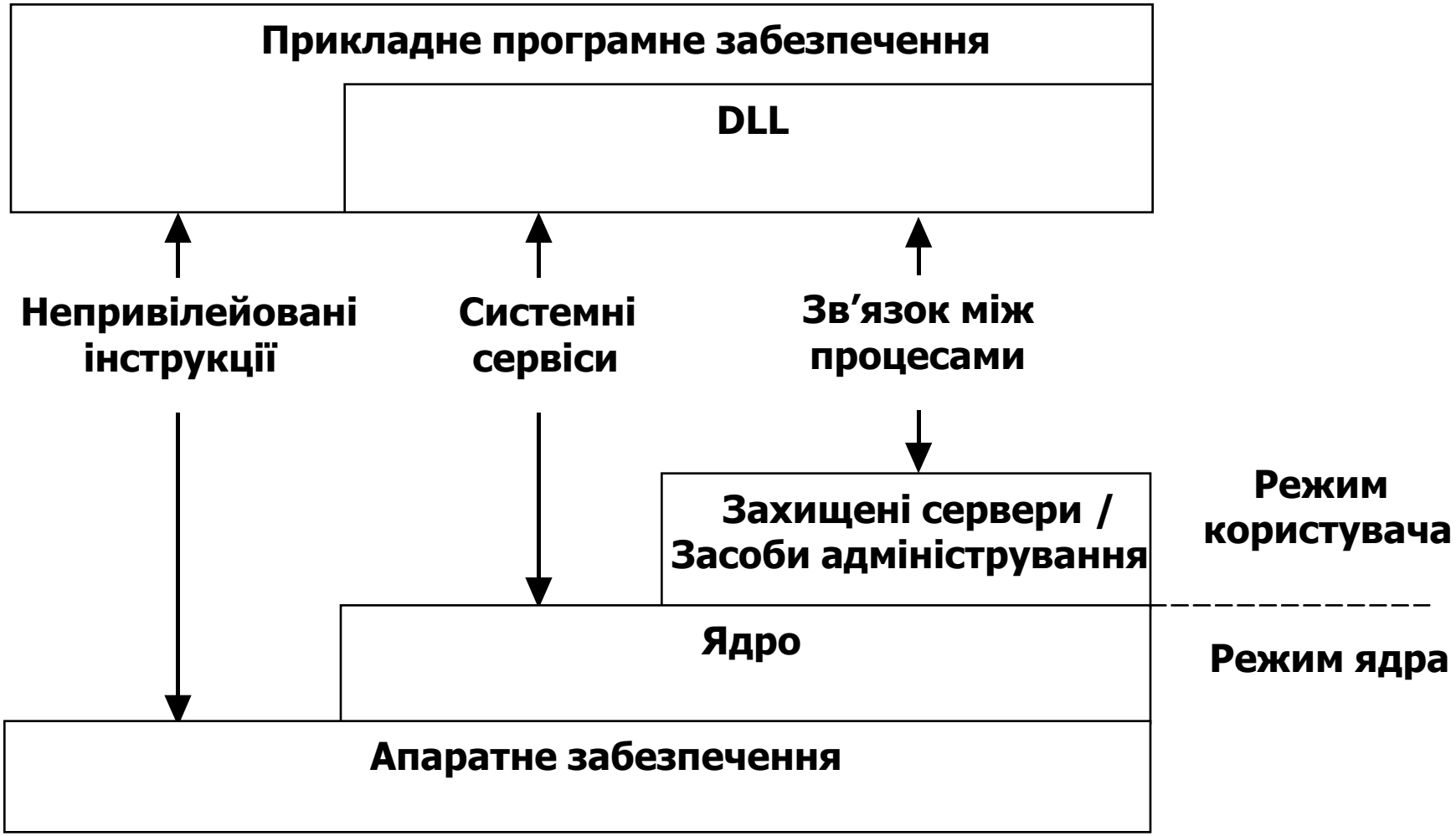
Безпека операційних систем і комп’ютерних мереж

