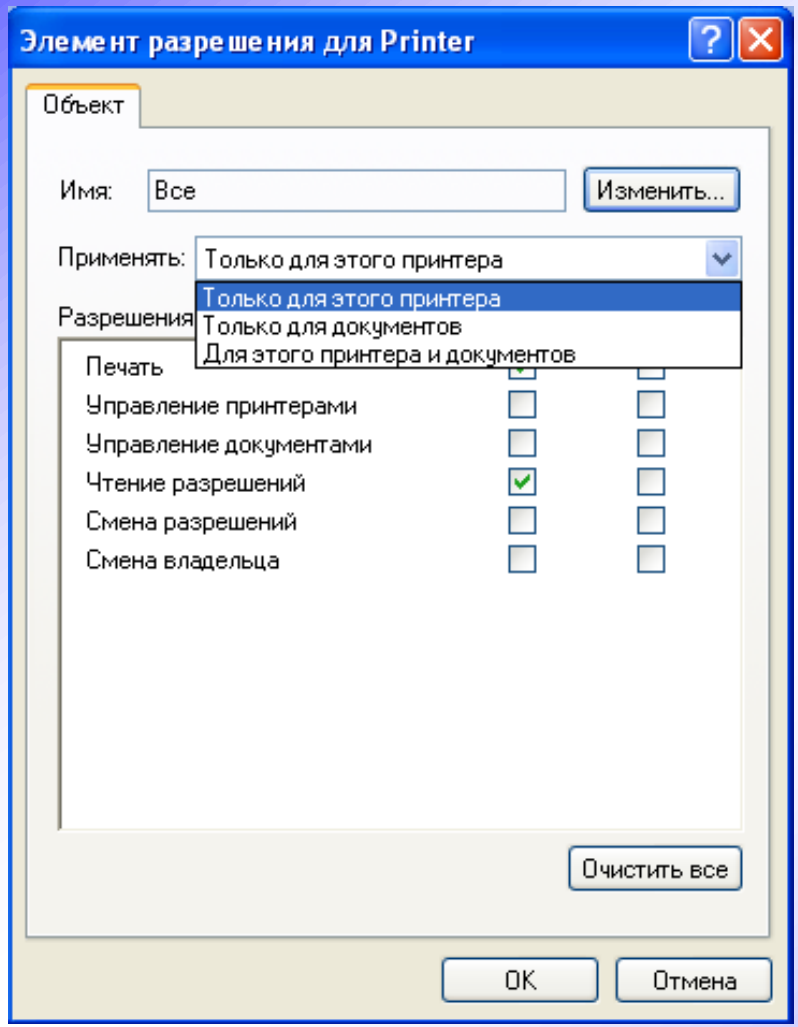
Лекция №6

Управление доступом к ресурсам ОС

(часть 3)

Разграничение доступа к устройствам

Управление доступом к принтеру в Windows XP



- Управление принтерами – возможность установки свойств принтера, его предоставления в общий доступ.
- Управление документами – возможность приостановки, отмены, возобновления печати.

Разграничение доступа к устройствам

- Разграничение доступа к устройствам позволяет определять разрешения на доступ к различным устройствам и портам, а также тип доступа к ним.
- Возможно разграничение доступа на уровне интерфейса (порта) и на уровне экземпляра устройства (съёмное устройство, принтеры, жёсткие диски и т.д).
- Часть устройств проверяется на обоих уровнях, часть – только на одном.

Разграничение на уровне интерфейса

- ИК-порт – устройства, которые могут быть подключены к компьютеру через инфракрасный порт (чтение, запись).
- FireWire-порт – устройства, подключаемые к FireWire-порту, кроме хабов (чтение, запись, форматирование, извлечение).
- USB-порт – устройства, подключаемые к USB-порту, кроме хабов (чтение, запись, форматирование, извлечение).

Разграничение на уровне интерфейса

- Параллельный порт – устройства, подключаемые через параллельный порт (LPT) (чтение, запись).
- Последовательный порт – устройства, подключаемые через последовательный порт (COM), включая внутренние модемы (чтение, запись).

