С. В. Запечников, А. К. Плешков

МОДЕЛЬ РАЗГРАНИЧЕНИЯ И КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Введение

Современные тенденции развития информатизации в обществе приводят к укрупнению компаний посредством роста количества отдельных предприятий, увеличения численности персонала и появления новых средств автоматизации производства, обрабатывающих информацию различного уровня конфиденциальности, что влечет за собой интеграцию отдельных информационных систем (ИС) в крупные многофункциональные системы. Построение таких интегрированных ИС предполагает необходимость создания подсистемы разграничения и контроля доступа как к каждой ИС в составе интегрированной ИС, так и внутри каждой ИС в отдельности, поскольку одна из самых существенных проблем в настоящее время связана с необходимостью противодействия внутренним нарушителям — инсайдерам [1].

Попытки создания механизмов контроля доступа, пригодных для работы в таких условиях, предпринимались неоднократно, однако почти все они предназначались для контроля доступа к данным, хранимым в базах данных, сетях хранения данных или подобных им хранилищах данных. Так, два наиболее известных подхода к синтезу систем контроля доступа для распределенных хранилищ данных принадлежат H. Gobioff [2] и R. Ch. Burns [3]. В работе [2] был предложен метод контроля доступа к средствам хранения данных в распределенной среде при использовании сетевых файловых систем NFS либо AFS. Сам этот метод ориентирован на реализацию в качестве механизма защиты, встроенного в сетевую файловую систему (ФС). В работе [3] предложен метод контроля доступа, который носит условное наименование «метод цветов и оттенков». Он ориентирован скорее на контроль доступа к блокам данных, но все решения о присвоении блокам атрибутов защиты и о допуске клиентов для выполнения операций с блоками принимаются на уровне файлов. Для отображения применяемой к файлам политики контроля доступа на отдельные блоки файла используется механизм выделения смещений и длин блоков внутри файла. Дальнейшим развитием этих двух методов явилась модель контроля доступа, предложенная одним из автором настоящей статьи [4]. Однако она также была ориентирована на применение в сетях хранения данных, которые, конечно же, составляют важную часть современных интегрированных ИС, но являются далеко не единственными носителями объектов контроля доступа в современных ИС. В работе [5] эта модель получила дальнейшее развитие в направлении обеспечения стойкости механизма контроля доступа к частичному разрушению распределенной аппаратно-программной компьютерной среды, в которой он функционирует.

В настоящей работе на основе дальнейшего развития идей, высказанных в работах [2–5], была поставлена задача предложить обобщенный механизм разграничения и контроля доступа, пригодный для использования независимо от конкретного вида информационных ресурсов и их носителей.

1. Субъектно-объектные отношения в интегрированной ИС

Для анализа задач контроля доступа в интегрированных ИС целесообразно пользоваться хорошо зарекомендовавшей себя субъектно-объектной терминологией.

Обозначим через $O = \{o_1 \ldots o_q\}$ множество *объектов доступа* — компонентов ИС, развернутых на отдельных аппаратных платформах, связанных между собой в рамках одной компьютерной сети либо на уровне правил доступа к различных сегментам сети.

Основными объектами защиты типовой ИС обычно являются информационные ресурсы, функциональные подсистемы, осуществляющие процессы обработки информации, интерфейсы

взаимодействия между подсистемами, информационная инфраструктура, системы и средства защиты информации, данные мониторинга ИС, журналы событий.

На практике ценность объектов защиты, а также меры по дополнительной защите отдельных объектов должны определяться владельцами этих объектов.

Под носителем объекта данных будем понимать тот физический компонент ИС, на котором хранится либо пребывает в течение некоторого времени объект контроля доступа и который может своими внутрисистемными средствами вести учет прав доступа и контроль полномочий субъектов ИС при доступе к находящимся на них объектам: сервер, клиентская рабочая станция, сетевой маршрутизатор, средство хранения данных в составе сети хранения данных и пр.

Обозначим через $S = \{s_1 \dots s_m\}$ множество *субъектов доступа*, которыми могут являться как отдельные пользователи, так и рабочие станции, серверы, прикладные программы (ПП) и сервисы, работающие в автоматическом режиме. В зависимости от назначения, физического расположения и выполняемых функций субъекта доступ к объекту может осуществляться как через выделенный шлюз доступа, так и напрямую по локальной вычислительной сети.

