СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ И ОБРАБОТКА ИНФОРМАЦИИ

УДК 355.01: 004.056

С.В. Жуков, В.А. Маклаев, П.И. Соснин

МОДЕЛИРОВАНИЕ СТАНДАРТА ГОСТ Р ИСО/МЭК 15408 «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. КРИТЕРИИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ»

Жуков Станислав Владиславович, *окончил факультет экономической кибернетики Московского экономико-статистического института (МЭСИ). Соискатель Ульяновского государственного университета. [e-mail: texthapb@mail.ru].*

Маклаев Владимир Анатольевич, *кандидат технических наук. Окончил радиотехнический факультет Ульяновского политехнического института. Генеральный директор ФНПЦ ОАО «НПО «Марс». Имеет статьи в области САПР. [e-mail: mars@mv.ru].*

Соснин Петр Иванович, *заслуженный работник высшей школы РФ, доктор технических наук, профессор. Окончил радиотехнический факультет Ульяновского политехнического института. Заведующий кафедрой «Вычислительная техника» УлГТУ. Имеет многочисленные труды в области концептуального проектирования автоматизированных систем. [e-mail: sosnin@ulstu.ru].*

Аннотация

Информационная безопасность автоматизированных систем должна строиться на базе современных стандартов. Предлагаются решения по разработке средств защиты, ориентированные на материализацию требований стандартов в базе прецедентов.

Ключевые слова: автоматизированная система, информационная безопасность, метрика, проектирование, профиль безопасности.

Stanislav Vladislavovich Zhukov, *graduated from the Faculty of Economical Cybernetics of Moscow Institute of Economics and Statistics; applicant at Ulyanovsk State University. e-mail: texthapb@mail.ru.*

Vladimir Anatolyevich Maklaev, *Candidate of Engineering, graduated from the Faculty of Radioengineering of Ulyanovsk Polytechnic Institute; Director General of Federal Research-and-Production Center Open Joint-Stock Company 'Research-and-Production Association 'Mars'; author of articles in the field of CAD. e-mail: mars@mv.ru.*

Petr Ivanovich Sosnin, *honored worker of the Higher School of the Russian Federation, Doctor of Engineering, Professor; graduated from the Faculty of Radioengineering of Ulyanovsk Polytechnic Institute; head of the Chair 'Computers' at Ulyanovsk State Technical University; author of numerous papers in the field of conceptual design of computer-aided systems. e-mail: sosnin@ulstu.ru.*

Abstract

Information security of computer-aided system is to be based on contemporary standards. The article suggests solutions to the development of security facilities in order to materialize standard requirements in a precedent base.

Key words: computer-aided system, information security, metrics, design, protection profile.

Введение

Специфику последних десяти лет теории и практики информационной безопасности определяет коренная ломка ее онтологии, нашедшая свое выражение в ряде международных стандартов, нацеленных на единообразное понимание информационной безопасности и унификацию ее материализации, открытую для общепринятого оценивания.

Основу новой системы стандартов, обобщающих опыт разработок и эксплуатации защищенных систем, определяет стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Этот стандарт, часто называемый «Общими критериями» (Common Criteria, CC), регламентирует и представляет библиотеку требований (метрик защиты), которую следует использовать в разработке защищенных систем (статью интересуют защищенные автоматизированные системы или АС).

В зависимости от специфики создаваемой $АС_i$ для нее разрабатывается или выбирается типовой профиль защиты (Protection Profile, PP), содержание которого PP_i определяет подходящий набор метрик защиты $\{m_k\}$, выбранных из библиотеки CC. За материализацию PP_i в «теле» $АС_j$ «отвечает» задание по безопасности (Security Target, ST_i), выполняющее функции технического задания на реализацию защиты для соответствующего профиля. Вопросы разработки профилей защиты и заданий по безопасности лежат за рамками стандарта ГОСТ Р ИСО/МЭК 15408 (англоязычный оригинал ICO/IEK 15408 [1]). Успешные образцы таких конструктов предлагаются разработчикам АС в форме нормативных рекомендаций.

Полезными источниками ответов на вопросы разработчиков по профилям защиты и заданиям по безопасности являются другие стандарты, в число которых входят ISO/IEC 13335, ISO/IEC 15446, ISO/IEC 17799 и ISO/IEC 19791.