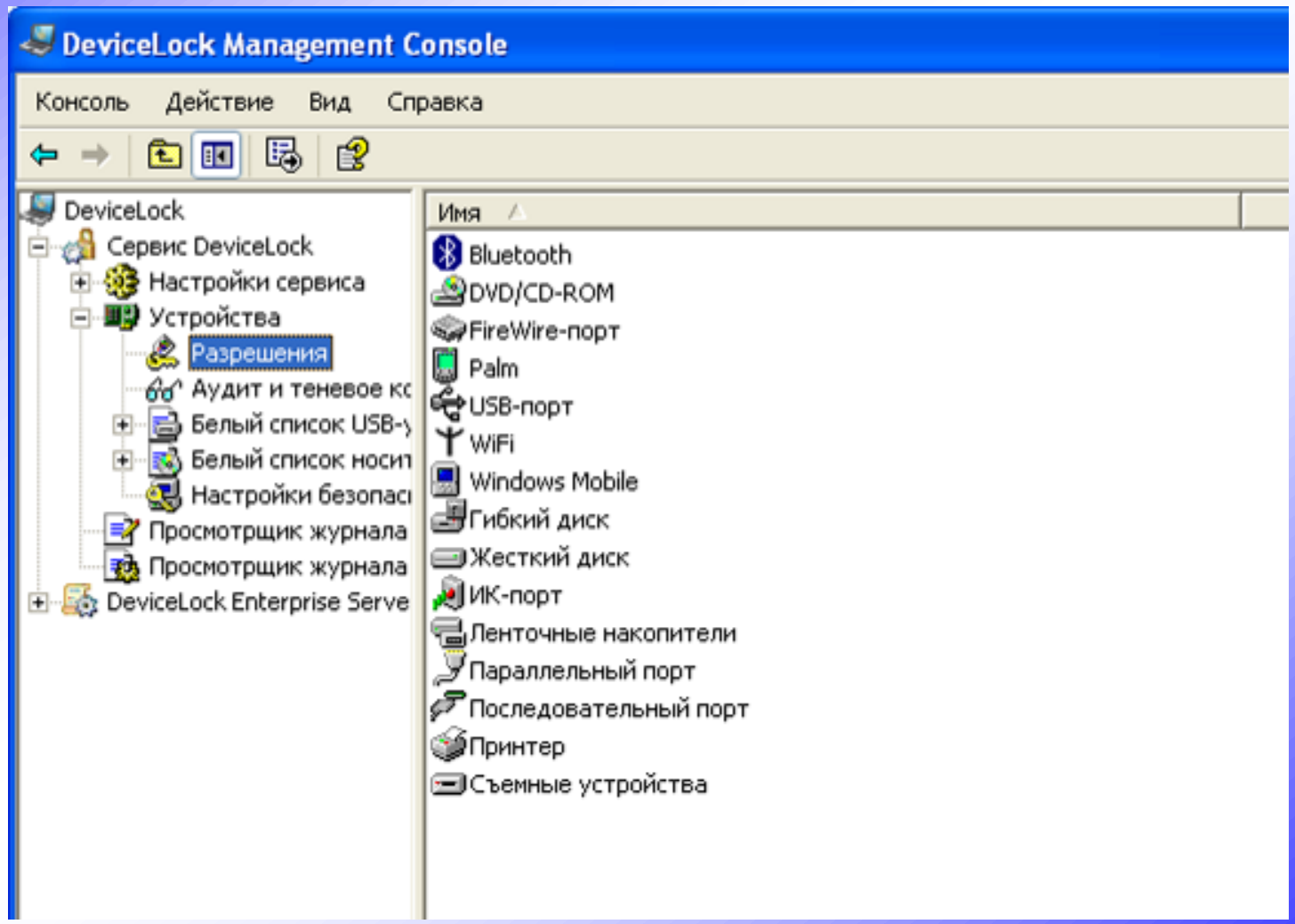
Разграничение на уровне экземпляра устройства

- Устройства «Bluetooth» (чтение, запись).
- CD/DVD-приводы (чтение, запись).
- Устройства, работающие под управлением ОС для мобильных телефонов (чтение, запись, специальные ограничения).
- Дисководы гибких дисков (чтение, запись, форматирование, извлечение).
- Внешние и внутренние ленточные накопители (чтение, запись, форматирование, извлечение).

