Лекция №4

Управление доступом к ресурсам ОС

(часть 1)

Задачи механизмов управления доступом

Основная задача – разграничение доступа субъектов (пользователей и запускаемых ими процессов) к защищаемым информационным и техническим ресурсам – объектам.

Задачи механизмов управления доступом

- У прикладного пользователя не должно быть возможности работы с информацией, устройствами ввода-вывода, каналами связи, к которым ему запрещён доступ.
- В системе не должна предоставляться возможность несанкционированного обмена данными между пользователями (механизм санкционированного обмена данными должен предоставляться).
- Прикладной пользователь не должен иметь доступ к настройкам, связанным с безопасностью системы.

Требования к управлению доступом

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Дискреционный принцип контроля доступа (6 класс):

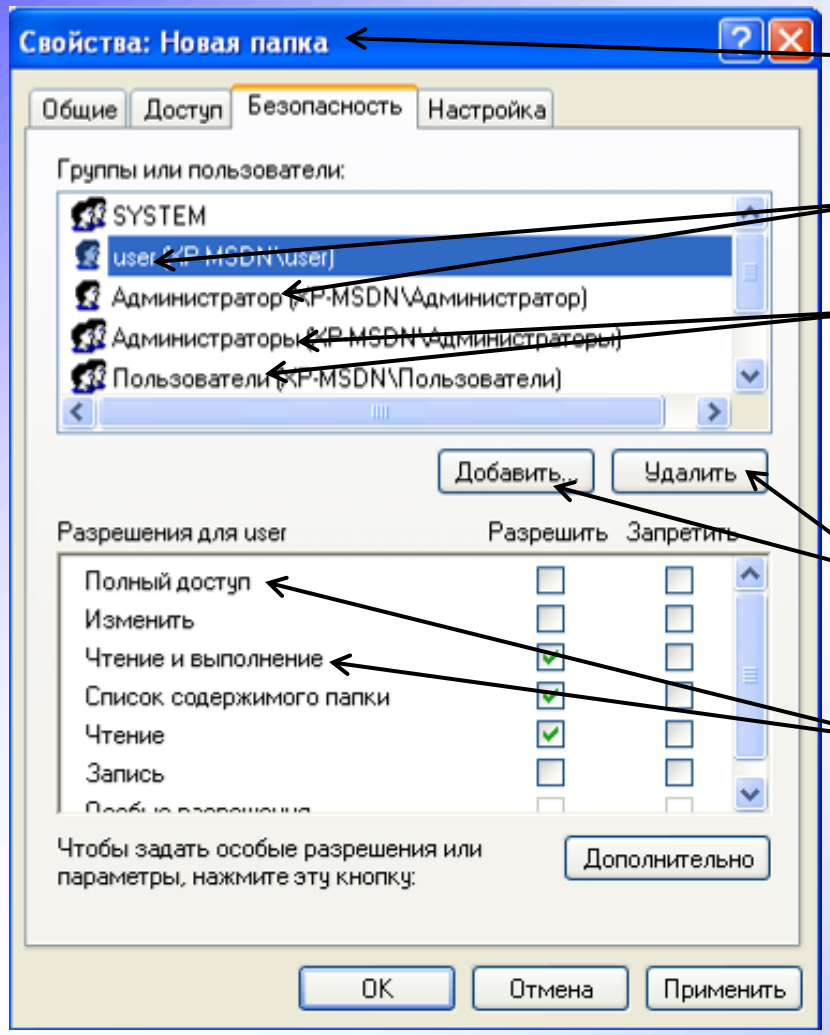
- комплекс систем защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.);
- для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту);
- КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Дискреционный принцип контроля доступа (6 класс):

- контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов);
- механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил разграничения доступа (ПРД), в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов;
- права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.);
- 5 класс: должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Дискреционное разграничение доступа в Windows



Наименованный объект

Наименованные субъекты

Группы субъектов

Изменение списка пользователей

Типы доступа

Пример матрицы доступа

Пример матрицы доступа для субъектов:

- «Администратор»;
- группа «Пользователи».

	Администратор	Пользователи
Программа1	чтение, запись, выполнение	чтение, выполнение
Принтер1	печать, управление очередью	печать
Съёмные носители	чтение, запись	чтение

Преимущества и недостатки дискреционной модели

Преимущества:

- гибкость настроек доступа – любому субъекту можно назначить индивидуальные права доступа.

Недостаток:

- усложнение администрирования системы при задании настроек, поддержании их в актуальном состоянии, а также при вводе в систему новых пользователей и ресурсов (усложнение администрирования может привести к большему количеству ошибок при разграничении доступа).

