УДК: 81.93.29

МАНДАТНАЯ МОДЕЛЬ ДОСТУПА К ДАННЫМ

Аканов А.Д., докторант II курса специальности 6D060200 «Информатика»
Научный руководитель: Сагындыков К.М., к.т.н., доцент
Казахский гуманитарно-юридический инновационный университет г.Семей Республики Казахстан

Ограничение доступа к информации является одним из важнейших вопросов безопасности при разработке приложений, основанных на базах данных. Одним из методов, широко применяемых при осуществлении ограничения доступа к данным является мандатный метод (англ. Mandatory access control, MAC).

При использовании мандатного метода осуществляется присвоение меток конфиденциальности объектам и субъектам базы данных, согласно которым и определяется уровень доступа к данным. Чем больше уровень секретности, тем меньше метка доступа. Мандатный принцип разграничения доступа также называют принудительным контролем, так как пользователь не имеет возможность изменять права доступа к информации, которые, в свою очередь, четко определены самой политикой безопасности. Согласно политики безопасности, к примеру, если скопировать информацию с грифом «секретная информация» и перенести ее в объект с меткой «для общего пользования», объект, куда перенесена информация сменит значение метки на «секретная информация».

Следует также отметить, что мандатная модель определяет только возможности чтения и изменения объектов, возможность удалять объекты в данном случае не предусмотрена.

Выделяют неиерархические и иерархические виды категорий. В первом случае производится сравнение значений меток конфиденциальности на равенство. Если эти значения для субъекта и объекта равны, то осуществляется доступ к записи и чтению информации, если нет – то доступ не осуществляется.

При использовании иерархической категории производится более детальное сравнение значений меток. Здесь может быть три варианта:

1. Значение мандатной метки пользователя меньше значения метки доступа объекта. В данном случае пользователь получает права только на чтение информации;
2. Если значение метки пользователя равно значению метки объекта, тогда пользователь получает право на запись и на чтение информации;
3. Если значение мандатной метки пользователя больше значения метки объекта, тогда пользователь получает право только на запись.

Таким образом, пользователь имеет право чтения информации объекта:

- для иерархической категории: в случае, когда значение метки доступа объекта больше или равна значению метки доступа пользователя;

- для неиерархической категории: в случае равенства значений меток доступа объекта и пользователя.

Пользователь имеет право на запись:

- для иерархической категории: в случае, когда значение мандатной метки объекта меньше или равна значению метки пользователя;
- для неиерархической категории: в случае, когда значение мандатной метки объекта равно значению метки пользователя.

Пользователь имеет право на запись и чтение лишь в том случае, когда значения мандатных меток пользователя и рассматриваемого объекта совпадают. Данные правила должны быть соблюдены и при наличии нескольких категорий данных с различным набором уровней конфиденциальности в вопросах чтения и записи.

Использование мандатного метода также предусматривает наличие метки доступа «0», которая подразумевает отказ в доступе на чтение и на запись. Если такая метка присвоена пользователю, то он не имеет доступ ни к одному объекту. Если метка «0» присвоена объекту, то ни один пользователь не имеет права доступа к этому объекту.

Существует ряд требований к реализации мандатного метода:

1. Мандатный принцип разграничения доступа основывается на использовании специальных меток доступа, поэтому для каждого субъекта и объекта доступа должны быть предусмотрены такие метки, значение которых будет в дальнейшем определять уровень доступа.
2. При вводе новых данных (объектов) необходимо производить запрос и получать от санкционированного пользователя значения меток доступа к этим данным. При санкционированном добавлении нового пользователя (субъекта) также необходимо присвоение этому субъекту метки доступа. Причем внешние метки субъектов и объектов должны в обязательном порядке соответствовать внутренним меткам, предусмотренным защитной системой.
3. Доступ на основе сравнения значений мандатных меток должен осуществляться относительно всех объектов при явном или скрытом доступе со стороны любого из пользователей:

- Пользователь имеет доступ к объекту с возможностью чтения, если иерархическая классификация пользователя больше или равна иерархической классификации объекта (Рисунок 1).

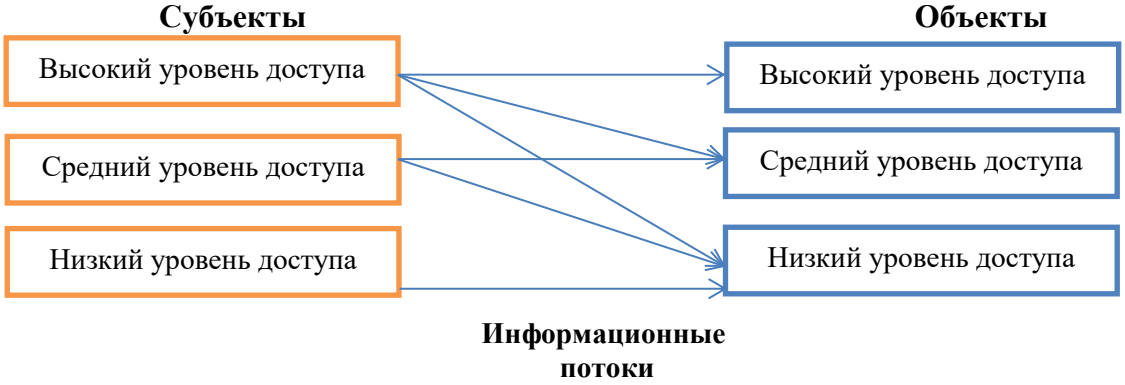

Рисунок 1. Чтение информации

- Пользователь может производить записи в объект только тогда, когда в иерархической классификации значение мандатной метки пользователя не больше значения метки объекта.

