УДК 004.056.52

ТРЕХМЕРНАЯ МОДЕЛЬ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Жилин В. В., Дроздова И. И., Черкесова Л. В., Сафарьян О. А.
Донской государственный технический университет, Ростов-на-Дону, Российская Федерация
zhilin95@inbox.ru,
irina_23011995@mail.ru,
chia2002@inbox.ru,
safari_2006@mail.ru

Рассмотрены известные модели безопасности компьютерных систем. Приведено общее описание алгоритма трехмерной модели безопасности. Описаны отношения, возникающие между ее субъектами. Рассмотрены особенности модели, дополненной временным параметром. Выявлены основные недостатки и возможные угрозы трехмерной модели безопасности.

Ключевые слова: модель безопасности, компьютерная система, объект, субъект, доступ, время, массив, полномочия, операции, база данных, иерархические отношения.

UDC 004.056.52

THREE-DIMENSIONAL MODEL OF COMPUTER SYSTEMS SECURITY

Zhilin V. V., Drozdova I. I., Cherkesova L. V., Safaryan O. A.
Don State Technical University, Rostov-on-Don, Russian Federation
zhilin95@inbox.ru,
irina_23011995@mail.ru,
chia2002@inbox.ru,
safari_2006@mail.ru

The article considers the known models of computer systems security. General description of an algorithm of three-dimensional model of computer systems security is provided. The relations arising between its subjects are described. The features of the model supplemented with a time parameter are considered. The main drawbacks and possible threats of the three-dimensional security model are revealed.

Keywords: security model, computer system, object, subject, access, time, array, powers, operations, database, hierarchical relations.

Введение. В настоящее время одной из актуальных задач теории компьютерной безопасности является разработка математических моделей безопасности управления доступом и информационными потоками в компьютерных системах (КС). 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.

Целью данной работы является разработка алгоритма функционирования новой модели безопасности, объединяющей достоинства известных моделей.

Для реализации поставленной цели необходимо решить ряд задач:

1) рассмотреть известные модели безопасности;
2) выделить их достоинства и недостатки;
3) описать собственную разработку;
4) выявить ее уязвимости.

Модели безопасности компьютерных систем (МБКС) позволяют сформулировать условия безопасности для конкретной системы. С помощью МБКС можно проанализировать свойства заданной системы и составить перечень потоков информации, которые в ней разрешены [1].

Дадим точные определения используемых в данной работе терминов и понятий: доступ к информации, правила разграничения доступа, объект и субъект доступа.

Доступ подразумевает ознакомление с информацией и проведение с нею таких операций, как обработка, копирование, модификация и уничтожение [2].

Правила разграничения доступа регламентируют права доступа субъектов к объектам доступа [3].

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения [4].

Субъект доступа — лицо или процесс, действия которого регламентируются правилами разграничения [5].

В основе всех известных моделей безопасности лежит так называемая политика безопасности. Она может зависеть от использования различных технологий обработки информации, программно-аппаратных средств и от местоположения предприятия, для которого разрабатывается [6].

Рассмотрим основные модели безопасности: пятимерное пространство Хартсона, модели на основе матрицы доступа, а также take-grant [7].

Пятимерное пространство Хартсона получило свое название по количеству используемых элементов:

1) установленные полномочия (A),
2) пользователи (U),
3) операции (E),
4) ресурсы (R),
5) состояния (S).

Для определения области безопасности в пятимерном пространстве необходимо найти Декартово произведение этих элементов. В данном случае доступом будут считаться введенные пользователями запросы, под которыми подразумеваются какие-либо операции с ресурсами компьютерной системы.

Пользователи могут запрашивать доступ к ресурсам системы. Если доступ разрешается, система переходит в новое для нее состояние. В данном случае под запросом будет пониматься четырехмерный набор следующего вида:

$$q = (u, e, R', s),$$

где $u \in U$, $e \in E$, $s \in S$, $R' \subseteq R$ (R' — требуемый набор ресурсов).

Достоинство представленной модели — возможность управления доступом с точностью до каждой отдельной операции над отдельным объектом. Однако данная модель не лишена недостатков. Ее реализация является весьма трудоемкой. По этой причине она не получила широкого практического применения, в отличие от модели на основе матрицы доступа — прямоугольной таблицы, строки которой соответствуют субъектам доступа, а столбцы — объектам доступа [7].