Основными субъектами доступа по отношению к защищаемым объектам выступают пользователи, имеющие права доступа к ресурсам и процессам обработки информации в ИС, смежные прикладные ИС, администраторы ИС и администраторы информационной безопасности.

A — выделенный аппаратно, при этом входящий в состав ИС набор сервисов контроля доступа, который может быть реализован в виде одного или нескольких выделенных серверов (в зависимости от масштаба ИС). В число функций A входит: аутентификация субъектов из множества S при доступе к объектам O; учет и верификация прав доступа, используемых в ИС; назначение и отзыв полномочий по доступу субъектов из множества S к объектам O.

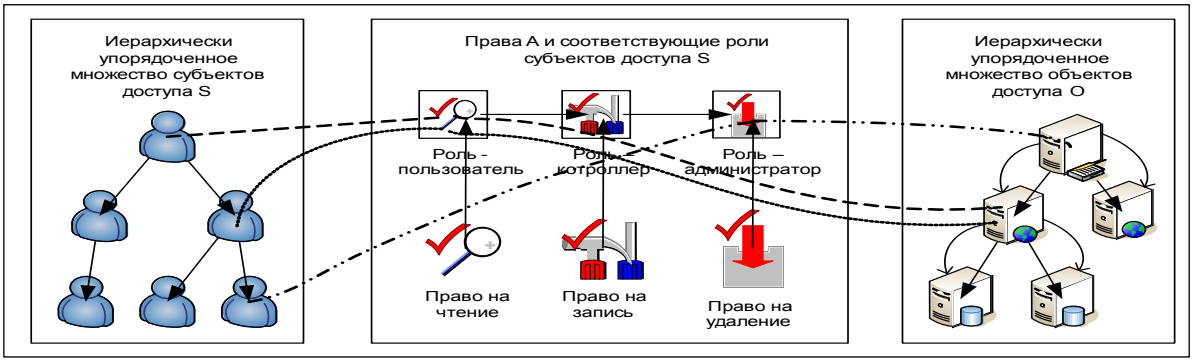


Рис. 1. Обобщенная схема контроля доступа при взаимодействии субъектов с объектами сложной интегрированной ИС

На рис. 1 показана обобщенная схема контроля доступа при взаимодействии субъектов с объектами сложной интегрированной ИС. Типичной для такой ИС является ситуация, когда объекты доступа O и субъекты доступа S упорядочены в виде более или менее сложной иерархии, что требует обеспечения возможности достаточно гибкой и динамичной настройки прав доступа. В частности, классическим примером таких систем являются интегрированные автоматизированные банковские системы, включающие в себя информационно-аналитические, учетно-операционные подсистемы и целый ряд других обеспечивающих подсистем.

2. Требования к механизму контроля доступа и условия его функционирования

Как показал анализ ранее предложенных методов контроля доступа к данным, обрабатываемым в распределенной компьютерной среде, в современных информационных системах в целом наблюдается

тенденция к перенесению механизмов принятия решений о допуске к данным на более низкий уровень (от файлов — к блокам). Однако все ранее предложенные методы так или иначе используют службы сетевой файловой системы (ФС). Данное обстоятельство можно объяснить практическим полным отсутствием до последнего времени протоколов блочного обмена данными через ЛВС. Все это ограничивает сферу применения рассмотренных методов, снижает их универсальность и, в свою очередь, определяет требования к разработке новых методов, свободных от названных недостатков.

При разработке модели контроля доступа к данным приняты следующие исходные требования:

- Для контроля доступа не должны привлекаться механизмы сетевой ФС. Все решения о контроле доступа должны осуществляться только на уровне отдельных физических блоков данных. Это условие сделало бы возможным универсальное использование механизма контроля доступа с любыми типами ПП, как использующими, так и не использующими ФС. Стандартизация протоколов блочного обмена данными через транспортную подсистему локальной или глобальной вычислительной сети, таких как iSCSI, позволит реализовать этот механизм наиболее эффективным образом.
- Необходимо минимизировать вычислительную нагрузку, возлагаемую непосредственно на носители объектов доступа O, переместив большую часть работы по принятию решений о допуске субъектов к чтению/записи блоков данных на сервис A.
- Необходимо минимизировать требования к специальному аппаратному обеспечению, размещаемому на носителях объектов доступа O, ограничив его минимально необходимым для проверки данных, связанных с наличием у субъектов полномочий на чтение/запись блока данных.
- Желательно полностью использовать возможности параллельного чтения/записи блоков данных на различных носителях объектов доступа O, потенциально реализуемые в распределенной компьютерной среде.

