**Лекция 7**

**Управление и настройка списков контроля доступа в Windows 10/11**

Список управления доступом (ACL) — это список ACE, созданных операционной системой для управления поведением безопасности, связанным с определенным (защищенным) объектом определенного типа. В Windows существует два типа списков управления доступом:

* **Дискреционный список ACL** . Это список из нуля или более ACE, описывающих права доступа для защищенного объекта. Он является дискреционным, так как предоставленный доступ предоставляется по усмотрению владельца или любого пользователя с соответствующими правами.
* **Системный ACL** — это список из нуля или более ACE, описывающих политику аудита и сигнализации для защищенного объекта.

Термин "дискреционный" означает различие между обязательным и дискреционным контролем. В среде, в которой используются обязательные элементы управления, владелец объекта может не предоставить доступ к объекту. В дискреционной среде, например Windows, владельцу объекта разрешено предоставлять такой доступ. Обязательные элементы управления обычно связаны с очень жесткими средами безопасности, такими как те, которые используют секции безопасности, где система должна предотвратить раскрытие конфиденциальной информации между пользователями в одной системе.

Драйвер, создающий список ACL, будет выполнять несколько ключевых действий.

1. Выделение хранилища для списка ACL.
2. Инициализируйте список ACL.
3. Добавьте в список ACL ноль (или более) ACE.

В следующих примерах кода показано, как создать ACL:

C++

dacl = ExAllocatePool(PagedPool, PAGE\_SIZE);

if (!dacl) {

return;

}

status = RtlCreateAcl(dacl, PAGE\_SIZE, ACL\_REVISION);

if (!NT\_SUCCESS(status)) {

ExFreePool(dacl);

return;

}

Предыдущий фрагмент кода создает пустой список ACL. В примере кода выделяется значительный объем памяти, так как мы не знаем размер, необходимый для ACL.

На этом этапе список ACL пуст, так как в нем нет записей ACE. Пустой ACL запрещает доступ всем пользователям, пытающимся получить доступ к объекту, поскольку отсутствуют записи, предоставляющие такой доступ. Следующий фрагмент кода добавляет ACE в этот список ACL:

C++

status = RtlAddAccessAllowedAce(dacl, ACL\_REVISION, FILE\_ALL\_ACCESS, SeExports->SeWorldSid);

if (!NT\_SUCCESS(status)) {

ExFreePool(dacl);

return;

}

Теперь эта запись предоставляет доступ к любой сущности, которая обращается к объекту . Это предназначение идентификатора безопасности доступа к миру (SeWorldSid), который обычно представляется как доступ "Все" в других системных служебных программ Windows.

Обратите внимание, что при создании списков управления доступом важно упорядочить запрещенные записи ACE в начале списка управления доступом, а затем получить доступ к разрешенным записям ACE в конце списка управления доступом. Это связано с тем, что, когда монитор ссылок на безопасность выполняет оценку ACL, он предоставит доступ, если он найдет ACE, предоставляющий доступ, до того, как он найдет запрещенные ACE. Это поведение хорошо задокументировано в Microsoft Windows SDK, но оно относится к конкретному механизму, который используется монитором ссылок на безопасность для определения того, следует ли предоставлять или запрещать доступ.