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Дискреционный принцип контроля доступа (4 класс):

- КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств – системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" – иные действия, в том числе с использованием собственных программ работы с устройствами;
- дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД;
- дискреционные ПРД должны быть эквивалентны мандатным правилам, т.е. всякий запрос на доступ должен быть санкционированным или несанкционированным одновременно и по дискреционным, и по мандатным ПРД (2 класс).

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Мандатный принцип контроля доступа (4 класс и выше):

- для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа;
- КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Мандатный принцип контроля доступа (4 класс и выше):

- КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

  субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

Требования к системе защиты по РД ГТК «СВТ. Защита от НСД»

Мандатный принцип контроля доступа (4 класс и выше):

субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта;

- реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

Мандатное управление доступом

- Мандатное управление доступом – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Метки конфиденциальности

- Метки конфиденциальности чаще всего являются иерархическими, описывая т.н. полномочия.
- Метки конфиденциальности характеризуют:
  - уровень доступа к информации (при назначении субъектам доступа);
  - уровень конфиденциальности (при назначении объектам доступа).
- Пример иерархических меток: «Общедоступно», «Конфиденциально» и «Строго конфиденциально».

Реализация мандатного управления доступом

- Формальное сравнение метки субъекта, запросившего доступ, и метки объекта, к которому запрошен доступ.
- Принятие решения о предоставлении доступа на основе правил, направленных на противодействие снижению уровня конфиденциальности защищаемой информации.

Пример набора правил доступа

- Субъект может читать объект, только если уровень метки субъекта в иерархии не ниже, чем уровень метки объекта.
- Субъект осуществляет запись в объект, только если уровень метки субъекта равен уровню метки объекта.

Формальное представление правил доступа

- Субъект С имеет доступ к объекту О на «Чтение» в случае, если выполняется условие $Mc \geq Mo$.
- Субъект С имеет доступ к объекту О на «Запись» в случае, если выполняется условие $Mc = Mo$.

Представление правил в виде матрицы доступа

	Мс=Общедоступно	Мс=Конфиденцально	Мс=Строго конфиденцально
Мо=Общедоступно	Чт/Зп	0	0
Мо=Конфиденцально	Чт	Чт/Зп	0
Мо=Строго конфиденцально	Чт	Чт	Чт/Зп

Результат использования правил доступа

- Запрет чтения файла с меткой «Конфиденциально» субъектом с меткой (уровнем доступа) «Общедоступно».
- Возможность контроля потоков информации, защищающего конфиденциальные данные от разглашения (при попытке копирования информации из файла с меткой «Конфиденциально» в файл с меткой «Общедоступно» субъект будет вынужден повысить уровень конфиденциальности общедоступного файла).

Преимущества и недостатки многоуровневой модели

Преимущество:

- более простое администрирование по сравнению с дискреционной моделью, что приводит к меньшему количеству ошибок.

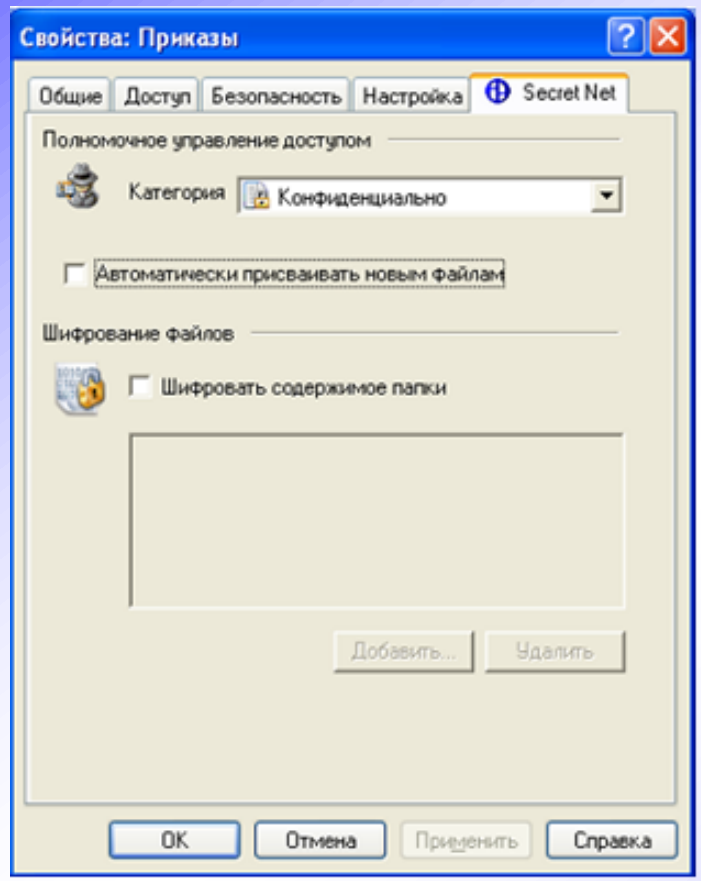
Недостаток:

- отсутствует разграничение доступа в пределах одного уровня конфиденциальности.