Лекція 7

Засоби захисту Windows

Вертикальна декомпозиція архітектури ОС Windows



Компоненти КЗЗ Windows (1/7)

- **Монітор безпеки** (англ. – Security Reference Monitor, SRM)
  - Компонент системи (%SystemRoot%\System32\Ntoskrnl.exe), що виконується в режимі ядра і відповідає за перевірку прав доступу до об'єктів, операції над привілеями (правами користувачів) й генерацію повідомлень аудиту безпеки
- **Підсистема локальної автентифікації** (англ. – Local Security Authentication Subsystem, Lsass)
  - Процес режиму користувача (%SystemRoot%\System32\Lsass.exe), що відповідає за політику безпеки в локальній системі (наприклад, визначає коло користувачів, що мають право на вхід в систему, правила, пов'язані з паролями, привілеї, що видані користувачам та їх групам, параметри аудиту безпеки системи), а також за автентифікацію користувачів і передачу повідомлень аудиту безпеки в Event Log.
  - Основну частину цієї функціональності реалізує сервіс локальної автентифікації Local Security Authority Service - Lsasrv (%SystemRoot%\System32\Lsasrv.dll) – DLL-модуль, що його завантажує Lsass.

Компоненти КЗЗ Windows (2/7)

- **База даних політики Lsass**
  - База даних, що зберігає параметри політики безпеки локальної системи
  - Розташована в розділі реєстру HKLM\SECURITY й включає таку інформацію:
    - яким доменам довірено автентифікацію спроб входу до системи
    - хто має права на доступ до системи й яким чином
    - кому надані ті або інші привілеї
    - які види аудиту потрібно виконувати
  - База даних політики Lsass також зберігає «таємниці», які включають в себе реєстраційні дані, що застосовуються для входу до домену та під час виклику Win32-сервісів.
- **Диспетчер облікових записів безпеки** (англ. – Security Accounts Manager, SAM)
  - Набір процедур, що відповідають за підтримку бази даних, яка зберігає імена користувачів і груп, визначених на локальній машині
  - Служба SAM, реалізована у модулі %SystemRoot%\System32\Samsrv.dll, виконується в процесі Lsass

Компоненти КЗЗ Windows (3/7)

- **База даних SAM**
  - База даних, що зберігає інформацію про локальних користувачів та групи, разом з їхніми паролями та іншими атрибутами
  - Ця база даних розташована в розділі реєстру HKLM\SAM
- **Active Directory**
  - Служба каталогів, що зберігає базу даних із відомостями про об'єкти в домені (*домен* – це сукупність комп'ютерів і зіставлених з ними груп безпеки, керування якими здійснюється як єдиним цілим)
  - Active Directory зберігає інформацію про об'єкт домену, у тому числі про користувачів, групи й комп'ютери. Відомості про паролі й привілеї користувачів домену та їхні групи зберігаються в Active Directory та реплікуються на комп'ютери, що виконують роль контролерів домену.
  - Сервер Active Directory реалізований у модулі %SystemRoot%\System32\Ntdsa.dll, виконується в процесі Lsass

Компоненти КЗЗ Windows (4/7)

- **Пакети автентифікації**
  - DLL-модулі, що виконуються як у контексті процесу Lsass, так і у контексті клієнтських процесів, і реалізують політику автентифікації у Windows.
  - DLL-автентифікація відповідає за перевірку пароля й імені користувача, а також повернення Lsass (у разі вдалої перевірки) докладної інформації про права користувача.
- **Інтерактивний диспетчер входу в систему** (Winlogon)
  - Процес режиму користувача (%SystemRoot%\System32\Winlogon.exe), що відповідає за підтримку SAS (Secure Attention Sequence) і керування сеансами інтерактивного входу в систему
  - В процесі входу користувача в систему Winlogon створює перший процес користувача

Компоненти КЗЗ Windows (5/7)