Но реальность разработок защищенных АС такова, что их создатели практически лишены автоматизированной поддержки в их действиях по построениям PP и ST, отличных от типовых и даже в настройках на специфику АС типовых PP и ST. Этот факт обусловлен исключительной сложностью и неудобными формализмами CC, вложенными в документацию стандарта ГОСТ Р ИСО/МЭК 15408 объемом около 700 страниц, а также в объемные руководства по типовым профилям в сотни страниц.

В статье представлен подход к моделированию стандартов информационной безопасности и применение этого подхода к моделированию стандарта ГОСТ Р ИСО/МЭК 15408.

Специфику подхода определяют следующие установки:

1. За каждым стандартом, относящимся к проектированию, стоит реальный практический опыт, аккумулирующий образцы, которые рекомендуется или требуется использовать в проектной деятельности. Опыт, вложенный в стандарты в текстовой форме (в виде текстовых моделей), следует представить в виде моделей, более приспособленных к оперативной работе проектировщиков.

2. К моделированию образцов опыта, вложенных в стандарты, рационально подходить с позиций их повторного использования, то есть с позиций типовых (повторных) действий, получивших название «прецеденты». Любой прецедент – это активность человека или группы лиц, связанная с действием или решением или поведением, осуществленным в прошлом, которая полезна как образец для повторных использований и/или оправдания повторных действий по такому образцу.

3. Основными образцами опыта, специфицированными в стандарте ГОСТ Р ИСО/МЭК 15408, являются метрики безопасности, каждую из которых полезно представить моделью соответствующего прецедента, а систему метрик – базой прецедентов.

4. Совокупность моделей стандарта ГОСТ Р ИСО/МЭК 15408 должна быть реализована как корпоративный ресурс (система специализированных активов), доступный с рабочих мест проектировщиков в корпоративной сети.

В соответствии с установками подхода для стандарта ГОСТ Р ИСО/МЭК 15408 разработана система моделей, реализация которых осуществлена в вопросно-ответной моделирующей среде WIQA (Working In Questions and Answers). В систему моделей включены база метрик, библиотека профилей безопасности и библиотека методик, обслуживающих работу проектировщиков с моделями.

Наиболее близки к решениям, предлагаемым в статье, публикации [2, 3], в которых также отмечены проблемы применения современных стандартов информационной безопасности и описаны средства автоматизированного доступа к их содержанию, вложенному в базу знаний. Однако вопросы материализации метрик защиты, обеспечивающей их включение в коды АС, причем не только с позиций информационной помощи, в названных публикациях даже не поднимаются.

Обобщенная схема проектирования защиты АС

Необходимость использовать в общем случае стандарты, дополнительные к стандарту ISO/IEC 15408, обусловлена тем, что он изначально ориентирован на процессы разработок АС, защищенных от несанкционированного доступа. Именно расширение потенциала информационной защиты на этапы эксплуатации АС привело к созданию стандарта ISO/IEC 19791, роль которого до его введения выполнял и способен выполнять в настоящее время стандарт ISO/IEC 17799. Разумеется, в реальной практике информационной защиты необходим выход и за рамки ответственности только по линии несанкционированного доступа.

Предлагаемые метод и средства проектирования защиты (обозначим для краткости МСПЗ) изначально рассчитаны на угрозы, исходящие не только от преднамеренного несанкционированного доступа, но и от случайных попыток несанкционированного доступа лиц (но только лиц), находящихся как за рамками, так и внутри АС. Для оперативного учета лиц, представляющих угрозы АС актуально и потенциально, в число предлагаемых средств включена компонента, моделирующая оргструктуру АС и ее «враждебного» окружения.

Отметим и то, что ответственность МСПЗ распространяется на следующий набор функций защиты: идентификацию и аутентификацию, управление доступом, протоколирование и аудит, а также на шифрование, анализ защищенности и управление. Выбор названных функциональностей, в реализации которых объединяются подходящие метрики защиты, обусловлен ориентацией на угрозы, исходящие только от человека.