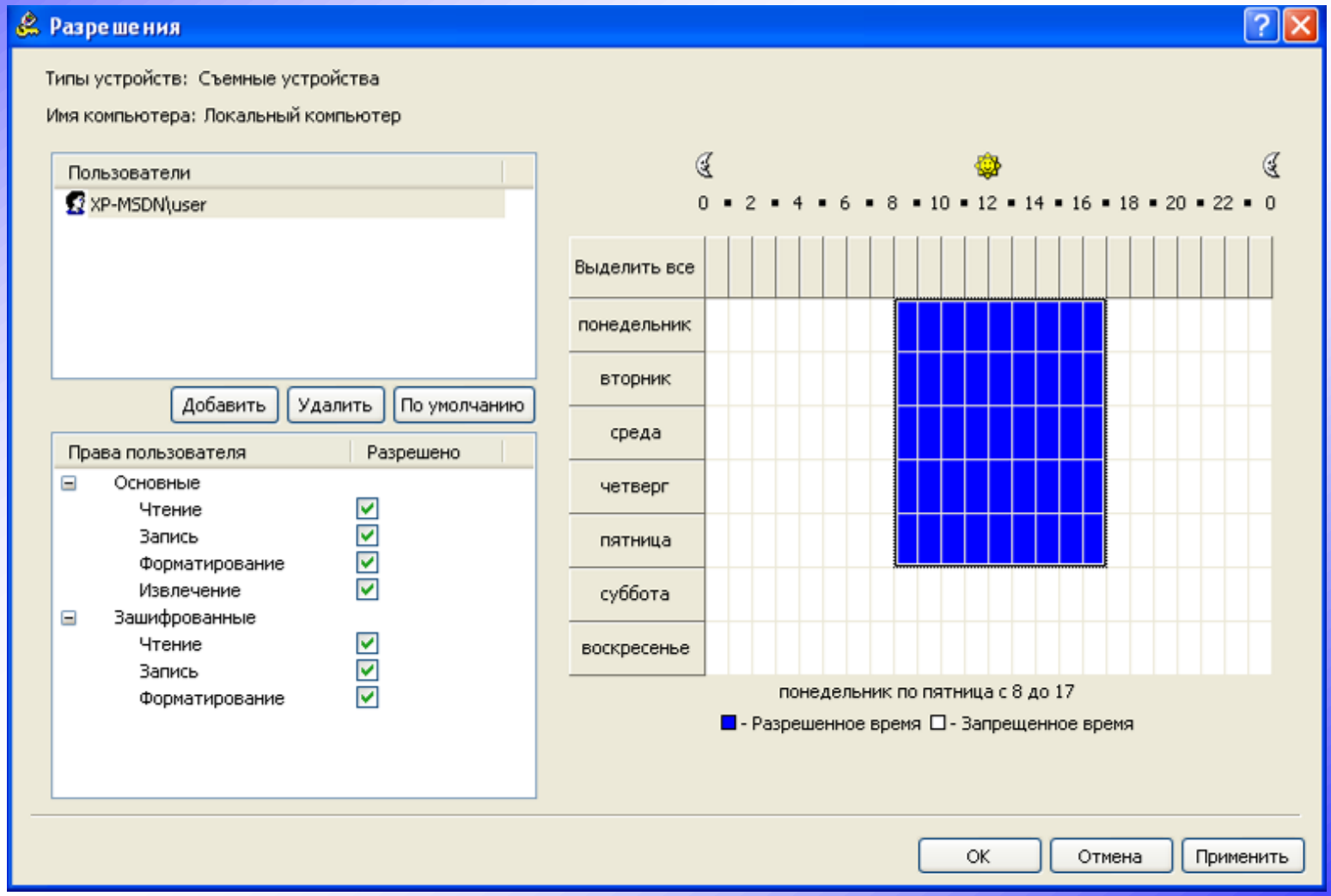
Разграничение на уровне экземпляра устройства

- WiFi – WiFi-адаптеры (чтение, запись).
- Внешние и внутренние жёсткие диски (чтение, запись, форматирование).
- Принтер – локальные, сетевые, виртуальные принтеры (печать).
- Съёмные устройства – устройства, распознаваемые ОС «Windows» как сменные накопители (чтение, запись, форматирование, извлечение).