- **Користувацький інтерфейс входу в систему — Logon user interface (LogonUI)**
  - Процес режиму користувача (%SystemRoot%\System32\LogonUI.exe), що надає користувачам інтерфейс, який може бути застосований ними для самоідентифікації у системі.
  - Процес стартує по запиту від Winlogon під час виконання SAS
  - LogonUI використовує постачальників облікових даних («провайдерів») для запиту облікових даних користувача за допомогою різних методів
- **Постачальники облікових даних — Credential providers (CP)**
  - COM-об'єкти, що використовують для одержання імені користувача і пароля, PIN-кода смарт-карти або біометричних даних (наприклад, відбитка пальця)
  - Стандартними CP є бібліотеки %SystemRoot%\System32\authui.dll и %SystemRoot%\System32\SmartcardCredentialProvider.dll.

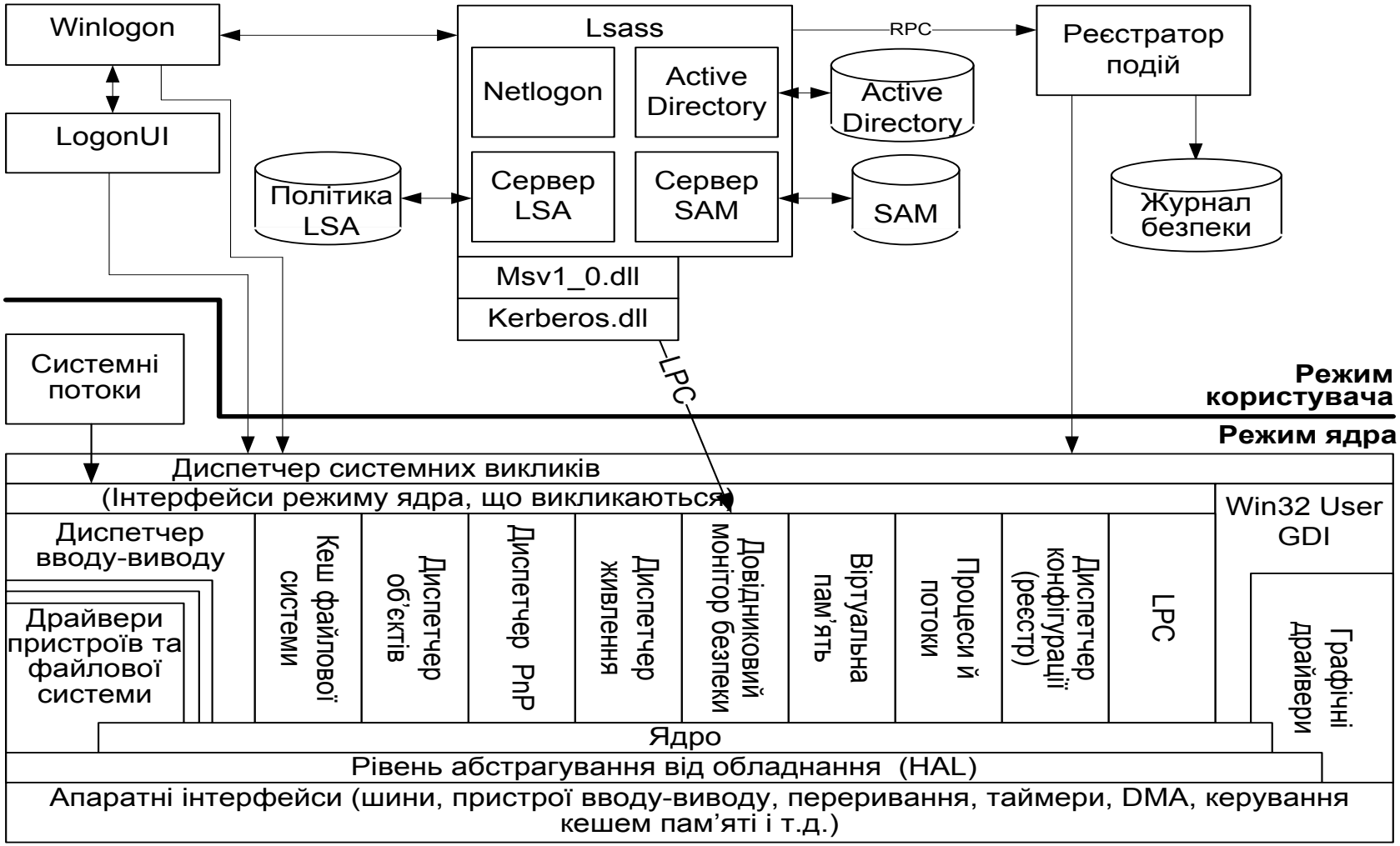
Компоненти КЗЗ Windows (6/7)

