Управление доступом в Linux

Курс Операционные системы

Файловая система Linux

Виртуальная файловая система – подключение (монитирование) устройств, сетевых потоков, процессов в виде каталогов, файлов или их данных

Общий корень для всего

Специальные каталоги для диагностики и настройки

Подключение томов как каталогов

ФС как универсальное API

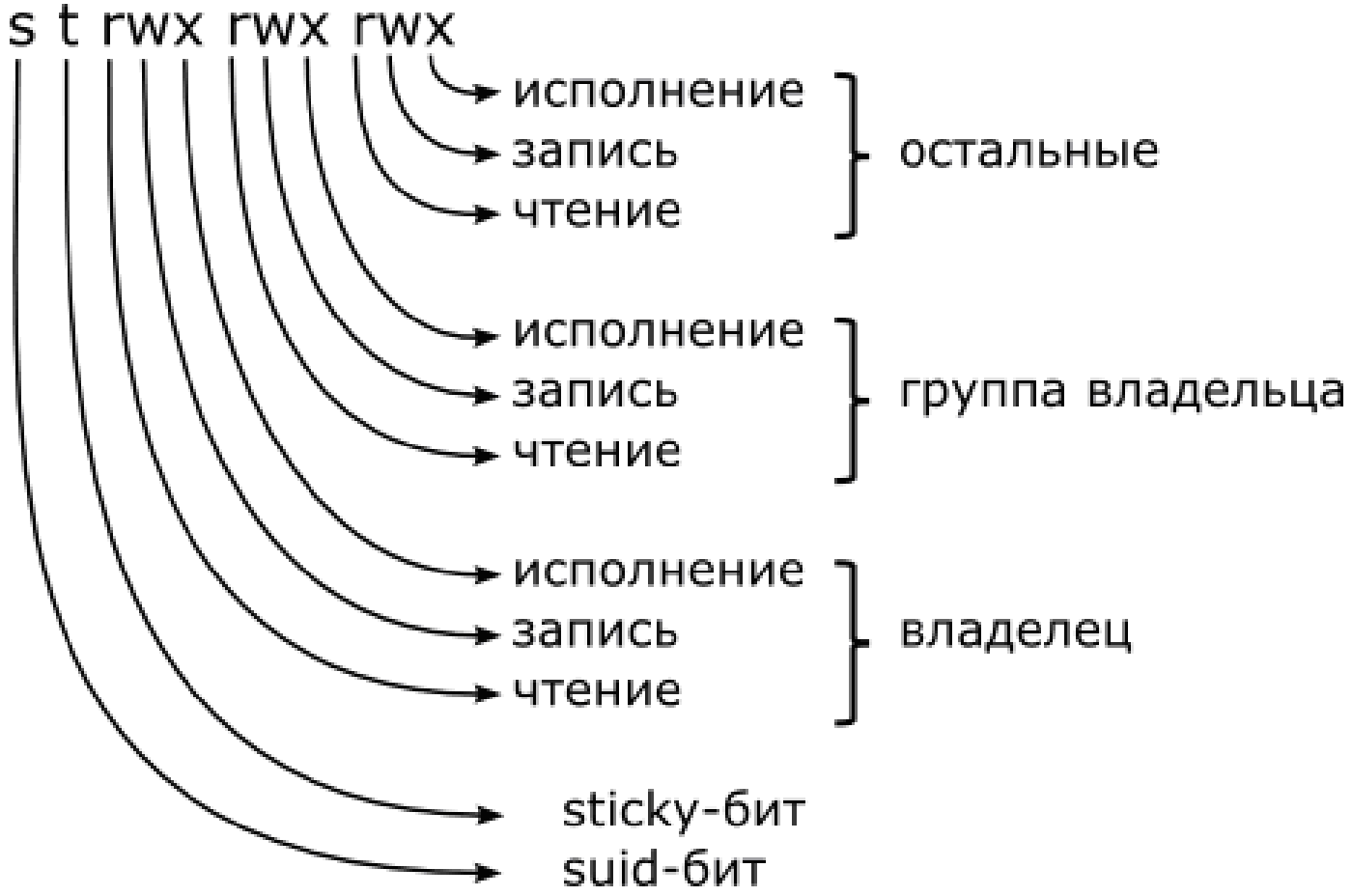
Специальные каталоги ФС Linux

- **/boot** — загрузочный каталог
- **/etc** — каталог конфигураций (**текстовых** конфигурационных файлов) всех подсистем.
- **/dev** — каталог устройств
- **/proc** — каталог системных файлов (псевдофайлов), отображающих состояние различных параметров системы
- **/sys** — более поздняя подсистема для диагностики и управления ОС, во многом аналогичная **/proc**.
- **/usr** — каталог пользовательского программного обеспечения
- **opt** — эквивалент /usr в некоторых операционных системах