3. Модель механизма контроля доступа в интегрированной ИС

С учетом рассмотренных условий можно предложить следующую модель контроля доступа субъектов S к объектам доступа O.

Центральным элементом модели контроля доступа является сервис контроля доступа (СКД). Он выполняет три основные функции.

1. *Аутентификация субъектов ИС* осуществляется посредством проверки их идентификаторов: паролей, ключей, биометрической информации. При наличии в составе ИС большого числа субъектов для этих целей возможно выделить специальный сервер аутентификации либо использовать имеющиеся в составе ОС средства аутентификации, такие как Kerberos. Такие средства имеются, например, в большинстве современных версий UNIX-подобных ОС и ОС семейства Windows.

2. *Учет прав доступа субъектов к объектам* осуществляется посредством ведения таблиц (рис. 2): таблицы классов доступа и таблицы атрибутов классов. *Классом доступа к объекту контроля доступа* будем называть некоторый условный двоичный код, присваиваемый одному или группе объектов контроля доступа, отражающий некоторое единое логическое объединение объектов (например, группу файлов, директорию, к которой должен быть ограничен доступ, все файлы с грифом «секретно» и т. п.). *Подклассом доступа к объекту контроля доступа* будем называть расширение двоичного кода класса доступа, используемое в качестве счетчика и показывающее текущую «версию» класса доступа.

Таблица классов доступа:

	C_1	C_2	C_3	...	C_m
S_1	1	0	0	…	0
S_2	1	1	0	…	1
S_3	0	0	1	…	0
…	…	…	…	…	…
S_k	0	1	0	…	1

0 — класс доступа C_j закрыт для субъекта U_i;
1 — класс доступа C_j открыт для субъекта U_i.

Таблица атрибутов класса:

Класс доступа	**Подкласс**	**«Окно»**	**Атрибуты класса**					
			r	w	m	c	g	e
C_1	SC_1	T_1	1	1	0	0	1	0
C_2	SC_2	T_2	1	1	1	0	0	0
C_3	SC_3	T_3	1	0	0	1	0	0
…	…	…	…	…	…	…	…	…
C_m	SC_m	T_m	1	1	1	1	1	1

0 — атрибут не назначен; 1 — атрибут назначен.

Атрибуты объектов контроля доступа, размещенных на носителе:

Номер (идентификатор) объекта контроля доступа	**Класс доступа**	**Подкласс доступа**	**Блок данных, составляющий объект контроля доступа**
1	C_1	SC_1	b_1
2	C_2	SC_2	b_2
3	C_3	SC_3	b_3
…	…	…	…
N	C_N	SC_N	b_N

Рис. 2. Структуры данных, используемые в модели контроля доступа

В таблице классов доступа в строках указываются все субъекты, которые будут получать права доступа, в столбцах перечислены классы доступа. В ячейках таблицы содержатся биты {0,1}, указывающие для каждого S, какие классы доступа открыты для этого субъекта. Таблица, таким образом, является двоичной матрицей.

В таблице атрибутов классов для каждого класса указываются текущее значение подкласса и набор прав доступа, ассоциированный с этим классом: r — чтение блока данных; w — запись блока данных; m — модификация блока данных (чтение старого значения блока и запись в него нового значения); c — назначение блоку нового класса доступа; g — «захват» нового блока; e — освобождение занятого блока.

Определим логические операции над классами доступа: $C_3 = C_1 \cup C_2$ — над объектами, которым присвоен класс доступа C_3, разрешается осуществлять все операции, разрешенные классом C_1 либо классом C_2; $C_3 = C_1 \cap C_2$ — над объектами, которым присвоен класс доступа C_3, разрешается осуществлять только те операции, которые одновременно разрешены классом C_1 и классом C_2.