- **Служба мережного входу до системи** (Net Logon, Netlogon)
  - Win32сервіс (%SystemRoot%\System32\Netlogon.dll), виконується в Lsass і реагує на запити мережного входу від Microsoft LAN Manager 2 під керуванням Windows NT (будь-яких версій до Windows 2000). В цьому випадку автентифікація відпрацьовується як при локальній реєстрації – дані передаються Lsass для перевірки. У Netlogon також вбудовано службу локатора, що потрібна для пошуку контролерів домену.
- **Kernel Security Device Driver** (KSecDD)
  - Бібліотека функцій режиму ядра, що реалізує інтерфейси локального виклику процедур (англ. – local procedure call, LPC), які використовуються іншими компонентами захисту режиму ядра – у тому числі файловою системою, що шифрує (англ. – Encrypting File System, EFS) – для взаємодії з Lsass у режимі користувача
  - KSecDD знаходиться у %SystemRoot%\System32\Drivers\Ksecdd.sys

Компоненти КЗЗ Windows (7/7)

- **AppLocker**
  - Механізм, що дозволяє адміністраторам визначати, які виконувані файли, DLL-бібліотеки і сценарії можуть використовуватись конкретними користувачами і групами.
  - AppLocker складається з драйвера (%SystemRoot%\System32\Drivers\AppId.sys) і служби (%SystemRoot%\System32\AppIdSvc.dll), що виконується у процесі SvcHost.

Взаємодія компонентів й БД системи безпеки



Основні принципи реалізації системи розмежування доступу

- Windows реалізує дискреційну модель розмежування доступу
- Підтримує 4 типи суб'єктів та 13 типів об'єктів доступу
- Керування доступом здійснюється за допомогою модулю SRM
  - реалізується викликом функції SeAccessCheck ядра ОС при будь-якій спробі суб'єкта отримати доступ
- Використовуються дві структури даних:
  - *маркер доступу суб'єкта*, що є носієм його повноважень
  - *дескриптор захисту об'єкта*, що містить
    - ідентифікатори власника об'єкта та його первинної групи
    - список дискреційного контролю доступу (*Discretionary Access-Control List, DACL*)
    - список аудиту (*Security Access-Control List, SACL*)
- Матриця доступу зберігається у вигляді множини списків контролю доступу об'єктів, які мають нефіксовану довжину і можуть містити довільну кількість елементів контролю доступу (*Access Control Entry*, *ACE*), які можуть дозволяти або забороняти доступ
  - ACE, що забороняють доступ, мають більший пріоритет
  - У випадку відсутності ACE, що визначає потрібні права, у доступі буде відмовлено (реалізується принцип мінімуму повноважень)
- Задавати права доступу до файлових та принтерних об'єктів можна за допомогою Windows Explorer, а також за допомогою консольної команди **cacls**

Суб’єкти доступу Windows

1. Користувачі
   - звичайні користувачі
   - псевдокористувачі:
     - SYSTEM – ОС локального комп’ютера
     - <ім’я_комп’ютера>$, де ім’я_комп’ютера – мережеве ім’я комп’ютера; представляють ОС інших комп’ютерів в мережі і використовуються під час автентифікації робочої станції на контролері домену
2. Групи користувачів
3. Спеціальні (тимчасові) групи
   - Належність користувача до спеціальних груп визначається ОС в залежності від його дій:
     - INTERACTIVE
     - NETWORK
     - DIAL_UP
   - Спеціальна група не може бути первинною групою користувача
4. Відносні суб’єкти
   - мають сенс лише стосовно об’єкта, для якого визначаються права доступу
     - CREATOR_OWNER – власник об’єкта
     - CREATOR_GROUP – первинна група власника об’єкта

