УДК 004.056.52 004.056.53

Объединение моделей логического разграничения доступа для сложноорганизованных распределенных информационных систем

А. А. Иткес

Московский государственный университет им. М. В. Ломоносова, 119992, Москва, Россия
Научно–исследовательский институт механики Московского государственного университета им. М. В. Ломоносова, 119992, Москва, Россия

Рассматриваются вопросы построения моделей логического разграничения доступа к информационным активам, вычислительным и коммуникационным ресурсам сложноорганизованной, распределенной информационной системы на основе аналогичных моделей ее отдельных компонент. Анализируются свойства таких моделей и описаны методы их объединения, основанные на понятии отношения доверия. Получены критерии, гарантирующие возможность объединения моделей логического разграничения доступа. Предложена новая модель, аналогичная многоуровневой модели, реализующая более гибкие механизмы интеграции по сравнению с механизмами традиционной многоуровневой модели логического разграничения доступа.

Ключевые слова: информационная безопасность, разграничение доступа, распределенные информационные системы, интеграция моделей логического разграничения доступа.

This article deals with the problem of integrating different access control models. The author has analyzed some properties of various access control models and developed some criterias of possibility of integrating access control models. The author also has developed a new access control model that inherits strengths of the multilevel security model, but such models are easier to integrate.

Key words: Information security, access control, distributed information systems, integrating access control models.

Введение. В последние годы сфера применения сложных, территориально распределенных информационных систем неуклонно расширяется. Одновременно возрастает величина потенциального ущерба, который может быть причинен в результате некорректной работы подобных систем. Сбои в их работе могут возникать случайно, а также в результате намеренных действий как лиц, внешних по отношению к системе, так и администраторов, ответственных за те или иные аспекты сопровождения системы. Потенциальными нарушителями могут быть и подростки, ищущие приключений, и террористические и военно-политические организации, имеющие цель на длительное время вывести из строя жизненно важные для страны информационные системы, причинив государству как можно больший ущерб. Такой ущерб может иметь не только экономические, но и социальные, политические последствия. Отказы или сбои в работе современных информационных систем могут привести к экологическим или техногенным катастрофам, человеческим жертвам. Учитывая тенденции развития общества и темпы развития телекоммуникаций, необходимо отметить, что в будущем риски подобных событий увеличатся.

При анализе методов защиты сложных информационных систем часто упоминается "правило слабого звена", которое заключается в том, что система защищена настолько надежно, насколько можно гарантировать защиту самой слабой ее компоненты. Во многом указанное утверждение справедливо. Однако не следует также пренебрегать защитой системы в целом, в случае если ее часть оказывается под контролем злоумышленников. Подобная постановка задачи обусловлена несколькими факторами. Во-первых, как бы хорошо ни были защищены компоненты распределенной информационной системы от внешней угрозы, злоумышленник может получить контроль над одной из них в каком-то смысле "случайно". Во-вторых, тем, что часто организации сталкиваются с нападениями не только внешних, но и внутренних нарушителей. Следует также учитывать "комбинированные" угрозы, исходящие как извне, так и изнутри организации. Если противник − террористическая организация или крупная

преступная группировка, то вполне вероятно, что перед нападением злоумышленники попытаются подкупить кого-либо из служащих организации, имеющей прямое отношение к процессу эксплуатации системы. Третья причина, по которой необходимо разрабатывать меры безопасности, предназначенные для функционирования, в том числе и в условиях, когда некоторые компоненты системы контролируются злоумышленником, состоит в том, что многие крупные распределенные информационные системы создаются путем объединения более мелких ее компонент. До объединения эти подсистемы могут иметь различные уровни защищенности. Некоторые из них, по крайней мере на начальном этапе их совместной работы, могут быть защищены недостаточно надежно.

С учетом изложенного представляет практический интерес разработка способов построения политик безопасности сложноорганизованных, территориально распределенных информационных систем. С одной стороны, такие подходы и способы должны минимизировать взаимозависимость компонент системы и уменьшать возможный ущерб от несанкционированного доступа к некоторым из них. С другой стороны, они призваны сделать компоненты достаточно сильно связанными, для того чтобы система в целом могла успешно выполнять основные функции. Необходимо уделить внимание защите гетерогенных систем, отдельные компоненты которых имеют различные, не согласованные друг с другом политики информационной безопасности. Однако в силу объективных причин пользователи этих систем вынуждены участвовать в интенсивном обмене информацией посредством незащищенных каналов сетей связи общего пользования.

Прежде чем перейти к изложению основных результатов, заметим, что модель логического разграничения доступа не существует безотносительно к объекту доступа (данные, вычислительные и коммуникационные ресурсы). Поэтому используемое в дальнейшем выражение "модель логического разграничения доступа" без привязки к объекту следует рассматривать как сокращенную форму, описывающую модель логического разграничения доступа субъектов к объектам системы. Это находит строгое описание в формальных определениях.

В настоящей работе описываются несколько используемых на практике моделей логического разграничения доступа и возможности их использования в гетерогенных распределенных информационных системах, а также разработанный автором метод объединения политик безопасности, основанных на этих моделях. Указанный метод основан на понятии отношения доверия. Получены критерии применимости данного метода для различных видов моделей логического разграничения доступа.

1. Отношения доверия. Понятие отношения доверия активно используется при построении моделей логического разграничения доступа (ЛРД) для распределенных информационных систем.