В ячейках табл. 1 описаны все операции над объектами, которые разрешены субъекту.

Таблица 1

Матрица доступа

	O_1	O_2	…	O_j	…	O_N
S_1		w				
S_2	r					
…						
S_i				r, w		
…						
S_M						e

Здесь w обозначена запись объекта, r — чтение, e — запуск. Значения, записанные в ячейках таблицы, определяют виды безопасных доступов соответствующего субъекта к соответству-

ющему объекту. В сравнении с пятимерным пространством Хартсона данное отображение прав доступа гораздо удобнее. Однако у него есть серьезный недостаток: права доступа существуют отдельно от данных. Если пользователь получил доступ к конфиденциальной информации, он может записать ее в общедоступный файл либо заменить полезную утилиту «троянским» аналогом.

Далее рассмотрим модель take-grant, основанную на структуре графов (объектов, содержащих вершины и ребра) [8]. В качестве узлов в такой модели используются либо объекты, либо субъекты. Узлы (вершины) соединяются дугами (ребрами). Значения дуг характеризуют права, которыми обладает узел. Существуют четыре правила преобразования: take, grant, create, remove.

Правило take позволяет субъекту брать права другого субъекта. Grant позволяет субъекту предоставлять собственные права другому субъекту. Create позволяет субъекту создавать новые объекты. Remove позволяет субъекту удалять права, которыми он обладает в отношении какого-либо объекта.

Введем следующие обозначения:

— O — множество объектов;
— S — множество субъектов;
— R = {r1, r2, r3, r4, …, rn } ∪ {t, g} — множество прав доступа;
— t — возможность брать права доступа;
— g — возможность давать права доступа;
— G = (S, O, E) — конечный, помеченный, ориентированный граф без петель;
— × — объекты, элементы множества O;
— • — субъекты, элементы множества S.

На рис. 1 представлены все права данной модели. Отметим, что в общем виде данные правила выглядят следующим образом: take (r, x, y, s), grant (r, x, y, s), create (r, x, s), remove (r, x, s). При этом r ∈ R, s ∈ S, x,y ∈ O — вершины графа G.

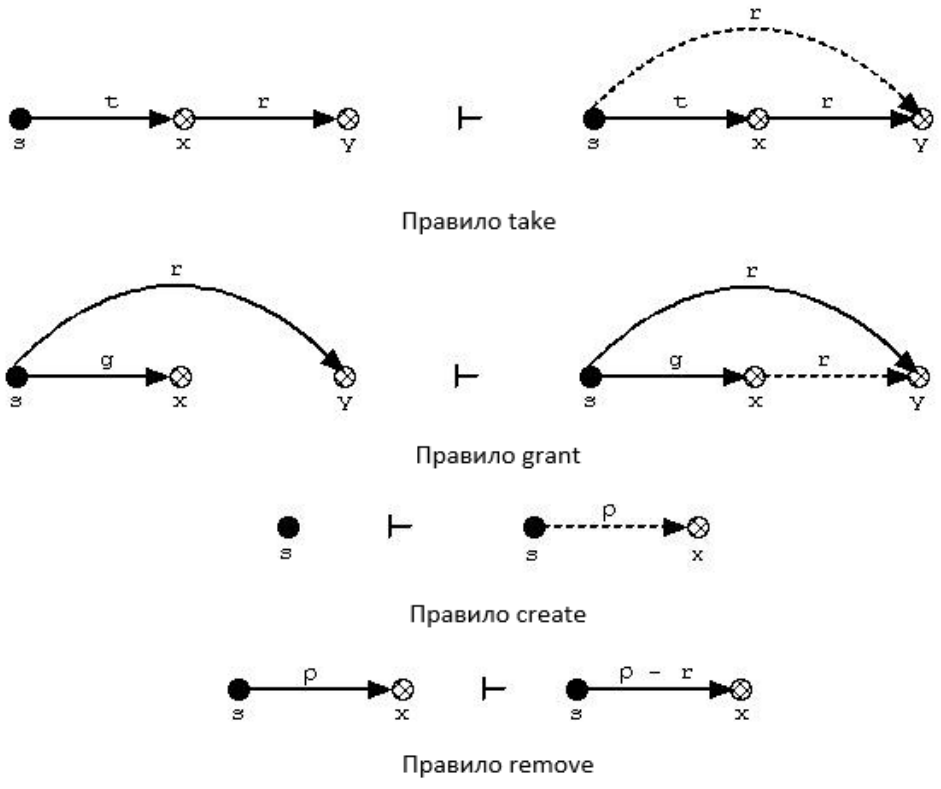

Рис. 1. Правила преобразования

При использовании модели take-grant можно однозначно определить изменения состояния системы при изменении прав субъектов над объектами.