Перечень устройств для разграничения доступа



Возможности разграничения доступа к устройствам



Белый лист устройств

Белый лист устройств позволяет исключить конкретное устройство из общего списка разрешённых или запрещённых устройств данного типа по одному из правил:

- исключает все устройства одной и той же модели.
- исключает конкретное уникальное устройство.

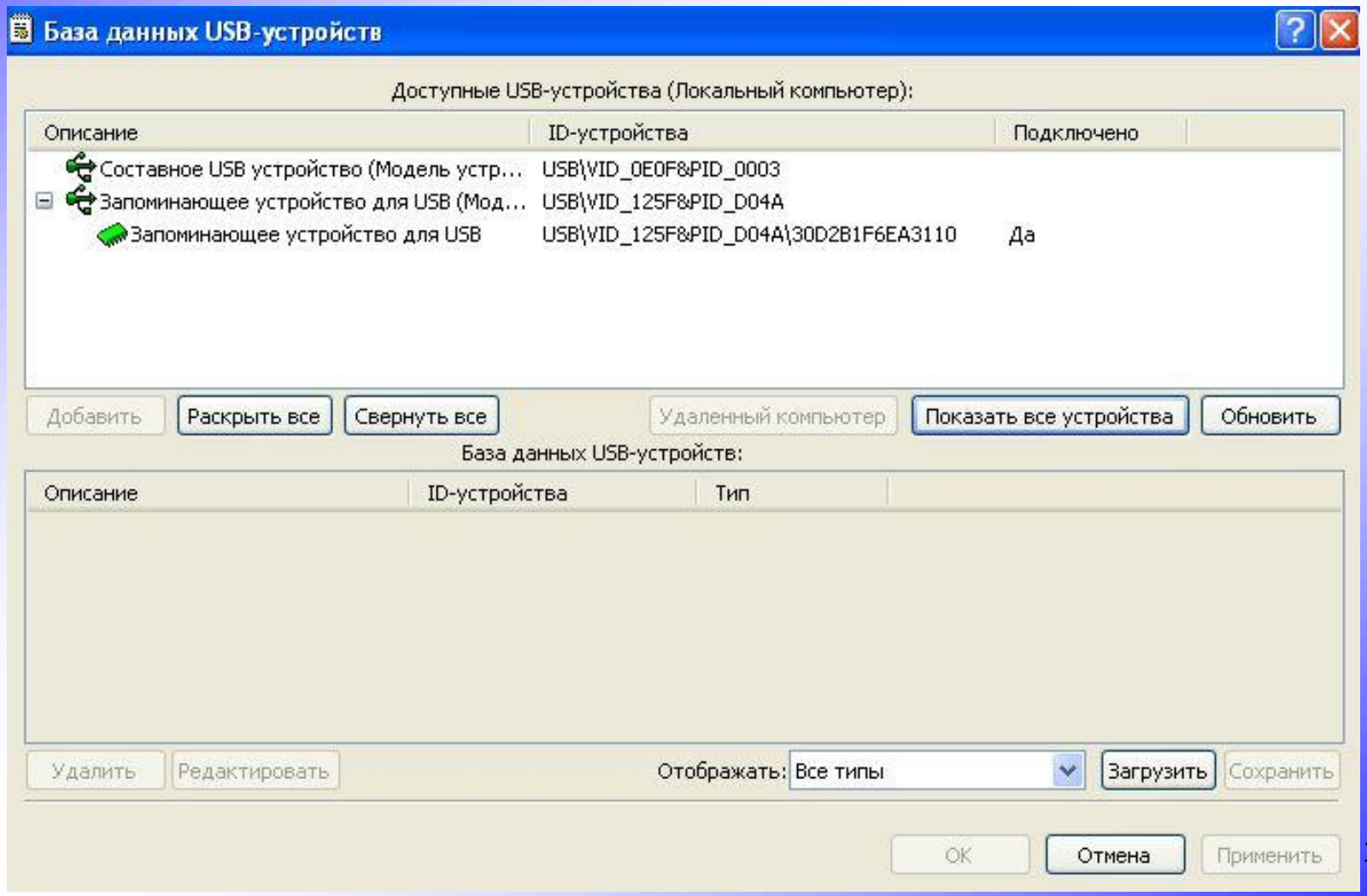
Исключение всех устройств одной модели

- Каждое устройство идентифицируется по комбинации идентификатора производителя (VID) и продукта (PID).
- Все устройства данной модели данного производителя будут распознаны как одно устройство.

