

Программа контрольной работы 3

Архитектура ОС Windows

1. БЕЗОПАСНОСТЬ. Контекст безопасности, маркер доступа, привилегия, домен Windows. Виды маркеров доступа. Функции получения и использования маркера доступа. Базы данных безопасности. Структура компонентов безопасности. Монитор состояния защиты. Подсистема LSASS. Компоненты аутентификации. Служба сетевого входа, (Netlogon.dll), драйвер устройства безопасности ядра (Ksecdd.sys), AppLocker. Идентификаторы защиты (SID): идентифицируемые объекты, формат. Назначение идентификатора компьютеру домена. RID предопределённых пользователей, общеизвестные SID. Списки управления доступом. Дескриптор защиты. Отсутствующий и пустой DACL. Функции работы с базой данных локальных политик. Функции работы с привилегиями. Уровни целостности. Выбор уровня целостности для дочернего процесса и объекта. Мандатные политики. Ограниченный маркер, случаи, в которых он создаётся, правила создания. Проверки прав доступа к объекту, влияющие на них флаги маркера. Изоляция привилегий пользовательского интерфейса. Настройки requestedExecutionLevel манифеста приложения. Виртуализация, случаи её отключения. Алгоритм вывода запроса системы на повышение прав доступа. Запуск программы с запросом повышения прав.
2. ПЛАНИРОВАНИЕ ЗАДАЧ. Диспетчер ядра, случаи запуска процедуры планирования. Приоритеты потоков, функции установки приоритетов в Windows. Динамические уровни приоритета и уровни реального времени. Базовый и текущий приоритеты потока. Уровни прерываний, правила их изменения. Использование системой программных прерываний. Уровни прерываний диспетчеризации/DPC и APC: их использование и различия. Повышение динамического приоритета.

Инверсирование приоритета. Повышение приоритета при помощи службы планировщика классов мультимедиа. Состояния потоков и переходы между ними. База данных диспетчера ядра, переключение контекста. Правила выбора кванта времени, вытеснения потока. Поток простоя. Маски аффинности. особенности планирования задач на многопроцессорных системах.