УДК 004.632

ТИПЫ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА

В.А. Бопп

В работе рассматриваются модели разграничения доступа. В основе мандатной модели – метки конфиденциальности. Дискреционная модель предоставляет доступ с использованием матрицы доступа, однако не так проста в администрировании, как ролевая, которая позволяет быстро переназначать пользовательские роли и более гибко настраивать права доступа.

Ключевые слова: модели доступа, мандатная, ролевая, дискреционная, разграничение прав.

В настоящее время современный мир переживает технологическую революцию. Информация не только переносится в электронный вид, но и может иметь только цифровой вариант. Утрата важных данных всегда приводила к потерям: временным, финансовым и репутационным. Исключить такие потери полностью невозможно, однако реально снизить риск утраты данных и снизить последующие издержки.

В настоящее время существует множество различных способов обеспечения сохранности данных в информационных системах. Все они базируются на известных технологиях, одна из которых – обеспечение безопасности доступа к данным.

Под безопасностью доступа к данным следует понимать грамотное разграничение доступа к информации, где конечный пользователь имеет доступ только к тем данным, которые для него предназначены и может выполнять только те действия, которые ему разрешены. Такой подход осуществим с использованием политик безопасности с мандатным, ролевым и дискреционным доступом [1].

Мандатный способ управления доступом подразумевает использование метки конфиденциальности, хранящейся на объекте для определения возможности доступа субъекта к этой информации [2].

Когда пользователь обращается к файлу или информационному ресурсу, система запрашивает метку конфиденциальности у пользователя и принимает решение о предоставлении доступа.

Мандатная модель управления доступом может иметь вид иерархической (рис. 1) и неиерархической. При иерархической структуре пользователь с уровнем доступа выше, чем требует метка конфиденциальности, получает доступ к файлу или ресурсу.

В обратном случае, когда метка конфиденциальности объекта выше по значимости, чем метка пользователя, то пользователь получить доступ не может. При неиерархическом способе мандатного доступа определяется совпадение меток. Пользователь может получить доступ к информации только в случае равенства метки пользователя и метки файла или ресурса.

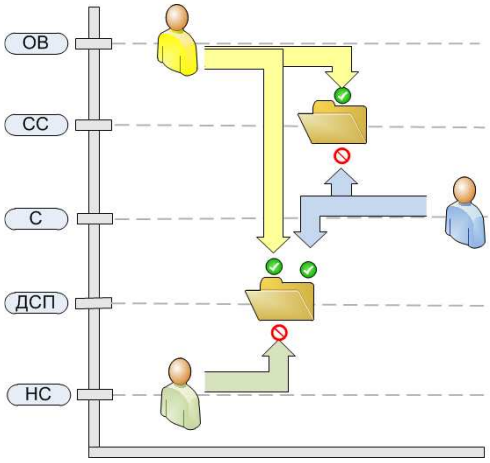

Рис. 1. Мандатная модель управления доступом

Пользователь с высшим уровнем доступа, чем требует метка конфиденциальности, в отличие от иерархической структуры, не получит доступ к запрашиваемому ресурсу. Такая модель применяется в системах с чёткой классификацией информации и высоким уровнем конфиденциальности.

В основе дискреционной модели лежит определяющая права доступа матрица (рис. 2), где строки – субъекты, а столбцы – объекты. В такой модели ресурсы системы принадлежат пользователям, доступ к ресурсам определяет его владелец. Дискреционная модель доступа позволяет определить какие операции разрешены с запрашиваемыми ресурсами. Для каждого из них определяются права доступа: право на просмотр, изменение, выполнение или удаление объекта [3].

Преимущество такого способа в простоте его реализации и его универсальности, поскольку дискреционная модель управления доступом поддерживается всеми операционными системами семейства Windows и Linux.

Один из главных недостатков заключается в том, что пользователь, имеющий право на чтение, может передать это право другим, не имеющим прав, пользователям без уведомления владельца. Нет уверенности, что информация не станет доступна пользователям, у которых нет к ней доступа.

Развитием дискреционной модели является ролевая модель доступа. Она заключается в предоставлении доступа к запрашиваемому объекту на основе роли пользователя, которая определяется на основе типов активностей в системе. Вместо предоставления доступа каждому пользователю к каждому объекту, доступ предоставляется группе пользователей, входящих в роль.