Исключение уникального устройства

- Каждое устройство идентифицируется по комбинации идентификатора производителя (VID), продукта (PID) и серийного номера.
- Устройство может быть добавлено в белый список как уникальное устройство только в том случае, если производитель присвоил ему серийный номер на этапе изготовления.

Включение устройства в белый список



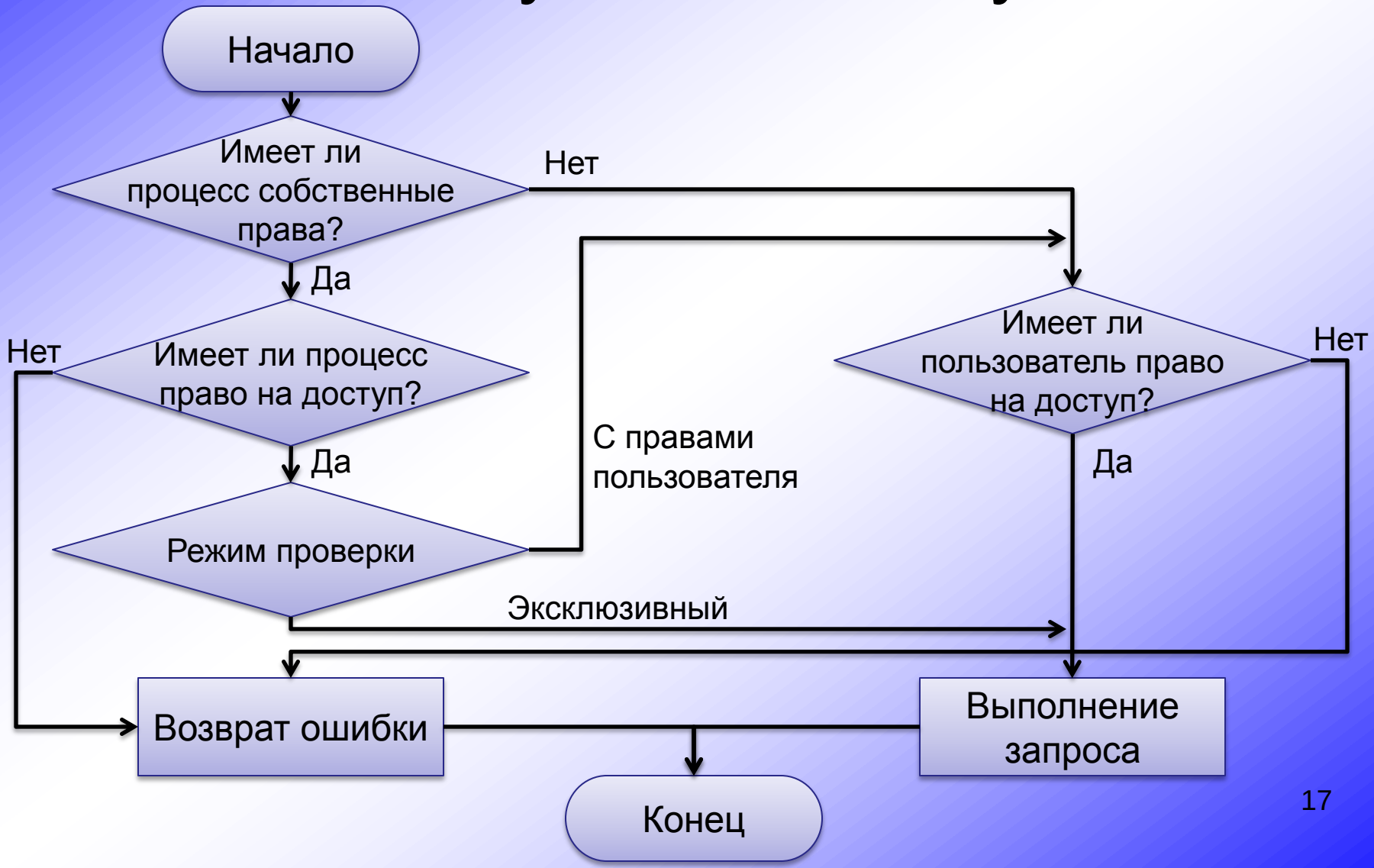
Разграничение доступа на уровне процессов