Данная модель анализирует системы безопасности дискреционных политик безопасности. В ней описаны условия передачи или несанкционированного получения прав доступа. Чаще всего возникающие на практике взаимосвязи объектов довольно просты. Правила take и grant практически не используются, в отличие от операций на доступ к чтению и записи. В этом смысле основная идея данной модели неактуальна с точки зрения практического использования, и это ее главный недостаток.

Таким образом, основой дискреционной политики безопасности можно назвать дискреционное управление доступом, которое предполагает реализацию двух основных правил [8]:

— все субъекты и объекты, используемые в данной модели, должны быть однозначно определены или идентифицированы;

— права доступа субъекта системы к объекту определяются из некоторого заранее не описанного правила.

Достоинством дискреционной политики безопасности является простая реализация механизмов защиты, так как современные автоматизированные системы удовлетворяют правилам конкретной политики безопасности.

Недостатком можно назвать отсутствие гибкости в настройке системы. К тому же при использовании дискреционной политики возникает вопрос о том, какие правила распространения прав доступа следует использовать и как они влияют на безопасность системы в целом.

Общее описание модели. Как можно заметить, у каждой из рассмотренных моделей есть достоинства и недостатки. Ниже представлена трехмерная модель, основанная на трех параметрах: субъект, объект, время. По трем первым буквам английских слов subject, object, time она получила название SOT-массив.

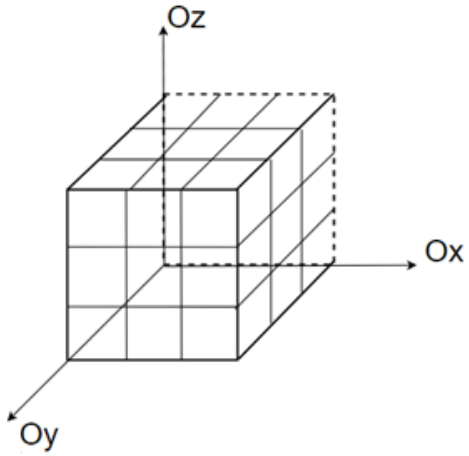

Рис. 2. SOT-массив

От рассмотренных ранее данная модель отличается дополнительным элементом — время.

Как было показано ранее, двумерная матрица представляет собой прямоугольную таблицу, строки которой соответствуют субъектам, а столбцы — объектам доступа (см. табл. 1). В ячейках такой таблицы описаны все операции над объектами, которые разрешены субъекту.

В трехмерном массиве помимо субъектов и объектов доступа используется временной параметр, который также учитывается при определении разрешенных операций над объектом. Список разрешенных операций указан в соответствующих координатах данного SOT-массива. Права доступа субъекта к объекту с течением времени могут измениться. Кроме того, используемые в модели субъекты представляют собой некоторую иерархическую структуру, описанную в соответ-

ствующей базе данных. Такая связь позволяет запрашивать доступ на проведение операции над объектом у вышестоящего субъекта.

Для более подробного описания модели рассмотрим следующие вопросы:

1) элементы SOT-массива,
2) права пользователей,
3) использование базы данных субъектов,
4) принцип иерархических отношений между субъектами,
5) возможности модели с привязкой к параметру t (время),
6) права администратора безопасности.

Элементы SOT-массива. Напомним, что SOT-массив состоит из трех элементов: subject (субъект), object (объект) и time (время).

В данном случае субъект — это лицо или процесс, действия которого регламентируются правилами разграничения доступа. Объект — единица ресурса автоматизированной информационной системы, доступ к которой регламентируется правилами разграничения доступа. Применение элемента «время» в данном алгоритме будет описано далее.

Права пользователей. В рассматриваемой модели безопасности субъекты обладают следующими правами над объектами:

а) w — запись объекта (write),
б) r — чтение объекта (read),
в) e — активация процесса (enable),
г) i — запрос (inquiry).