Представленные ограничения выбраны из-за намеренной ориентации МСПЗ на разработчиков систем, проблемы защищенности которых связаны с человеческим фактором доступа к АС. В то же время МСПЗ специфицированы и реализуются так, чтобы набор функциональностей информационной защиты мог быть расширен и открыт для модификаций.

Кроме того, комплекс МСПЗ специфицирован и реализуется так, чтобы их ответственность распространялась не только на этапы разработки АС, но и на этапы эксплуатации. Такая ответственность обеспечивается за счет потенциальной возможности присоединения комплекса МСПЗ к разработанной АС.

И, наконец, комплекс МСПЗ реализуется в инструментально-технологической среде WIQA.Net в ее комплектации [4], обслуживающей разработку сложных АС, что позволяет решать задачи проектирования защиты, используя богатый набор отлаженных средств этой среды.

К числу базовых установок, управляющих созданием МСПЗ, относится и понимание «информационной безопасности» как «искусственного явления», которое не инкапсулируется в отдельную подсистему АС, из-за чего ее коды приходится распределять среди других кодов разрабатываемой АС. Другими словами, существование необходимой информационной защиты проявляет себя через «следы», которые «явление» информационной безопасности оставляет в процессах АС в ситуациях явных или потенциальных угроз. К числу таких «следов» относятся активности метрик защиты.

Эта базовая установка специально выведена в пункт, раскрывающий обобщенную схему проектирования защиты с использованием МСПЗ, поскольку она указывает на то, что коды метрик защиты и их совокупностей должны активизироваться событийно и автоматически. Выявление в процессах АС таких «событийных точек» и их спецификаций в виде «если событие, то активизация метрики» является одной из наиболее важнейших задач проектирования защиты АС. Этот факт следует признать существенным аргументом в пользу материализации метрик и их связных совокупностей как прецедентов. Именно по этой причине в состав средств комплекса МСПЗ, обобщенная схема которого приведена на рисунке 1, включена база прецедентов БП($\{m_k\}$).

На рисунке 1 отражено принципиально значимое место оргструктуры (ОРГ) разрабатываемой АС (выделена штриховым контуром). Для работ с оргструктурой в состав средств МСПЗ включена специальная компонента «Оргструктура», функциональности которой доступны с рабочих мест среды проектирования.

Разумеется, на первом месте в проектировании защиты находятся особенности включения метрик защиты в проект АС, в том числе и включение кодов метрик в коды АС. К особенностям такого включения относятся:

- использование аспектно-ориентированного подхода и механизмов распределения метрик защиты по задачам проекта АС;
- представление работ по проектированию защиты в виде решения совокупности типовых задач, представленных в специальном разделе библиотеки типовых задач инструментальной среды WIQA.Net;
- включение любой метрики защиты или совокупности метрик в проект связано с экземпляром типовой задачи защиты, которая встраивается в определенную «точку» общего дерева задач проекта;
- использование агентов, нацеленных на этапе эксплуатации на выявление событий, требующих защитных реакций;
- регистрация метрик, включенных в проект АС и в ее тело в форме, удобной для аудиторских проверок как результата проектирования, так и защитных реакций на этапе эксплуатации АС.