Требования к диспетчеру доступа при учёте процессов

Диспетчером доступа по отношению к объектам должны реализовываться следующие возможности:

- разграничение прав доступа процессов к объектам вне разграничений прав пользователей;
- разграничение прав доступа пользователей к объектам вне разграничений прав процессов;
- комбинированное разграничение прав доступа – разграничение прав доступа процессов к объектам в рамках разграничений прав пользователей (совместное разграничение доступа процессов и пользователей).

Обработка диспетчером запроса доступа к объекту



Локализация прав доступа приложений к ресурсам

При работе с виртуальными машинами (макросы для Office, JVM) несанкционированные действия могут выполняться под именем санкционированного процесса, поэтому необходимо:

- выделить отдельный каталог для работы приложений;
- запретить доступ к другим приложениям и системному диску.

При работе с базами данных к файлам, содержащим таблицы, должен быть разрешён доступ только приложениям со встроенными средствами разграничения доступа на уровне таблиц.

Разграничение доступа к программному обеспечению

Механизм обеспечения замкнутости программной среды

Механизм обеспечения замкнутости программной среды – управление запуском программ в системе (запрет на запуск всех программ, кроме санкционированных).

Способы реализации:

- в виде задания списков исполняемых файлов;
- в виде задания каталогов исполняемых файлов.

Задание списков исполняемых файлов

Механизм состоит в задании для каждого пользователя списка файлов, которые ему разрешено запускать.

Требования к корректности функционирования механизма:

- исполняемый файл должен быть задан с указанием его полного пути;
- пользователю должен быть запрещён запуск программ с внешних устройств ввода (локальных и общих), а также из общих папок;
- пользователю должен быть задан список разрешённых исполняемых файлов (к ним разрешён доступ на «выполнение», а к остальным файлам – запрещён);
- пользователю должен быть запрещён доступ на «изменение» исполняемых файлов и системного диска.

Недостатки задания списков исполняемых файлов

- Необходимо перечислять в списках все процессы, разрешённые к запуску пользователем, в том числе и процессы, порождаемые уже разрешёнными процессами.
- Усложнение администрирования при добавлении и удалении программ (и связанных с ними процессов).

Задание каталогов исполняемых файлов

- Пользователю задаётся каталог, откуда ему разрешено запускать программы (разрешён доступ на «выполнение», запрещён доступ на «изменение»).
- В данный каталог администратор устанавливает программы, разрешённые пользователю для запуска.
- Ко всем остальным каталогам, а также к устройствам (съёмным дискам, CDROM и т.д.), разделяемым сетевым ресурсам пользователю должен быть запрещён доступ на «выполнение».
- К системному диску, а также к каталогам с исполняемыми файлами остальных пользователей должен быть запрещён доступ на «изменение».

Политика ограниченного использования программ

- Политика ограниченного использования программ (ПОИП) позволяет идентифицировать программы, запускаемые в ОС Windows и разрешать или запрещать их выполнение на локальном компьютере.

Уровни безопасности ПОИП

- Неограниченный – программное обеспечение выполняется со всеми правами пользователя, вошедшего в систему (не выполняются только исключения).
- Не разрешено – приложения не могут быть запущены (выполняются только исключения).

Правила ПОИП

- Правило для хеша.
- Правило для сертификата.
- Правило для пути.
- Правило для зоны Интернета.

Правило для хеша

- Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл.
- При создании правила для хеша вычисляют хеш для программы. Когда пользователь пытается открыть программу, хеш программы сравнивается с существующим правилом.
- Хеш переименованного или перемещенного в другую папку файла не изменяется. Однако при любом изменении файла значение хеша изменяется, позволяя обойти ограничения.

