Поясним работу алгоритма 2. Пусть построено $role$-замыкание системы $\Sigma(G^*, OP, G_0)$. В этом состоянии доступы владения субъект-сессий отсутствуют. Это следует из определения $role$-замыкания и того, что применение правил $grant\_right()$ и $take\_role()$ не приводит к появлению доступов владения субъект-сессий. Новые же права доступа ролей без возникновения доступов владения субъект-сессий появиться не могут. Это следует из определения правила $grant\_right()$ и функции $de\_facto\_actions$. Поэтому на шаге 3 выполняется проверка возможности осуществления доступа владения с помощью правила $access\_own()$. Если этого сделать нельзя, то текущее состояние системы не изменится.

В процессе работы алгоритма формируется список доступов владения субъект-сессий, в котором рассмотренные элементы помечаются. Данные доступы рассматриваются последовательно друг за другом. Алгоритм завершает свою работу, когда в списке не останется непомеченных элементов. Данное условие обязано выполниться в силу конечности множества S и его неизменности в процессе работы алгоритма.

Шаги 6–12 алгоритма соответсвуют выполнению правила $grant\_right()$, причем на шаге 8 выполняется вычисление функции $de\_facto\_actions()$ для рассматриваемых x и y. Шаг 12 соответствует корректировке функционально ассоциированных сущностей в рамках предположения 1. Шаги 13–17 соответствуют применению правил $access\_write$ и $access\_append$, шаги 20–24 — правила $post()$, шаги 25–28 — правила $control()$. Правила преобразований рассматриваются в порядке влияния применения одного правила на возможные аргументы других, причем после шага 30 никакое применение правила из $OP_{acs} \setminus \{create\_first\_session(), take\_role()\}$ с учетом только доступа владения (x, y, own_a) не изменит текущего состояния системы.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Базовая ролевая ДП-модель // Прикладная дискретная математика. 2008. № 1 (1). С. 64–70.

УДК 004.94

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ С ФУНКЦИОНАЛЬНО ИЛИ ПАРАМЕТРИЧЕСКИ АССОЦИИРОВАННЫМИ СУЩНОСТЯМИ

Д. Н. Колегов

В настоящее время одной из актуальных задач теории компьютерной безопасности является разработка математических моделей безопасности современных компьютерных систем (КС), реализующих управление доступом и информационными потоками. Данная задача возникает как при теоретическом анализе безопасности КС с применением их формальных моделей, так и при тестировании механизмов защиты КС с использованием процедур, методов и средств автоматизации и компьютерного моделирования. На необходимость формализации процедур оценки безопасности, разработки общих методологий и моделей угроз безопасности КС указывается в «Концепции оценки соответствия автоматизированных систем требованиям безопасности информации» [1]. Более того, в соответствии с «Критериями оценки безопасности информационных технологий» [2] для КС с высоким уровнем доверия обязательным является разработка формальной модели их политики безопасности управления доступом и информационными потоками.

Как правило, для теоретического анализа и обоснования безопасности КС используется подход, основанный на применении классических моделей Take-Grant, Белла – ЛаПадулы, систем военных сообщений, ролевого управления доступом, а также субъектно-ориентированной модели изолированной программной среды и семейства ДП-моделей [3]. С их использованием анализируется безопасность управления доступом и информационными потоками в КС с дискреционным, мандатным или ролевым управлением доступом. Последние две модели адекватно описывают безопасность КС с функционально ассоциированными с субъектами сущностями. При этом ни в одной из известных автору моделей не рассматриваются параметрически ассоциированные с субъектами сущности и не учитывается возможность нарушения безопасности КС при реализации запрещенных информационных потоков по памяти от таких сущностей, что не позволяет моделировать политики управления доступом и информационными потоками в реальных КС.

Другой подход, используемый для анализа безопасности КС, ориентирован на построение потенциально возможных путей нарушения безопасности КС с применением компьютерного моделирования, включающего тестирование безопасности и автоматизированное выявление возможности проникновения. Как правило, данный подход основан на моделях формального описания и верификации политик безопасности или моделях анализа графов атак. В этих моделях используются оригинальные определения элементов и механизмов защиты КС, а применяемый математический аппарат часто недостаточен для анализа условий нарушения безопасности КС и формального обоснования методов и механизмов их защиты. В то же время известны модели, сочетающие теоретический подход к обоснованию безопасности КС с практическим моделированием условий ее нарушения.