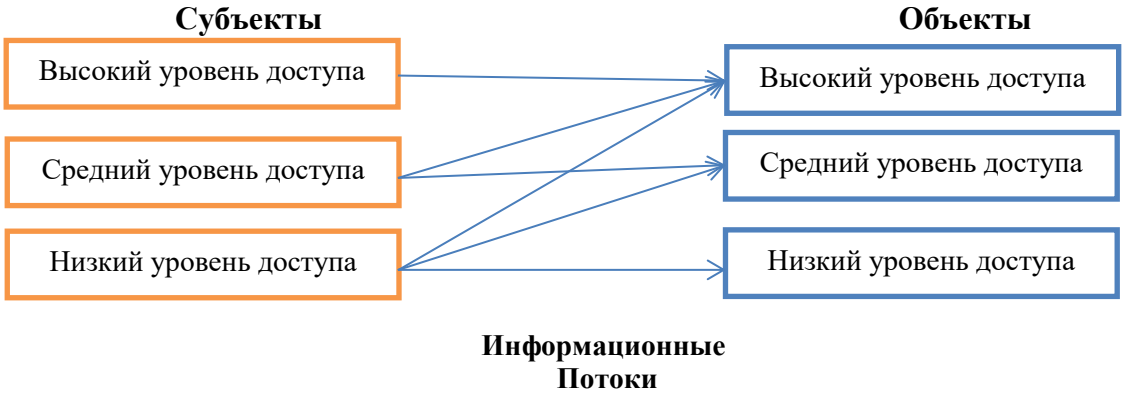

Рисунок 1. Запись информации

4. Реализация мандатной модели должна предусматривать наличие специального субъекта (пользователя), который имеет возможность сопровождения и изменения значений меток доступа всех субъектов и объектов.

Рассмотрим небольшой пример реализации мандатного метода ограничения доступа. Допустим, имеется иерархическая категория, для которой предусмотрены 3 вида меток:

0. доступ запрещен;
1. для служебного пользования;
2. ограниченный доступ;

И 3 пользователя со следующими значениями мандатных меток:

1) Пользователь 1 – значение метки доступа 0.
2) Пользователь 2 – значение метки доступа 1.
3) Пользователь 3 – значение метки доступа 2.

Тогда получается, следующие разграничения доступа:

К объекту с меткой доступа «0» доступ запрещен для всех пользователей.

К объекту с уровнем доступа «1» доступ:

- имеет пользователь 2 в режиме чтения и записи;
- имеет пользователь 3 в режиме записи.

К объекту с уровнем доступа «2» доступ:

- имеет пользователь 3 в режиме чтения и записи;
- имеет пользователь 2 в режиме чтения.

Пользователь 1, для которого значение метки доступа «0» не имеет доступа к объекту.

Пользователь 2 (значение метки доступа 1) имеет право:

- читать и записывать информацию для служебного пользования;
- читать информацию для ограниченного доступа.

Пользователь 3 (значение метки доступа 2) имеет право:

- чтения и записи информации для ограниченного доступа;

- записи информации для служебного пользования.

Основным преимуществом мандатной системы управления является то, что субъект не может полностью управлять доступом к данным, которые он создаёт. Мандатная система запрещает пользователю или процессу с определенной меткой доступа, получать доступ к информации, процессам или устройствам более защищённого уровня. В целом, мандатное ограничение доступа позволяет существенно упростить задачу администрирования.

К недостатку системы с мандатным ограничением доступа можно отнести тот факт, что отдельно взятые категории одного уровня равнозначны, что приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующих уровней.

Чаще всего мандатное ограничение доступа используется совместно с дискретной или ролевой моделями.

Список используемой литературы:

1. Алгоритмы и модели ограничения доступа к записям баз данных / Баранчиков А.И., Баранчиков П.А., Пылькин А.Н. – М.: Горячая Линия – Телеком, 2011, 182 с.
2. Брейман А. Д. Автоматизация администрирования баз данных //Автоматиз. и соврем, технол. N 5. — 2005. — 25−27.
3. https://cyberpedia.su/6x4749.html
4. Полтавцева М.А. Задача хранения прав доступа к данным в РСУБД на примере Microsoft SQL Server // Актуальные направления фундаментальных и прикладных исследований: матер. V Междунар. науч.-практич. конф. 2015.
5. Баранчиков А.И., Баранчиков П.А., Пылькин А.Н. Алгоритмы и модели доступа к записям БД. М.: Горячая линия–Телеком, 2011.