Разграничение доступа к элементам защищаемой информации заключается в том, чтобы каждому зарегистрированному пользователю предоставить возможности беспрепятственного доступа к информации в пределах его полномочий и исключить возможности превышения своих полномочий. В этих целях разработаны и реализованы на практике методы и средства разграничения доступа к устройствам ЭВМ, программам обработки информации, полям (областям ОЗУ, ПЗУ) и массивам (базам) данных

Что такое права доступа

Правом доступа называют разрешение выполнять определенные операции в отношении объектов инфраструктуры: целевых систем, приложений и программ, сетевого оборудования, данных, СЗИ. Например, один пользователь может только читать файлы, другой — редактировать и отправлять документы, третий — осуществлять системные настройки, управлять оборудованием и средствами защиты.

Основные компоненты прав доступа:

- Пользователи или учетные записи (УЗ), которым назначаются полномочия разного уровня.
- Ресурсы, используемые компанией: информационные системы, базы данных, приложения, СЗИ и др.
- Разрешения, которые пользователи приобретают в рамках назначенных полномочий.

Разные виды прав доступа могут назначаться пользователям, группам пользователей или учетным записям. Чтобы определить необходимый уровень полномочий, нужно проанализировать все используемые системы и сервисы, составить список ресурсов, которые потребуются для работы конкретным сотрудникам. Также при назначении привилегий следует учитывать степень конфиденциальности и характер обрабатываемых данных. Например, у рядовых пользователей не может быть доступа к финансовой отчетности, с которой работает бухгалтер.

Виды прав доступа

Глобально права доступа можно разделить на три группы: административные, пользовательские и групповые. Расскажем об особенностях каждой категории.

Административные права доступа

Наличие административных полномочий позволяет получить полный доступ к объектам инфраструктуры и возможность вносить изменения в круг прав рядовых пользователей и групп пользователей.

Кто может иметь административные полномочия:

- Сотрудники администрирующие информационные ресурсы.
- Владельцы информационных ресурсов.
- Другие пользователи, которым были назначены административные привилегии.

Сотрудники с правами администратора могут управлять пользователями и устройствами, формировать требования к целевым системам, изменять настройки СЗИ и оборудования, создавать и удалять объекты. Кроме того, эти сотрудники имеют доступ на предоставление/изменение/удаление полномочий.

Пользовательские виды прав доступа

Пользовательские полномочия позволяют получить необходимый уровень доступа к тем ресурсам, которые нужны для выполнения служебных обязанностей. По типу присвоенных привилегий и рангу сотрудников можно условно разделить на четыре группы: администраторы, операторы, менеджеры и рядовые пользователи. У рядовых пользователей самый узкий круг полномочий, у администраторов — самый широкий.

Виды пользовательских прав доступа на работу с системами и базами данных:

- Чтение — разрешение на просмотр информации без права на изменение.
- Запись — разрешение на изменение объектов, внесение дополнительных сведений.
- Изменение структуры БД и удаление — полномочия на модификацию и удаление объектов, присутствующих в базах данных.
- Администрирование — право на управление целевыми системами и БД.

- Изменение разрешений — право сужать или расширять круг полномочий в отношении конкретных объектов инфраструктуры.

Как правило, рядовые пользователи не имеют полномочий на изменение и удаление объектов инфраструктуры. Таким образом, можно снизить риски несанкционированного использования данных и потери критической информации.

Групповые права доступа

Это права, назначенные группе пользователей, выполняющих одинаковые рабочие задачи. Такой подход к разграничению полномочий считается гибким и подходит для крупных организаций. Он позволяет автоматизировать рутинные операции и сэкономить время сотрудников, которые вручную назначают права каждому пользователю.

Если отдельным сотрудникам будет недостаточно общего круга полномочий, можно запросить дополнительные привилегии по заявке. В случае одобрения запроса ответственными лицами заявителю будут назначены временные права, необходимые для выполнения задач в рамках текущих проектов. По окончании проектов полномочия аннулируются.

Как назначаются разные виды прав доступа

Разграничение доступа по спискам контроля доступа заключается в том, что для каждого элемента защищаемых данных (файла, базы, программы) составляется список всех тех пользователей, которым предоставлено право доступа к соответствующему элементу, или, наоборот, для каждого зарегистрированного пользователя составляется список тех элементов защищаемых данных, к которым ему предоставлено право доступа.