На рисунке 1 отражено и то, что средства проектиро-

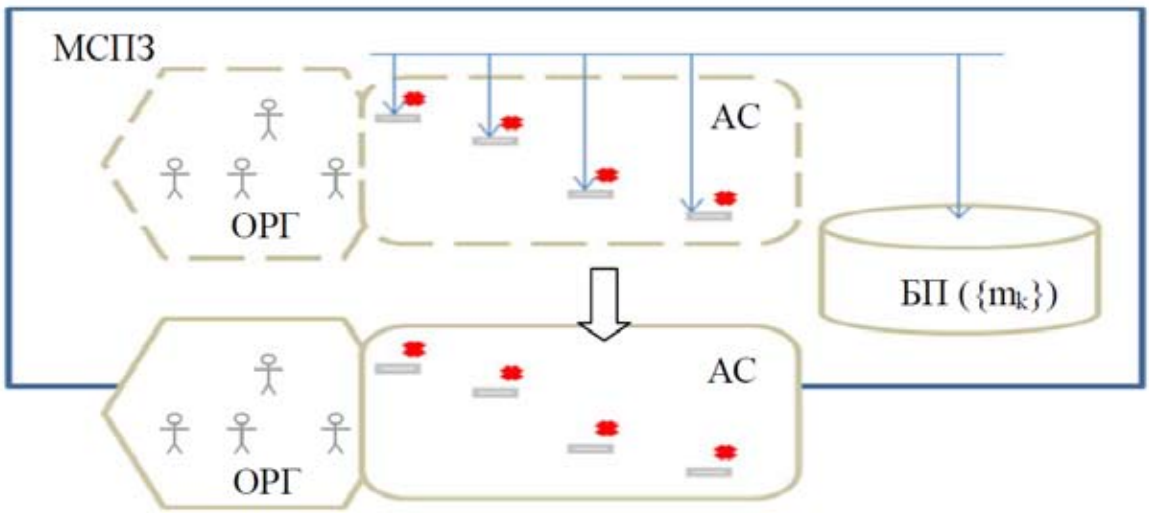

Рис. 1. Обобщенная схема проектирования защиты

вания защиты открыты для их включения в состав разработанной АС (отмечена сплошным контуром).

Моделирование метрик стандарта

Независимо от того, что прецеденты разнообразны как по структуре, так и по содержанию, в их представлениях есть общее, и это общее определяется логической моделью прецедента. Общим является и то, что в построениях представления каждого прецедента, обеспечивающего его повторное применение, если оно осуществляется в среде разработки АС, можно выделить состояния **жизненного цикла** и связать с состояниями **специализированные модели прецедента.**

Такое моделирование прецедентов было встроено в ряд систем, построенных в среде **WIQA.Net** [4]. В этих приложениях при разработке представлений прецедентов выделялись и регистрировались их состояния (модели), приведенные на рисунке 2.

В набор практически полезных специализированных моделей прецедента, порождаемых в процессе его разработки, включены:

- **текстовая модель P^T**, представляющая постановку задачи **$Z(P_i)$**, в результате решения которой создан образец прецедента (как определенный результат интеллектуального освоения реального прецедента);
- **логическая модель P^L**, конкретизирующая типовую логическую модель (представлена на рисунке 2) в виде формулы логики предикатов, записанной на языке постановки задачи **P^T**;
- **графическая модель прецедента P^G**, представляющая его обобщенно с использованием **«block and line»** средств (например, диаграммы активности на языке **UML**);
- **вопросно-ответная модель P^{QA}**, соответствующая задаче **$Z(P_i)$**;
- **модель P^I**, представляющая вложенное в прецедент поведение в форме **исходного кода** его программы;
- **модель P^E**, выводящая на **исполняемый код** программы, кодирующей образец прецедента;
- **схематическая модель прецедента P^S** в виде его схемы (framework), интегрирующей все специализированные модели прецедента в единое целое.

Схематическая модель прецедента, с которой связывается материальная форма образца прецедента, размещаемая в базе прецедентов комплекса **WIQA.Net**, приведена на рисунке 3.

Материализация образца прецедента в приложениях WIQA подтвердила не только свою достаточную полноту и полезность, но и необходимость ее адаптации к конкретным применениям. Для прецедентно-ориентированного представления метрик стандарта ГОСТ Р ИСО/МЭК 15408 из интегральной схемы исключены модели P^L и P^G, а для кодирования P^I использован язык C#.

Для материализации метрик в виде прецедентов проведен их предварительный анализ [5] по информационному содержанию стандарта ГОСТ Р ИСО/МЭК 15408. Результат анализа для каждой метрики включает следующие позиции (но не только): нормативное имя метрики, ее содержание (в виде постановки задачи), требования к реализации, специфику событийного управления, кодовую материализацию, комментарии. По результатам анализа для каждой метрики были построены ее модели P^T, P^{QA} и P^I, которые объединены в соответствующую модель прецедента. Доступ к метрикам осуществляется с помощью интерфейсной формы, представленной на рисунке 4.