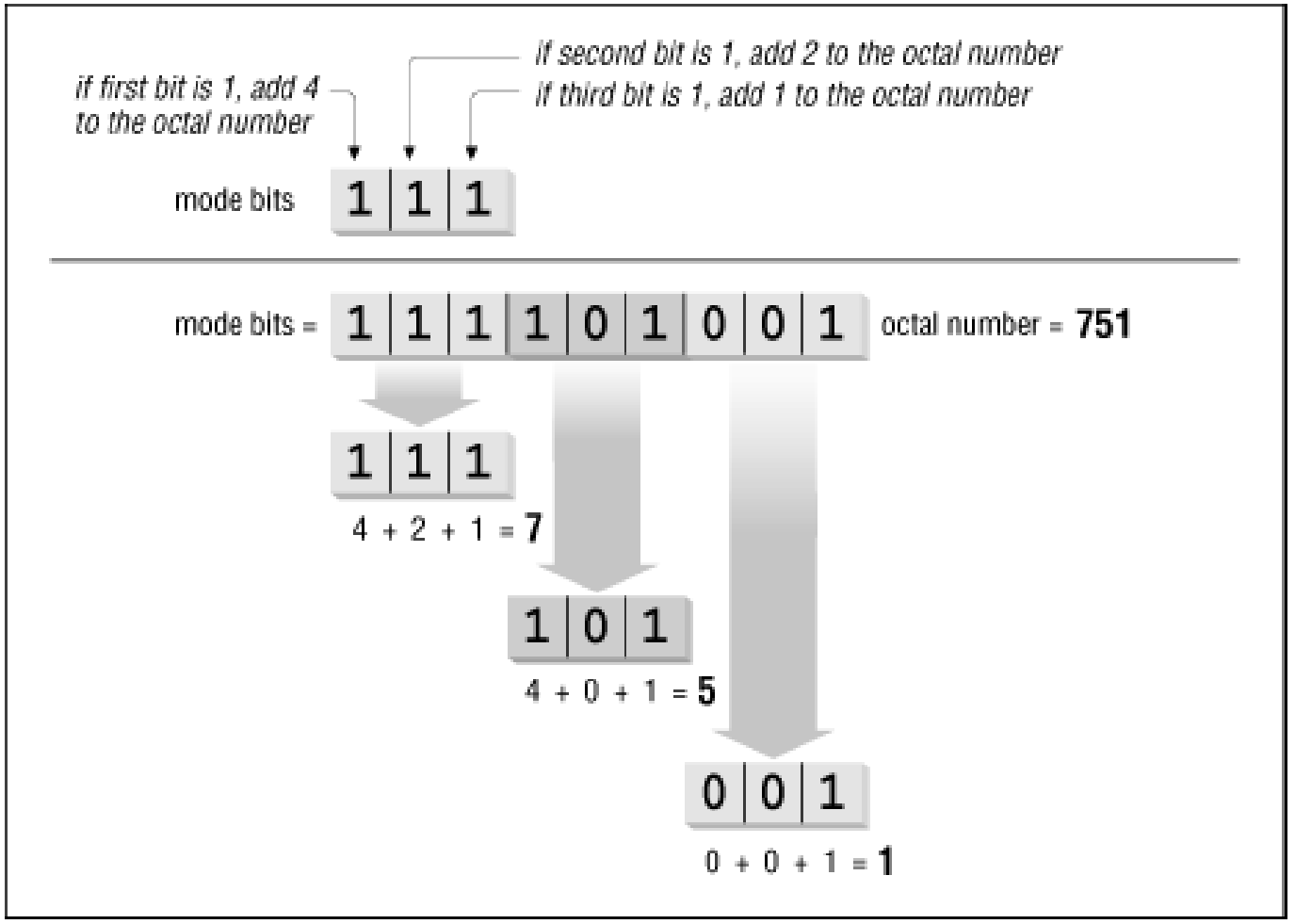
Специальные каталоги ФС Linux

- **/home** — каталог, содержащий домашние каталоги всех пользователей, зарегистрированных в системе.
- **/root** — домашний каталог администратора пользователя **root**
- **/run** — каталог текущей информации о запущенных программах
- **/var** — каталог служебных и временных данных системы
- **/var/log** — каталог системных журналов.
- **/mnt** — традиционный (POSIX) каталог для монтирования новых поддеревьев в иерархию файловой системы.
- **/media** — новый (не описываемый в POSIX) каталог для автоматического монтирования подключаемых устройств средствами программной подсистемы **udev**.

Базовые возможности управления доступом



Битовая маска разрешений



Для каталога

R – просмотр списка файлов в каталоге

W – создание и удаление файлов в каталоге

X – «вход» в каталог

Контрольные вопросы:

- Если не дано право входа в каталог, но дано право на чтение файла в этом каталоге, то сможет ли пользователь прочитать этот файл?
- Если для каталога заданы W и X, то сможет ли пользователь создать файл в этом каталоге?
- А потом прочитать его?

suid (sgid) bit

Определяет ассоциированного с запущенным процессом пользователя - процесс может получать разные наборы прав

