Труды научно-технической конференции кластера пензенских предприятий,
обеспечивающих **БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**
Том 8, Пенза-2012, С 27-31 (http://пниэи.рф/activity/science/BIT/T8-p27.pdf)

ЯЗЫК ОПИСАНИЯ СХЕМ РАБОТЫ ПРЕОБРАЗОВАТЕЛЯ БИОМЕТРИЯ-КОД ДЛЯ ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

Язов Ю.К. (г. Воронеж), Майоров А.В. (г. Пенза)

Согласно ГОСТ Р 52633.4–2011 [1] доступ к преобразователю биометрия-код осуществляется с помощью унифицированного программного интерфейса. Гибкость программного интерфейса позволяет использовать его для представления различных схем преобразования в процессе высоконадежной биометрической аутентификации (ВБА). Схемы преобразования могут строиться с учетом особенностей разных биометрические технологии, способов обработки биометрических данных, различного числа участников и вариантов мультибиометрического слияния.

Наличие специальных терминов ВБА, моделей обучения, тестирования и выполнения преобразования биометрия-код средствами ВБА делают целесообразным определение специализированного языка описания процессов ВБА, понятного широкому кругу специалистов. Основная цель разработки языка – создание единого информационного пространства взаимодействия разработчиков средств ВБА и биометрических приложений. Вторая по важности задача – упрощение процедуры сертификации разрабатываемых средств высоконадежной биометрической аутентификации с использованием нотаций этого языка.

Единый формальный языка биометрической аутентификации делают возможным автоматический синтез автоматов обучения, тестирования и использования преобразователей биометрия-код различных вариантов. Единый подход к моделирование средств ВБА будет способствовать повышению качества научно-преподавательской деятельности, проводимых научно-исследовательской и опытно-конструкторской работ.

Несмотря на достоинства существующих формальных языков, следует указать ограничения их применимости при описании процессов ВБА. Низкоуровневые языки программирования (Assembler, CIL) ориентируются на особенности конкретных вычислительных платформ. Функциональные и объектно-ориентированные языки (C, Pascal, Lisp, Java) обладают достаточной гибкостью, но затрудняют восприятие предметной области и требуют высокой квалификации прикладных специалистов. Логические языки программирования (Prolog) отличаются недостаточной прозрачностью представления сложно организованных схем и процедур взаимодействия предикатов, что не соответствует модели преобразования биометрия-код. Языки обработки баз данных (SQL) удобны для описания отношений между данными, но обладают меньшей наглядностью при описании моделей преобразований. Универсальный язык моделирования (UML) является удобным способом описания процессов, структур данных и отношений, но создает сложности при выполнении автоматической трансляции схем преобразования в тесты. Графические языки подходят для наглядного представления отношения между элементами (Дракон, SFC, LD, CFC), но не учитывают специфику процессов ВБА.

Разрабатываемый язык должен обладать достоинствами перечисленных языков: универсальностью при описании предметной области (как C++), наглядностью и интерактивностью (как Simulink), простотой в изучении (как XML), – но учитывать особенности предметной области.

Схема преобразования представляет собой направленный граф выполнения преобразований над входными параметрами с целью получения выходного кода и значений индикаторов. Каждое отдельное преобразование является узкоспециализированной функцией обработки данных. Настройка каждого преобразования и его тестирования выполняется индивидуально. Каждое преобразование, в свою очередь, может быть представлено в виде ряда вложенных преобразований, имеющих те же стадии жизненного цикла, что и родительское преобразование.

Для представления организации такой структуры вычислений удобно использовать модель агентов, каждый из которых решает определенный класс задач обработки данных, действует независимо от других агентов и взаимодействует с ними посредством потоков данных и сигналов. Потоки данных и сигналов связываются с параметрами агентов. Набор принимаемых параметров (данных и сигналов) определяет интерфейс агента, строго ограниченный рамками предметной области. Каждый агент может либо порождать сигналы и данные (находится в активном состоянии), либо реагировать в ответ на внешнее воздействие сигналом (находиться в состоянии ожидания).

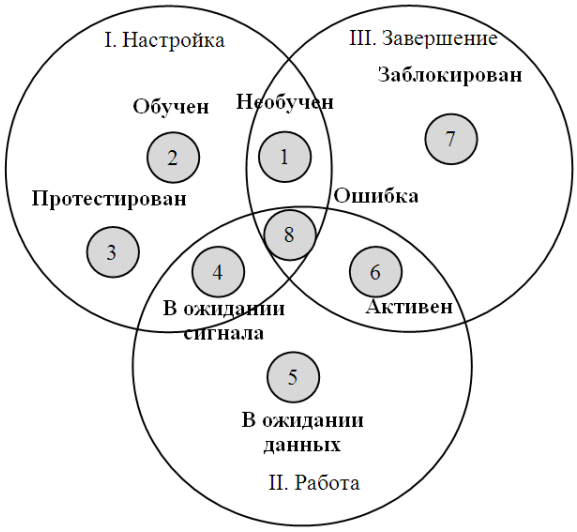

Рисунок 1. Модель состояний агента

Каждый агент может находиться в одном из 8 состояний, которые показаны на рисунке 1:

- "Необучен". Определяет начальное состояние агента или состояние неисправности, при котором гарантировано верными являются только его интерфейсы и связи с другими агентами. Агент не может использоваться по назначению без его настройки;
- "Обучен". Настроены параметры выполнения преобразования. Агент может быть включен в работу;
- "Протестирован". Качество работы агента и используемых им гипотез подтверждено путем его тестирования;
- "В ожидании сигнала". Агент находится в ожидании управляющего сигнала для начала своей деятельности;
- "В ожидании данных". Агент находится в ожидании данных на некоторых слотах для формирования отклика на поданный сигнал;

- "Активен". Агент находится в состоянии обработки или генерации сигналов или данных на определенном такте функционирования системы;

- "Заблокирован". Прием или передача сигналов агента приостановлена;

- "Ошибка". Результат деятельности агента по назначению содержит ошибку. Попытка обработки данных должна быть повторена или переданы другие данные для обработки.

Выполнение переходов между состояниями осуществляется каждым агентом самостоятельно. Важным свойством предлагаемой модели независимых агентов является возможность оптимизации вычислений с помощью механизма обратных запросов, а также устойчивое функционирование системы при исключении некоторых агентов из схемы преобразования во время работы.

Агенто-ориентированная концепция языка соответствует задаче описания процессов ВБА. Элементарные преобразователи средств ВБА систем представляются в виде агентов языка, имеющих интерфейс преобразователя. Их параметры и функции отображаются в виде параметров агентов. Используемые биометрические параметры и образы, результаты промежуточных вычислений передаются в виде потоков данных, обладающих признаками (например, "Свой", "Чужой", "Все чужие"). Состояние преобразователей представляется в виде состояний агентов. Хранимые данные – в виде информационных агентов, принимающих сигналы экспорта и импорта данных.

Управление и синхронизация деятельности агентов осуществляется извне, путем подачи на их входы сигналы, соответствующие решаемым задачам преобразователя биометрия-код. Например, во время обучения, агентам может быть отправлен сигнал ".train", а во время использования ".process". Каждый сигнал, поступающий агенту, обрабатывается им независимо от других агентов. При необходимости получения данных агент обращается с базовыми запросами данных ".ask_data" к связанным с ним слотам. Минимально достаточные данные, необходимые для продолжения деятельности определяются агентом самостоятельно. Для обращения за сигналом к другим агентам используется запрос ".ask_signal". Сложные агенты, содержащие вложенные агенты, могут обращаться к своим дочерним агентам с запросом ".ask_state" для контроля их состояния. Каждый из агентов должен поддерживать запрос на сохранения состояния ".serialize" или описания средства требуемого уровня. Логика выполнения основных запросов и преобразований, выполняемых агентами, соответствующих элементарным преобразователям, определяется в соответствии с требованиями пакета стандартов ГОСТ Р 52633.

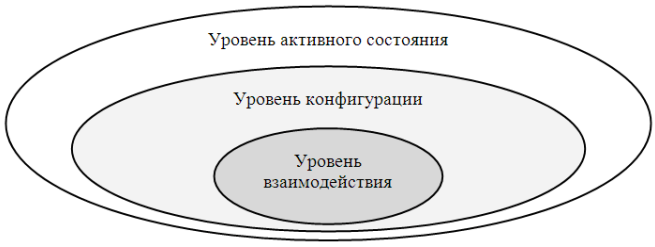

Рисунок 2

Для описания средств высоконадежной биометрической аутентификации на разных этапах использования предлагается выделить 3 уровня описания состояния, как показано на рисунке 2.

Уровень взаимодействия используется для определения метаописания агентов и их отношений: по данным, сигналам, общности, принадлежности. Для

хранения данных этого уровня для преобразователя биометрия-код достаточно использоваться формат схемы преобразования.

Уровень конфигурации включает данные уровня взаимодействия, а также параметры обученных (протестированных) агентов, готовых в работе. Для хранения данных этого уровня для преобразователя биометрия-код можно использовать формат биометрического контейнера.

Уровень состояния определяет текущее состояние агентов системы. Хранимые данные этого уровня включают в себя данные уровня конфигурации, а также внутреннее состояние агентов на момент его сохранения, установленные параметры и сигналы. Формат хранения параметров этого уровня должен определяться средой моделирования, например, использовать расширенный биометрический контейнер.

Для наглядного представления отношений между агентами предлагается использовать графические обозначения, как показано на рисунках 3-5.