С демонстрационными целями представим две модели и P^T и P^I для метрики FAU_STG.4, специфицирующей предотвращение данных аудита:

1. Постановка задачи (модель P^E)

Определить режим функционирования при переполнении журнала аудита. Реализовать соответствующую реакцию для каждого режима функционирования при переполнении журнала аудита. Имена в макете кода и их семантика:

Перечисляемый тип Deistie_Pri_Narushenii, который определяет действия, совершаемые при нарушении правил;
UserBlock – блокировка действий пользователя;
SystemBlock – блокировка системы;
Warning – просто предупреждение.

Рис. 2. Жизненный цикл построения образца прецедента

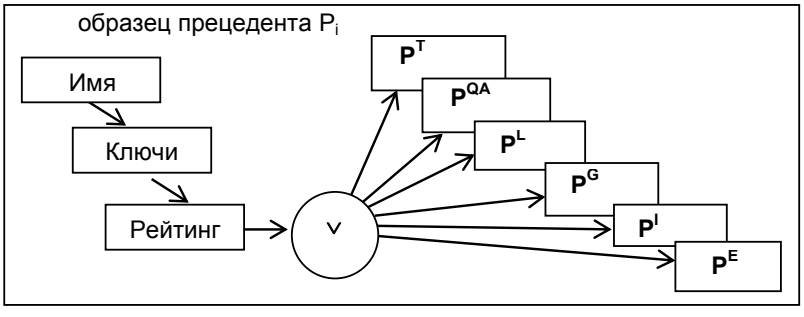

Рис. 3. Интегральная схема образца прецедента

2. Макет исходного кода (модель P^I):

```
switch (BreachAction) {
case BreachAction.UserBlock:
    BlockUser();
    break;
case BreachAction.SystemBlock:
    System.Block();
    break;
case BreachAction.Warning:
    MessageBox.Show(«Warning!»);
    break;
}
```

Представление методик

Реальность проектирования защиты такова, что в задачах такого проектирования используются совокупности метрик. Для демонстрации применения групп метрик представим одну из методик комплекса МСПЗ.

Методика «Настройка журнала аудита»:

1. Определить список событий, подвергаемых аудиту (FAU_GEN.1);
2. Выбрать уполномоченных пользователей, которые имеют доступ к просмотру данных аудита (FAU_SAR1);
3. Выбрать разрешенные действия для уполномоченных пользователей (FAU_SAR.3);
4. Выбрать атрибуты безопасности для избирательного аудита (FAU_SEL 1);
5. Выбрать настройки для хранения данных аудита (FAU_STG);
6. Определить правила, по которым можно будет судить о нарушениях (FAU_SAA);
7. Определить реакцию системы при обнаружении возможного нарушения безопасности (FAU_ARP).

Представленная методика состоит из указаний на действия, которые должен выполнить проектировщик. Каждая методика представляет программу действий, в исполнении которой проектировщик выполняет функции «интеллектуального процессора», которому, в общем случае, приходится принимать интеллектуальные (творческие) решения. По этой причине взаимодействия проектировщиков с методиками в рамках возможного следует автоматизировать.

Для оперативной работы с методиками в инструментальной среде WIQA проектировщикам предоставляются:

1. Комплекс средств кодирования методик (с использованием средств вопросно-ответного протоколирования) в виде псевдокодовых программ.
2. Средства исполнения методик проектировщиками с помощью «Интерпретатора псевдокодовых программ».
3. Библиотека методик.

Обобщенная схема работ с методиками приведена на рисунке 5.

Создание любой методики начинается с выбора «точки» ее загрузки в дерево задач (или библиотеку методик) как новой задачи. Индексное имя новой задачи (1) будет использоваться как начальный адрес для вычисления индексных имен операторов исходного кода методики (как псевдокодовой программы), который будет формироваться проектировщиком в области (2) специализированного текстового редактора. Индексированная копия исходного кода будет формироваться в памяти редактора и визуализироваться в его области (3). После сохранения текущего состояния псевдокода его индексированная копия загружается в вопросно-ответную базу и визуализируется в области (5) основной интерфейсной формы системы WIQA. В любой момент времени псевдокод методики может быть загружен в редактор снова либо для продолжения его построений, либо для исправлений или модификации.

Любая методика в любом состоянии ее псевдокода может быть загружена (6) в интерпретатор для ее проверки или исполнения. Каждый исполняемый оператор визуализируется в специальной интерфейсной области (7), причем в любой момент времени проектировщик может переобъявить любое ключевое слово любого оператора, введя его синоним (8).