Прежде чем определить понятие отношения доверия, необходимо ввести некоторые базовые обозначения. Пусть A − произвольная информационная система, возможно, распределенная. Тогда обозначим через $O(A)$ множество объектов системы A, а через $S(A)$ − множество субъектов системы A. При этом будем считать, что $S(A) \subset O(A)$.

Определение 1.1. Отношением доверия между информационными системами A и B называется подмножество $T_{A,B} \subset S(A) \times S(B)$.

Смысл указанного отношения в том, что если пара $(a,b) \in T_{A,B}$, то субъект a может получить доступ к объектам системы B посредством субъекта b. В этом случае будем считать, что субъект b доверяет субъекту a.

Рассмотрим несколько примеров отношений доверия. Наиболее типичный пример − это доверие веб-сервера к веб-клиенту (браузеру). В этом случае браузер может читать файлы удаленного компьютера посредством веб-сервера. Аналогичным образом можно рассматривать доверие между клиентом и сервером для различных сетевых протоколов уровня приложения − FTP, SSH, Telnet и др.

Иногда целесообразно рассматривать так называемые локальные отношения доверия. Отношение доверия называется локальным, если в приведенном определении A и B − одна и та же информационная система. Иными словами, локальное отношение доверия − это подмножество $T_{A,A} \subset (A) \times S(A)$.

Рассмотрим пример. В операционной системе (ОС) Linux многие происходящие под ее контролем события фиксируются в системном журнале, к механизмам защиты которого предъявляются следующие требования: каждый пользователь может добавлять информацию в журнал, только администратор имеет право модифицировать или удалять ее. Однако реализация этих требований затруднена вследствие того, что в ОС Linux нельзя разрешить какому-либо субъекту доступ к некоторому объекту на добавление информации и при этом запретить доступ на

запись. Для решения данной задачи используется приложение syslogd. С одной стороны, это приложение имеет доступ на запись к файлам системного журнала. С другой стороны, оно спроектировано таким образом, чтобы иметь возможность только добавлять информацию в журнал. Если пользовательскому приложению необходимо добавить информацию к системному журналу, оно производит эту операцию посредством syslogd. Таким образом, syslogd доверяет некоторым пользовательским приложениям.

2. Основные модели логического разграничения доступа. Рассмотрим три достаточно широко используемые на практике модели ЛРД. Ролевая модель применяется в информационных системах различного назначения в течение многих лет. Многоуровневая модель ЛРД также активно используется для обеспечения информационной безопасности, однако является более узкоспециализированной. Эта модель обладает дополнительной устойчивостью к некоторым видам атак. Модель Type-Enforcement, как и ролевая модель ЛРД, является средством обеспечения информационной безопасности для широкого класса объектов.

2.1. *Ролевая модель логического разграничения доступа.* Ролевые модели ЛРД используются в различных информационных системах с 1970 г. Однако на протяжении многих лет отсутствовал единый стандарт применения подобных моделей, поэтому в настоящее время существует большое количество различных определений ролевой модели ЛРД. Некоторые из них приведены в [1, 2]. В настоящей работе используется достаточно простое определение, включающее понятие субъекта, принципиально важное для работы с отношениями доверия.

Определение 2.1. Пусть в информационной системе A заданы*:* P − множество привилегий; R − множество ролей; U − множество пользователей, S − множество субъектов. При этом пусть каждой роли r соответствует множество привилегий $P(r)$*,* каждому пользователю u − множество ролей $R(u)$, а каждому субъекту s − пользователь-владелец $u(s)$ и подмножество его ролей $R(s) \subset R(u(s))$. В этом случае будем считать, что в системе A задана ролевая модель ЛРД.

В указанной модели каждому субъекту s соответствует набор привилегий $P(s) = \bigcup_{r \in R(s)} P(r)$. Использование ролей позволяет значительно упростить представление того, какими привилегиями обладает тот или иной пользователь. В реальных системах роль, как правило, соответствует той или иной должности в организации, защита ресурсов которой обеспечивается. Как следствие использование понятия роли в модели ЛРД позволяет легко модифицировать систему при переходе кого-либо из сотрудников подконтрольной организации на другую должность.

2.2. *Многоуровневая модель логического разграничения доступа.* Многоуровневая модель ЛРД (multi-level security, MLS) отличается несколько ограниченной по сравнению с рассмотренными в подп. 2.1, а также в подп. 2.3 моделями областью применения. Наряду с этим данная модель обладает повышенной устойчивостью к некоторым атакам типа атаки "троянских коней". Это возможно вследствие того, что модель ориентирована на ограничение действий не только потенциального злоумышленника, но и потенциального объекта деструктивного воздействия.

Определение 2.2. Пусть в информационной системе A зафиксирована некоторая решетка L*,* называемая решеткой ценностей. Пусть каждому объекту o системы A поставлен в соответствие некоторый уровень $l(o) \in L$. При этом к каждому объекту системы возможны доступы на чтение и запись. Пусть доступ субъекта s к объекту o на чтение разрешается в том и только том случае, когда $l(s) \geq l(o)$*,* а на запись – в том и только том случае, когда $l(s) \leq l(o)$. Тогда будем считать, что в системе A задана многоуровневая модель ЛРД.

Приведенная модель ЛРД также может быть сформулирована в терминах понятия информационных потоков. В ряде случаев представление данной модели с помощью информационных потоков может быть весьма полезным.

