спеціальне устаткування (термінал). Шнайер і Шостак (Schneier and Shostack) рекомендують об'єднати власника карти й власника даних в одну особу [4]. Часто вони і є одною особою, але програми смарт-карт не завжди приймають цей факт і розділяють доступ - це найпростіший і найдешевший спосіб захиститися від певного виду атак, які є бідою для багатьох систем, заснованих на смарт-картах. Альтернативний та більш дорогий спосіб зменшити проблеми поділу повноважень - введення в карту пристрою введення даних і екрана.

Таким чином при використанні смарт-карт в системах моделювання необхідно проаналізувати три основних фактори розподілу повноважень і відповідальності за інформацію, що використовується, наявність засобів захисту від реінженірінгу і атак при безпосередньому використанні карток.

Висновок. Проведений аналіз дозволяє оцінювати ризики використання смарт-карти як компоненти інформаційної системи і є основою для розширення бази моделювання системи захисту комп'ютеризованих систем.

1. *Андрей Межутков* Атаки на смарт-карты. Спецвыпуск: Хакер, номер #061, стр. 90-95.
2. *Патрик Гель* ПК и чип-карты**:** Пер. с фр. - М.: ДМК Пресс, 2003. - 144 с.
3. *Сергій Скоробогатов, Росс Андерсон* Смарт-карты – взгляд на безопасность при свете фотовспышки. -. IV ежегодная конференция MasterCard International, Дублин, 15-16 мая 2002 г.
4. *Нильс Фергюсон, Брюс Шнайер.* Практическая криптография. Practical Cryptography, Издательство: Вильямс, 2005 г, 424 с.

Поступила 15.01.2009р.

УДК 683.03

Ю.М.Коростиль, Г.А.Максименко

ОСНОВНЫЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ, ОРИЕНТИРОВАННОЙ НА ИСПОЛЬЗОВАНИЕ В СИСТЕМАХ РАДИО МОНИТОРИНГА

Сбор данных по радиочастотной обстановке не ограничивается только физической регистрацией источников радиосигналов, анализом их технических характеристик и определением значений их параметров. Необходимость расширенного анализа данных, которые могут быть получены в результате сбора данных РЧО в том числе и за счет радиочастотного мониторинга, определяется широким распространением индивидуальных средств приема-передачи информации, проникновением

радиосредств в бытовую сферу и сферу жизнедеятельности человека, широким развитием телеметрических служб и высокой степенью индивидуализации соответствующих радиосредств [1]. Вторая причина определяющая необходимость развития системы сбора данных радиочастотной обстановки состоит в динамичном увеличении номенклатуры типов радиоканалов, которые широко распространяются на рынке услуг и к которым можно отнести:

- радиоканалы мобильных систем связи;
- радиоканалы спутниковых систем связи;
- вещательные и телевизионные радиоканалы;
- каналы беспроводного радио доступа и персональных радиосистем;
- каналы новых радио сервисов (телеметрических услуг, радиочастотных меток, внутридомовых радиосетей и т.д.).

Более высокой ступенью развития системы радиомониторинга является ее дополнение информационным мониторингом состояния радиосетей и радиоканалов, который должен проводится в узлах соответствующих систем связи и характеризуется большим количеством измеряемых параметров и объединяется в единую систему сбора данных радиочастотной обстановки. Однако, в связи с высокой интенсивностью информационных потоков в таких узлах и по ряду других причин различного характера, обеспечить необходимую полноту анализа данных сложно.

Следующий фактор, обуславливающий необходимость расширения радиомониторинга системами анализа данных состоит в том, что в настоящее время радиосредства приема/передачи данных (сообщений) покрывают значительные территории и обладают высоким уровнем динамической распределенности в пространстве. Это особенно актуально в связи с развитием сетей и средств мобильной радиосвязи имеющих развитый набор информационных сервисов.

Динамическая распределенность радиосредств определяется их способностью с достаточно большой скоростью изменять свое пространственное местоположение в период между сеансами работы. При этом, возможность мониторинга такого перемещения может исключаться самим пользователем [2].

Количество возможных аргументов, обосновывающих необходимость расширения функциональных возможностей систем сбора данных по радиочастотной обстановке, может увеличиваться в зависимости от расширения задач, на решение которых ориентированы средства приема/передачи данных использующие для связи радиоканалы.