В методике «Настройка журнала аудита», кроме содержания действий, приведены имена метрик, используемые в стандарте ГОСТ Р ИСО/МЭК 15408. Легко заметить, что с

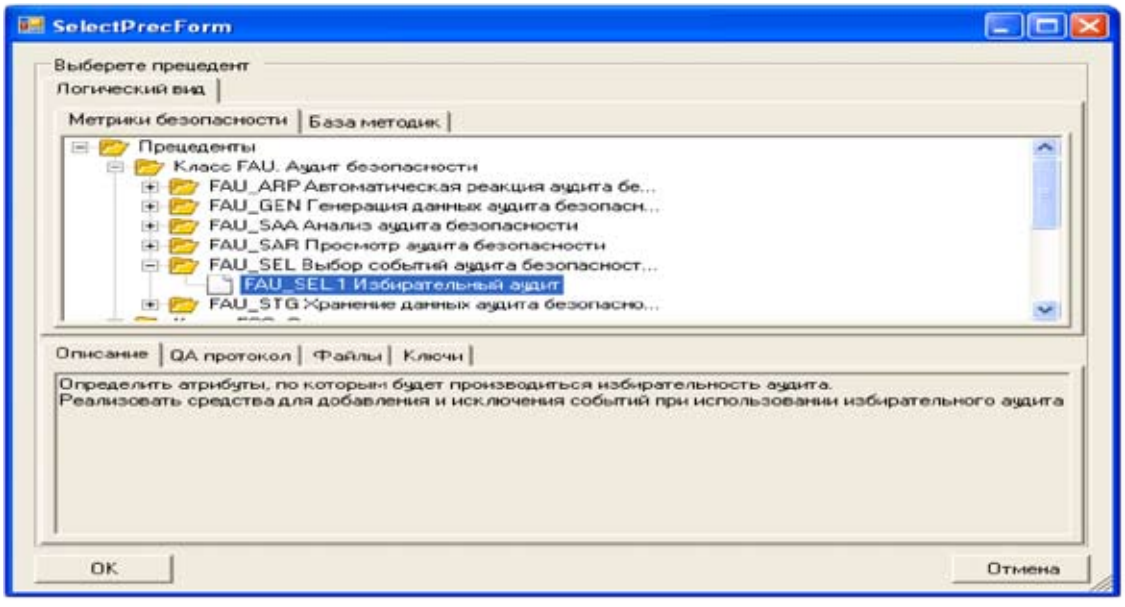

Рис. 4. Интерфейс доступа к базе метрик безопасности

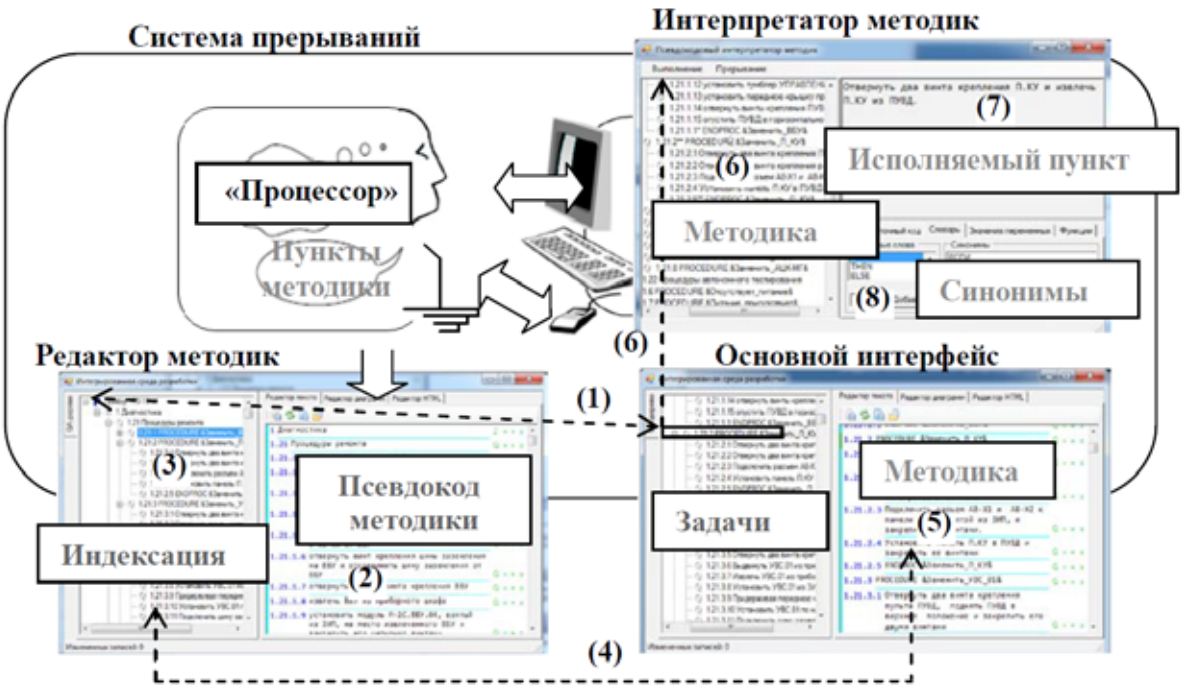

Рис. 5. Средства взаимодействия с методиками

каждым действием методики связано принятие решения, которое затем должно найти материальное воплощение в кодах защиты. Ясно и то, что такие решения, хотя и допускают вариативность, связаны общей задачей методики, а значит должны быть согласованы. Именно по этой причине для согласования методик проектировщикам следует исходить из общей задачи проектирования защиты, для которой в обязательном порядке приходится определяться с подходящим профилем защиты и заданием по безопасности. А задачу проектирования защиты просто необходимо согласовать с задачей разработки АС. Такое согласование в инструментальной среде WIQA обеспечивается единообразным представлением задач любых типов и использованием единого дерева задач [5].

Представление профилей безопасности

Пример с методикой демонстрирует то, что типовые образцы профилей защиты и заданий по безопасности придется настраивать на специфику разрабатываемой АС. Но такая работа проще, чем создание профиля и задания без образцов. По этой причине в состав комплекса МСПЗ включена библиотека типовых профилей защиты и заданий по безопасности, в состав которой входят образцы для дискреционного, мандатного и ролевого доступа, а также образец для доступа к базе данных. Эта библиотека открыта для включения в нее новых образцов.

Шаблон выбранного проектировщиками профиля безопасности загружается в общее дерево разрабатываемого проекта как задача документирования, после чего типовое содержание шаблона становится доступным для адаптации