Определение 2.3. Пусть s − произвольный субъект, а o − произвольный объект системы. Будем считать, что от субъекта s к объекту o разрешен непосредственный информационный поток, если s имеет доступ к o на запись. Будем также считать, что от объекта o к субъекту s разрешен непосредственный информационный поток, если s имеет доступ к o на чтение.

Определение 2.4. Пусть o_s и o_f − объекты информационной системы. Будем считать, что от объекта o_s к объекту o_f разрешен информационный поток, если существуют объекты $o_s=o_0,o_1, \ldots,o_n=o_f$, такие что для каждого $j=1, \ldots, n$ разрешен непосредственный информационный поток от o_{j-1} к o_j.

В терминах данных выше определений определение многоуровневой модели ЛРД можно сформулировать следующим образом:

Определение 2.5. Пусть в информационной системе A зафиксирована некоторая решетка L и каждому объекту o системы A поставлен в соответствие некоторый уровень $l(o) \in L$. При этом к каждому объекту системы возможны доступы на чтение и запись. Пусть информационный поток от объекта o_1 к объекту o_2 возможен в том и только том случае, когда $l(o_1) \le l(o_2)$. Тогда будем считать, что в системе A задана многоуровневая модель ЛРД.

Среди моделей, используемых в настоящее время на практике, представленная модель ЛРД является одной из самых узконаправленных. Ее можно рассматривать как частный случай использования двух других моделей ЛРД, описанных в подп. 2.1 и 2.3.

Любая многоуровневая модель ЛРД может быть выражена в терминах моделей ЛРД RBAC и Type-Enforcement.

2.3. *Модель Type-Enforcement.* Модель ЛРД Type-Enforcement (принудительной типизации) представляет собой одну из модификаций лэмпсоновой матрицы доступа [3]. Матрица доступа Лэмпсона − это матрица, столбцы которой пронумерованы субъектами системы, а строки − объектами. В каждой ячейке этой матрицы находится множество прав доступа указанного субъекта к указанному объекту. Данный подход неприменим, поскольку множество объектов крайне велико. Вследствие этого первые версии модели Type-Enforcement предполагали нумерацию ячеек таблицы не парами субъект – объект, а парами домен – тип, где каждый домен соответствует множеству субъектов, а каждый тип − множеству объектов. При этом множества доменов и типов имеют приемлемую мощность и редко изменяются во времени. Современные версии рассматриваемой модели предполагают учет "сущности" объекта, а также включение множества доменов в множество типов. В настоящее время данная модель ЛРД активно используется на практике, являясь, например, основой механизмов ЛРД программного комплекса SELinux [4].

Определение 2.6. Пусть в информационной системе A заданы множества T и C, при этом T называется множеством типов, а C − множеством классов. Пусть каждому объекту o в системе приписаны тип $t(o)$ и класс $c(o)$ и заданы функции $f: T\times T\times C\times A \to \{allow, deny\}$ и $g: T\times T\times C \to T$, где A − множество всех возможных видов доступа в системе. В этом случае будем считать, что в системе задана модель ЛРД Type-Enforcement. При этом собственно решение о предоставлении субъекту s доступа a к объекту o определяется значением $f(t(s),t(o),c(o),a)$. Вторая функция (g) используется при создании в системе нового объекта. Она определяет тип создаваемого объекта по типу создающего субъекта, типу объекта, на основе которого создается новый объект (например, процесс на основе исполнимого файла), и класса создаваемого объекта. В приведенной модели доменом называется тип, который может быть присвоен какому-либо субъекту.

На практике метка класса обычно идентифицирует "сущность" объекта, в то время как тип объекта используется для обозначения владельца содержащихся в нем данных и их важности. Некоторые виды доступа неприменимы для объектов некоторых классов. Например, вид доступа "послать сигнал" имеет смысл только в том случае, если объект доступа является процессом.

В настоящее время модификация описанной выше модели используется в программе Security-Enhanced Linux (SELinux), встроенной в ядро ОС Linux ветки 2.6.

2.4. *Сравнительный анализ выразительности моделей логического разграничения доступа.* Рассмотрим вопросы сведения друг к другу описанных выше моделей ЛРД. Докажем следующее утверждение, характеризующее выразительные свойства ролевой модели ЛРД и модели Type-Enforcement:

Теорема 2.1. *Любая модель ЛРД Type-Enforcement может быть выражена в терминах ролевой модели ЛРД.*

Для доказательства данного утверждения необходимо определить следующее дополнительное понятие.

Определение 2.7. При использовании модели ЛРД Type-Enforcement привилегией называется тройка $p = (t,c,a)$, где t − тип, c − класс, a − вид доступа. Будем считать, что тип t' обладает привилегией $p = (t,c,a)$, если $f(t',t,c,a) = allow$.

Доказательство. Пусть в системе A применяется политика безопасности, основанная на модели ЛРД Type-Enforcement, P − множество привилегий системы A в смысле приведенного определения. Данное множество будет также использоваться в качестве множества привилегий для ролевой модели ЛРД, которую необходимо построить для системы A.

Пусть множество ролей системы совпадает с множеством ее типов. Пусть каждый субъект системы имеет единственную роль, совпадающую с его типом. Пусть каждой роли r соответствует множество привилегий $P(r) = \{(t,c,a): f(r,t,c,a) = allow\}$. Таким образом, для системы A построена ролевая модель ЛРД.

