

На основе данного выражения можно описать среду доступа и для ультраконтейнера U , $U_n \rightarrow UD_n\{U_1, U_2,\ldots,U_n\}$, где $U_1 \rightarrow U_2 = U\,D_1 \rightarrow U\,D_2$ при $D_1 = D_2$.

Вопросами активирования среды радикалов занимаются системы, которые называются активаторы.

Активатор системы доступа обеспечивает навигацию в среде опорных радикалов, а также выделение в среде радикалов тех или иных схем для последующей активации.

Определение: Активатор доступа *AD* есть правило, определяющее среду взаимодействия между средами доступа *uD*, *CD*, *UD*.

При реализации доступа каждый u при нормализации среды для системы в соответствии с процессным походом имеет среду взаимодействия (SV) – это область возможных взаимодействий элементов системы с учетом функциональности, которая основывается на целях, требованиях, функциях и задачах системы и записывается в виде множества взаимосвязанных уникумов $\{u_1, u_2, \ldots, u_n\}$, контейнеров $\{c_1, c_2, \ldots, c_n\}$ и ультраконтейнеров $\{U_1, U_2, \ldots, U_n\}$.

Таким образом, активатор A_u определяет порядок взаимодействия уникумов с учетом ограничений контейнеров C и ультраконтейнеров U, $A_u = f(u_1 \rightarrow u_n)$ при ограничении на C и U.

В случае сложности системы при организации процессного подхода существует активатор контейнеров $A_c = f(c_1 \rightarrow c_n)$ при ограничении U и активатор ультраконтейнеров $AU=f(U_1 \rightarrow U_n)$.

Таким образом, для обеспечения безопасного функционирования системы необходимо сформировать активатор доступа $AD=\{A_u, A_c, A_U\}$.

Определение: Активатор доступа *AD* безопасен для системы в том случае, если A_u, A_c, A_U обеспечивают бесконфликтную работу системы в целом.