Важной особенностью персонализированных средств мобильной радиосвязи, является их возможность принимать и передавать информацию в достаточно широком диапазоне методов ее представления, что в зависимости от решаемой задачи может существенно усилить ее информационное и управляющее воздействие на объект (субъект) управления (получателя

информации). Второй, не менее важной особенностью является то, что такой обмен может носить не только односторонний, но и многосторонний характер, а также служить причиной появления других многосторонних информационных связей. Под многосторонней связью, в данном контексте, подразумевается связь, при которой абонент, получивший информацию, может стать источником (инициатором) новых сеансов связи, устанавливаемых с другими абонентами. Причиной многосторонних информационных связей может стать первичная информация, полученная от первичного сеанса реализованной связи между абонентами.

Рассмотрим основные информационные компоненты информационной технологии, которая является одним из средств, обеспечивающих необходимое расширение функциональных возможностей системы сбора данных о радиочастотной обстановке.

Следует отметить, что в силу физических возможностей распространения радиоволн технические средства, обеспечивающие сбор данных о радиочастотной обстановке, должны представлять собой иерархическую структуру. В данном случае будем рассматривать информационную технологию и, соответственно, информационные компоненты такой технологии, для систем локального сбора данных об РЧО, которые находятся на низких уровнях иерархии. Информационные компоненты систем сбора данных об РЧО можно разделить на следующие типы:

- статические информационные компоненты;
- динамические информационные компоненты;
- функциональные информационные компоненты;
- интерпретационные информационные компоненты.

Проведем краткий анализ каждого из перечисленных классов информационных компонент.

Статические информационные компоненты S_i представляют собой средства, которые формируются на этапе инициализации или инсталляции определенной информационной технологии и в процессе функционирования такой технологии не изменяются. Примерами таких статических средств могут служить: семантические словари S_c, энциклопедии S_E, специализированные словари S_{pi}, интерпретаторы S_u.

Прежде чем приводить описание S_c, S_E, S_{pi} и S_u, отметим, что информационная технология в целом и, соответственно, информационные компоненты отличаются от других объектов и технологий следующими особенностями:

- базовым элементом информационных технологий является элемент, использующий для своего описания язык, который отличен от языка, используемого для описания тех или иных технических или программных компонент и, чаще всего, представляет собой естественный язык пользователя;

- каждый фрагмент информационной компоненты, который описывается естественным языком, выполняет не только роль описания, но и может использоваться для анализа функциональных возможностей, а также и для реализации отдельных функциональных возможностей;

- в процессе функционирования информационной технологии компоненты, которые представляются в виде описаний на естественном языке, могут приводить к порождению новых описаний, касающихся новых объектов или процессов, которые возникают в процессе функционирования информационных технологий [3].

Приведенные выше особенности информационных компонент являются существенными для определения информационной технологии, поскольку они позволяют отличить последние от информационных систем, для которых характерно использование исключительно статических информационных компонент, каковыми являются базы данных, отдельные массивы данных и другие формы сохранения данных и которые в процессе функционирования информационных систем могут накапливаться, преобразовываться и использоваться для решения различных задач.

Динамические информационные компоненты представляют собой описания допустимых изменений, которые можно осуществлять с тем или иным объектом или процессом, который описывается в статических компонентах. Все дело в том, что объекты, которые используются в некоторой системе, могут преобразовываться различными способами. Например, аналитическими преобразованиями, логическими преобразованиями или качественными преобразованиями и т.д.

Аналитическим преобразованиям, как правило, подвергаются объекты, которые характеризуются теми или иными численными значениями выбранных параметров. В этом случае, функциональные преобразования приводят к изменениям числовых значений-параметров, которыми соответствующий объект характеризовался в текущий момент времени. Логическое преобразование, в первую очередь, выполняется над элементами, которые имеют логическую интерпретацию. При этом логическому преобразованию может поддаваться только такой объект, который для своего описания использует более одного логического параметра. В рамках динамической компоненты может реализовываться процесс изменения описания типа интерпретации параметров объекта, что может приводить к возможности применения логических преобразований к объектам, которые до таких изменений могли поддаваться только функциональным преобразованиям.

Качественные преобразования представляют собой преобразования, которые описываются в динамических и информационных компонентах и могут реализовываться по отношению к объектам, которые описываются качественными параметрами. Поскольку объектом анализа в системах радиочастотного мониторинга, кроме самого источника радиоизлучения,

может являться и приемник информации, которую несет радиоизлучение, и таким приемником является не только техническое средство приема, но и человек или социальный объект, то использование качественных параметров, для описания соответствующих объектов, является совершенно необходимым. Под социальным объектом подразумевается группа людей, которая описывается одним или несколькими объединяющими их параметрами.

