Применение иерархического метода для построения защищенной операционной системы.

Выполнила
Шилова О. И-411

Существуют две проблемы при построении защищенных информационных систем:

1) распределение задач администрирования средствами защиты информации между субъектами управления системой;
2) использование встроенных механизмов защиты на всех уровнях иерархии системы.

Первая проблема обусловлена иерархическими принципами построения сложной системы.




Уровни сложной системы:

1) уровень платформы (операционная система),

2) общесистемный уровень (СУБД и другие системные средства),

3) уровень приложений.

Каждый уровень требует своего администрирования.

В сложной системе выделяются задачи администрирования:

1. системное администрирование (настройка ОС, конфигурация и маршрутизация сетевого трафика и т.п.);
2. администрирование СУБД и других общесистемных средств;
3. администрирование прикладных приложений.

На уровне системного администрирования может присутствовать разделение задач по функциональному назначению объектов - рабочие станции, файл-серверы и серверы приложений, серверы доступа к внешним сетям и др.

В сложной системе вводятся соответствующие администраторы, каждый из которых отвечает за свою компоненту управления.

В защищенных информационных системах выделяется самостоятельное управление - управление информационной безопасностью системы.

- Возникают две проблемы включения этой компоненты в исходную схему администрирования:

1. Связана с тем, что администратором каждого уровня иерархии управления решаются в том числе и задачи администрирования информационной безопасностью в рамках соответствующего уровня иерархии.

2. Связана с использованием встроенных средств защиты, распределением задач между встроенными и добавочными средствами защиты.

Для разрешения этих проблем возможны следующие альтернативные подходы:

- Все задачи администрирования информационной безопасностью системы возложить на администратора безопасности.
- Задачи администрирования информационной безопасностью системы распределить между администраторами на всех уровнях иерархии.

Метод уровневого контроля целостности списков санкционированных событий.

- Суть метода:

  Все ресурсы системы делятся на уровни по функциональному признаку. Текущая конфигурация каждого уровня заносится в эталонный список, хранящийся в системе защиты и недоступный никому, кроме администратора безопасности.

  При обнаружении расхождений текущего и эталонного списка является признаком несанкционированного доступа, в качестве реакции на которое средство защиты может выполнить дополнительные реакции.

Метод распределения функций администрирования безопасностью в системе.

Все настройки информационной безопасности на соответствующих уровнях иерархии задаются соответствующим системным администратором, администратором приложений, администратором СУБД при контроле со стороны администратора безопасности.

По завершении настроек они сохраняются администратором безопасности в эталонных списках средств защиты информации, к которым имеет доступ только администратор безопасности.

В процессе функционирования системы данные списки непрерывно контролируются и автоматически восстанавливаются из эталонных копий в случае обнаружения их искажений.

Метод противодействия ошибкам и закладкам в средствах информационной системы:

При любом доступе пользователя к информации должен произойти ряд событий - авторизация пользователя, должна быть запущена программа на исполнение, при доступе к информации должны быть проверены права доступа пользователя.

Средство защиты информации создает эталонные копии списков контролируемых событий и осуществляет их непрерывный контроль в процессе функционирования системы. При искажении исходного списка вырабатывается реакция средства защиты информации.

Таким образом, если доступ к информации осуществляет санкционированный пользователь, он получает доступ к информации. В противном случае, нарушителю необходимо осуществить какое-либо изменение контролируемого события при доступе к информации, иначе доступ к информации невозможен.

Преимущества рассмотренных принципов реализации системы защиты:

- она реализуется на прикладном уровне, т.е. практически инвариантна к типу используемых в информационных системах ОС, СУБД и приложений,
- ее применение практически не приводит к снижению надежности функционирования системы.

Спасибо за внимание!