УДК 519.6

РАЗГРАНИЧЕНИЕ ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ УЧЕТА И КОНТРОЛЯ ЯДЕРНЫХ МАТЕРИАЛОВ

А. А. Анищенко, К. В. Иванов
(РФЯЦ-ВНИИЭФ)

Рассматриваются проблемы, связанные с решением задачи разграничения доступа в автоматизированных системах учета и контроля ядерных материалов. Описано частное решение этой задачи на примере системы ACCORD-2005.

Введение

В автоматизированных системах учета и контроля (СУиК) ядерных материалов, используемых на предприятиях Росатома, как правило, обрабатывается информация, содержащая государственную тайну. Поэтому для этих систем исключительно важными являются вопросы, связанные с защитой информации от несанкционированного доступа.

Согласно требованиям по защите информации, предъявляемым к СУиК [1], выделено три класса систем в соответствии с условиями их функционирования. Критериями при выборе класса защищенности СУиК для конкретного случая являются:

- наличие в СУиК информации различной степени секретности;
- уровень полномочий субъектов доступа (пользователей) на доступ к секретной информации;
- порядок и условия размещения и функционирования, физическая защищенность средств вычислительной техники СУиК.

Если обрабатывается информация строго одной степени секретности и все субъекты доступа имеют равные права доступа (полномочия) ко всей информации СУиК, то могут быть применены системы 3-го класса. В случае наличия информации нескольких степеней секретности и разных прав доступа к ней у субъектов допустимо применение СУиК не ниже 2-го класса (т. е. 2-го и 1-го). Как следствие, ключевыми вопросами при проектировании комплекса средств защиты информации для систем 2-го и 1-го классов СУиК являются вопросы разграничения доступа.

Способы реализации разграничения доступа в СУиК

В состав любой СУиК, как правило, входят следующие компоненты:

- операционная система (ОС);
- система управления базами данных (СУБД);
- прикладное программное обеспечение (ППО).

В общем случае разграничение доступа может обеспечиваться как одним из этих компонентов, так и несколькими одновременно.

Одними из важнейших требований, предъявляемых к подсистемам разграничения доступа СУиК 2-го и 1-го классов, являются требования наличия контроля доступа по мандатному принципу [2] и управления потоками информации. Рассмотрим различные варианты архитектурных решений, позволяющие выполнить вышеуказанные требования и обеспечить разграничение доступа в СУиК 2-го класса защищенности. Необходимо отметить, что если речь идет о разграничении доступа средствами ОС или СУБД, имеет смысл рассматривать только те продукты, которые имеют сертификат соответствия 3-му классу защищенности средств вычислительной техники и выше (СВТ 3-го класса и выше) [3] или СУиК 2-го класса [1].

Разграничение доступа средствами ОС. В настоящее время на рынке представлено

несколько ОС на базе ОС Linux, реализующих мандатный принцип контроля доступа и имеющих сертификат соответствия 2-му и 3-му классам СВТ. Кроме того, существуют сертифицированные программы, повышающие защитные свойства ОС до нужного уровня.

При проектировании системы разграничения доступа СУиК на основе ОС ключевой задачей является *увязывание* объектов защиты ОС с объектами защиты непосредственно СУиК. Это обусловлено тем, что в ОС объектами защиты являются файлы, папки, ключи реестра и т. д, в то время как объекты защиты СУиК, как правило, ассоциируются с объектами базы данных (БД) — таблицами, строками таблиц, полями, группами полей. Решением данной проблемы может быть, например, распределение информации по БД с различными уровнями секретности, доступ к которым дополнительно регулируется ОС [4]. Однако здесь возникают трудности, связанные с логической целостностью информации, репликацией данных, реализацией *бизнес-логики* [4] (компонент, реализующий бизнес-логику, также должен быть сертифицирован).