3. Назначение и отзыв полномочий доступа субъектов к объектам осуществляется посредством генерации и выдачи субъектам ИС сервисом контроля доступа специальных структур данных, которые по аналогии с принятой для Kerberos терминологией будем называть билетами. Схема выдачи билетов такова. Любой субъект, успешно прошедший аутентификацию, может направить СКД запрос на выдачу билета к необходимому ему объекту данных. Местоположение и номер объекта определяются посредством обращения к сервису размещения данных. Сервис размещения данных указывает СКД класс доступа, присвоенный найденному объекту. СКД по таблице классов доступа проверяет, открыт ли для данного субъекта запрашиваемый класс доступа, и если да, то выдает ему билет на доступ к объекту. В противном случае возвращает код ошибки.

Список классов доступа является открытым. Субъекты ИС вправе запросить любой класс доступа. Решение о разрешении либо запрещении доступа принимается СКД на основе таблицы классов доступа. Значение подкласса доступа для каждого класса неизвестно субъектам. Оно назначается СКД и известно только СКД и тем носителям объектов контроля доступа, на которых размещены соответствующие объекты. Также оно указывается в билетах, выдаваемых СКД субъектам ИС. Проверка билетов осуществляется носителями объектов контроля доступа, когда от клиента поступает запрос на операцию с контролируемыми ими объектами.

Пусть SC_i — текущее значение подкласса класса C_i, назначенное СКД, K_i — значение подкласса, содержащееся в билете. Если $|SCi - Ki| \geq T$, где T — некоторая константа, задаваемая СКД, билет считается недействительным. Если сервис периодически (например, раз в сутки) увеличивает значение подкласса на величину T^*, то по истечении периода T/T^* все билеты, которые не были обновлены за это время, становятся недействительными. В случае необходимости отозвать у какого-либо пользователя право на доступ к объектам какого-либо класса доступа величина подкласса для этого класса может быть сразу увеличена на T или более. И тогда доступ всех субъектов будет возможен только после получения новых билетов в СКД.

4. Протоколы контроля доступа

Функции СКД осуществляются во взаимодействии с субъектами и объектами контроля доступа путем реализации ряда протоколов. На рис. 3 показаны протоколы:

а) аутентификации клиента для СКД — простой протокол с использованием пароля (вместо него может использоваться протокол Kerberos);

б) запроса и выдачи билета на доступ к блоку данных между субъектом и СКД;

в) доступа к блоку данных между субъектом и носителем объекта;

г) обновления подкласса доступа к блоку данных между СКД и носителем объекта (при этом с целью унификации правил доступа СКД предъявляет носителю объекта билет с номером N_T^*, выданный самому себе).

Протоколы чтения, записи, модификации, «захвата», освобождения и изменения класса доступа между субъектом и носителем объекта аналогичны с точностью до заполнения полей передаваемых сообщений, поэтому объединены в протокол (в) доступа к блоку данных.

В протоколах использованы следующие обозначения: S — субъект ИС; A — сервис контроля доступа; O — объект контроля доступа (при выполнении протокола от имени объекта выступает его носитель); C_i — класс доступа к объекту контроля доступа; SC_i — подкласс доступа к объекту контроля доступа; n_X — случайное число, генерируемое участником протокола X; $K_{X,Y}$, $P_{X,Y}$ — общие секретные величины участников X и Y (пароль, ключ); $E_K\{m\}$ — сообщение m, зашифрованное на ключе K; $H(m)$ — хеш-код сообщения m; T — билет, выданный СКД субъекту; N_T — номер билета; b, b^* — содержимое объекта контроля доступа (произвольный блок данных); N_b — номер (идентификатор) объекта.

5. Анализ корректности протоколов

Проведем анализ корректности разработанных протоколов, т. е. покажем, что они в самом деле выполняют те функции, для которых были предназначены. Для этой цели воспользуемся формальным методом верификации протоколов безопасности, известным как BAN-логика [6].

Запишем все шаги протоколов в идеализированной форме:

Протокол (а):

(1) $S \to A : [n_S]$;

(2) $A \to S : \left[\langle n_A, n_S \rangle_{P_{A,S}} \right]$;

(3) $A,S : K_{A,S} = H(n_A, P_{A,S})$.