Информационные компоненты динамического типа, структурно близки к объектам статического типа, но отличаются от последних тем, что они содержат описания допустимых преобразований над одним или совокупностью объектов, к которым такое описание относится. Второе отличие состоит в том, что такое описание может быть представлено не только в виде текстового описания на естественном языке, но и в виде формальных математических соотношений, компоненты которого описывают соответствующий объект. При этом описания преобразований могут носить системный характер. В этом случае, описание преобразований состоит из функциональных преобразований, которые могут соединяться с логическими описаниями преобразований, а также могут быть синтезированы с текстовыми описаниями преобразований. При этом возникает задача синтеза различных по своей природе и по используемым средствам описаний в единое комплексное описание преобразований некоторого объекта или процесса.

Функциональные информационные компоненты представляют собой систему правил преобразования текстовых элементов информационных компонент. Эти правила строятся на основе формальных описаний правил грамматики языка, который используется для формирования текстовых фрагментов на основе анализа семантики соответствующих описаний.

Интерпретационные информационные компоненты представляют собой совокупность средств, которые определяют способ вычисления значений семантических параметров текстовых элементов информационных компонент. Такие средства представляют собой не только способы вычисления значений семантических параметров, но и методы определения алгоритмов таких вычислений. Это означает, что в состав интерпретационных компонент входят и условия по которым производится изменение алгоритмов вычисления значений семантических параметров.

Рассмотрим более детально способы описания статических информационных компонент. Первым из таких компонент является семантический словарь. Семантический словарь S_c представляет собой список интерпретационных описаний на естественном языке потребителя объектов и процессов, которые составляют предметную область исследований. В случае информационной технологии системы сбора данных о радиочастотной обстановке, таких предметных областей несколько:

- предметная область описания технических средств радиопередающих

устройств и радиосигналов (W_P);

- предметная область информационного потока сообщений или информационных посылок, которые исходят от радиосредств передачи сообщений к потребителю (W_I);

- предметная область, описывающая различные категории потребителей информации, которые могут представлять собой отдельных лиц или отдельные социальные объекты (W_S);

- предметная область, описывающая различные аномальные ситуации, возникающие в сети при передаче сообщений и порождаемые внешними и внутренними факторами нестабильности (W_A).

Использование четырех различных предметных областей определяет возможность решения задачи, которая состоит в описании взаимосвязей между отдельными объектами этих областей, а также процессами, которые в этих предметных областях происходят: **внешнее событие (факт) → излучение сообщений ИРИ → аномалия информационного потока в сети → потребитель сообщения (информации)**.

Поскольку перечисленные предметные области отличаются между собой физической природой компонент, которые их образуют, то возникает необходимость описывать их взаимосвязь в рамках различных средств, каждое из которых характерно для отдельной предметной области. Это определяет необходимость использования таких информационных компонент, как энциклопедии S_E.

Основное отличие энциклопедии S_E от словаря S_c состоит в том, что в S_E описываются на качественном уровне взаимосвязи между элементами различных предметных областей. Такие описания могут носить характер гипотетических утверждений и, поэтому, подвержены в наибольшей мере модификациям в процессе функционирования информационной технологии. Соответствующие описания в большинстве случаев носят эвристический характер. Для исследования других отличий между S_E и S_c, рассмотрим методы формального описания этих информационных компонент.

Семантический словарь состоит из однотипных элементов, каждый из которых записывается в виде:

$$x_i:=<\alpha_{i1},...,\alpha_{in}>_1 | \ \dots \ | <\alpha_{i1},\dots, \alpha_{im}>_k , \qquad (1)$$

где x_i – объект, с которым производятся функциональные преобразования в процессе функционирования информационной технологии. Эти преобразования реализуются аналитической составной частью информационной технологии; α_{ij} – слово естественного языка, которое используется для составления одной фразы интерпретационного описания; $<\alpha_{i1},...,\alpha_{in}>_m$ отдельная фраза или отдельное предложение, которое используется в интерпретационном описании.

В случаях, когда интерпретационные описания не будут приводиться в явной форме, будем соотношение (1) записывать в следующем виде:

$$x_i = j(x_i), \qquad (2)$$

где j – идентификатор интерпретационного описания.