Ввиду вышеперечисленных проблем создание функционально полной, применимой на практике СУиК 2-го класса защищенности, разграничивающей доступ только средствами ОС, видится практически невозможным. Кроме того, для долгосрочного успешного применения такого сложного программного продукта, как ОС, требуется его постоянная поддержка со стороны производителя, которая подразумевает как выпуск новых усовершенствованных версий, так и написание драйверов, офисных приложений и т. д. Во всех этих случаях у производителя возникают трудности, связанные как с вопросами финансирования разработок, так и с техническими проблемами в плане продления срока действия сертификата.

На данный момент авторам не удалось найти сертифицированную по требуемому классу защищенности ОС, применимую в промышленных масштабах.

Разграничение доступа средствами СУБД. Что касается СУБД, сертифицированных на сегодняшний день по требуемому классу защищенности (СВТ выше 3-го класса или СУиК 2-го класса), авторам статьи известно только о СУБД Линтер (СВТ 2-го класса). Разумеется, при проектировании СУиК гораздо проще и логичнее возложить функции по разграничению доступа на СУБД, чем на ОС, так как объекты учета хранятся в БД. Однако в этом случае возникают проблемы, связанные с управлением потоками информации вне СУБД.

Например, рассмотрим сеть, внутри которой расположен сервер с сертифицированной СУБД, а пользователи обращаются к этому серверу с рабочих станций. Именно такая архитектурная модель чаще всего используется в СУиК на практике. В этом случае можно быть уверенным только в том, что доступ разграничивается лишь внутри СУБД, и нет никакой гарантии, что потоки информации разного уровня конфиденциальности не перемешиваются на рабочих станциях. Выходом из такой ситуации может служить выделение подсетей равного доступа и разделение их сертифицированными межсетевыми экранами.

Все это создает существенные трудности в организационном и экономическом плане. Кроме того, поскольку современные СУБД по своей сложности сопоставимы с ОС, для них проблемы сопровождения сродни тем, что описаны выше для ОС.

Защищенные интегрированные системы (ЗИС). Сертифицированные ЗИС, включающие в себя как ОС, так и СУБД, по мнению авторов, часто малоэффективны, а в отдельных случаях вообще неприменимы.

Как правило, увязывание объектов защиты ОС с объектами защиты СУБД основано на том, что таблицы СУБД хранятся в файловой системе в виде файлов ОС и к ним применяется механизм разграничения доступа ОС. При таком подходе необходимо иметь в БД множество таблиц (определяемое количеством групп пользователей) для хранения объектов учета одного типа. Для СУиК масштаба предприятия, в которых наиболее востребованы системы 2-го класса, это практически невыполнимо.

Кроме того, как отмечено в [4], современные СУиК чаще всего имеют трехуровневую архитектуру, т. е., кроме СУБД и интерфейса пользователя, существует уровень бизнес-логики. Весь обмен информацией между пользователем и СУБД выполняется через сервис бизнес-логики, и нет никакой гарантии, что потоки информации разной конфиденциальности не перемешиваются на этом уровне. Таким образом, для трехуровневых СУиК, кроме сертификации ОС и СУБД в составе ЗИС, требуется

также сертификация, как минимум, прикладного сервиса бизнес-логики.

Разграничение доступа с помощью ППО. Рассмотрим теперь вариант, при котором разграничение доступа реализуется средствами ППО. В этом случае разработчик СУиК может получить относительную независимость от ОС и СУБД как в плане защиты информации, так и в плане логической архитектуры системы. Но при этом требуется сертификация ППО по 2-му или 1-му классу СУиК.

СУиК ядерных материалов ACCORD-2005

СУиК ядерных материалов ACCORD-2005 разрабатывается на базе хорошо зарекомендовавшей себя системы ACCORD-2000 [5] в соответствии с требованиями, предъявляемыми к СУиК 2-го класса [1]. В качестве ОС может использоваться Windows NT/2000/XP, в качестве СУБД — MS SQL 2000.

ACCORD-2005 располагает реализованными в ППО независимыми от ОС и СУБД подсистемами:

- разграничения доступа;
- идентификации и аутентификации пользователей на основе протокола Kerberos V.5;
- регистрации и учета;
- контроля целостности.