Протокол (б):

(4) $S \to A : \left[\langle C_i, n_A \rangle_{P_{A,S}} \right]$;

(5) $A \to S : \left\{ \langle C_i, SC_i, N_T \rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}; S \overset{R_{S,O}}{\Leftrightarrow} O \right\}_{K_{A,S}}$.

Протокол (в):

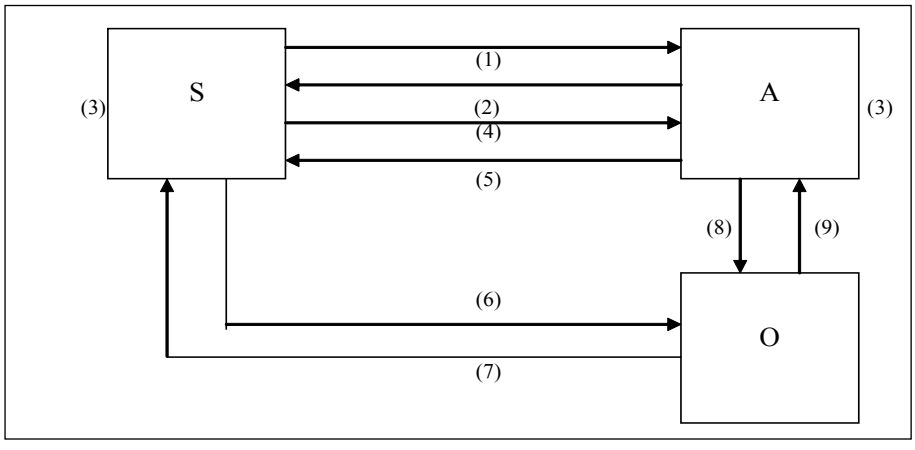
(6) $S \to O : \left\langle \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O} \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}$;

(7) $O \to S : \left\langle b^*, n_S^*, N_T \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}$.

Протокол (г):

(8) $A \to O : \left\langle C_i, SC_i, SC_i^*, N_T^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}$;

(9) $O \to A : \left\langle C_i, SC_i^*, N_T^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}$.



Протокол (а):

(1) S → A : [S, n_S];

(2) A → S : [n_S, n_A, $H(n_S, n_A, P_{A,S})$];

(3) S, A : $K_{A,S}=H(n_A, P_{A,S})$.

Протокол (б):

(4) S → A : [C_i, O, n_A, $H(C_i, O, n_A, P_{A,S})$];

(5) A → S : $\left[E_{K_{A,S}}\left\{R_{S,O} = H\left(S, N_T, P_{A,S}\right), T = \left[C_i, SC_i, O, N_T, H\left(C_i, SC_i, O, N_T, P_{A,S}\right)\right]\right\}\right]$.

Протокол (в):

(6) S → O : $\left[S, T, N_b, b, n_S^*, H\left(S, O, N_b, b, n_S^*, N_T, R_{S,O}\right)\right]$;

(7) O → S : $\left[O, S, b^*, n_S^*, N_T, H\left(O, S, b^*, n_S^*, N_T R_{S,O}\right)\right]$.

Протокол (г):

(8) A → O : $\left[A, C_i, SC_i, SC_i^*, N_T^*, H\left(A, O, C_i, SC_i, SC_i^*, N_T^*, P_{A,O}\right)\right]$;

(9) O → A : $\left[O, A, H\left(O, A, C_i, SC_i^*, N_T^*, P_{A,O}\right)\right]$.

Рис. 3. Протоколы, используемые в модели контроля доступа

Запишем начальные предположения для всех протоколов в формальном выражении:

$O \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O$; $A \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O$; $S \mid\equiv A \mid\Rightarrow S \overset{R_{S,O}}{\Leftrightarrow} O$; $A \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S$; $S \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S$; $A \mid\equiv \#(n_A)$;

$S \mid\equiv \#(n_S)$; $S \mid\equiv \#(n_S^*)$; $A \mid\equiv \#(N_T)$; $A \mid\equiv \#(N_T^*)$; $O \mid\equiv \#(N_T)$; $S \mid\equiv O \mid\Rightarrow (b^*, N_T)$;

$S \mid\equiv A \mid\Rightarrow (n_A)$.