Применяется к исполняемым файлам

0 – процесс работает под УЗ запустившего

1 – процесс работает под УЗ владельца файла

sgid для каталога – файлы, созданные в нём наследуют ID группы каталога, а не ID пользователя

sticky bit

- Сохранение запущенного процесса в памяти
- Ускорение для часто запускаемых программ - атавизм
- 0 – удаление файла в каталоге при наличии права W
- 1 – удалять файл в каталоге может только владелец

Группы

В системе существует ряд системных групп

- Используются для предустановленного доступа к ресурсам системы

При создании нового пользователя указывается его группа

Если при создании пользователя не указать группу – будет создана одноимённая группа

Контрольные вопросы

- Можно ли выдать разные права разным произвольным группам на один ресурс?
- Допустимо ли вложение групп?

Проблемы классической системы управления доступом

Любой процесс, запущенный пользователем, имеет равные пользователю права

Высокие привилегии root

Единая точка отказа – файловая система

Сложность управления доступом для нескольких пользователей и\или групп (совместный доступ)

LSM

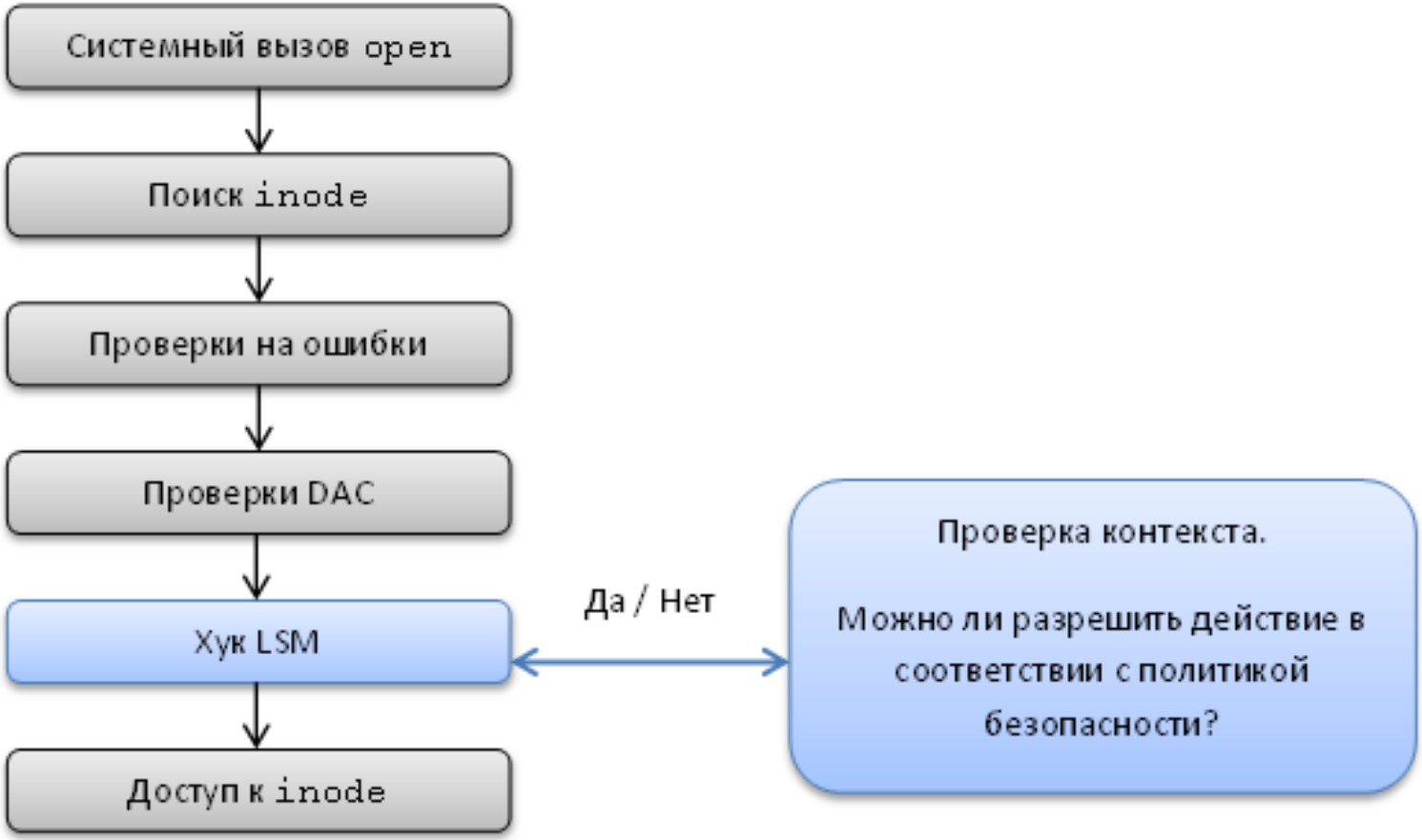
Позволяет СА изменить (улучшить) систему управления доступом