Такой подход, дополненный рядом организационно-технических мероприятий, позволяет изолировать ППО от ОС и СУБД с точки зрения необходимых для СУиК 2-го класса функций безопасности и, как следствие, избавляет от обязательного наличия сертификатов у ОС и СУБД.

Правила разграничения доступа в системе ACCORD-2005

Рассмотрим более подробно подсистему разграничения доступа ACCORD-2005. Данная подсистема реализует модели *дискреционной* и *мандатной* защиты данных (см. ниже). При этом действуют *два глобальных правила*:

1. Доступ к объектам, имеющим дискреционную и мандатную защиту, должен быть санкционирован согласно обеим моделям защиты. Если отвергается доступ хотя бы по одной из них (дискреционной или мандатной), то запрос на доступ будет отвергнут (принцип эквивалентности).
2. При отсутствии у субъекта доступа к какому-либо объекту по одной из моделей защиты (если в отношении субъекта и объекта действуют обе модели) он не сможет ни управлять доступом к этому объекту, ни получить доступ к нему. В этом отношении среди пользователей выделяется только администратор безопасности, который может изменять метки доступа пользователей.

Модель дискреционной защиты. Каждому защищаемому объекту ставится в соответствие маска доступа ACL (Access Control List), которая содержит список всех допущенных к данному объекту групп пользователей. Каждый пользователь включен в одну или несколько групп. Доступ пользователя к объекту разрешен, если хотя бы одна группа, к которой принадлежит пользователь, содержится в списке допущенных к данному объекту. Доступ пользователя к объекту запрещен, если ни одна из групп, к которой принадлежит пользователь, не содержится в списке допущенных к данному объекту.

Модель мандатной защиты. С каждым защищаемым объектом и субъектом связана структура (мандат) вида $M = \{L, [C_0, \ldots, C_k]\}$, где L — фиксированный уровень из диапазона от 0 до N (соответственно минимальный и максимальный уровни секретности), а $[C_0, \ldots, C_k]$ — битовое множество категорий. Объект (субъект) относится к категории C_i, если $C_i = 1$ и не относится, если $C_i = 0$.

В основе принятой концепции лежат следующие принципы:

- доступ к объекту по чтению разрешен только тогда, когда уровень объекта не превышает уровня субъекта и множество категорий объекта целиком содержится в множестве категорий субъекта;
- доступ к объекту по записи разрешен только тогда, когда уровень субъекта не превышает уровня объекта и множество категорий субъекта целиком содержится в множестве категорий объекта;
- при создании субъекта он получает классификацию и категории, назначаемые администратором безопасности;

– при создании объекта он получает классификацию и категории субъекта, создавшего данный объект.

В общем случае, учитывая первое глобальное правило, имеем:

– доступ к объекту по чтению разрешен в том случае, если разрешен доступ по модели дискреционной защиты и доступ по чтению согласно модели мандатной защиты;
– доступ к объекту по записи разрешен в том случае, если разрешен доступ по модели дискреционной защиты и доступ по записи согласно модели мандатной защиты.

Реализация правил разграничения доступа в системе ACCORD-2005

Выполнение принятых правил разграничения доступа обеспечивает сервер бизнес-логики ACCORD-2005 (mcasecur), через который проходят все запросы пользователей к защищаемым объектам. Сервер бизнес-логики формирует SQL-запросы таким образом, чтобы обеспечить проверку прав доступа.

Например, рассмотрим запрос, изменяющий тип детали:

```
UPDATE Material SET Type = 3,
       TranCreator = 30
WHERE Material.Id = 1.
```

Для того чтобы осуществить проверку выполнения правил разграничения доступа, этот запрос нужно изменить следующим образом:

```
UPDATE Material SET Type = 3,
       TranCreator = 30
FROM MaterialView
WHERE Material.Id = 1 AND
Material.Id = MaterialView.Id AND
1=dbo.CheckAccess_w(0x04,0x56,2,ACL,
Category,ISL).
```

В разделе `WHERE` добавляется условие

```
1=dbo.CheckAccess_w(0x04,0x56,2,ACL,
Category,ISL),
```

которое позволяет изменить только те детали, доступ по записи к которым разрешен.