Проведем теперь пошаговый анализ протоколов, пользуясь правилами формальной BAN-логики согласно [6]:

Протокол (а):

(1) $A \mid\triangleright n_S$

(2) $\dfrac{S \mid\triangleright \langle n_A, n_S\rangle_{P_{A,S}}; S \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S}{S \mid\equiv A \mid\sim (n_S, n_A)}$, $\dfrac{S \mid\equiv A \mid\sim (n_A, n_S); S \mid\equiv \#(n_S)}{S \mid\equiv A \mid\equiv n_A}$, $\dfrac{S \mid\equiv A \mid\equiv n_A; S \mid\equiv A \mid\Rightarrow n_A}{S \mid\equiv n_A}$.

(3) Этот шаг выполняется A и S локально — передачи сообщений нет: $\dfrac{S \mid\equiv n_A; S \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S}{S \mid\equiv \langle n_A\rangle_{P_{A,S}}}$;

$\dfrac{S \mid\equiv \langle n_A\rangle_{P_{A,S}}}{S \mid\equiv A \overset{K_{A,S}}{\Leftrightarrow} S}$ (это справедливо, так как $K_{A,S} = H(n_A, P_{A,S})$); $\dfrac{A \mid\equiv n_A; A \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S}{A \mid\equiv \langle n_A\rangle_{P_{A,S}}}$;

$\dfrac{A \mid\equiv \langle n_A\rangle_{P_{A,S}}}{A \mid\equiv A \overset{K_{A,S}}{\Leftrightarrow} S}$ (это справедливо, так как $K_{A,S} = H(n_A, P_{A,S})$).

Протокол (б):

(4) $S \to A : \left[\langle C_i, n_A\rangle_{P_{A,S}}\right]$: $\dfrac{A \mid\triangleright \langle C_i, n_A\rangle_{P_{A,S}}; A \mid\equiv A \overset{P_{A,S}}{\Leftrightarrow} S}{A \mid\equiv S \mid\sim (C_i, n_A)}$; $\dfrac{A \mid\equiv S \mid\sim (C_i, n_A), A \mid\equiv \#(n_A)}{A \mid\equiv S \mid\equiv C_i}$.

(5) $A \to S: \left\{ \left\langle C_i, SC_i, N_T \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}, S \overset{R_{S,O}}{\Leftrightarrow} O \right\}_{K_{A,S}}$:

Обозначим: $\left\langle C_i, SC_i, N_T \right\rangle_{A \overset{S_{A,O}}{\Leftrightarrow} O} = Y$, $S \overset{R_{S,O}}{\Leftrightarrow} O = Z$. Тогда: $\dfrac{S \mid\rhd \{Y,Z\}_{K_{A,S}}; S \mid\equiv A \overset{K_{A,S}}{\Leftrightarrow} S}{S \mid\equiv A \mid\sim (Y,Z)}$;

$\dfrac{S \mid\equiv A \mid\sim (Y,Z); S \mid\equiv \#(K_{A,S}) S \mid\sim \{Y,Z\}_{K_{A,S}}}{S \mid\equiv A \mid\equiv (Y,Z)}$ и $\dfrac{S \mid\equiv A \mid\equiv (Y,Z)}{S \mid\equiv A \mid\equiv Z}$; $\dfrac{S \mid\equiv A \mid\equiv Z; S \mid\equiv A \mid\Rightarrow Z}{S \mid\equiv Z}$,

т. е. $S \mid\equiv S \overset{R_{S,O}}{\Leftrightarrow} O$.

Протокол (в):

(6) $S \to O: \left\langle \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O} \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}$:

$$\frac{O \mid\rhd \left\langle \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O} \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}}{O \mid\rhd \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}; O \mid\rhd S \overset{R_{S,O}}{\Leftrightarrow} O};$$

$$\frac{O \mid\rhd \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O}; O \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O}{O \mid\equiv A \mid\sim \left(C_i, SC_i, N_T, N_b, b, n_S^*\right)};$$

