УДК 004.8

КВАДРАТ БЕЗОПАСНОСТИ

К.А. Бугайский
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: kabuga@ipu.ru

Ключевые слова: информационная безопасность, открытые системы, модель, вычислительная система, управление конфигурацией, монитор безопасности.

Аннотация: В докладе показано как расширенная модель открытых систем позволяет дать новое прочтение таких классических терминов информационной безопасности как «монитор безопасности объектов « и «монитор безопасности субъектов» вычислительной системы. Прежде всего за счет введение в модель слоев отображающих обрабатываемые данные и пользователей системы, которые позволяют по-новому описывать взаимодействие программных и аппаратных компонент в процессе обработки данных. а также в части управления. Разработанные в модели механизмы коммуникаций и механизмы управления позволяют моделировать и оценивать работу мониторов безопасности на основе конфигураций для наборов программ и пользователей вычислительной системы.

1. Введение

Современные информационные системы представляют собой гетерогенные структуры с широким применением различных механизмов виртуализации и архитектурного приема «инфраструктура как код» [4]. Работа подобных структур повсеместно опирается на принцип открытых систем заложенного в соответствующей референсной модели – OSE/RM. Разработка расширенной модели открытых систем (далее – модели) позволило показать возможность использования принципов, заложенных OSE/RM, для решения задач защиты информации в современных информационных системах. Модель рассматривает вычислительную систему (ВС) как совокупность программных и технических компонент обработки данных, способных функционировать самостоятельно или в составе других систем [1]. Классический подход предполагает рассмотрение вопросов защиты информации в парадигме отношений «субъект-объект» и допустимых между субъектом и объектом операций. При этом в силу факта работоспособности ВС подразумевается выполнение свойства транзитивности при представлении отношения «субъект-объект» как композиции отношений $субъект \rightarrow объект = (субъект \rightarrow приложение) \circ (приложение \rightarrow данные)$. В качестве потенциальных нарушений свойства транзитивности отношений «субъект-объект» рассматриваются ошибки реализации, уязвимости и слабости (прежде всего в части программного обеспечения) [5, 6, см. литературу там же]. Вместе с тем, разработанная модель дает основания для более внимательного исследования условий выполнимости свойства транзитивности для отношения «субъект-объект». Прежде всего речь идет о следующих положениях относительно структуры базовой плоскости модели.

Во-первых это связано с представлением любых объектов ВС (данных, файлов программ, конфигураций и т.п.) в виде информационных единиц (ИЕ), распределенных по физическим носителям информации в ВС.

Во-вторых, это связано с представлением структуры базовой плоскости модели в виде графа G^{op}, $op \in OPS$, где OPS – множество операции которые может выполнять программная сущность (ПС) с ИЕ на данном физическом носителе [2]. Каждый такой граф является деревом, имеющим в качестве корня монитор обращений M. При этом, в силу описания ПС через take- и grant-функции [2], граф G^{op} является орграфом. Напомним, что функции типа take обеспечивают по результатам внутренних вычислений запрос на выполнение необходимых операций в другой ПС, а функции типа grant, обеспечивают инициализацию выполнения необходимых вычислений в самой ПС в ответ на запрос от другой ПС.

В третьих, применительно к базовой плоскости в модели дано разграничение аккаунтов по типам, каждый из которых отнесен к одному из уровней базовой плоскости – HW, OW, MW и AW, имеющих выраженный функциональный характер [1]. При этом принято, что уровни HW и OW, а также аккаунт типа kernel соответствуют монитору обращений M. Таким образом, без потери общности структуру аккаунтов модели можно также представить в орграфа с корневой вершиной kernel. Направленность графа обусловлена иерархией уровней базовой плоскости на основе механизмов коммуникаций модели [2, 8, 9].

В-четвертых, в модели принято, что на каждом уровне базовой плоскости и для каждой вершины графа G^{op} характеристики (прежде всего права доступа) соответствующих аккаунтов и ПС описываются параметрами конфигураций [2, 3].

В-пятых, на основании предыдущих положений и описания плоскости администрирования модели, можно также представить структуру ИЕ в виде иерархии на основе орграфа [7, 9], где в качестве вершины определены конфигурации монитора обращений М и аккаунта типа kernel.

2. Структура модели

При изложении основной части будем использовать следующие компоненты модели: в качестве субъекта – окружение аккаунта (А), в качестве объекта – ИЕ на физическом носителе, а в качестве приложения – ПС на всех уровнях базовой плоскости. Структура ВС с учетом указанных ранее положений модели показана на рис. 1.

