Изменения политик управления доступом

Медведев Денис, ООО «Базальт СПО»

Управление изменениями жизненного цикла

- После разработки информационной системы она может претерпевать разнообразные изменения - добавления элементов, удаление элементов, смена среды эксплуатации.
- Должно обеспечиваться безопасное состояние.
- Как можно изменять политику управления доступом для обеспечения безопасного состояния при изменениях?

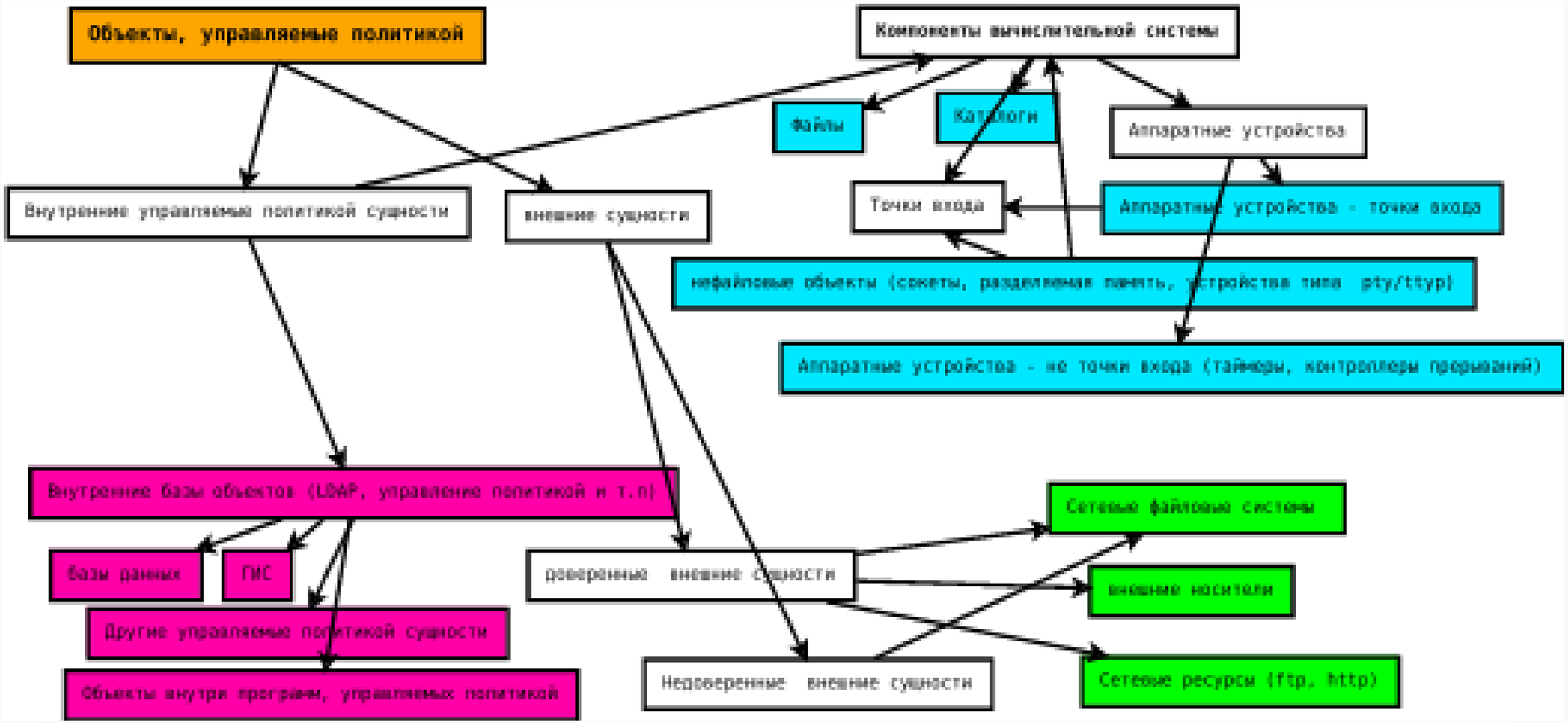
Политика управления доступом

- Вводит ограничения доступа субъектов к объектам
- Вводит понятия уровней доступа,атрибутов объектов
- Имеет базовую часть, инварианты, нарушение которых приводит к нарушению безопасного состояния.

Примеры изменений

- **В систему устанавливают PostgreSQL, умеющую работать с данными различных уровней.**
- **В системе потребовалась работа с внешней сетью через WiFi.**
- **Отпала необходимость авторизации пользователей по протоколу nis+**

Объекты политики управления доступом:



Варианты изменений вычислительной системы, относящихся к политике управления доступом.

- Добавление нового одноуровневого компонента
- Добавление нового многоуровневого компонента, внутреннее устройство которого совместимо с текущей политикой
- Добавление нового многоуровневого компонента, внутреннее устройство которого мало совместимо с текущей политикой.
- Удаление компонента вычислительной системы.

Добавление одноуровневого компонента

- Присваивается фиксированный атрибут - данные компонента считаются несущими атомарный признак. Пример - монтирование USB устройств с FAT в Linux.
- Требуется изменение инициализирующих элементов (скриптов, стартовых данных назначений меток).

Добавление нового многоуровневого компонента, внутреннее устройство которого совместимо с текущей политикой

- Требуется написание модуля базовой политики или дополнение правил
- Возможно будет требоваться адаптация базовой политики.

Добавление нового многоуровневого компонента, внутреннее устройство которого мало совместимо с текущей политикой.

- Инкапсулируется в контейнер или прокси, предоставляющий внутреннему компоненту атрибуты адаптированные для его условий API, а в вычислительную систему поставляющий соответствующие её политике атрибуты.
- Лучше переделывать компонент, чем политику системы.

Удаление компонента

- Может приводить к лишним, избыточным правилам в политике.
- Компонент мог использоваться для предоставления доступа к другим компонентам - будет требоваться переделка архитектуры ИС.

Контроль изменений

- Математическое доказательство непротиворечивости изменений
- Покрытие политики управления доступа тестами, проверяющими ее инвариант.

Спасибо за внимание!

nbr@basealt.ru
http://www.baseal
t.ru