$$\frac{O \mid\equiv A \mid\sim \left(C_i, SC_i, N_T, N_b, b, n_S^*\right) O \mid\equiv \#(N_T)}{O \mid\equiv A \mid\equiv \left(C_i, SC_i, N_T, N_b, b, n_S^*\right)}. \quad O \mid\rhd S \overset{R_{S,O}}{\Leftrightarrow} O, \text{ где } R_{S,O} = H\left(S, N_T, P_{A,S}\right), \text{ т. е.}$$

$$O \mid\equiv A \mid\equiv (C_i, SC_i)$$

справедливо, что $\left(S \overset{R_{S,O}}{\Leftrightarrow} O \right) = \left\langle S, N_T \right\rangle_{P_{A,O}}$. Тогда: $\dfrac{O \mid\rhd \left\langle S, N_T \right\rangle_{P_{A,O}}; O \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O}{O \mid\equiv A \mid\sim \left\langle S, N_T \right\rangle_{P_{A,O}}}$;

$$\frac{O \mid\equiv A \mid\sim \left\langle S, N_T \right\rangle_{P_{A,O}}; O \mid\equiv \#(N_T)}{O \mid\equiv A \mid\equiv \left[\left(\left\langle S, N_T \right\rangle_{P_{A,O}} \right) = \left(S \overset{R_{S,O}}{\Leftrightarrow} O \right) \right]}; \quad \frac{O \mid\equiv A \mid\equiv S \overset{R_{S,O}}{\Leftrightarrow} O; O \mid\equiv A \mid\Rightarrow S \overset{R_{S,O}}{\Leftrightarrow} O}{O \mid\equiv S \overset{R_{S,O}}{\Leftrightarrow} O};$$

$$\frac{O \mid\rhd \left\langle \left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O} \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}; O \mid\equiv S \overset{R_{S,O}}{\Leftrightarrow} O}{\dfrac{O \mid\equiv S \mid\sim \left(\left\langle C_i, SC_i, N_T, N_b, b, n_S^* \right\rangle_{A \overset{P_{A,O}}{\Leftrightarrow} O} \right)}{\dfrac{O \mid\equiv S \mid\sim \left(C_i, SC_i, N_T, N_b, b, n_S^*\right)}{O \mid\equiv S \mid\sim (C_i, SC_i, N_T, N_b, b)}}};$$

$$\frac{O \mid\equiv S \mid\sim (C_i, SC_i, N_T, N_b, b); O \mid\equiv \#(N_T)}{O \mid\equiv S \mid\equiv (C_i, SC_i, N_T, N_b, b)};$$

$$O \mid\equiv S \mid\equiv (C_i, SC_i, N_b, b)$$

$$(7)\ O \to S : \left\langle b^*, n_S^*, N_T \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O} : \frac{S \mid\rhd \left\langle b^*, n_S^*, N_T \right\rangle_{S \overset{R_{S,O}}{\Leftrightarrow} O}; S \mid\equiv S \overset{R_{S,O}}{\Leftrightarrow} O}{S \mid\equiv O \mid\sim \left(b^*, n_S^*, N_T\right)};$$

$$\frac{S \mid\equiv O \mid\sim \left(b^*, n_S^*, N_T\right); S \mid\equiv \#\left(n_S^*\right)}{\dfrac{S \mid\equiv O \mid\equiv \left(b^*, n_S^*, N_T\right)}{S \mid\equiv O \mid\sim \left(\left(b^*, N_T\right) = m_O\right)}}; \quad \frac{S \mid\equiv O \mid\equiv (m_O); S \mid\equiv O \Rightarrow m_O}{S \mid\equiv m_O}.$$

Протокол (г):

$$(8)\ A \to O : \left\langle C_i, SC_i, SC_i^*, N_T^* \right\rangle_{P_{A,O}} : \frac{O \mid\rhd \left\langle C_i, SC_i, SC_i^*, N_T^* \right\rangle_{P_{A,O}}; O \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O}{O \mid\equiv A \mid\sim \left(C_i, SC_i, SC_i^*, N_T^*\right)};$$

$$\frac{O \mid\equiv A \mid\sim \left(C_i, SC_i, SC_i^*, N_T^*\right); O \mid\equiv \#\left(N_T^*\right)}{\dfrac{O \mid\equiv A \mid\equiv \left(C_i, SC_i, SC_i^*, N_T^*\right)}{O \mid\equiv A \mid\equiv \left(C_i, SC_i, SC_i^*\right)}}.$$