Как отмечалось выше, многоуровневая модель ЛРД является наиболее частной из рассматриваемых в данной работе. Докажем, что многоуровневая модель может быть выражена в терминах любой из двух других.

Теорема 2.2. *Любая многоуровневая модель ЛРД может быть выражена в терминах модели ЛРД Type-Enforcement и в терминах ролевой модели ЛРД.*

Доказательство. Докажем первое из утверждений теоремы. Пусть в системе A задана политика безопасности, основанная на многоуровневой модели ЛРД (для краткости − многоуровневая политика безопасности).

Зададим в системе единственный класс и два вида доступа r и w, означающие доступ на чтение и запись. Назовем типом каждого объекта его уровень. Определим функцию разрешения доступа: $f(t',t,c,a) = allow$, если $a = r$ и $t' \geq t$, или $a = w$ и $t' \leq t$.

Таким образом, построена модель ЛРД Type-Enforcement, эквивалентная исходной многоуровневой модели ЛРД.

Второе утверждение теоремы очевидным образом следует из первого.

Легко привести примеры ролевой модели ЛРД и модели ЛРД Type-Enforcement, не выражающихся в терминах многоуровневой модели ЛРД. Таким образом, многоуровневая модель ЛРД является наиболее частной из рассматриваемых в данной работе. Вместе с тем заметим, что в настоящее время открытым остается вопрос об эквивалентности ролевой модели ЛРД и модели ЛРД Type-Enforcement.

3. Объединение моделей логического разграничения доступа с помощью отношений доверия. Рассмотрим возможные способы построения модели ЛРД, которую можно использовать для реализации единой политики информационной безопасности распределенной информационной системы при заданных политиках безопасности ее подсистем, основанных на различных моделях ЛРД.

3.1. *Объединение ролевых моделей логического разграничения доступа.* Приведем полученный автором критерий, гарантирующий возможность объединения ролевых моделей ЛРД с помощью отношений доверия. Для формулировки указанного утверждения необходимо ввести следующее вспомогательное понятие.

Определение 3.1. Подмножество привилегий P называется корректным, если существуют роли $r_1, ..., r_n$, такие что $P = P(r_1) \cup ... \cup P(r_n)$.

Теорема 3.1. *Пусть информационные системы A и B имеют политики безопасности, основанные на ролевой модели ЛРД* (*для краткости − ролевые политики безопасности*)*. Пусть система C составлена из объектов систем A и B и также имеет ролевую политику безопасности. Пусть множество привилегий системы C имеет вид* $P(C) = P(A) \cup P(B)$*, и ограничение модели ЛРД системы C на каждую из подсистем совпадает с локальной моделью ЛРД этой подсистемы. В этом случае объединение моделей ЛРД систем A и B в модель ЛРД системы C может быть реализовано с помощью отношений доверия тогда и только тогда, когда для любой роли* r_C *системы C набор ее привилегий* $P(r)$ *имеет вид* $P(r) = P_A(r) \cup P_B(r)$*, где множества привилегий* $P_A(r) = P(r) \cap P(A)$ *и* $P_B(r) = P(r) \cap P(B)$ *корректны в смысле локальной модели ЛРД систем A и B.*

Доказательство. Необходимость. Пусть $T_{A,B}$ и $T_{B,A}$ − отношения доверия между системами A и B. Пусть s_A − произвольный субъект системы A, имеющий единственную роль $r_C(s_A)$. Пусть $P_C(s_A)$ − множество привилегий этого субъекта (а значит, и указанной роли) в системе C. Пусть $P_A(s_A) = P_C(s_A) \cap P(A)$, $P_B(s_A) = P_C(s_A) \cap P(B)$ − ограничения множества привилегий субъекта s_A на каждую из подсистем. По условию теоремы множество привилегий $P_A(s_A)$ корректно, так как является множеством привилегий субъекта s_A в системе A. Пусть $s_{B,1},...,s_{B,n}$ − субъекты системы B, доверяющие s_A. Пусть $r_{B,1},...,r_{B,N}$ − все роли всех субъектов $s_{B,.i}$, занумерованные в произвольном порядке. Тогда множество $P_B(s_A)$ имеет вид $P_B(s_A) = \bigcup_j P_B(r_{B,.j})$, а следовательно, является корректным набором привилегий системы B.

Достаточность. Возьмем в системе A произвольный субъект s_A. Пусть $r_1, ..., r_n$ − роли в системе B, такие что $P_B(s_A) = \bigcup_j P_B(r_j)$, где $P_B(s_A) = P_C(s_A) \cap P(B)$ − множество привилегий системы B, которыми обладает субъект s_A. По условию теоремы такие роли существуют. Добавим в систему B субъект s_B, имеющий роли $r_1,..., r_n$ и никакие дру-

гие, и пусть s_B доверяет s_A. Таким образом строится отношение доверия $T_{A,B}$. Аналогичным образом строится отношение доверия $T_{B,A}$.

3.2. *Объединение многоуровневых моделей логического разграничения доступа.* С помощью отношений доверия многоуровневые модели ЛРД могут быть объединены лишь в частных случаях, при которых локальные политики информационной безопасности объединяемых информационных систем изначально являются согласованными. Это можно сформулировать в виде следующей теоремы.