Стандартні суб’єкти доступу (1/2)

- В усіх екземплярах ОС Windows присутні такі суб’єкти доступу, що мають наперед задані ідентифікатори:
  - SYSTEM
  - INTERACTIVE
  - NETWORK
  - DIAL_UP
  - CREATOR_OWNER
  - CREATOR_GROUP
  - Everyone
- Під час інсталяції Windows автоматично створює таких визначених наперед суб’єктів доступу:
  - Administrator – адміністратор ОС
  - Guest – гість, користувач з мінімальними правами, який входить до системи анонімно
  - Administrators – група адміністраторів ОС
  - Users – група користувачів ОС, за умовчанням члени цієї групи мають дуже обмежені права

Стандартні суб’єкти доступу (2/2)

- Backup Operators – група операторів резервного копіювання
- Replicator – суб’єкт доступу, що використовується для автоматичної реплікації файлів і ключів реєстру між комп’ютерами домену
- Power Users (створюється лише на робочих станціях) – група користувачів, які мають більші права, ніж звичайні користувачі
- Account Operators (створюється лише на серверах) – група користувачів, які можуть працювати з обліковими записами непривілейованих суб’єктів доступу
- Print Operators (створюється лише на серверах) – група адміністраторів друкування
- Server Operators (створюється лише на серверах) – група операторів сервера, що за умовчанням має дещо більші повноваження, ніж звичайні користувачі

- В доменах Windows існують також наперед визначені глобальні групи, спільні для усіх комп’ютерів домену:
  - Domain Admins – адміністратори домену
  - Domain Users – користувачі домену
  - Domain Guests – гості домену

Стандартні типи об’єктів доступу Windows (1/3)

1. Файлові об’єкти
   - файли
   - дискові директорії (каталоги)
   - пристрої – об’єкти, що використовуються для взаємодії застосувань з драйверами фізичних і логічних пристроїв
   - канали (pipes) – об’єкти, що використовуються для організації взаємодії процесів
   - поштові скриньки (mailslots) – об’єкти, що використовуються для асинхронної передачі повідомлень між процесами
2. Об’єктові директорії (англ. – object directories) – об’єкти, що містять в собі інші об’єкти. На відміну від дискових директорій, об’єктові директорії можуть містити в собі будь-які об’єкти.
3. Ключі реєстру (англ. – registry keys)
4. Процеси – екземпляри програм, що виконуються в поточний момент на цьому комп’ютері
5. Потоки або нитки (англ. – threads) – ланцюги машинних команд, що послідовно виконуються в цей момент на цьому комп’ютері

Стандартні типи об’єктів доступу Windows (2/3)

6. Диспетчер сервісів (англ. – Service Control Manager) – об’єкт Windows, що використовується для керування сервісами
7. Сервіси (англ. – services) – програмні модулі ОС Windows NT, керування якими здійснюється диспетчером сервісів
   - Сервіси Windows NT дуже подібні до драйверів, і керування ними здійснюється аналогічно, але на відміну від драйверів сервіси виконуються в режимі користувача, а не ядра
8. Об’єкти керування вікнами (англ. – window-management objects):
   - робочі столи (англ. – desktops) – сукупності вікон, що взаємодіють між собою; вікна різних робочих столів не можуть бути видимими на екрані комп’ютера одночасно;
   - віконні станції (англ. – window stations) – сукупності робочих столів, на різних віконних станціях можуть одночасно працювати різні користувачі.
9. Порти (англ. – ports) – об’єкти, що використовуються під час передачі повідомлень між процесами
10. Секції розділюваної пам’яті (англ. – shared memory sections) – області пам’яті, що розділяються між кількома процесами

Стандартні типи об’єктів доступу Windows (3/3)