В трехмерной модели безопасности «матрица доступа» имеет вид параллелепипеда, ось Ox которого представлена субъектами, Oy — объектами, а Oz — временными отрезками. Однако, так же, как и в двумерной матрице доступа значения, записи в ячейках трехмерного массива определяют виды безопасных доступов соответствующего субъекта к соответствующему объекту.

Под запросом i будем понимать ситуацию, при которой субъект, не имеющий права доступа к объекту, может послать запрос на временное предоставление ему соответствующих прав.

Запрос одного субъекта к другому на выполнение операций над объектами имеет следующий вид:

$$i\left(s_k\left((o_1,x),(o_2,x),\dots,(o_n,x)\right)\right)\rightarrow s_m,$$

где $n,k,m=1,2,3\dots;\ x\in O: O=\{w,r,e\}$.

В данном примере субъект S_k посылает запрос субъекту S_m на выполнение операций x над объектами O_1, O_2, …, O_n. При этом множество O содержит все возможные операции над объектами (write, read, enable).

Далее субъект S_m отправляет ответ S_k на посланный им запрос:

$$s_m\left(f_{o_1,x},f_{o_2,x},\dots,f_{o_n,x}\right)\rightarrow s_k.$$

Здесь $n,k,m=1,2,3\dots;\ x\in 0: 0=\{w,r,e\},\ f=\{0,1\}$ — результат запроса на проведение операции, где 0 — отказ, 1 — подтверждение.

Использование базы данных субъектов. Ось Ox трехмерного массива составлена из всех субъектов, которые осуществляют работу над компьютерной системой и над ее объектами в целом. На сервере, в базе данных (БД) субъектов хранится информация о них: логины и пароли (если субъекты — реальные пользователи); id (если субъект — процесс), а также список вышестоящих и нижестоящих в иерархии субъектов. Для обеспечения безопасности в БД хранятся хеш-значения логинов и паролей или id-процессов (табл. 2).

Таблица 2

База данных

hash (s) OR hash (id)	z_1	z_2
hash ($login_1$ + $password_1$)	S_4, S_8	S_2, S_{13}
…		
hash(id_1)	S_{15}, S_{23}	S_6, S_5

В данной таблице в первом столбце содержатся хеш-значения логинов, паролей или id-процессов. Во втором и третьем столбце хранятся данные о связанных ниже- и вышестоящих по иерархии субъектах.

Во время работы сервера SOT-массив динамически формируется и корректируется, в зависимости от действий администратора безопасности.

Если по каким-либо причинам конкретный субъект теряет возможность совершать действия над объектами, из SOT-массива удаляются все упоминания об этом субъекте. Однако в БД сохраняются все записи, включая хеш-значение, вычисленное на основе конкатенации логина и пароля. Это делается с целью предотвращения возможных атак, инициируемых данным субъектом.

Принцип иерархических отношений между субъектами. Субъекты компьютерной системы связаны друг с другом иерархическими отношениями. Рассмотрим данный принцип на конкретном примере (рис. 3).

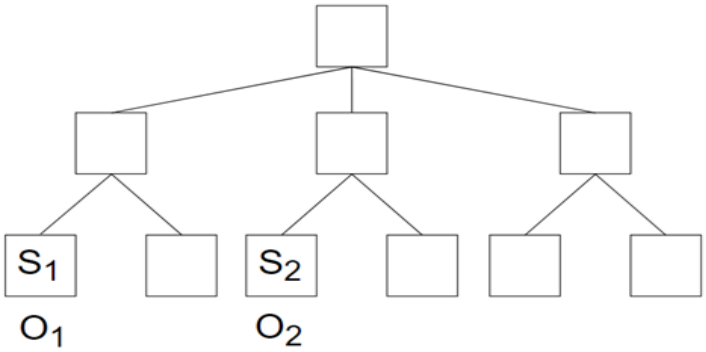

Рис. 3. Иерархия субъектов

Субъект S_1 с доступом к объекту O_1 хочет получить доступ к объекту O_2, к которому есть доступ у субъекта S_2. Как видно из рисунка, эти субъекты не связаны отношением иерархии, поэтому для получения доступа к необходимому объекту субъект S_1 должен послать запрос вышестоящему субъекту, с которым он связан иерархическими отношениями. Если субъект, получивший запрос, также не связан с интересующим субъекта S_1 объектом O_2, запрос посылается далее, пока не будет найдет субъект, иерархически связанный с объектом O_2. Вышестоящий субъект может послать или отклонить запрос.