Теорема 3.2. *Пусть информационные системы A и B имеют политики безопасности, основанные на многоуровневой модели ЛРД* (*для краткости − многоуровневые политики безопасности*). *Пусть в обеих системах на каждом уровне есть хотя бы один субъект. Пусть система C состоит из объектов систем A и B и также имеет многоуровневую политику безопасности, причем ограничение модели ЛРД объединенной системы на каждую из подсистем совпадает с локальной моделью ЛРД этой подсистемы. Пусть при этом модель ЛРД объединенной системы такова, что ни в одной из подсистем не могут возникнуть информационные потоки "снизу вверх" с использованием объектов другой подсистемы.* (*Информационным потоком "снизу вверх" называется информационный поток от некоторого объекта o_1 к объекту o_2, в случае если не выполнено условие $l(o_1) \le l(o_2)$.)*

В указанных условиях модели ЛРД систем A и B могут быть объединены с помощью отношений доверия в том и только том случае, когда решетки ценностей систем A и B изоморфны между собой. При этом решетка ценностей объединенной системы также изоморфна решеткам ценностей ее подсистем.

Доказательство. Необходимость указанного условия полностью доказана в [5], в настоящей работе приведены лишь несколько положений доказательства. Сначала необходимо доказать, что решетки систем A и B обязаны быть вложены в решетку системы C. Для этого, в свою очередь, требуется вспомогательное утверждение о том, что два субъекта системы A имеют один и тот же уровень в системе A тогда и только тогда, когда они имеют один и тот же уровень в объединенной системе. В силу симметрии условия теоремы относительно подсистем A и B аналогичное утверждение будет верно для субъектов системы B.

Докажем достаточность. Пусть системы A и B имеют многоуровневые политики безопасности с одной и той же решеткой L. Пусть каждый субъект системы B доверяет тем и только тем субъектам системы A, которые имеют одинаковый с ним уровень секретности. Аналогично этому пусть каждый субъект системы A доверяет тем и только тем субъектам системы B, которые имеют одинаковый с ним уровень секретности. Таким образом, объединенная система C также получает многоуровневую политику ЛРД с решеткой L, при этом каждому из ее объектов присваивается тот уровень, который этот объект имел в "своей" подсистеме.

Таким образом, объединение многоуровневых моделей ЛРД с помощью отношений доверия возможно лишь в определенных частных случаях.

3.3. *Объединение моделей Type-Enforcement.* Для моделей ЛРД Type-Enforcement существует критерий возможности объединения, аналогичный соответствующему критерию возможности объединения ролевых моделей ЛРД. Для формулировки данного критерия необходимо использовать понятие привилегии в модели ЛРД Type-Enforcement, имеющие здесь тот же смысл, что и в подп. 2.4, где приведено его определение. Необходимо также определить вспомогательный объект, называемый корректным множеством привилегий.

Определение 3.2. Пусть в информационной системе A задана модель ЛРД Type-Enforcement. Множество привилегий P называется корректным, если существуют типы $t_1,...,t_n$, такие что все привилегии каждого из типов t_j входят в множество P, и каждая привилегия из P принадлежит хотя бы одному из типов t_j.

Данное определение означает, что набор привилегий является корректным, если он является набором привилегий некоторого набора субъектов.

Теорема 3.3. *Пусть информационные системы A и B имеют политики безопасности, основанные на модели ЛРД Type-Enforcement* (*далее − политики безопасности Type-Enforcement*). *Пусть система C состоит из объектов систем A и B и также имеет политику безопасности Type-Enforcement. При этом все три системы имеют одинаковые множества классов и доступов. Пусть при этом ограничение модели ЛРД объединенной системы на каждую из подсистем совпадает с локальной моделью ЛРД этой подсистемы. Подобное объединение моделей ЛРД Type-Enforcement может быть реализовано с помощью отношений доверия тогда и только тогда, когда набор прав доступа каждого субъекта к объектам каждой из подсистем описывается корректным подмножеством привилегий этой подсистемы.*

Доказательство. Необходимость. Пусть $T_{A,B}$ и $T_{B,A}$ − отношения доверия между системами A и B. Пусть a − произвольный субъект системы A. Набор прав доступа субъекта a к объектам системы A соответствует множеству привилегий типа этого субъекта и, следовательно, является корректным. Остается доказать утверждение для доступа субъекта a к объектам системы B. Пусть $b_1, ..., b_n$ − субъекты системы B, доверяющие a, а $t_1, ...,t_n$ − их типы. Тогда множество доступов субъекта a к объектам системы B соответствует объединенному набору привилегий этих типов.

Достаточность. Возьмем в системе A произвольный субъект a. Пусть $t_1, ..., t_n$ − типы в системе B, такие что множество доступов субъекта a к объектам системы B представляется объединением наборов привилегий указанных типов. По условию теоремы такие типы существуют. В этом случае субъекту a должны доверять субъекты системы B, имеющие типы $t_1,... t_n$ и никакие другие. Заметим, что все типы, обладающие какими-либо привилегиями, являются доменами, поэтому для каждого из типов t_j в системе B существует по крайней мере один субъект, имеющий этот тип. Так же строится отношение доверия $T_{A,B}$. Аналогично строится отношение доверия $T_{B,A}$.

Таким образом, получен критерий возможности объединения политик безопасности, основанных на модели ЛРД Type-Enforcement, аналогичный критерию возможности объединения для ролевых моделей ЛРД.

4. Обобщенная многоуровневая модель логического разграничения доступа. Рассмотрим обобщенную многоуровневую модель ЛРД, являющуюся альтернативой многоуровневой модели. По сравнению с традиционными многоуровневыми моделями ЛРД данные модели имеют более гибкие механизмы интеграции в распределенных информационных системах.