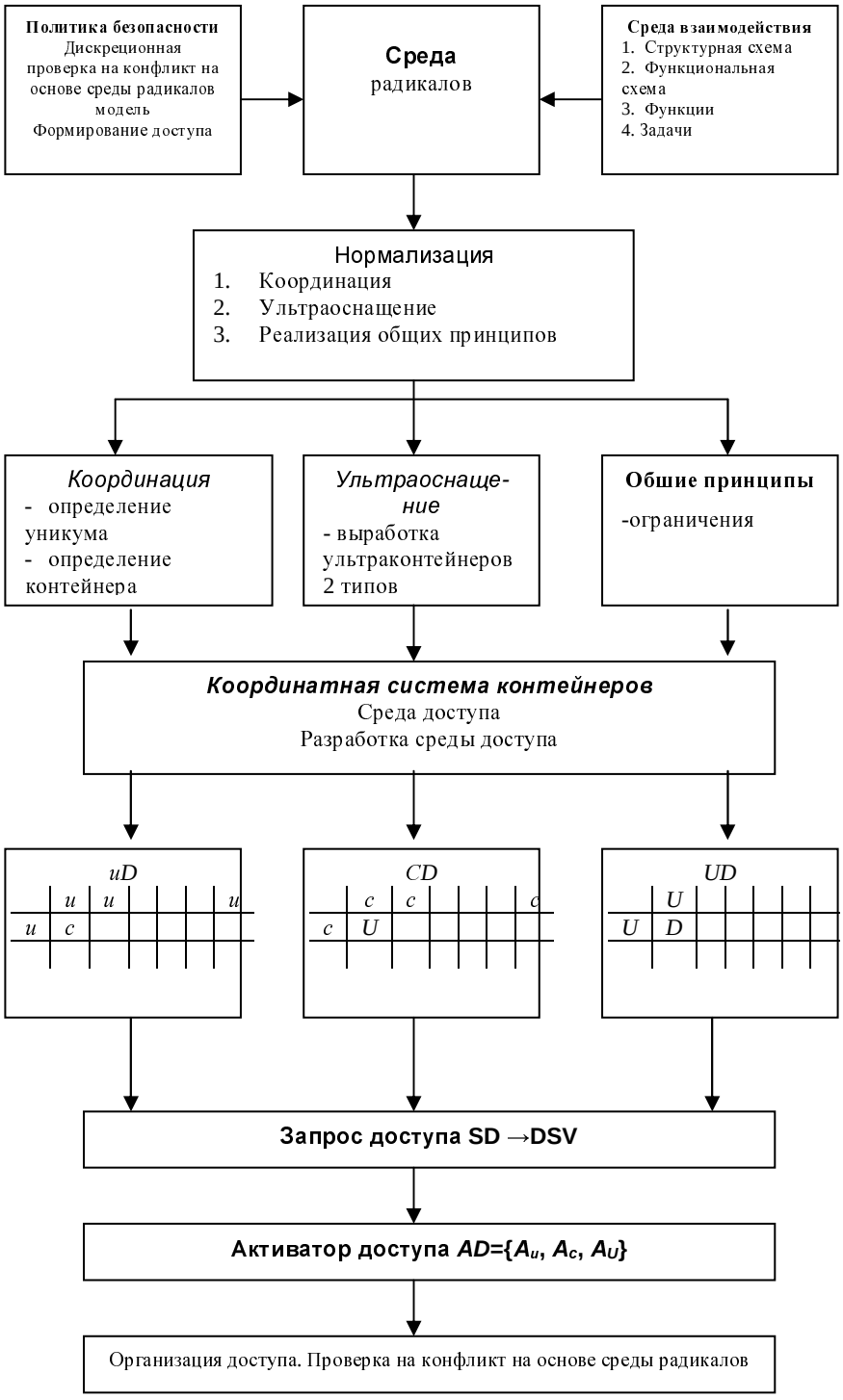

Рис. 1. Реализация функционально-дискреционной модели на основе среды радикалов

Доступ определяется как безопасное взаимодействие уникумов $u_1, u_2, \ldots, u_n$ в системе при согласовании контейнеров C и ультраконтейнеров U. Общая формула доступа есть сравнение доступа среды взаимодействия DSV-системы при функционировании и среды доступа SD=(uD, CD, UD) – область разрешенных взаимодействий с точки зрения безопасности элементов системы, заданной политикой безопасности: DSV=SD → доступ, DSV≠SD → доступ по совпадающим uD, CD, UD, где безопасность определяется как бесконфликтность взаимодействия сред доступа u_1D_1 и u_2D_2, C_1D_1 и C_2D_2, U_1D_1 и U_2D_2.

Таким образом, функционально-дискреционная модель – *это разграничительная модель доступа на основе среды радикалов с учетом процессного подхода*. Реализация функционально-дискреционной модели на основе среды радикалов представлена на рис. 1.

Исходной информацией для реализации функционально-дискреционной модели является описанная политика безопасности и среда взаимодействия системы. Данная информация переносится через среду радикалов и нормализуется через координацию, ультраоснащение, реализацию общих принципов функционирования.

Реализованная координатная система контейнеров позволяет провести разработку среды доступа *SD=(uD, CD, UD)*. Запрос доступа *SD →DSV* формирует активатор доступа *AD={Au, Ac, AU}*. Проводится проверка на конфликт, используя среду радикалов, и при положительном исходе организуется доступ.

Данная методика реализует доступ в системе с учетом процесса функционирования на основе внедрения системного принципа и пересмотра реализации моделей доступа, позволяет организовать доступ с учетом состояния и возможности реализации функций и задач системой.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Лепешкин О.М.* Исследование функциональной безопасности систем государственного управления // Инфокоммуникационные технологии. – 2007. – Т. 5. – №3.

2. *Пирогов М.В., Чечкин А.В.* Технология решения задач в нормализованной среде радиалов // Мат. конф. "Интеллектуальные системы и компьютерные науки". – М., 2006.

3. *Симанков В.С.* Системный анализ функциональной стабильности критичных информационных систем: Монография / В.С. Симанков, П.В. Сундеев. – Краснодар: Институт современных технологий и экономики. – 132 с.

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

Лепешкин Олег Михайлович
Научно-исследовательская лаборатория Ставропольского военного института связи и ракетных войск.
E-mail: lom@stavsu.ru.
355000, г. Ставрополь, проезд Северный, 13.
Тел.: 8 (905) 4100255.
Начальник.

Lepeshkin Oleg Mihailovich
Research laboratory Stavropol Military Institute of Connection and Rakete Troops .
E-mail: lom@stavsu.ru.
13 North Passage, Stavropol, 355000, Russia.
Phone: 8 (905) 4100255.
Head.