**Реализация модели политики безопасности посредством управления доступом**

**Цель:** ознакомиться со способами реализации модели безопасности

**Порядок работы:** изучить теоретические сведения, составить матрицу доступа для конкретного образовательного учреждения.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Объект /  Субъект | Дневник | Журнал | Интернет | Библиотека | Список учеников |
| 1. Администратор | Полные  права | Полные права | Полные  права | Полные права | Полные права |
| 2. Уборщик | Запрет | Запрет | Запрет | Запрет | Запрет |
| 3. Директор | Чтение,  передача прав | Чтение,  запись | Полные  права | Запрет | Чтение |
| 4. Учитель | Частичный доступ | Чтение, запись | Полные права | Частичный доступ | Ограниченно |
| 5. Ученик | Чтение | Чтение | Полные права | Частичный доступ | Чтение |
| 6. Родитель | Чтение | Чтение | Запрет | Запрет | Запрет |

**Контрольные вопросы**

1. **Что понимается под политикой безопасности в автоматизированной системе?**

* организационно-техническая система, которая представляет собой совокупность определенных компонентов, способная выполнять автоматизированную обработку информации с целью удовлетворения информационных потребностей субъектов информационных отношений. **Безопасность автоматизированной системы** - защищенность всех её **компонентов** от различного рода нежелательного воздействия.

1. **Каково соотношение политики безопасности учреждения и автоматизированной системы данного учреждения?**
2. **В чем заключается модель дискреционной политики безопасности ?**

* политика безопасности осуществляемая на основании заданного администратором множества разрешенных отношений доступа.

Основой дискреционной (дискретной) политики безопасности является дискреционное управление доступом, которое определяется двумя свойствами:

* все субъекты и объекты должны быть идентифицированы;
* права доступа субъекта к объекту системы определяются на основании некоторого внешнего по отношению к системе правила (заранее не закладывается в систему).

К достоинствам дискреционной политики безопасности можно отнести относительно простую реализацию соответствующих механизмов защиты. Этим обусловлен тот факт, что большинство распространенных в настоящее время АС обеспечивают выполнение положений именно данной политики безопасности.

1. **Что понимается под матрицей доступа в дискреционной политике безопасности? Что хранится в данной матрице?**

* таблица, в которой строки соответствуют субъектам, столбцы — объектам доступа, а на пересечении строки и столбца содержатся правила (разрешения) доступа субъекта к объекту.

1. **Какие действия производятся над матрицей доступа в том случае, когда один субъект передает другому субъекту свои права доступа к объекту системы?**

* Дискреционная политика безопасности*.* Пусть *О -* множество объектов компьютерной системы, над которыми могут производиться различные операции, *U -* множество пользователей (субъектов) компьютерной системы, которые могут производить операции над объектами, *S -* множество всевозможных операций (действий) субъектов над объектами. Дискреционная политика безопасности определяет отображение *О —>U* (объектов на пользователей-субъектов). В соответствии с данным отображением, каждый объект *Oj* є *О* объявляется собственностью соответствующего пользователя *Uk E:U ,*который может выполнять над ними определенную совокупность действий 5- С *S*, в которую могут входить несколько элементарных действий (чтение, запись, модификация и т.д.). Пользователь, являющийся собственником объекта, иногда имеет право передавать часть или все права другим пользователям (обладание администраторскими правами).Указанные права доступа пользователей-субъектов к объектам компьютерной системы записываются в виде так называемой *матрицы доступов.* На пересечении *i-й* строки и j-ro столбца данной матрицы располагается элемент *Sy -* множество разрешенных действий *j-ro* субъекта над *і-м* объектом.

1. **Как соотносятся матрица доступа и ролевой доступ?**

* При большом количестве пользователей традиционные подсистемы управления доступом становятся крайне сложными для администрирования. Число связей в них пропорционально произведению количества пользователей на количество объектов. Необходимы решения в объектно-ориентированном стиле, способные эту сложность понизить.

Таким решением является ролевое управление доступом (РУД). Суть его в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

Ролевой доступ нейтрален по отношению к конкретным видам прав и способам их проверки; его можно рассматривать как объектно-ориентированный каркас, облегчающий администрирование, поскольку он позволяет сделать подсистему разграничения доступа управляемой при сколь угодно большом числе пользователей, прежде всего за счет установления между ролями связей, аналогичных наследованию в объектно-ориентированных системах. Кроме того, ролей должно быть значительно меньше, чем пользователей. В результате число администрируемых связей становится пропорциональным сумме (а не произведению) количества пользователей и объектов, что по порядку величины уменьшить уже невозможно. Отношение "субъекты-объекты" можно представить в виде **матрицы доступа**, в строках которой перечислены субъекты, в столбцах – объекты, а в клетках, расположенных на пересечении строк и столбцов, записаны дополнительные условия (например, время и место действия) и разрешенные виды доступа.

1. **В каких случаях целесообразно использовать ролевой доступ?**

* По сравнению с указанными выше моделями, ролевое управление доступом обладает рядом важных положительных свойств.
* Возможность построения иерархии ролей с наследованием набора прав. Это позволяет упростить ролевую модель, особенно в организациях с разнородной инфраструктурой, где используется много информационных систем. С использованием иерархии нет необходимости повторно указывать права в нескольких подобных ролях, достаточно поместить их в одну большую роль, как дочерние, указав лишь уникальные права для каждой роли.
* Просто и эффективно осуществляется предоставление одинаковых прав большому количеству пользователей – достаточно назначить пользователям одну роль.
* При необходимости изменения набора прав большому количеству пользователей достаточно изменить набор прав в роли.
* Возможность реализации принципа разделения полномочий (SoD – Segregation of Duties). Это значительно снижает риск предоставления пользователям избыточных полномочий, например, когда две роли не могут быть в один момент времени назначены одному пользователю.

Вывод: Изучил модели политики безопасности посредством управления доступом, составил матрицу доступа для конкретного образовательного учреждения, ответил на контрольные вопросы по теме.