Определение 4.1. Пусть в информационной системе A зафиксированы некоторая решетка L и множество разделов D. Пусть каждому объекту o системы A соответствует некоторый уровень $l(o) \in L$ и подмножество разделов $D(o) \subset D$. Пусть доступ субъекта s к объекту o на чтение разрешается в том и только том случае, если $l(s) \geq l(o)$ и $D(o) \subset D(s)$, а на запись − в том и только том случае, если $l(s) \leq l(o)$ и $D(o) \subset D(s)$. При указанных условиях будем считать, что в системе A задана обобщенная многоуровневая модель ЛРД.

Описанная выше модель ЛРД является обобщением традиционной многоуровневой модели ЛРД с некоторыми дополнительными ограничениями. Именно такая модель ЛРД лежит в основе политики безопасности распределенной информационной системы, компоненты которой имеют политики безопасности, базирующиеся на многоуровневой модели ЛРД. Приведенное утверждение, доказанное автором данной работы, имеет следующую строгую математическую формулировку.

Теорема 4.1. *Пусть информационные системы A и B имеют политики безопасности, основанные на обобщенных многоуровневых моделях ЛРД* (*далее − обобщенные многоуровневые политики безопасности*). *Пусть множества $T_{A,B}$ и $T_{B,A}$ представляют собой пару отношений доверия между системами A и B. Пусть с учетом приведенных отношений доверия в системе C, состоящей из объектов систем A и B, не могут появиться информационные потоки между объектами, нарушающие локальные политики безопасности систем A и B. Кроме того, пусть в каждой из подсистем может существовать информационный поток между любыми двумя объектами, лежащими на одном уровне. Тогда права доступа субъектов к объектам в системе C могут быть описаны обобщенной многоуровневой моделью ЛРД.*

Для доказательства данного утверждения потребуется ряд лемм.

Лемма 4.1.1. *В условиях теоремы если обе пары субъектов* (a_1,b) *и* (a_2,b) *принадлежат множеству $T_{A,B}$ или $T_{B,A}$, то субъекты a_1 и a_2 лежат в системе A на одном уровне.*

Доказательство. Если субъекты a_1 и a_2 лежат на разных уровнях, то передача информации либо от a_1 к a_2, либо от a_2 к a_1 невозможна. Предположим для определенности, что запрещены информационные потоки от a_1 к a_2. В случае если (a_1,b) и (a_2,b) принадлежат $T_{A,B}$, субъект a_1 может получить доступ на запись к некоторому объекту o системы B посредством субъекта b, а субъект a_2 может получить к тому же объекту o доступ на чтение. Таким образом, возможен информационный поток от a_1 к a_2, что приводит к противоречию.

В случае если (a_1,b) и (a_2,b) принадлежат $T_{B,A}$, субъект b системы B может получить доступ на чтение к объектам системы A посредством субъекта a_1, т. е. возможен информационный поток от a_1 к b. Одновременно субъект b может получить доступ на запись к объектам системы A посредством субъекта a_2, т. е. возможен информационный

поток от субъекта b к субъекту a_2, а значит, и от субъекта a_1 к субъекту a_2. Таким образом, этот случай также приводит к противоречию.

Лемма 4.1.2. *В условиях теоремы если обе пары субъектов* (a_1,b_1) *и* (a_2,b_2) *принадлежат множеству* $T_{A,B}$ *или* $T_{B,A}$*, то субъекты* a_1 *и* a_2 *лежат в системе A на одном уровне тогда и только тогда, когда субъекты* b_1 *и* b_2 *лежат в системе B на одном уровне.*

Доказательство. Предположим, что субъекты a_1 и a_2 лежат в системе A на одном уровне. Тогда по условию теоремы в системе A может существовать информационный поток как от субъекта a_1 к субъекту a_2, так и от субъекта a_2 к субъекту a_1. Если субъекты b_1 и b_2 лежат в системе B на разных уровнях, то передача информации от b_1 к b_2 либо от b_2 к b_1 запрещена. Предположим для определенности, что запрещены информационные потоки от b_1 к b_2.

Пусть пары (a_1,b_1) и (a_2,b_2) принадлежат отношению доверия $T_{A,B}$, т. е. субъект b_1 доверяет a_1, а b_2 доверяет a_2. В этом случае субъект a_2 может передавать информацию субъекту b_2, а субъект a_1 − получать информацию от b_1. Таким образом, от субъекта b_1 к субъекту b_2 возможен информационный поток посредством субъектов a_1 и a_2.

В случае если пары (a_1,b_1) и (a_2,b_2) принадлежат отношению доверия $T_{B,A}$, т. е. субъект a_1 доверяет b_1, а a_2 доверяет b_2, субъект b_1 может передавать информацию субъекту a_1, а субъект b_2 − получать информацию от субъекта a_2. Таким образом, информационный поток от b_1 к b_2 также возможен.

Таким образом, субъекты b_1 и b_2 лежат в системе B на одном уровне.

Доказательство. Пусть L_A и L_B − решетки ценностей систем A и B. Построим по ним решетку L_C системы C. Пусть L'_A − подмножество уровней решетки L_A, содержащих субъекты, которые доверяют субъектам системы B либо которым доверяют субъекты системы B. Аналогичным образом строится подмножество $L'_B \subset L_B$. Тогда частично упорядоченные множества L'_A и L'_B изоморфны.