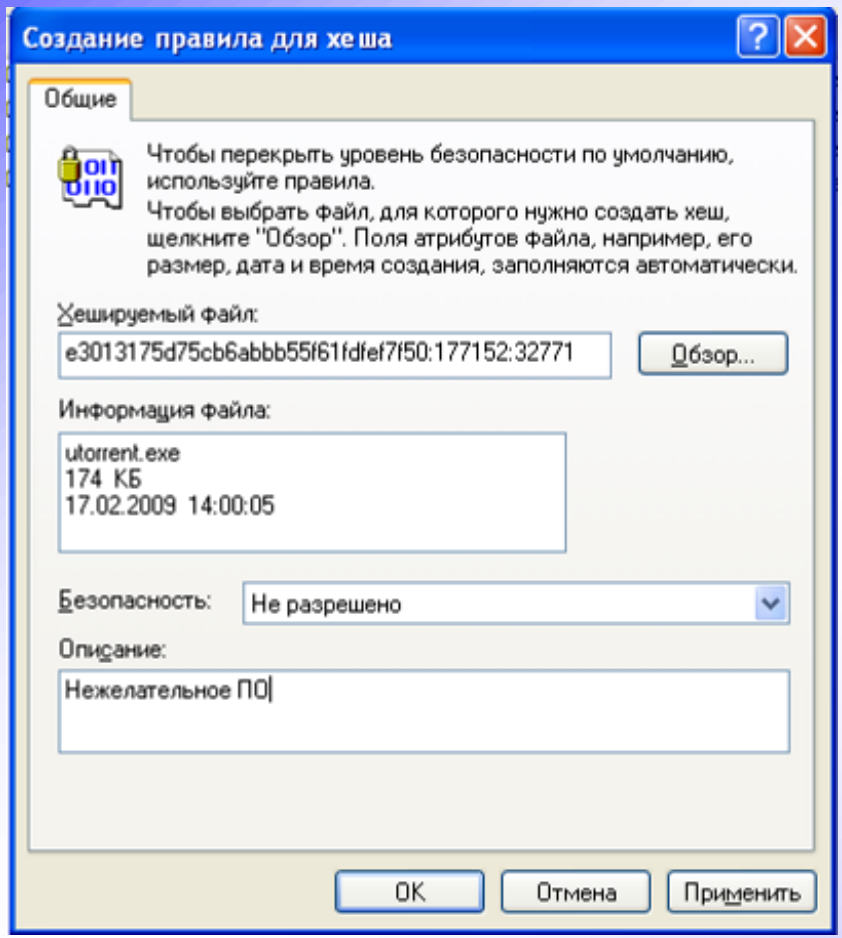
Правило для сертификата

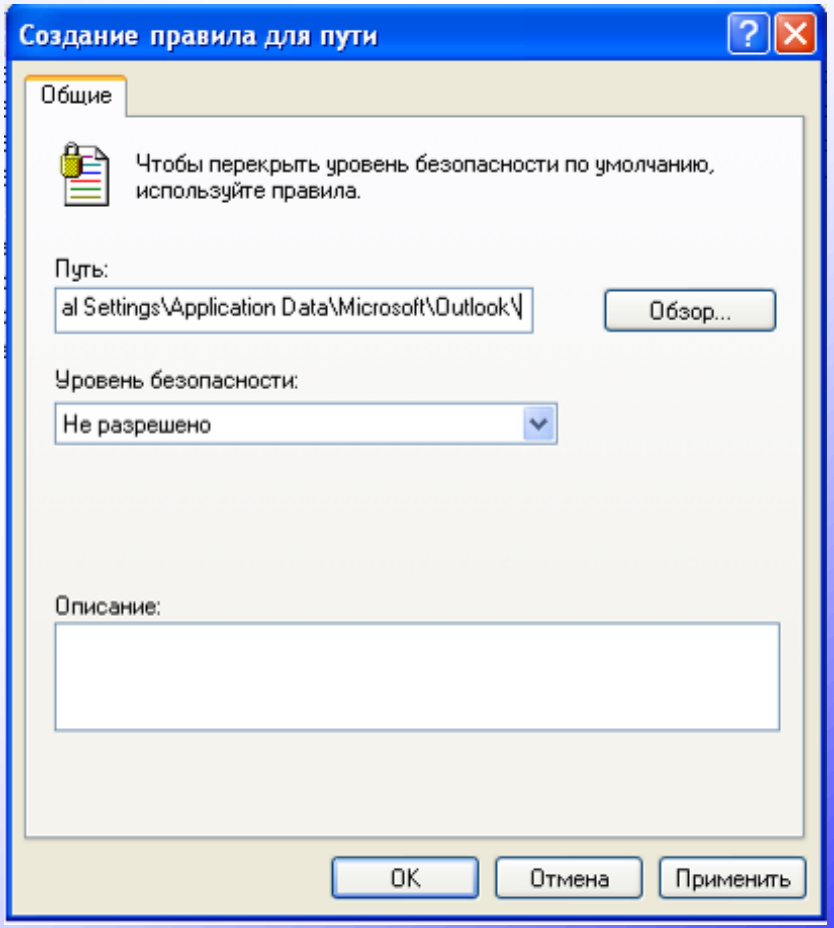
- Имеется возможность создать правило для сертификата, идентифицирующее приложение и затем, в зависимости от уровня безопасности, позволяющее или не позволяющее его запустить.
- Например, можно использовать правила для сертификатов, чтобы автоматически доверять программам из проверенного источника.