Возможности модели с привязкой к параметру t (время). В данной модели безопасности зависимость доступа от времени может быть реализована следующими способами.

Первый: право доступа к объекту определяется фактическим временем. Субъект имеет доступ к объекту в конкретные временные промежутки. Текущее время определяется и хранится в зашифрованном виде на сервере, который берет информацию из различных взаимозаменяемых ресурсов.

Например, серверное время 00:00. При этом в SOT-массиве указано, что в период с 00:00 до 10:00 субъект S_3 имеет право на запись объекта O_3, т. е. он может выполнять операцию w в любое

время в рамках данного интервала. В другое время субъект S_3 может совершать иные действия, если они предусмотрены в SOT-массиве. Если же в данном массиве нет информации о допустимых операциях субъекта над объектом в указанное время, то у субъекта полностью отсутствует право доступа к объекту.

Второй: право доступа субъекта к объекту не привязано к серверному времени, а основано на принципе таймера. Допустим, указано, что субъект имеет доступ к объекту на определенное время t. В этом случае, как только субъект осуществит любое действие с объектом, сервер активирует таймер. По истечении определенного времени доступ может быть изменен или запрещен.

Права администратора безопасности. В права администратора безопасности SOT-модели входят создание и корректировка трехмерного массива доступа субъектов к объектам. Кроме того, он может изменять значения базы данных, в которой содержатся данные о самих субъектах и об их связях с другими элементами модели.

При изменении трехмерной модели, а именно временного параметра (в случае, если субъектом является реальный пользователь), администратор обязан учитывать такие ситуации как:

— выходные и праздничные дни;

— увольнение сотрудника или появление нового;

— изменение штатного расписания;

— повышение или понижение сотрудника, перевод его на другую должность, с иными правами доступа к объектам компьютерной системы.

Возможные угрозы и недостатки модели безопасности

1. В случае, если некоторое нелегитимное лицо узнает действующий логин и пароль реального пользователя, оно может получить права данного субъекта.
2. Для защиты от атак рекомендуется комплексное использование программных и программно-аппаратных средств.
3. Динамическое изменение SOT-массива предполагает высокие требования к вычислительным системам.
4. В случае некорректного заполнения базы данных субъектов может возникнуть зацикливание при отправке запроса к субъекту, стоящему выше в иерархии. Например, субъекты при запросе будут постоянно обращаться друг к другу.

Заключение. В рамках данной работы рассмотрены существующие модели доступа, обозначены их достоинства и недостатки. На основе этого анализа представлена (в том числе графически) новая модель безопасности компьютерных систем. Описаны база данных субъектов, их иерархические отношения и функционирование алгоритма модели безопасности.

Проведенный анализ позволил выявить возможные угрозы безопасности и недостатки разработанной модели. Она не является окончательной и может быть модифицирована.

Библиографический список

1. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Н. Девянин. — Москва : ГЛТ, 2013. — 338 с.

2. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Н. Девянин. — Москва : ГЛТ, 2012. — 320 с.

3. Девянин, П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками / П. Н. Девянин. — Москва : Горячая линия — Телеком, 2016. — 320 с.

4. Алексенко, В. С. Модели повышения эффективности и безопасности производства посредством совершенствования организации и оплаты труда / В. С. Алексенко, Ф. И. Акшенцев, О. Б. Браун. — Москва : Горная книга, 2012. — 52 с.

5. Северцев, Н. А. Системный анализ и моделирование безопасности / Н. А. Северцев. — Москва : Высшая школа, 2006. — 462 с.

6. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А. Ф. Чипига. — Москва : Гелиос АРВ, 2010. — 336 с.

7. Васильков, А. В. Безопасность и управление доступом в информационных системах / А. В. Васильков, И. А. Васильков. — Москва : Форум ; НИЦ ИНФРА-М, 2013. — 368 с.

8. Дейтел, Х. М. Операционные системы. Т. 2. Распределенные системы, сети, безопасность / Х. М. Дейтел, П. Д. Дейтел, Д. Р. Чофнес ; пер. с англ. С. М. Молявко. — Москва : БИНОМ, 2013. — 704 с.