На данный момент для формирования запросов используются заранее заготовленные шаблоны (параметризованные запросы), однако предложенный подход в принципе позволяет реализовать транслятор SQL-запроса.

Учитывая то, что применяется *недоверенная* ОС, необходимо исключить возможность обмена информацией между пользователями через жесткий диск компьютера. Для этого осуществляется *строгий* вход в ОС, допускающий использование только одного приложения — консоли управления ACCORD-2005. Это исключает несанкционированное чтение информации пользователем с жесткого диска компьютера. Кроме того, каждому компьютеру назначается гриф $ISL_{\text{к}}$ и категория секретности $C_{\text{к}}$. При входе пользователя в систему ему присваиваются эффективные $ISL_{\text{э}}$ и $C_{\text{э}}$ по правилам

$$ISL_{\text{э}} = \min(ISL_{\text{п}}, ISL_{\text{к}}); \quad C_{\text{э}} = C_{\text{п}} \& C_{\text{к}},$$

где $ISL_{\text{п}}$ и $C_{\text{п}}$ — гриф и категория пользователя, назначенные ему администратором; & — операция логического "И", применяемая к каждому биту.

Именно $ISL_{\text{э}}$ и $C_{\text{э}}$ используются в дальнейшем при принятии решений о предоставлении доступа к защищаемым объектам. Такой подход препятствует попаданию на компьютер информации с грифом, превышающим гриф компьютера, или имеющей категорию, не входящую в множество категорий компьютера. Как следствие, данный подход позволяет вести учет жестких дисков не обязательно по максимальным грифам и категориям обрабатываемой информации, что упрощает организацию физической защиты информации.

Заключение

Проанализировав все достоинства и недостатки различных способов реализации разграничения доступа в СУиК, авторы предлагают для решения этой задачи подход, основанный на использовании средств ППО, который применен в системе ACCORD-2005.

СУиК ACCORD-2000, на базе которой создается ACCORD-2005, в течение достаточно продолжительного времени успешно применяется на предприятиях Росатома (Северский химический комбинат, горно-химический комбинат в Железногорске, ПО "Маяк"). Сети, в которых работает ACCORD-2000, аттестованы по 3-му классу СУиК.

Система ACCORD-2005,обладая всеми положительными свойствами системы ACCORD-

2000, соответствует требованиям, предъявляемым к СУиК 2-го класса. В настоящее время идет подготовка к сертификации системы. Сертификат соответствия требованиям СУиК 2-го класса позволит применять ACCORD-2005 в системах, обрабатывающих информацию, которая содержит государственную тайну, данные различных уровней конфиденциальности и допускающих наличие разных прав доступа к информации у пользователей.

Список литературы

1. Требования по защите от несанкционированного доступа к информации в автоматизированных системах учета и контроля ядерных материалов. Министерство Российской Федерации по атомной энергии. Гостехкомиссия России. Москва, 1997.

2. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. С.-Пб.: Наука и техника, 2004. С. 177—187.

3. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации. Министерство Российской Федерации по атомной энергии. Гостехкомиссия России. Москва, 1992.

4. *Федосеев В. Н., Мизин П. П., Шанин О. И.* Подход к программному обеспечению для российских СУиК следующего поколения // Новости ФИС. 2003. № 3. С. 21—30.

5. *Анищенко А. А., Бурцев С. В., Григорьев А. М. и др.* Система учета и контроля ядерных материалов ACCORD-2000 // Вопросы атомной науки и техники. Сер. Математическое моделирование физических процессов. 2002. Вып. 1. С. 38—46.

Статья поступила в редакцию 19.12.07.