Позволяет реализовать и подгрузить модули ядра, отвечающие за управление доступом

В ядре используются хуки для перехвата и перенаправления запросов на доступ

Перехваченный запрос обрабатывается реализованным модулем

LMS - Linux Security Modules

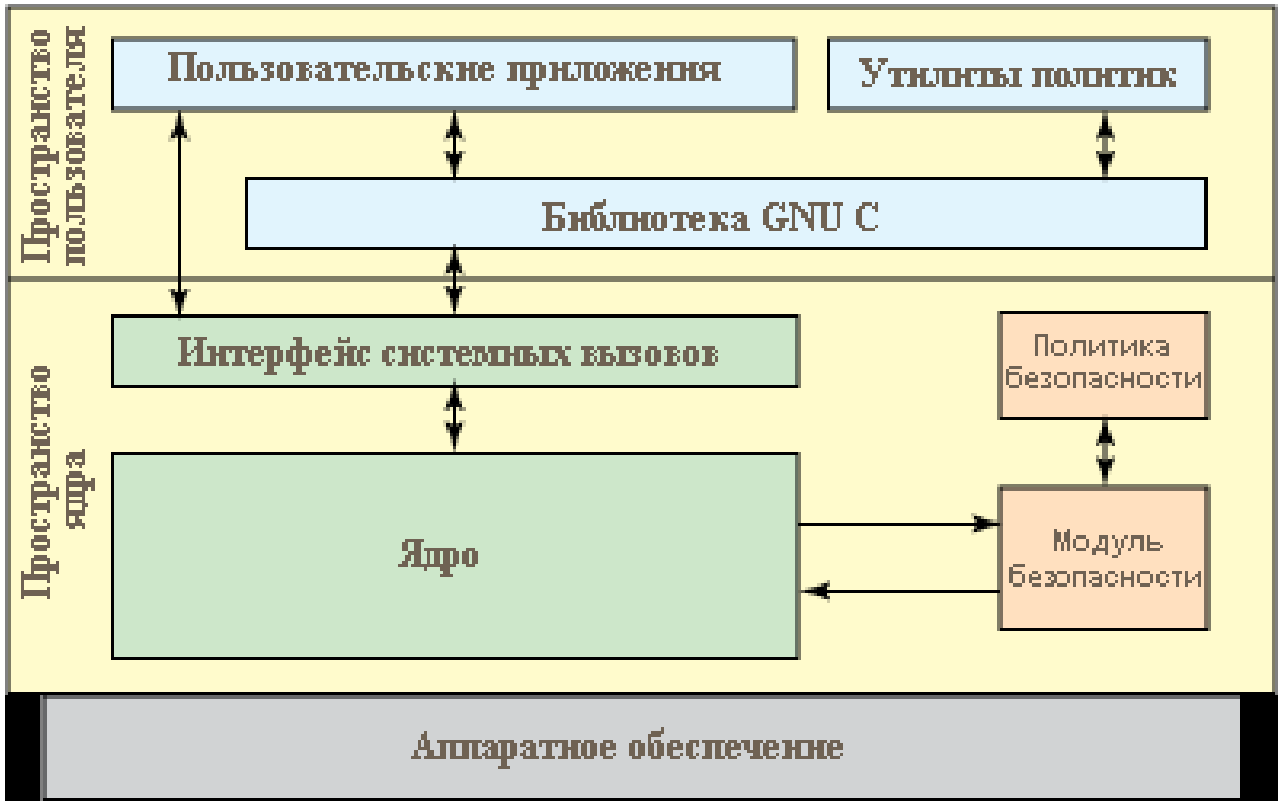


Популярные модули LMS

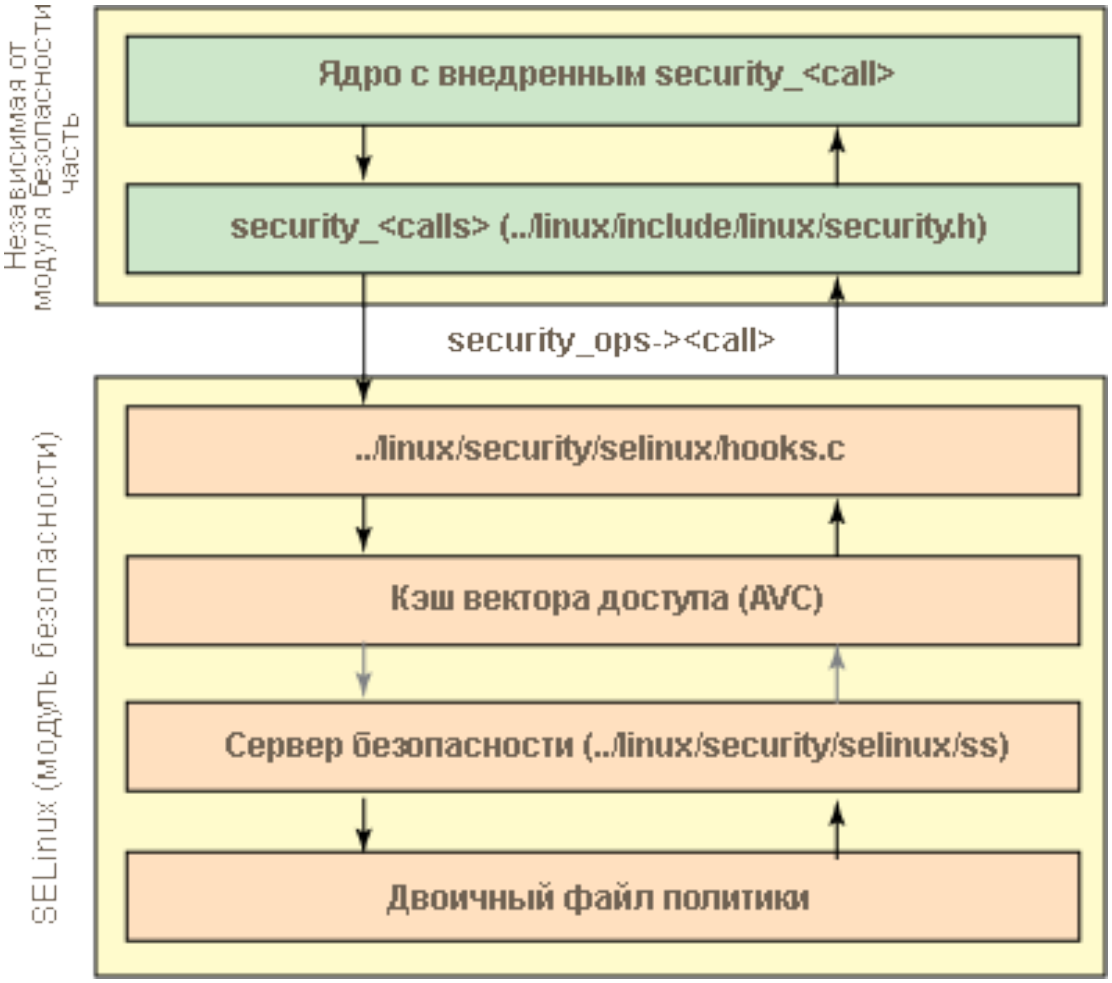
- AppArmor
- LoadPin
- SELinux
- Smack
- TOMOYO
- Yama