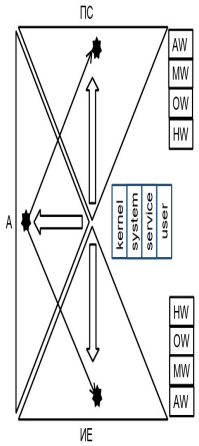

Рис. 1. Структура ВС.

На рис. 1 звездочками и одинарными стрелками отображаются элементы отношений «субъект-объект». Двойные стрелки отображают направление доминирования уровней иерархии и, следовательно параметров конфигурации, прежде всего с точки зрения прав доступа к объектам ВС. Такое доминирование в модели обеспечивается за счет механизмов коммуникаций и управления в основе работы которых лежит различение логического (имя) и физического (идентификатор) именования ПС, ИЕ и А. На основании категорного подхода ВС может быть представлена схемой морфизмов приведенной на рис. 2.

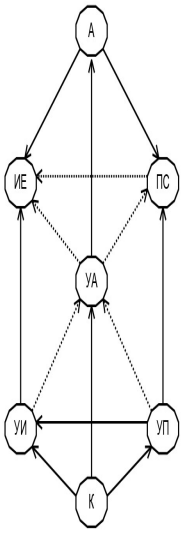

Рис. 2. Морфизмы ВС.

Рассмотрим сначала морфизмы обозначенные сплошными стрелками – то есть те отношения между сущностями, которые обеспечиваются архитектурой современных ВС и являются системными. Ядро системы (К) обеспечивает физическую адресацию ПС, ИЕ и А за счет соответствующих морфизмов: *К→УП*, *К→УИ* и *КУ→УА*. Кроме того, в современных ВС по умолчанию обеспечиваются морфизмы *УИ→ИЕ*, *УП→ПС* и *УА→А*. Также архитектура ВС обеспечивает управление ПС и ИЕ со стороны А за счет морфизмов *А→ПС* и *А→ИЕ*. Как правило, все перечисленные морфизмы в той или иной степени отражают права доступа в рамках отношения «субъект-объект». Поскольку реально работа с данными всегда осуществляется на физическом уровне (как минимум с использованием памяти и процессора), то морфизм *УП→УИ* выражает отношение *приложение → данные* и является следствием коммутативности диаграммы для вершин К,УИ,УП [7, 8, см. литературу там же].

Вместе с тем, перечисленные системные морфизмы рис. 2 не дают оснований для построения морфизма *ПС→ИЕ* с учетом *реальных – физических* – идентификаторов основных сущностей ВС – УИ, УП и УА. Следовательно, можно говорить об отсутствии монотонности в представлении прав доступа субъекта А к ПС и ИЕ при переходе от физического к логическому их именованию. Таким образом, модель показывает наличие имманентной предрасположенности к реализации различных угроз за счет нарушения прав доступа и параметров конфигураций на уровне (в терминах) А, ИЕ и ПС. Следует отметить, что подобная проблема достаточно давно осознана экспертным сообществом, которое рассматривает ее решение на основе внедрения в ВС мониторов безопасности (например, [9]). Схема ВС на рис. 2 позволяет уточнить роль и

место мониторов безопасности в архитектуре современных ВС. Для этого рассмотрим морфизмы схемы рис. 2 представленные пунктирными линиями. Морфизмы *УП→УА∘УА→ИЕ*, а также *УИ→УА∘УА→ПС* обеспечивают непосредственное отображение идентификаторов ИЕ и ПС (физической адресации) на логическое представление (имя) ПС и ИЕ соответственно. То есть, за счет морфизмов *А→ПС∘*, *ПС→ИЕ=А→ИЕ* обеспечивается контролируемая, вплоть до именования на физическом уровне, по правам доступа обработка информации в интересах субъекта. Таким образом, модель предоставляет инструменты для контроля необходимого (прежде всего с точки зрения прав доступа) уровня выполнения отношений *субъект → объект = (субъект → приложение)∘(приложение → данные)*.

При рассмотрении роли и места мониторов безопасности в структуре ВС необходимо обратить внимание на следующие особенности систем:

- все ПС системы образуют единое иерархическое пространство, обозначенное на рис. 1 в виде треугольника ПС;
- все ИЕ системы также образуют единое иерархическое пространство, обозначенное на рис. 1 в виде треугольника ИЕ;
- любое взаимодействие ПС и ИЕ обеспечивается механизмами коммуникаций, реализующих в итоге рекуррентную формулу от уровня AW до уровня HW;
- любое взаимодействие ПС и ИЕ в рамках прав доступа аккаунта А непосредственно зависит от параметров конфигураций ПС и А от уровня user до уровня kernel.