В силу леммы 4.1.2 для каждого уровня $l_A \in L'_A$ существует единственный уровень $l_B \in L'_B$, кроме того, соответствие между ними биективно. Данный уровень l_B можно определить как уровень, содержащий все субъекты, доверяющие субъектам уровня l_A, и все субъекты, которым доверяют субъекты уровня l_A. Из леммы 4.1.2 следует, что все такие субъекты лежат на одном уровне в системе B.

Далее, решетка L_B строится как объединение решеток L_A и L_B с отождествлением подмножеств L_A и L'_B.

Множество разделов системы C строится как дизъюнктивное объединение множеств разделов систем A и B. Каждому пассивному объекту системы C присваиваются те же разделы, к которым он относился в своей подсистеме, и не присваиваются разделы другой подсистемы. Для субъекта a системы A множество разделов будет иметь вид $D_C(a)=D_A(a) \cup \bigcup_{b:(a,b)\in T(A,B)} D_B(b)$. Аналогично устанавливается множество разделов для субъектов системы B.

Теорема верна для случая, когда системы A и B имеют многоуровневые политики безопасности, так как политики указанного вида можно представить в виде обобщенных многоуровневых политик безопасности, каждое множество разделов которых состоит из одного элемента.

Определение 4.2. Привилегией в обобщенной многоуровневой модели ЛРД называется тройка $p = (l,d,a)$, где $l \in L$ − уровень секретности, $d \in D$ − один из разделов системы, а $a \in \{r,w\}$ – вид доступа. Будем считать, что субъект s обладает привилегией $p = (l,d,a)$, если выполнены два условия:

1) $d \in D(s)$;

2) если $a = r$, то $l \le l(s)$, если $a=w$, то $l \ge l(s)$.

Определение 4.3. Набор привилегий P называется корректным, если

– он имеет центральный уровень, т. е. такой уровень l_0, что для любой привилегии $p \in P$ вида (l,d,r) выполняется неравенство $l \le l_0$, а для любой привилегии $p = (l,d,w) \in P$ выполняется неравенство $l \ge l_0$;

– вместе с любой привилегией $p = (l,d,a)$ набор P также содержит все привилегии вида (l,d,w) для всех $l \ge l_0$ и (l,d,r) для всех $l \le l_0$.

Легко заметить, что в таком случае набор привилегий каждого субъекта является корректным. Кроме того, объединенный набор привилегий нескольких субъектов, относящихся к одному уровню, также является корректным.

Теорема 4.2. *Все корректные множества привилегий имеют вид* $P(l_0,D_0) = P_r(l_0,D_0) \cup P_w(l_0,D_0)$*, где* $P_r(l_0,D_0) = \{p=(l,d,r): l \le l_0,\ d \in D_0\}$*, а* $P_w(l_0,D_0) = \{p=(l,d,w): l \ge l_0, d \in D_0\}$*. Все множества привилегий указанного вида являются корректными.*

Доказательство. Пусть множество привилегий P корректно, l_0 − его центральный уровень, а D_0 − множество всех разделов, фигурирующих по крайней мере в одной привилегии из P. Тогда $P \subset P(l_0,D_0)$, так как любая привилегия $p = (l,d,r) \in P$ входит в $P_r(l_0,D_0)$, а любая привилегия $p = (l,d,w) \in P$ входит в P_w (l_0,D_0). Остается доказать, что $P(l_0,D_0) \subset P$. Пусть $p = (l,d,r) \in P_r(l_0,D_0)$. Очевидно, что $l \le l_0$ и $d \in D_0$, а значит, существует привилегия $p = (l',d,a) \in P$. Тогда в силу корректности P содержит все привилегии вида $p'' = (l'',d,r)$ для $l'' \le l_0$ включая привилегию p. Поэтому $P_r(l_0,D_0) \subset P$. Аналогично доказывается, что $P_w(l_0,D_0) \subset P$.

Теперь докажем обратное утверждение. Очевидно, что множество привилегий $P = P(l_0,D_0)$ имеет центральный уровень l_0. Одновременно для произвольной привилегии $p = (l,d,a) \in P$ выполняется условие $d \in D_0$. Это означает, что P содержит все привилегии вида $p = (l,d,r)$, где $l \le l_0$, и все привилегии вида $p = (l,d,w)$, где $l \ge l_0$. Таким образом, второе условие корректности множества $P = P(l_0,D_0)$ также выполнено.

Теорема 4.3. *Пусть информационные системы A и B имеют обобщенные многоуровневые политики безопасности. Пусть система C, состоящая из объектов систем A и B, также имеет обобщенную многоуровневую политику безопасности, причем ограничение модели ЛРД системы C на каждую из подсистем совпадает с локальной моделью ЛРД этой подсистемы. Кроме того, пусть в каждой из подсистем может существовать информационный поток между любыми двумя объектами, лежащими на одном уровне. Также пусть ни в одной из подсистем не могут возникать информационные потоки "снизу вверх" с использованием объектов другой подсистемы. При указанных условиях объединение моделей ЛРД систем A и B может быть реализовано с помощью отношений доверия между системами A и B в том и только том случае, когда права доступа каждого субъекта системы C к объектам каждой из подсистем могут быть реализованы корректным набором привилегий этой подсистемы.*

Доказательство. Необходимость. Пусть $T_{A,B}$ и $T_{B,A}$ − отношения доверия между системами A и B. В этом случае выполнены условия теоремы 4.1 и можно использовать утверждение леммы 4.1.1. Это означает, что если субъекты b_1 и b_2 доверяют одному и тому же субъекту a, то они лежат на одном уровне.