SELinux

- Модуль усиленной безопасности Linux



Вызов в SELinux



Примеры использования

Управление разрешениями на операции в Android

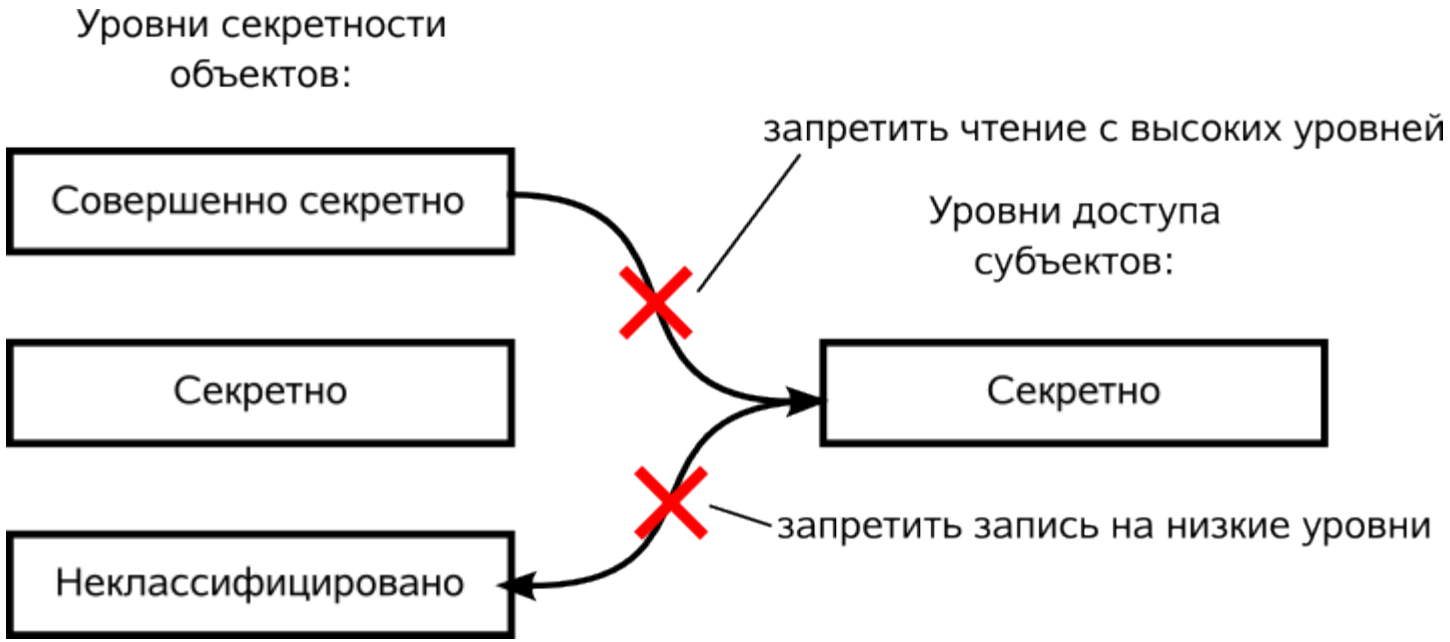
- Доступ к данным, компонентам системы, устройствам и сервисам