Таким образом, можно сказать, что известные теоретические модели безопасности, как правило, не позволяют учесть существенные особенности функционирования существующих КС, в том числе заключающиеся в наличии у субъектов КС параметрически ассоциированных сущностей, а имеющийся математический аппарат, используемый при компьютерном моделировании безопасности современных КС, недостаточен для ее теоретического анализа.

С целью обеспечения безопасности КС с функционально или параметрически ассоциированными с субъектами сущностями с дискреционным управлением доступом и информационными потоками разработана математическая модель (ФПАС ДП-модель), развивающая семейство дискреционных ДП-моделей и, в отличие от них, позволяющая анализировать безопасность данных КС. В модели рассматривается новый вид сущностей — параметрически ассоциированных с субъектами КС, реализация информационных потоков по памяти от которых позволяет нарушителю получать права доступа различных субъектов КС, в том числе и доверенных.

В рамках разработанной ФПАС ДП-модели предложены и теоретически обоснованы:

— необходимые и достаточные условия возможности получения недоверенным субъектом права доступа владения к доверенному субъекту;
— метод предотвращения возможности получения права доступа владения недоверенным субъектом к доверенному субъекту;
— алгоритм поиска всех возможных путей утечки права доступа или реализации запрещенного информационного потока;
— метод предотвращения утечки права доступа или реализации запрещенного информационного потока без изменения реализации субъектов.

На базе предложенной ФПАС ДП-модели КС также построена ДП-модель сетевых дискреционных КС с уязвимостями (СДУ ДП-модель). В ней предполагается, что нарушители могут использовать различные уязвимости (ошибки в системных и прикладных процессах, доверие, доступ к паролям, раскрытие параметров КС), позволяющие получать контроль над субъектами КС, в том числе и доверенными. В рамках построенной СДУ ДП-модели формализованы основные требования по тестированию возможности проникновения семейства к доверию «Анализ уязвимостей» руководящего документа ФСТЭК «Критерии оценки безопасности информационных технологий», а именно: формально описаны модели нарушителя (нарушителя с низким, умеренным и высоким потенциалом нападения) и дано математическое определение стойкости КС к проникновению. Рассмотрены также существующие подходы к построению потенциально возможных путей нарушения безопасности сетевых КС с дискреционным управлением доступом при компьютерном моделировании их безопасности и показано, каким образом в этих подходах может быть применена СДУ ДП-модель.

Таким образом, для теоретического анализа безопасности современных КС с дискреционным управлением доступом с функционально или параметрически ассоциированными сущностями разработана математическая модель, которая может быть использована и уже используется другими учёными [4] в дальнейших исследованиях по теории компьютерной безопасности, а также для формального анализа уязвимостей и моделирования политик управления доступом и информационными потоками в КС с дискреционным управлением доступом с высоким уровнем доверия к их безопасности и для разработки методов управления, администрирования и настройки параметров КС, позволяющих обеспечить защиту от нарушения их безопасности.

ЛИТЕРАТУРА

1. ФСТЭК России. Руководящий документ. Безопасность информационных технологий. Концепция оценки соответствия автоматизированных систем требованиям безопасности информации. М., 2004.
2. Гостехкомиссия России. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Ч. 1–3. М., 2002.
3. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.
4. *Буренин П. В.* Подходы к построению ДП-модели файловых систем // Прикладная дискретная математика. 2009. №1(3). С. 93–113.

УДК 004.56(06)

МНОГОЗНАЧНАЯ ЛОГИКА В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ НА ПРЕДПРИЯТИИ

М. М. Кучеров, А. А. Кытманов

В современной логике предложения иногда считаются не истинными и не ложными. Эта идея восходит еще к Аристотелю, который высказывался относительно будущего, в частности о не вполне определенных событиях, и реализована в системах многозначной логики. Существует также и «дуальная» идея, состоящая в том, что некоторые предложения могут рассматриваться как имеющие одновременно оба истинностных значения. Этот взгляд также имеет многочисленные плодотворные применения в информатике.