$$(9)\ O \to A : \left\langle C_i, SC_i^*, N_T^* \right\rangle_{P_{A,O}} : \frac{A \mid\rhd \left\langle C_i, SC_i^*, N_T^* \right\rangle_{P_{A,O}}; A \mid\equiv A \overset{P_{A,O}}{\Leftrightarrow} O}{A \mid\equiv O \mid\sim \left(C_i, SC_i^*, N_T^*\right)};$$

$$\frac{A \mid\equiv O \mid\sim \left(C_i, SC_i^*, N_T^*\right); A \mid\equiv \#\left(N_T^*\right)}{\dfrac{A \mid\equiv O \mid\equiv \left(C_i, SC_i^*, N_T^*\right)}{A \mid\equiv O \mid\equiv \left(C_i, SC_i^*\right)}}.$$

Итак, в результате анализа установлена справедливость следующих утверждений: $O \mid\equiv A \mid \equiv (C_i, SC_i)$ — из шага (6); $O \mid\equiv S \mid \equiv (C_i, SC_i, N_b, b)$ — из шага (6); $S \mid \equiv (b, N_T)$ — из шага (7); $O \mid\equiv A \mid \equiv (C_i, SC_i, SC_i^*)$ — из шага (8); $A \mid\equiv O \mid \equiv (C_i, SC_i^*)$ — из шага (9). Первое и второе из них означают, что носитель объекта достоверно знает, что субъект уполномочен СКД на выполнение операций с объектом, представленным блоком данных b под номером N_b, класс C_i и подкласс SC_i доступа для которого установлены СКД в соответствии с политикой безопасности ИС. Третье утверждение означает, что субъект S достоверно знает, что данные b^* получены им в ответ на запрос доступа к объекту контроля доступа по билету с номером N_T и исходят от носителя этого объекта. Четвертое и пятое утверждения означают, что носитель объекта и СКД достоверно знают соответственно происхождение запроса и результат выполнения запроса на изменение подкласса доступа с SC_i на SC_i^* для класса доступа C_i. Таким образом, корректность всех протоколов доказана.

Заключение

В статье предложена модель контроля доступа в интегрированной информационной системе, выраженная в терминах субъектно-объектных взаимодействий. Модель в основе своей является дискреционной и дополняется введением классов и подклассов доступа субъектов к объектам контроля доступа, обеспечивая таким образом возможности гибкого, динамичного и массового изменения прав доступа субъектов к объектам при возникновении необходимости в корректировке политики безопасности. Функции механизма контроля доступа реализуются через протоколы выдачи и проверки прав доступа субъектов ИС к блокам данных, размещенным на средствах хранения данных. Показано, что предложенные протоколы корректно реализуют политику безопасности ИС при выполнении установленных для них требований и предположений.

Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397

в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 г.

СПИСОК ЛИТЕРАТУРЫ:

1. *Плешков А. К.* Факторы инсайдерской деятельности // Безопасность информационных технологий. 2008. № 4. С. 155–158.
2. *Gobioff H.* Security for a high performance commodity storage subsystem. URL: http://www.pdl.cs.cmu.edu/PDL-FTP/NASD/hbg_thesis_abs.html.
3. *Burns R. Ch.* Data management in a distributed file system for storage area networks. URL: http://www.almaden.ibm.com/cs/storagesystems/stortank/papers.html.
4. *Запечников С. В.* Исследование и разработка алгоритмов обеспечения безопасности доступа к информации в сетях хранения данных. Дисс. ... канд. тех. наук. М.: МИФИ, 2003. – 195 с.
5. *Запечников С. В.* Модель системы контроля доступа к устройствам хранения данных, стойкой к частичному разрушению распределенной среды [электронный ресурс] // Труды IV Международной научной конференции «Параллельные вычисления и задачи управления» PACO'2008. Москва, 27–29 октября 2008 г. М.: Институт проблем управления им. В. А. Трапезникова РАН, 2008. С. 273–297. 1 CD-ROM.
6. *Burrows B., Abadi M., Needham R. M.* A logic of authentication // ACM Transactions on computer Systems. 1990. Vol. 8. № 1. P. 18–36.