В этом случае словарь S_c можно представить в виде:

$$S_c = \begin{cases} [x_1 :=< \alpha_{11},...,\alpha_{1m} >]\& \\ \&[x_2 :=< \alpha_{21},...,\alpha_{2n} >]\& \\ ..... \\ \&[x_n :=< \alpha_{n1},...,\alpha_{nk} >] \end{cases} \quad (3)$$

Для описания $j(x_i)$ в S_c существуют некоторые ограничения. Первое из них состоит в том, что в словаре S_c, x_i не может содержать слов α_{ij} таких, которые представляют собой элемент словаря x_j, для которого имеет место соотношение $j > i$. Второе ограничение состоит в том, что $j(x_i)$ должны представлять собой нормализованные описания на естественном языке. Это означает, что в $j(x_i)$:=<α_{i1}, …, α_{im}> не должны встречаться неоднозначности, избыточность и другие формы описаний, которые присутствуют в большинстве других языков. Третье ограничение состоит в том, что $j(x_i)$ содержит описания которые определяют объект как таковой, но не содержат описаний, которые представляют допустимые функциональные преобразования соответствующих объектов.

Для удобства обозначений, идентификаторы объектов из различных предметных областей будем обозначать соответствующим верхним индексом. Например, $W_P = \left\{x_1^P,....,x_m^P\right\}$, $W_I = \left\{x_1^I,....,x_n^I\right\}$, $W_S = \left\{x_1^S,....,x_k^S\right\}$ и $W_A = \left\{x_1^A,....,x_l^A\right\}$. Поскольку структура S_E аналогична структуре S_c, то отдельный элемент из S_E запишется в виде следующего соотношения:

$$[y_i = f_i(x_i^P, x_j^I, x_v^A)] :=< \alpha_{i1}^P,....,\alpha_{im}^P >1 |...| < \alpha_{j1}^I,....,\alpha_{jn}^I >k |...| < \alpha_{v1}^A,....,\alpha_{vn}^A >l, \quad (4)$$

где $f_i(\cdot)$ – функция взаимосвязи между объектами x_i^P из W_P, x_j^I из W_I и x_v^A из W_A. Эта функция описывается текстовым описанием $j(y_i)$. В связи с тем, что в данном случае $j(y_i)$ содержит некоторую часть описания $j(x_i^P)$, $j(x_j^I)$ и $j(x_v^A)$, то в $j(y_i)$ можно выделить фрагмент, который описывает саму функцию f_i. Очевидно, что в процессе функционирования информационной технологии, может произойти редукция, которая формально описывается соотношением:

$$[< \alpha_{i1}^P,....,\alpha_{im}^P >1 |...| < \alpha_{ji1}^I,....,\alpha_{jn}^I >k]|...| < \alpha_{v1}^A,....,\alpha_{vn}^A >l \to f_i^*(x_i^P, x_j^I, x_v^A), \quad (5)$$

где $f_i^*(x_i^P, x_j^I, x_v^A)$ функциональная зависимость, которая представляется в аналитическом виде, в табличном виде, в виде эмпирических зависимостей

или в виде логических формул. Это обстоятельство приводит к необходимости обладать развитыми средствами семантических преобразований, в рамках которых можно было бы строить процессы редукции, пример которой представлен в соотношении (5). Как и в случае семантического словаря, энциклопедия S_E формально запишется в виде:

$$S_E = \left\{ \begin{array}{l} [y_1 = f_1(x^P_{i1}, x^S_j)] := [< \alpha^P_{i1}, ..., \alpha^P_{ik} >_1 |....| < \alpha^S_{j1}, ..., \alpha^S_{jm} >_k] \\ [y_2 = f_2(x^I_{i2}, x^P_j)] := [< \alpha^I_{i1}, ..., \alpha^I_{ir} >_1 |....| < \alpha^P_{j1}, ..., \alpha^P_{jn} >_r] \\ ..... \quad ..... \quad ..... \\ [y_n = f_n(x^S_j, x^I_k)] := [< \alpha^S_{j1}, ..., \alpha^S_{jn} >_1 |....| < \alpha^I_{k1}, ..., \alpha^I_{km} >_e] \\ ..... \quad ..... \quad ..... \\ [y_l = f_l(x^S_\nu, x^A_\mu)] := [< \alpha^S_{\nu 1}, ..., \alpha^S_{\nu n} >_1 |....| < \alpha^A_{\mu 1}, ..., \alpha^A_{\mu m} >_u] \end{array} \right\}, \quad (6)$$

Следует отметить, что функция f_i может описывать зависимости между произвольным количеством переменных, которые идентифицируют объекты предметных областей W_P, W_I, W_S, W_A и в общем виде ее можно представить:

$$y_i = f_i(x^I_1, ..., x^P_i, ..., x^S_m, ..., x^A_l) . \quad (7)$$

Поскольку элементы S_E описывают взаимосвязи между объектами x^P_i и x^S_j, то в рамках $j(x^P_i)$ и $j(x^S_j)$ можно выделить такой фрагмент $\left\{ ... < \alpha^*_{i1}, ..., \alpha^*_{ik} > ... \right\}$, который представляет собой описание, имеющее отношение только к f_i. Очевидно, что для реализации редукции (5) используются и остальные фрагменты из $j(y_i)$. Введем следующее определение.