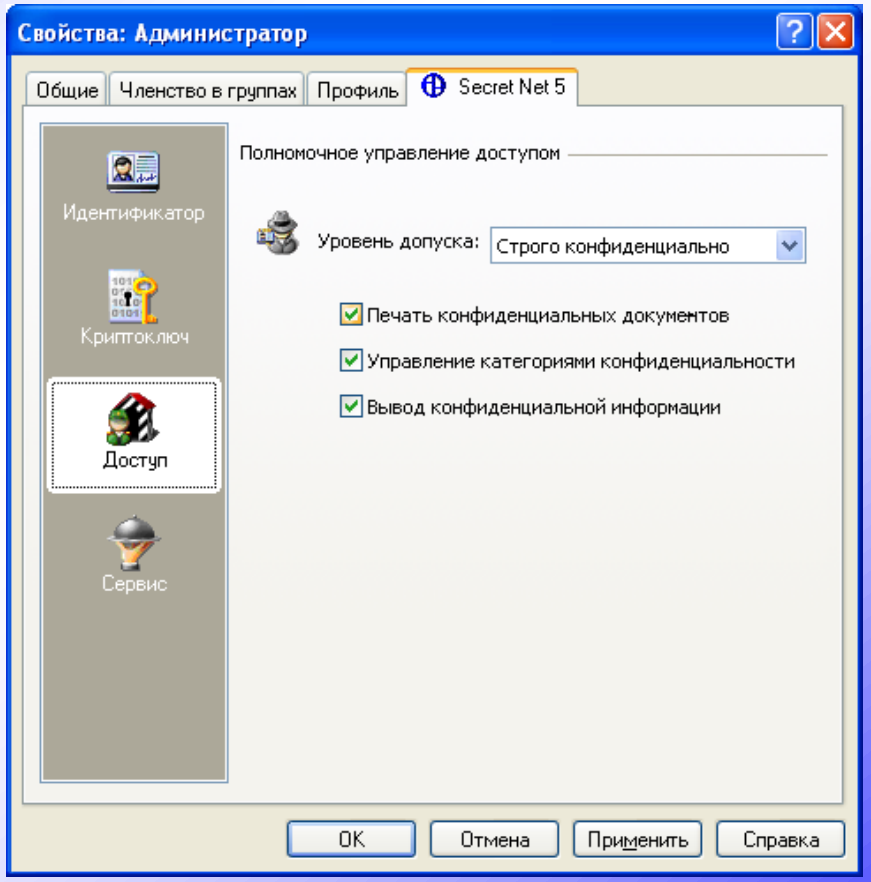
Упрощение администрирования

- Мандатное управление доступом позволяет при создании новых объектов или изменении прав доступа настраивать только один параметр – метку, что приводит к упрощению администрирования.

Реализация мандатного механизма



Присвоение метки объекту



Присвоение метки субъекту

Требования к системе защиты по «Базовому профилю защиты»

Класс «Защита данных пользователя»:

- ФБО должны осуществлять политику дискреционного управления доступом для списка субъектов и поименованных объектов и для всех операций между субъектами и объектами, на которые распространяется данная политика.
- ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

  для каждой операции должно быть правило(а), когда атрибуты безопасности субъекта соответствуют атрибутам управления доступом объекта;

  для каждой операции должно быть заданное по умолчанию правило, которое используется, когда атрибуты безопасности субъекта не соответствуют атрибутам безопасности объекта.

Требования к системе защиты по «Базовому профилю защиты»

Класс «Управление безопасностью»:

- ФБО должны осуществлять политику дискреционного управления доступом, чтобы предоставлять возможность запроса и изменения значения атрибутов безопасности объекта только уполномоченным администраторам и владельцам объекта;
- ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с пользователями, в пределах области действий функций безопасности только уполномоченным администраторам;
- отмена значимых для безопасности разрешений должна быть немедленной (например, при удалении учётных данных пользователя доступ немедленно прекращается).