Защита от несанкционированного доступа через уязвимость запущенного процесса

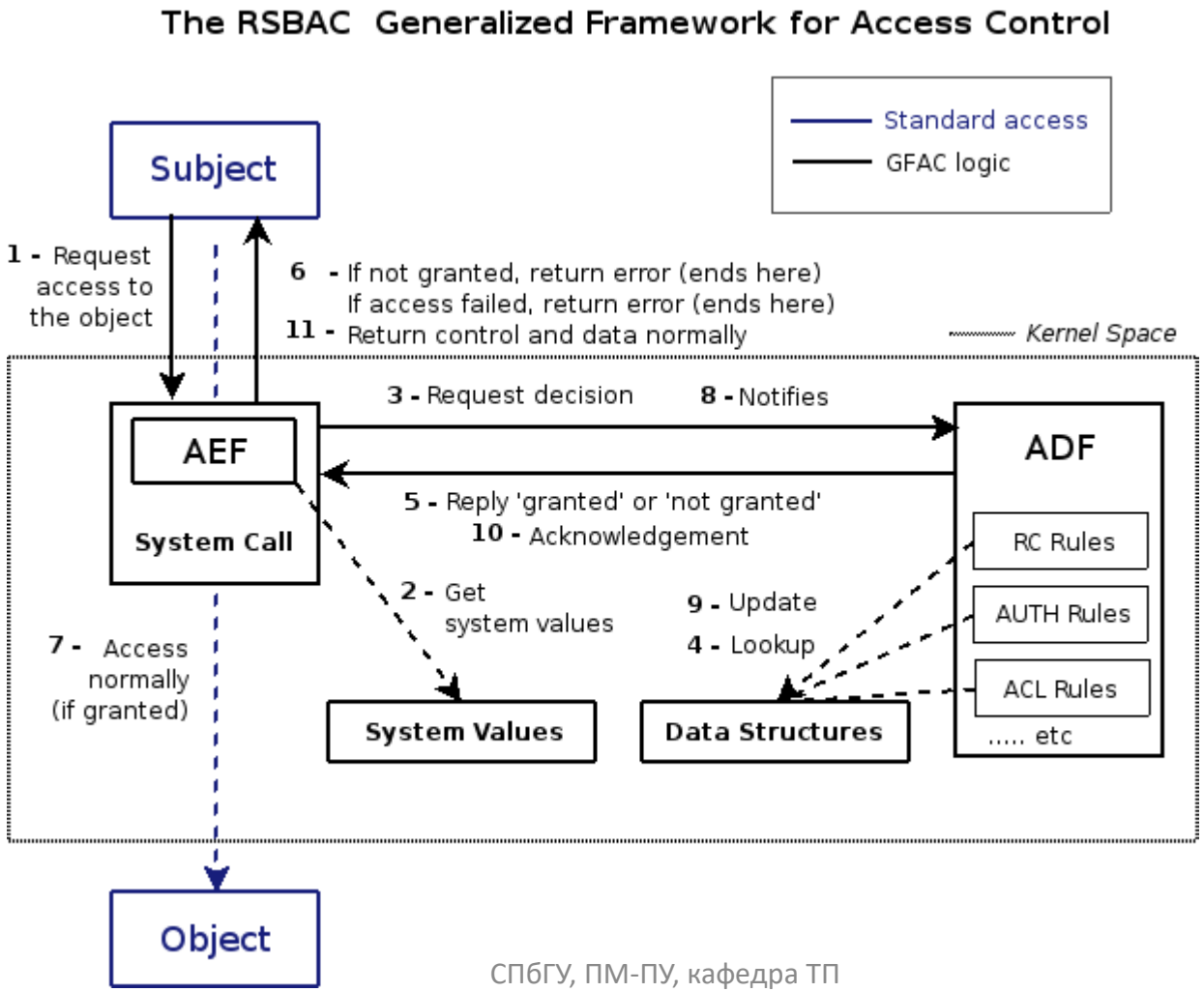
- Например, дополнительная защита для браузера или web сервера, который может иметь доступ к локальным ресурсам и «управляем» через сеть

Для понижения прав и привилегий root (и процессов, запущенных им)

MAC – Mandatory access control



RSBAC - Rule Set Based Access Control



Терминология RSBAC

Generalized Framework for Access Control (GFAC) - общий интерфейс управления доступом

Access Enforcement Facility (AEF) - Обеспечение доступа к подсистемам

Access Decision Facility (ADF) – Принятие решения доступа к подсистемам

Рекомендуемые ресурсы

- SELinux: теория и практика безопасности
- Анатомия SELinux
- Настройка окружения SELinux на примере LAMP-сервера
- Разрешения POSIX для файлов: Разделяем полномочия root
- Начало работы со службой хранения ключей в Linux
- Overview of the LSM and SELinux internal structure and workings
- https://www.rsbac.org/
- Пишем модуль безопасности Linux