Правило для пути

- Правило для пути идентифицирует программы по пути к файлу.
- Например, при уровне безопасности по умолчанию «не разрешено» можно разрешить полный доступ к указанной папке для всех пользователей.
- Могут быть использованы некоторые общие пути: %userprofile%, %windir%, %appdata%, %programfiles% и %temp%. Можно создавать правила для пути в реестре, использующие раздел реестра программы как его путь.

Создание правил для хеша и пути





Правило для зоны Интернета

- Правила для зоны влияют только на пакеты установщика Windows. Правило для зоны идентифицирует программное обеспечение из зоны, указанной посредством «Internet Explorer».
- Такими зонами являются Интернет, интрасеть, «Ограниченные узлы», «Надежные узлы».

Приоритеты использования правил

- Правило для хеша.
- Правило для сертификата.
- Правило для пути. При конфликте правил для пути приоритет имеет правило с большим ограничением. Набор путей в порядке от высшего приоритета (наибольшее ограничение) к низшему приоритету.
  - диск:\папка1\папка2\имя_файла.расширение
  - диск:\папка1\папка2*.расширение
  - *.расширение
  - диск:\папка1\папка2\
  - диск:\папка1\
- Правило для зоны Интернета.

Управление разграничением доступа

Множество субъектов доступа

Классы пользователей:

- администратор;
- пользователь, решающий прикладные задачи;
- пользователь «система» – виртуальный пользователь ОС.

Классы процессов:

- системные (привилегированные) процессы;
- прикладные процессы;
- скрытые или неидентифицируемые (процессы виртуальных машин).

Множество объектов доступа

Классы файловых объектов данных:

- системные каталоги и файлы, каталоги и файлы настроек ОС;
- пользовательские каталоги и файлы данных, включая сетевые;
- Разделы и подразделы реестра.

Классы файловых объектов программ:

- системные исполняемые файлы привилегированных процессов – системных процессов ОС и процессов защиты;
- пользовательские исполняемые файлы (исполняемые файлы пользовательских приложений).

Множество объектов доступа

Классы санкционированных устройств (установленных в ОС):

- устройства (дисковод, CD-ROM, принтер и т.д.), как локальные, так и сетевые (разделяемые в сети);
- отчуждаемые физические носители информации для устройств ввода/вывода (дисковод, CD-ROM и т.д.);
- файловые объекты (каталоги и файлы) на отчуждаемых физических носителях информации для устройств ввода/вывода (дисковод, CD-ROM и т.д.).

Неустановленные в системе устройства ввода/вывода:

- коммуникационные порты компьютера, к которым могут быть подключены устройства.

Множество действий субъектов доступа над объектами.

Категории доступа:

- категория доступа «запись» (установка категории доступа «запись» означает разрешение доступа на запись и чтение);
- категория доступа «чтение»;
- категория доступа «добавление» (установка категории доступа «добавление» означает разрешение записи с предотвращением возможности затирания и модификации информации, располагаемой в объекте доступа, и запрет чтения);
- категория доступа «исполнение» («запуск»);
- запрет любого доступа.

Рассмотренные вопросы

- Разграничение доступа на уровне процессов.
- Способы реализации механизма обеспечения замкнутости программной среды.
- Разграничение доступа к устройствам.

Всем спасибо – все свободны,

если нет вопросов