Требования к системе защиты по «Базовому профилю защиты»

ФБО должны поддерживать следующие роли:

- уполномоченного администратора;
- уполномоченные пользователи (т.е. пользователи, уполномоченные на использование некоторых ресурсов ОО);
- владелец объекта (пользователи, уполномоченные политиками дискреционного управления доступом на изменение значений атрибутов безопасности объекта);
- пользователи, уполномоченные на модификацию их собственных данных аутентификации;
- пользователи, не проходящие аутентификацию и получающие доступ к общедоступным объектам, если такие объекты существуют.

ФБО должны быть способны ассоциировать пользователей с ролями. ФБО должны требовать точный запрос для принятия следующих ролей: уполномоченного администратора; уполномоченных пользователей и др.

Права доступа к файловым объектам

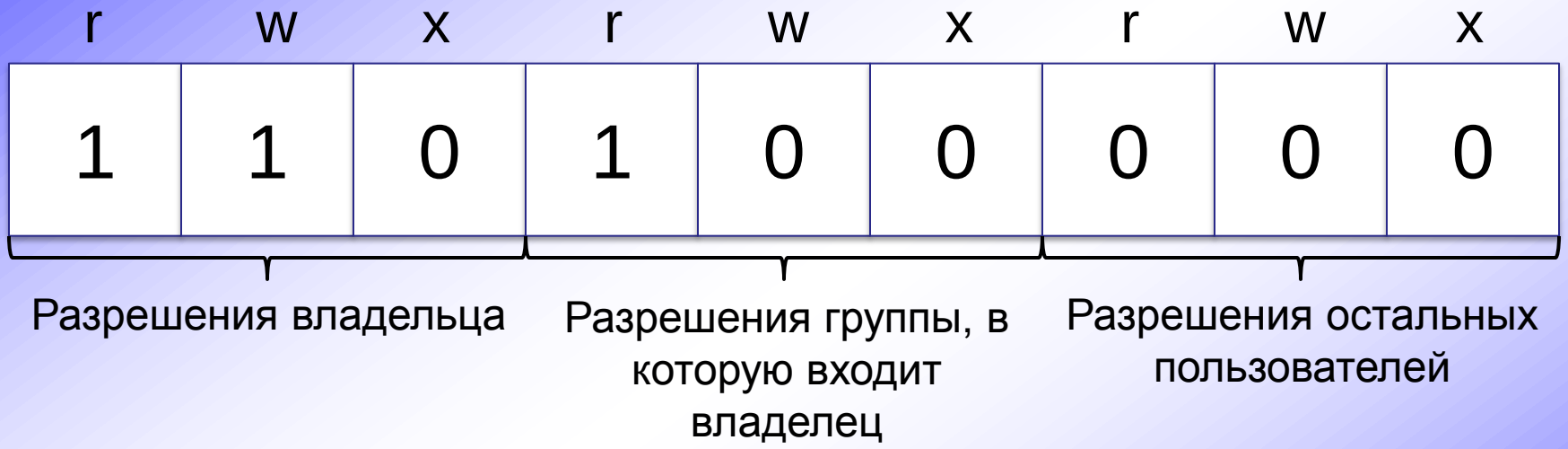
Права доступа к файлам в Unix-системах

- Каждому объекту (файлу, каталогу) присваивается набор атрибутов (16 бит), определяющих тип файла и разрешения на доступ к нему.
- Разрешения на доступ (последние 9 бит) устанавливаются для владельца объекта, группы владельца и остальных пользователей.
- Перечень разрешений для файлов: r – право на чтение; w – право на запись; x – право на выполнение.
- Перечень разрешений для каталогов: r – право на получение списка файлов в каталоге; w – право на создание файлов в каталоге; x – право на переход в каталог.

Формат поля, определяющего тип файла в UNIX-системах

- 4 бита определяют тип файла: 1000 – обычный файл; 0100 – каталог; 0110 – файл блочного устройства; 0010 – файл символьного устройства; 1010 – доменное гнездо (socket); 0001 – именованный канал (pipe); 1100 – символическая ссылка (link).
- 5-й бит – если равен 1, то исполняемый файл выполняется от имени владельца.
- 6-й бит – если равен 1, то исполняемый файл выполняется от имени группы владельца.
- 7-й бит – если равен 1, то удалить файл может только владелец файла, иначе любой имеющий доступ к файлу.

Формат поля прав доступа к объектам в UNIX-системах



В примере:

- владелец имеет право читать и изменять файл;
- пользователи, входящие в группу владельца, имеют право читать файл;
- остальные пользователи не имеют доступа к файлу.