Чтобы упорядочить процессы назначения полномочий и обеспечить контроль за соблюдением регламентов в части доступа, целесообразно использовать одну из четырех моделей управления доступом: Моделями называют системы распределения полномочий в информационной инфраструктуре компаний. Их ключевая задача – обеспечить необходимый уровень безопасности ресурсов и упростить контроль доступа.

Дискреционная модель

Дискреционная модель доступа DAC (Discretionary Access Control) имеет второе название – избирательная. Это метод управления, подразумевающий, что доступ к информационным системам и ресурсам назначает администратор (реже владелец ресурсов). В системах, использующих DAC, владелец объекта может определять, кто имеет доступ к объекту, и на какие операции с ним (чтение, запись, удаление и т.д.) этим пользователям разрешается совершать.

Основные характеристики DAC:

1. **Владение ресурсами**: Каждый объект в системе имеет владельца, который имеет право на управление доступом к этому объекту. Владельцы могут предоставлять доступ другим пользователям или группам пользователей.
2. **Уровни доступа**: Владельцы могут задавать различные уровни доступа, такие как чтение, запись и выполнение, определяя, что конкретные пользователи могут делать с объектом.
3. **Гибкость**: DAC позволяет пользователям изменять права доступа в зависимости от их потребностей, что делает модель более динамичной и удобной в использовании.

Примеры DAC:

- **Файловые системы**: В операционных системах, таких как Windows и Unix/Linux, пользователи могут устанавливать права доступа к своим файлам и папкам, определяя, кто может их просматривать или изменять.
- **Базы данных**: В некоторых системах управления базами данных (СУБД) администраторы могут предоставлять доступ к определённым таблицам или записям другим пользователям, основываясь на их ролях или потребностях.

Преимущества DAC:

- **Удобство**: Пользователи могут легко управлять доступом к своим ресурсам без необходимости обращения к администраторам.
- **Гибкость**: Возможность динамически изменять права доступа позволяет адаптироваться к изменяющимся требованиям и условиям работы.

Недостатки DAC:

- **Безопасность**: Поскольку пользователи могут свободно предоставлять доступ к своим ресурсам, это может привести к случайным утечкам данных или несанкционированному доступу.
- **Управление правами**: В крупных организациях управление правами доступа может стать сложным, если много пользователей и объектов, что увеличивает риски ошибок. Если права доступа назначают сами владельцы, вероятность инцидентов снижается, – и все же схему сложно назвать совершенной.

В целом, использование DAC может быть полезным при управлении доступом к ресурсам в небольших и маломасштабных системах, где количество пользователей и объектов относительно невелико. Однако, при работе в более крупных системах с более сложной структурой управления доступом, может потребоваться применение других методов разграничения прав доступа.

Мандатная модель управления доступом (Mandatory Access Control)

Мандатная, или обязательная, модель (MAC) базируется на принципах конфиденциальности. Каждому объекту (ресурсу) в информационном поле компании присваиваются метки типа «не секретно», «засекречено», «строго конфиденциально». Затем администраторы или владельцы систем назначают сотрудникам полномочия в соответствии с их должностными обязанностями. Например, кто-то получает право взаимодействовать только с объектами несекретного уровня, кто-то – с совершенно секретными ресурсами.

MAC (Mandatory Access Control) - это метод разграничения прав доступа, при котором доступ к объектам контролируется на основе политик безопасности, определенных администратором системы или безопасности. В MAC уровень доступа определяется на основе классификации объектов и пользователей в соответствии с уровнем секретности или другими параметрами, определяемыми политикой безопасности.

Принцип работы MAC состоит в том, что каждый объект в системе получает свою метку безопасности, которая указывает на уровень доступа к нему. Каждый пользователь также имеет свою метку безопасности, которая определяет его уровень допуска к объектам в системе. Таким образом, пользователи могут получать доступ только к тем объектам, уровень безопасности которых ниже или равен их метке безопасности.

Пример использования MAC можно привести для правительственных организаций или военных учреждений, где информация имеет разные уровни секретности. В таких системах каждый пользователь и каждый объект имеет свой уровень секретности, который указывается в метке безопасности. Пользователь может получить доступ только к тем объектам, уровень секретности которых не превышает его метку безопасности. Например, пользователь со секретностью "секретно" не может получить доступ к объектам с меткой "совершенно секретно".