11. Символічні зв’язки (англ. – symbolic links) – об’єкти, що дозволяють створювати синоніми для імені об’єкта
12. Маркери доступу (англ. – access tokens) – об’єкти, що містять інформацію про користувачів і псевдокористувачів, які працюють в системі
13. Об’єкти синхронізації:
    - події (англ. – events) – об’єкти, що використовуються при асинхронних зверненнях до файлових систем і пристроїв
    - пари подій (англ. – event pairs) – об’єкти, що використовуються при передаванні повідомлень від одного процесу до іншого
    - семафори (англ. – semaphores) – об’єкти, що використовуються для обмеження кількості одночасних звернень різних потоків до одного об’єкта
    - м’ютекси (англ. – mutexes) – об’єкти, що використовуються для виключення одночасного доступу кількох потоків до одного об’єкта ОС

- Файли, дискові директорії та ключі реєстру є постійними об’єктами і можуть зберігатись на дисках комп’ютера. Всі решта об’єктів є тимчасовими і зберігаються лише в оперативній пам’яті.

Методи доступу

- Загалом ОС Windows підтримує 22 методи доступу суб’єктів до об’єктів
- 6 з них підтримуються для об’єктів усіх типів, а саме:
  - видалення об’єкта,
  - отримання атрибутів захисту об’єкта,
  - зміна атрибутів захисту об’єкта,
  - зміна власника об’єкта,
  - отримання та зміна параметрів аудиту по відношенню до об’єкта (ACCESS_SYSTEM_SECURITY),
  - синхронізація (SYNCHRONIZE).
- Названі методи є стандартними методами доступу
- Для кожного типу об’єктів також підтримуються до 16 типів *специфічних методів доступу*

Специфічні методи доступу для деяких об’єктів (1/3)

Об’єкт	Методи доступу
Файл	• зчитування, • записування, • додавання інформації в кінець файлу • виконання, • отримання атрибутів, • зміна атрибутів, • отримання розширених атрибутів, • зміна розширених атрибутів.
Дисковий каталог	• перегляд, • створення нового файлу, • створення піддиректорії, • прохід (traverse), • видалення файла або піддиректорії, • отримання атрибутів, • зміна атрибутів, • отримання розширених атрибутів, • зміна розширених атрибутів.

Об’єкт	**Методи доступу**
Ключ реєстру	• зчитування значень, • зміна значень, • створення підключа, • перелік підключів, • вимога сповіщення при доступі до ключа іншого потоку, • створення символічного зв’язку.
Процес	• завершення, • створення нового потоку, • зміна атрибутів сторінок адресного простору, • зчитування адресного простору, • записування в адресний простір, • дублювання дескриптора, • отримання пріоритету, • зміна пріоритету.

Специфічні методи доступу для деяких об’єктів (2/3)

Об’єкт	Методи доступу
Потік	o завершення, o призупинка / поновлення, o отримання контексту, o зміна контексту, o отримання пріоритету, o зміна пріоритету, o призначення маркера доступу.
Сервіс	o запуск, o зупинка, o призупинка / поновлення, o отримання поточного стану, o оновлення поточного стану, o перелік залежних сервісів, o отримання конфігурації, o зміна конфігурації, o специфічний для цього сервісу метод доступу

Об’єкт	**Методи доступу**
Диспетчер сервісів	o підключення, o отримання статусу списку сервісів, o перелік сервісів, o створення нового сервісу, o блокування списку сервісів.
Робочий стіл	o зчитування елементів робочого столу, o зміна елементів робочого столу, o створення вікна, o створення меню, o встановлення фільтру (hook setting), o записування макрокоманди (journal recording), o відтворення макрокоманди (journal playback), o перелік, o відображення робочого столу на екрані.

Специфічні методи доступу для деяких об’єктів (3/3)

Об’єкт	Методи доступу
Віконна станція	o зчитування вмісту екрана, o закриття, o отримання атрибутів, o звернення до буферу обміну (clipboard), o звернення до таблиці атомів, o створення нового робочого столу, o перелік робочих столів, o перелік самої віконної станції.
Секція	o отримання інформації про поточний стан, o відображення для зчитування, o відображення для записування, o відображення для виконання, o зміна розміру.