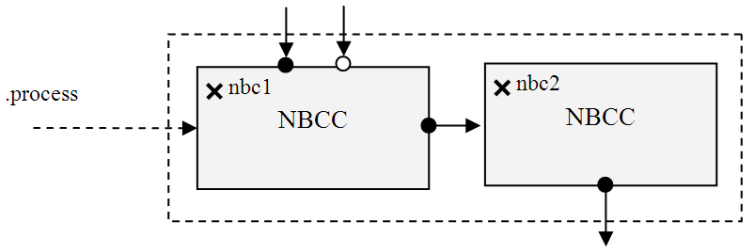

Рисунок 3. Обозначение агентов и их параметров

Агенты представляются в виде прямоугольных заштрихованных областей, имеющих тип и идентификатор (метку), и параметры. Параметры обозначаются в виде кругов, расположенных на границах областей агентов. Составные агенты обозначаются с помощью пунктирных областей.

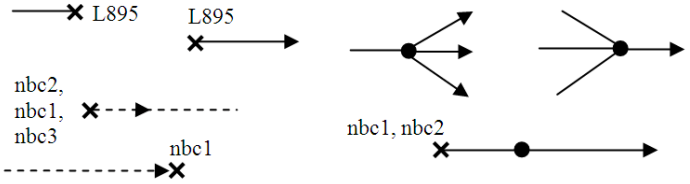

Рисунок 4. Обозначение потоков данных и сигналов

Потоки данных, потоки сигналов обозначаются в виде, соответственно, сплошных и пунктирных линий со стрелкой в пределах линии, указывающей основное направление передачи информации. Для упрощения читаемости графических схем допускается введение разрывов линий с назначением меток разрывам, объединение и разделение потоков данных и сигналов, а также множественное связывание потоков с входными и выходными параметрами агентов.

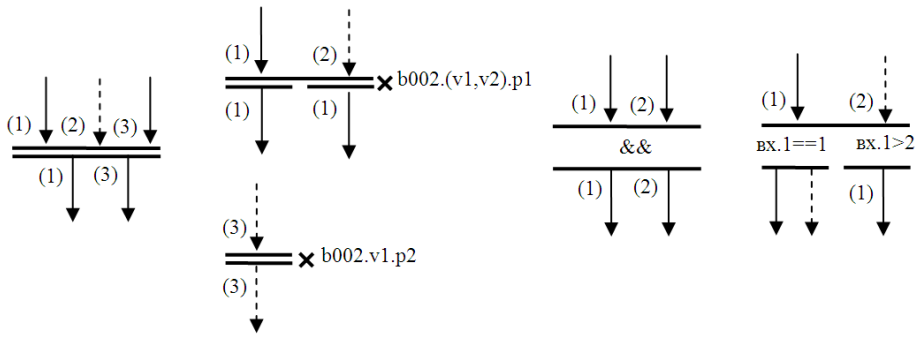

Рисунок 5. Обозначение условных конструкций

Для описания правил синхронизации агентов, а также внешних по отношению к ним целей, применяются условные конструкции. Условный элемент представляется в виде двух толстых сплошных линий, перпендикулярных входным и выходным потокам данных и сигналов, между которыми может размещаться некоторое условие, как это показано на рисунке 5. В случае наличия нескольких альтернатив, нижняя линия обозначения делится на требуемое число частей, над каждой из которых указывается условие срабатывания. Каждому входному и выходному потоку может быть присвоен номер. Для удобства размещения на схеме, одна и та же условная конструкция может быть разделена на несколько частей, снабженных одной и той же меткой.

Символьные элементы языка используются для записи меток, условных выражений, фильтров, признаков и комментариев.

Комментарии определяют текстовый блок, содержащий произвольную информацию, поясняющую работу схемы.

Метки определяют уникальные идентификаторы элементов языка: агентов, параметров, разрывов потоков данных и сигналов, условных конструкций и их частей. Метки позволяют повторно указать использование элементов языка без необходимости их дублирования, а также более компактно поместить основную информацию на схему преобразования. Доступ к отмеченным вложенным элементам схем осуществляется с помощью оператора ".".

Фильтры задают правила выбора из потока данных необходимых данных и, по сути, являются аналогами SQL запросов, выполняемых над составными потоками данных и сигналов языка. Операторы фильтров включают в себя элементы селективного и индексного доступа ("[]"), именного доступа (".name"), операции с множествами ("::"), а также проверки признаков.

Признаки используются для маркировки классов данных в потоке в соответствии с некоторыми условием или имеющимся фактом. С помощью признаков, например, могут быть определены множества образов "Свой", "Все чужие", "Чужой" и отношения между ними. Агенты, раздельно используя данные, с признаками "Свой" и "Все чужие", могут корректно выполнить процедуру обучения.

Запись условных выражений выполняется с помощью стандартных операторов языка C++, дополненных фильтрами данных.

Предложенная концепция языка позволяет учесть особенности процесса высоконадежной биометрической аутентификации, компактно описать различные схемы выполнения преобразования биометрия-код для использования во время разработки, тестирования и сертификации средств высоконадежной биометрической аутентификации.

Литература:

1. ГОСТ Р 52633.4–2011 Защита информации. Техника защиты информации. Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа.

Материалы поступили 01.03.2012, опубликовано в Интернет 20.04.2012 по положительной рецензии д.т.н., проф. Малыгина А.Ю. (Пенза).