В рамках мандатной модели нельзя превышать назначенный уровень доступа. Если по каким-то причинам это необходимо, администраторы или владельцы систем создают для пользователей новые профили под актуальную метку ресурса.

Основные преимущества MAC:

- Более высокий уровень безопасности, поскольку пользователь не может превысить свой уровень доступа.
- Централизованное управление доступом на основе политик безопасности, что обеспечивает более эффективное управление системой безопасности.

Такая схема легко реализуется, но не обладает достаточной гибкостью для внедрения в инфраструктуру крупных организаций. Она предназначена скорее для государственных учреждений и компаний, которым требуется повышенный уровень безопасности.

RBAC

RBAC (Role-Based Access Control) - это модель управления доступом, которая определяет, какие пользователи имеют доступ к каким ресурсам на основе их роли в организации.

Управление доступом на основе ролей востребовано там, где присутствует необходимость точного разграничения прав и установлен четкий круг обязанностей. Роли представляют собой совокупность делегированных прав на получение доступа к объектам. Такой подход сочетает элементы мандатного и избирательного управления доступом, при этом отличается повышенной гибкостью. Важным моментом здесь считается тот факт, что привилегии приобретаются за счет назначенной роли. Тем самым упрощается исполнение таких действий, как добавление или перевод пользователя в иное подразделение.

Преимущества и недостатки RBAC

Сильными сторонами RBAC считаются:

1. Высокая гибкость. Роли могут меняться для решения нужных задач. При необходимости легко добавить новую роль, дополнить старую, установить ее группе пользователей.

2. Облегчение рутинной административной работы. Роли привязаны к группам пользователей, легко обновляются и корректируются в автоматическом режиме. Нет нужды вручную настраивать права каждому отдельному сотруднику.

3. Повышение эффективности работы. Снижение лишней нагрузки на IT-отдел увеличивает эффективность его работы, снижает время ожидания предоставления прав.

4. Высокая безопасность. Управление доступом на основе ролей использует принцип наименьших привилегий, поэтому сотрудники располагают только теми правами, которые им нужны при исполнении своей работы.

5. Прозрачность управления. Система на базе ролей носит понятный, очевидный для персонала характер, где каждый участник занимается своим делом.

Слабыми сторонами RBAC считаются:

1. Высокая трудоемкость реализации. Разработка модели проводится индивидуально, требует времени и сил, чтобы задать первоначальные условия и настройки для использования.
2. Подходит в первую очередь для крупных и средних компаний. Ролевая модель и ее обслуживание оправдано при определенном количестве сотрудников, привилегий и ролей. Нет смысла ее использовать со штатом до 30-50 человек, где всего 5-6 разных ролей и 1-2 привилегированных пользователя.

RBAC (Role-Based Access Control) используется во многих сферах, где необходимо управление доступом к ресурсам на основе ролей. Некоторые примеры использования RBAC включают в себя:

1. Корпоративные системы - в организациях RBAC используется для определения доступа пользователей к корпоративным ресурсам, таким как сетевые ресурсы, базы данных, приложения и т.д.

2. Банковские системы - RBAC может использоваться в банковских системах для ограничения доступа к конфиденциальной информации на основе ролей, таких как менеджеры, кассиры, операторы и т.д.

3. Системы здравоохранения - в системах здравоохранения RBAC может использоваться для ограничения доступа к конфиденциальной медицинской информации на основе ролей, таких как врачи, медсестры, администраторы и т.д.

Модель на базе атрибутов (Attribute-based Access Control)

Система ABAC использует механизм авторизации, который связан с выполнением комплекса мероприятий, направленных на оценку представленных атрибутов. Атрибуты могут затрагивать объект и субъект доступа, связанные с ними операции, окружение среды. В отличие от ролевой модели здесь часто используются сложные наборы правил, при проверке которых происходит оценка большого количества атрибутов. За счет определения согласованных атрибутов субъектов и объектов посредством политик ABAC модель упрощает процесс управления списками доступа, группами пользователей.

ABAC система, несмотря на проигрыш по популярности ролевой модели, встречается в IT-сфере и разнообразных бизнес-системах. Так, например, ее используют в крупных IT-компаниях, когда встает вопрос о проектировании персональных систем безопасности, где счет персонала идет на тысячи сотрудников, а количество привилегий в два-три раза больше количества персонала.