Об’єкт	Методи доступу
Маркер доступу	o зчитування, o отримання інформації про підсистему, що створила маркер доступу, o вмикання / вимикання груп, o вмикання / вимикання привілеїв, o зміна атрибутів захисту по умовчанню, o призначення процесу, o призначення потоку, o копіювання.
Подія	o отримання стану, o зміна стану.
Семафор	o отримання стану, o зміна стану.
М’ютекс	o отримання стану, o зміна стану.

Спеціальні привілеї

- Частина методів доступу вимагають від суб’єкта доступу спеціальних привілеїв. До таких методів належать:
  - створення нового сервісу;
  - блокування списку сервісів;
  - запуск сервісу;
  - зупинка сервісу;
  - призупинення / поновлення сервісу;
  - призначення процесу маркера доступу;
  - отримання або зміна параметрів аудиту по відношенню до об’єкта.

Права доступу

- Специфічні
  - Кожному специфічному методу доступу, що підтримується для певного типу об’єктів, відповідає право на його здійснення
- Стандартні
  - Кожному стандартному методу доступу, за виключенням ACCESS_SYSTEM_SECURITY, також відповідає право доступу
- Загальні (*generic*) або відображувані (*mapped*)
  - Відображувані права доступу введені, головним чином, для сумісності з програмним інтерфейсом POSIX, який підтримує лише три права доступу, що визначені для усіх типів об’єктів, – зчитування, записування і виконання.
- Віртуальні
  - Віртуальні права доступу можуть бути запитані суб’єктом, але не можуть бути йому наданими

Відображувані права доступу

- До них відносяться:
  - зчитування (GENERIC_READ)
  - записування (GENERIC_WRITE)
  - виконання (GENERIC_EXECUTE)
  - усі дії (GENERIC_ALL)
- Кожне з відображуваних прав доступу є певною комбінацією стандартних і специфічних прав доступу
  - Відображуване право доступу надає можливість здійснити деякий набір методів доступу до об’єкта
- Відображувані права можуть бути наданими для доступу до об’єкта будь-якого типу
  - Конкретний зміст таких прав залежить від типу об’єкта, оскільки включає певні специфічні права.
- Процес перетворення відображуваного права доступу в набір стандартних і специфічних прав доступу називається *відображенням прав доступу*
  - Порядок відображення для об’єктів конкретного типу визначається при реєстрації цього типу об’єктів

Відображення права “зчитування”

- Для об’єкта типу “файл” це право дозволяє здійснювати доступ до об’єкта за методами:
  - зчитування файла,
  - отримання DOS-атрибутів файла,
  - отримання розширених атрибутів файла,
  - отримання атрибутів захисту файла,
  - синхронізація.
- В той самий час для об’єкта типу “ключ реєстру” це право дозволяє здійснювати доступ до об’єкта за методами:
  - зчитування значень ключа,
  - перелік підключів ключа,
  - вимога сповіщення при доступі до ключу іншого потоку,
  - отримання атрибутів захисту ключа,
  - синхронізація.

Віртуальні права доступу

- Віртуальні права доступу можуть бути запитані суб’єктом, але не можуть бути йому наданими.
- Існують два віртуальних права доступу:
  - MAXIMUM_ALLOWED,
  - ACCESS_SYSTEM_SECURITY.
- Якщо суб’єкт запитує віртуальне право MAXIMUM_ALLOWED, він в результаті отримує доступ до об’єкта за максимальною для цього суб’єкта множиною методів
  - Тобто, йому будуть надані всі методи, на які він має права
- Право ACCESS_SYSTEM_SECURITY – це право на здійснення однойменного стандартного методу доступу
  - Право є віртуальним, тому що насправді можливість доступу суб’єкта за цим методом контролюється відповідним привілеєм суб’єкта, який надає суб’єкту право доступу за цим методом до всіх без виключення об’єктів доступу
  - Заборонити чи дозволити доступ за цим методом конкретного суб’єкта до конкретного об’єкта неможливо.