С точки зрения информационной безопасности, при доступе конкретной ПС к определенной ИЕ в пространстве субъекта, наличие промежуточных ПС и аккаунтов можно рассматривать как потенциальный источник угроз. То есть иерархия ПС и А представляет собой иерархию уровней доверия. При этом одни и те же ПС или А могут относиться к различным уровням доверия в различных слоях базовой плоскости (принадлежать разным графам G^{op}). Таким образом, целесообразно мониторы безопасности (МБ) размещать вне имеющейся иерархии ПС, ИЕ и А, как показано на рис. 3. Тем более, что современные ВС обладают необходимыми ресурсами в виде наличия нескольких центральных процессоров. Структуру ВС, приведенную на рис. 3 целесообразно обозначить как квадрат информационной безопасности.

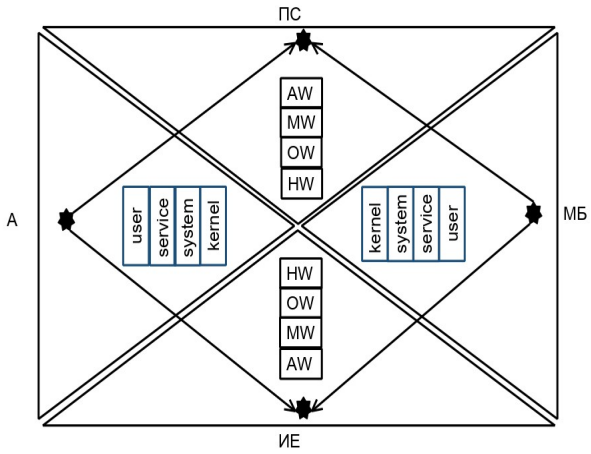

Рис. 3. Квадрат информационной безопасности.

Положения модели позволяют определить следующие роли мониторов безопасности современных ВС:

- приведенные на рис. 2 морфизмы *УИ→УА* и *УП→УА* описывают функционал МБ субъектов;
- приведенные на рис. 2 морфизмы *УА→УЕ* и *УА→ПС*, соответственно, описывают функционал МБ объектов .

Отметим, что в рамках модели функционал МБ субъектов и МБ объектов ВС фактически сводится к согласованию параметров конфигураций ПС и А используемых на различных уровнях и слоях базовой плоскости модели.

3. Заключение

Расширенная модель открытых систем предоставляет необходимые понятия и язык описания для рассмотрения вопросов функционирования вычислительных систем с точки зрения теории управления в терминах субъект управления (пользователь системы), объект управления (конфигурации). Разработанный подход к описанию механизма коммуникаций программных сущностей и механизма управления элементами конфигурации позволяет определить место мониторов безопасности и определить их место в архитектуре вычислительных систем.

Список литературы

1. Бугайский К.А., Бирин Д.С., Дерябин Б.О., Цепенда С.О. Расширенная модель открытых систем (Часть1) // Информация и безопасность. 2022. Т. 25, № 2. С. 169-178.
2. Бугайский К.А., Перескоков И.С., Петров Ал.О., Петров Ан.О. Расширенная модель открытых систем (Часть 2) // Информация и безопасность. 2022. Т. 25, № 3. С. 321- 330.
3. Бугайский К.А., Дерябин Б.О., Табаков К.В., Храмченкова Е.С., Цепенда С.О. Расширенная модель открытых систем (Часть 3) // Информация и безопасность. 2022. Т. 25, № 4. С. 501-512.
4. Калашников А.О., Бугайский К.А Инфраструктура как код: формируется новая реальность информационной безопасности // Информация и безопасность. 2019. Т. 22, № 4. С. 495-506.
5. Калашников А.О., Бугайский К.А., Аникина Е.В. Модели количественного оценивания компьютерных атак // Информация и безопасность. 2019. Т. 22, № 4. С. 517-528.
6. Калашников А.О., Бугайский К.А. Модель количественного оценивания агента сложной сети в условиях неполной информированности // Вопросы кибербезопасности. 2021. № 6 (46). С. 26-35.
7. Кузнецов Н.А., Кульба В.В. (ред.) Информационная безопасность систем организационного управления: теорет. основы / D 2 т. М. : Наука, 2006.
8. Лимончелли Т., Хоган К., Чейлап С. Практика системного и сетевого администрирования / 3-е издание. Пер. с англ. М.: Вильямс, 2018. 1104 с.
9. Щербаков Ф.Ю. Современная компьютерная безопасность. М.: Книжный мир, 2008. 352 с.