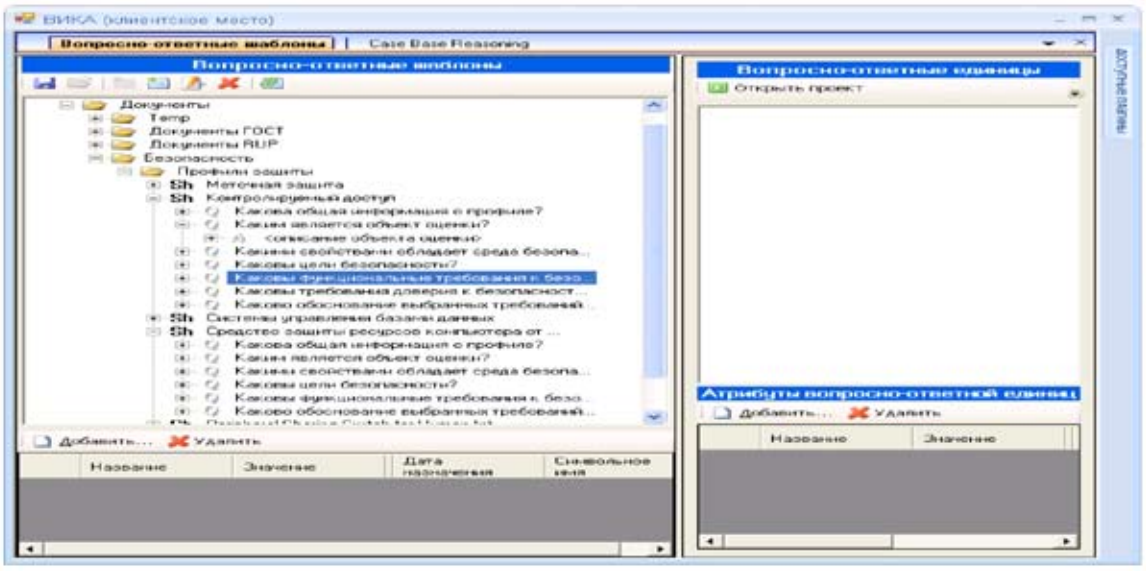

Рис. 6. Вопросно-ответная структура профиля меточной защиты

его содержания к специфике проекта. Взаимодействие с такой задачей документирования осуществляется через интерфейсную форму, представленную на рисунке 6.

Например, для профиля меточной защиты проектировщики, ответственные за решение задач информационной безопасности, должны будут специфицировать следующий фрагмент вопросно-ответной структуры профиля:

.....

Qi1. *Каковы цели безопасности?*

Qi1.1. *Каковы цели безопасности, относящиеся к Информационной Технологии?*

Ai1.1. *O.AUTHORIZATION Функции Безопасности Объекта оценки (ФБО) должны обеспечивать, чтобы только уполномоченные пользователи могли получить доступ к Объекту Оценки (ОО) и его ресурсам.*

Ai1.2*. O.DISCRENIONARY_ACCESS ФБО должны управлять доступом к ресурсам, который основан на идентификаторах пользователей. ФБО должны позволять уполномоченным пользователям определять, какие ресурсы могут быть доступны.*

Ai1.3. *O.AUDITING ФБО должны регистрировать относящиеся к безопасности ОО действия пользователей. ФБО должны предоставлять эту информацию уполномоченным администраторам.*

Ai1.4. *O.RESIDUAL_INFORMATION ФБО должны обеспечивать, чтобы любая информация, содержащаяся в защищаемом ресурсе, не раскрывалась при перераспределении ресурса.*

Ai1.5. *O.MANAGE ФБО должны предоставлять все необходимые функции и возможности для поддержки уполномоченных администраторов, которые являются ответственными за управление безопасностью ОО.*

.....

Подобным образом осуществляется работа и с задачами документирования типа «Задание по безопасности». Отметим, что богатейшая библиотека профилей безопасности (в виде текстов на английском языке) доступна по ссылке [6].

Заключение

Новизну предлагаемых решений по проектированию защищенных АС определяет материализация метрик защиты в виде прецедентов, каждый из которых представлен в версиях для автоматизированного и автоматического доступа, обслуживающих проектирование и эксплуатацию АС соответственно. Прецедентная форма представления метрик защиты и их совокупностей открывает возможность для их аспектно-ориентированного распределения в проекте и кодах АС и событийной активизации в режиме эксплуатации.

СПИСОК ЛИТЕРАТУРЫ

1. ISO/IEC 15408. Common Criteria for Information Technology Security Evaluation Part 1~3 Version 3.0, June 2005.

2. Ramirez Caceres G. H., Teshigawara Y. Design and Development of a Knowledge-based Tool for ST Developers Based on CC v3, The 7th International Common Criteria conference. Lanzarote, Spain. September, 2006. – URL: http://www.7iccc.es/index_en.html.

3. Ramirez Caceres G. H., Teshigawara Y. Study on a Threat-Countermeasure Model Based on International Standard Information. The 12th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2008, Orlando, Florida, USA. July, 2008. – pp. 227–232 (Best Paper).

4. Sosnin P. Means of question-answer interaction for collaborative development activity // Hindawi Publishing Corporation, Advances in Human-Computer Interaction, Volume 2009, Article ID 619405, 18 pages, doi:10.1155/2009/619405.

5. Zhukov S.V., Sosnin P.I. Approach to Materializing the Metrics of Information Technology Security // The 8th International conference on Interactive Systems and Technologies: the Problems of Human Computer Interaction.– Collection of scientific papers. – Ulyanovsk: ULSTU, 2009. – pp. 111–116.

6. U.S. Government Protection Profiles. – URL: http://www.niap-ccevs.org/ (дата обращения: 06.02.2012).