Предоставление доступа на уровне ролей позволяет настраивать систему таким образом, чтобы каждая роль со своими привилегиями наследовала привилегии других ролей, что позволяет гибко настраивать систему. В случае, когда у пользователя меняются обязанности, достаточно лишь удалить его связь со старыми ролями и назначить новые.

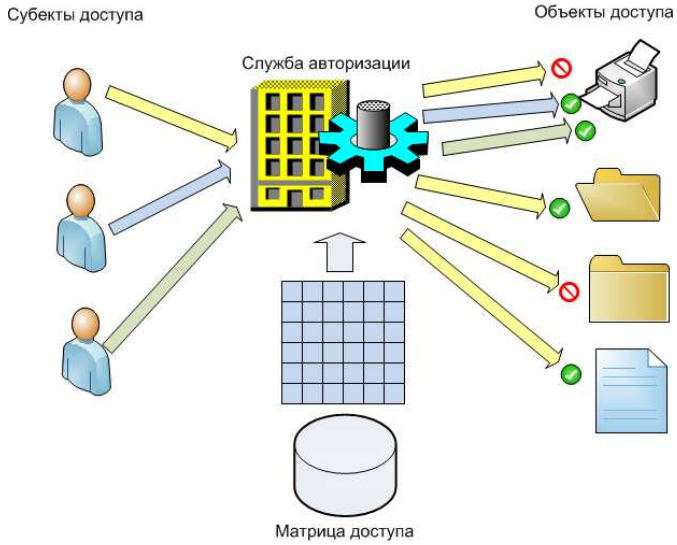

Рис. 2. Дискреционная модель управления доступом

Существуют операции, которые в целях безопасности и исключения мошенничества, не могут быть выполнены одним пользователем. Такой операцией может быть подготовка, подтверждение и выполнение платежа. Один пользователь подготавливает платёж, второй его подтверждает, третий – выполняет. Система ролевого управления позволяет обеспечить подобное разделение обязанностей. Кроме того, пользователю с большим количеством привилегий не всегда требуется использовать их все. В таком случае регистрация может происходить только с теми привилегиями, которые требуются для выполнения задачи.

Таким образом, модели доступа различаются между собой технологически, однако все они позволяют уменьшить вероятность несанкционированного взаимодействия с информацией, в том числе модификации и её безвозвратного удаления. Мандатная модель управления доступом позволяет получать доступ по меткам конфиденциальности, однако пользователь может получить доступ к любой менее конфиденциальной информации. Дискреционная модель позволяет более гибко распределять права доступа, но при таком способе невозможно в целях обеспечения наивысшей безопасности разделить операцию на нескольких пользователей. Это позволяет реализовать ролевая модель. Она проста в администрировании и позволяет быстро перераспределять роли в случае появления у пользователя необходимости в доступе к недоступным ранее ресурсам. Грамотная система распределения доступа и управления файловыми ресурсами позволяет значительно снизить вероятность неправомерного ознакомления, модификации и удаления информации из системы.

Список литературы

1. Обзор и сравнение существующих методов управления доступом // Институт вычислительных технологий СО РАН [Электронный ресурс]. URL: http://www.ict.nsc.ru/ws/YM2003/6312/ (дата обращения: 05.10.2019).

2. Мандатное управление доступом // Википедия - свободная энциклопедия. [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/ Мандатное_управление_доступом (дата обращения: 05.10.2019).

3. Избирательное управление доступом // Википедия - свободная энциклопедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/ Избирательное_управление_доступом (дата обращения: 05.10.2019).

Бопп Виктория Андреевна, магистрант, miss.blackbery@yandex.ru, Россия, Тула, Тульский государственный университет

TYPES OF ACCESS CONTROL MODELS

V.A. Bopp

The paper considers models of access control. The mandate model is based on privacy labels. The discretionary model provides access using the access matrix, but is not as easy to administer as the role model, which allows you to quickly reassign user roles and configure access rights more flexibly.

Key words: access models, mandate, role, discretionary, differentiation of rights.

Bopp Victoria Andreevna, master, miss.blackbery@yandex.ru, Russia, Tula, Tula State University