Определение 1. Фрагмент интерпретационного описания $<\alpha_{i1},\ldots,\alpha_{im}>$ в $j(y_i)$ называется ядром интерпретации y_i, если в $<\alpha_{i1},\ldots,\alpha_{im}>$ не входят α^P_i, α^I_i, α^S_i или α^A_i из предметных областей W_P, W_I, W_S, W_A.

Выделение ядра интерпретации из $j(y_i)$ является неизбежной процедурой для реализации редукции типа (5).

Рассмотрим более детально представление об интерпретаторах S_U. Как уже отмечалось выше, интерпретаторы описывают семантические параметры. Особенность таких описания состоит в том, что семантические параметры могут видоизменяться в процессе функционирования информационной технологии (ИТ) в среде $W = (W_I \cup W_P \cup W_S \cup W_A)$, что формально можно записать в виде:

$$F_1[P_S(x_i) \in [a_1, b_1]] \to F_2[P^*_S(x_i) \in [a_2, b_2]], \quad (8)$$

где F_i – функция фрагмента функционирования ИТ (W), $P_S(x_i)$ – семантический параметр, $[a_i, b_i]$ – диапазон значений, в котором определен параметр P_S . Мутация (видоизменение) в этом случае происходит при переходе от одного цикла работы ИТ к другому. Естественно, что процесс мутации может и не происходить. Условия инициации процесса мутации описываются в компоненте S_U. Как видно из определения процесса мутации (5.8), мутация семантических параметров в рамках ИТ не совпадает с определением мутации, известном из генетических алгоритмов [4]. В генетических алгоритмах мутация приводит к изменениям качественных характеристик гена, поскольку там происходят изменения в структуре гена. В данном, рассматриваемом нами случае, **мутация семантического параметра состоит в изменении способа вычисления значения параметра**. В этом случае, соотношение (8) можно переписать в более конструктивной форме:

$$\{P_S(x_i) = \varphi_i[\xi_i(j(x_i)), \xi_j(j(x_i))]\} \rightarrow \{P_S^*(x_i) = \varphi_j[\xi_k(j(x_i)), \xi_r(j(x_i))]\}, \quad (9)$$

где ξ_i – параметр интерпретационного описания объекта x_i, φ_i – функция определяющая способ использования параметра ξ_i для вычисления значения семантического параметра $P_S(x_i)$, а $P_S^*(x_i)$ – мутированный семантический параметр.

Очевидно, что $P_S(x_i)$ может зависеть более чем от одного параметра интерпретационного описания ξ_i. Рассмотрим на качественном уровне, в чем может состоять условие инициации процесса мутации семантических параметров. Такое преобразование, как мутация P_S в рамках данной ИТ, может быть необходимым вследствие того, что в ИТ в пределах одного цикла реализации процесса функционирования, могут использоваться различные предметные области W_P, W_I, W_S и W_A. Поскольку семантические словари S_c для каждой предметной области разные то, соответственно, разными являются объекты и их интерпретационные описания. Это означает, что различные параметры этих описаний могут в различных областях интерпретации различным образом определять семантический параметр типа P_{Si}, который по определению должен соответствовать одному и тому же семантическому смыслу. Это обстоятельство может привести к возникновению конфликтов или противоречий в ИТ, что может обусловить нежелательную мутацию P_{Si} в ИТ.

1. *Конахович Г.Ф.* Системи радіозв'язку. К.: НАУ, 2004. – 280 с.
2. *Максименко Г.А., Хорошко В.А.* Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К.: ООО «Полиграф-консалтинг», 2004. – 340 с.
3. *Гладкий А.В.* Формальные грамматики и языки. М.: Наука, 1973.
4. *Goldberg D.E.* Genetic Algorithms in Search, Optimization and Machine Learning. Addision – Wesley, 1989.

Поступила 16.01.2009р.