Пусть a − произвольный субъект системы A. В обозначениях теоремы 4.2 множество его привилегий в системе A имеет вид $P(l(a),D(a))$. Согласно теореме 4.2 указанное множество привилегий является корректным.

Множество привилегий субъекта a в системе B выражается формулой $P_B(a) = \bigcup_{b:\,(a,b)\in T(A,B)} P_B(l(b),D(b))$, т. е. является объединением множеств привилегий в системе B всех субъектов системы B, доверяющих a. Однако в силу леммы 4.1.1 все такие субъекты системы B лежат на одном уровне, а значит, все множества $P_B(l(b),D(b))$ имеют один и тот же центральный уровень l_0, поэтому $\bigcup_{b:\,(a,b)\in T(A,B)} P_B(l(b),D(b)) = P_B(l_0, \bigcup_{b(a,b)\in T(A,B)} D(b))$, т. е. множество привилегий субъекта a в системе B имеет вид $P(l_0,D_0)$ для некоторых l_0 и D_0, следовательно, является корректным.

Достаточность. Пусть a − произвольный субъект системы A. По условию теоремы множество его привилегий в системе B имеет вид $P_B(a)=P(l_0,D_0)$, где l_0 − некоторый уровень системы B, D_0 − некоторое множество разделов системы B. Пусть b − субъект системы B, лежащий на уровне l_0 и имеющий множество разделов D_0. Пусть субъект b доверяет субъекту a и более никакие субъекты системы B не доверяют. Таким образом субъект a получает в системе B необходимое множество привилегий. Указанным способом строится отношение доверия $T_{A,B}$. Аналогично строится отношение доверия $T_{B,A}$.

Приведенный критерий возможности объединения обобщенных многоуровневых моделей ЛРД аналогичен соответствующим критериям для ролевой модели и модели Type-Enforcement, за исключением одного нюанса. Легко убедиться, что при использовании моделей разграничения доступа TE и RBAC объединение корректных наборов привилегий всегда является корректным набором. В случае использования обобщенной многоуровневой модели ЛРД аналогичный факт неверен. Это означает, что два субъекта, лежащие на разных уровнях, не могут доверять одному и тому же субъекту другой системы. Указанное ограничение продиктовано невозможностью передачи информации "снизу вверх" в одной системе посредством объектов другой системы. При объединении ролевых моделей ЛРД и моделей ЛРД Type-Enforcement подобное ограничение отсутствует, что делает критерии возможности их объединения более мягкими.

Заключение. В связи с возрастанием роли распределенных информационных систем во многих сферах деятельности человека нельзя недооценивать важность задачи защиты подобных систем включая их защиту от зло-

намеренных действий пользователей. Поскольку гарантировать абсолютную защиту каждой из компонент сложноорганизованной распределенной системы невозможно, становится актуальной задача защиты отдельных сегментов системы в тех случаях, когда некоторые из компонент полностью или частично контролируются злоумышленником. Для решения данной задачи политики безопасности для распределенной информационной системы необходимо строить таким образом, чтобы, с одной стороны, минимизировать взаимозависимость настроек ЛРД и компонент указанной системы, с другой − сделать эту взаимозависимость достаточной для выполнения системой своих функций.

В данной работе рассмотрен один из подходов к формализации понятия доверия между компонентами распределенных информационных систем, позволяющий моделировать объединение политик безопасности, основанных на различных распространенных моделях логического разграничения доступа.

В настоящее время автором ведется работа над реализацией программного комплекса, служащего для контроля логического разграничения доступа в сложных распределенных информационных системах на основе отношений доверия. Данная программная система допускает возможность взаимодействия с различными программными средствами контроля ЛРД и поддерживает использование различных моделей ЛРД. Этот программный комплекс, получивший название Nettrust, в перспективе позволит эффективно контролировать выполнение заданной модели ЛРД для распределенных информационных систем любой сложности.

Список литературы

1. RAVI S. SANDHU, EDWARD J. COYNE, HAL L. FEINSTEIN, CHARLES E. YOUMAN. Role-based access control models // IEEE Computer. 1996. V. 29, N 2. P. 38–47.

2. DAVID F. FERRAIOLO, RAVI S. SANDHU, SERBAN GAVRILA, ET AL. Proposed nist standard for role-based access control models // Proc. of. the 15th National Computer Security Conf. Baltimore (USA), 1992. P. 554–563.

3. LAMPSON B. Protection // Proc. of the 5th Princeton conf. on information sciences and systems, Princeton, 1971. Repr. ACM Operating Systems Rev. 1974. V. 8, N 1. P. 18–24.

4. EARL BOEBERT. Some thoughts on the occasion of the NSA Linux release // Linux J., 2001.

5. ИТКЕС А. А., САВКИН В. Б. К развитию механизмов разграничения доступа в распределенных информационных системах // Материалы конф. "Проблемы безопасности и противодействия терроризму", Москва, 2–3 ноября 2005 г. М.: МЦНМО, 2006. С. 349−367.

Иткес Александр Александрович – мл. науч. сотр.
Ин-та механики Моск. гос. ун-та им. М. В. Ломоносова.
e-mail: itkes@imec.msu.ru

Дата поступления – 22.06.2009 г.