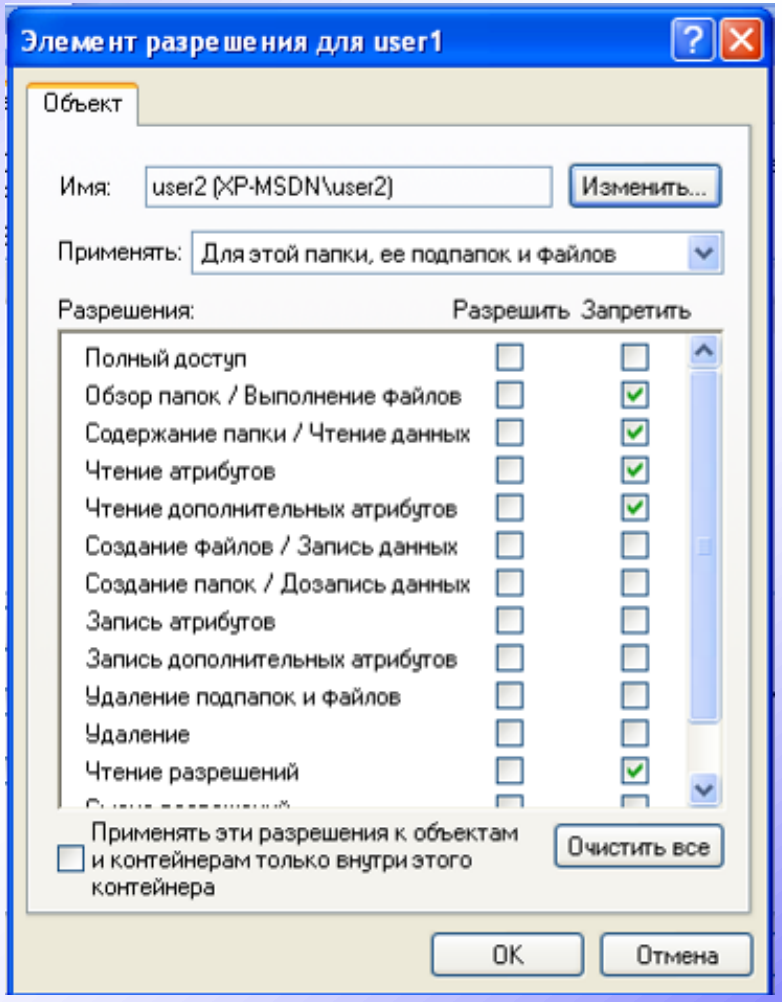
Права доступа в Windows

- Изменить – разрешает пользователям удалять файлы и папки, вносить изменения в разрешения или получать право собственности на файл или папку от другого пользователя.
- Чтение и выполнение – разрешает пользователям читать и запускать файлы, не внося изменений в содержание совместно используемого тома или папки.
- Список содержимого папки – позволяет пользователям просматривать содержимое папок.

Права доступа в Windows

- Чтение – разрешает пользователям просматривать содержимое тома или папки. Они также могут открывать файлы, но не имеют права сохранять изменения.
- Запись – разрешает пользователям делать записи в папках или томах, но запрещает открывать файлы или просматривать список файлов.

Дополнительные права доступа



Обзор папок/Выполнение файлов

- Для папок. Обзор папки применяется только к папкам. Это разрешение позволяет или запрещает пользователю перемещаться по папкам, чтобы перейти к другим папкам или файлам, даже если пользователь не имеет разрешений на обзор папок. Разрешение Обзор папки имеет действие только в том случае, если группе или пользователю не предоставлены права на Обход перекрёстной проверки. Обход перекрёстной проверки проверяет права пользователя в оснастке «Групповая политика». По умолчанию группе «Все» предоставлено право на Обход перекрёстной проверки.
- Для файлов. Выполнение файла разрешает или запрещает доступ к программным файлам, которые выполняются.
- Если разрешение на Обзор папки задано для папки, то разрешение Выполнение файла не задается автоматически для всех файлов этой папки.

Содержание папки/Чтение данных

- Содержание папки позволяет или запрещает пользователю просматривать имена файлов и вложенных папок в этой папке. Содержание папки применяется только к папкам и распространяется только на содержимое папки. Это разрешение не отменяется, если папка, для которой устанавливается разрешение, указана в списке папок.
- Чтение данных применяется только к файлам и разрешает или запрещает пользователям просматривать содержимое файла.

Чтение атрибутов и дополнительных атрибутов

- Чтение атрибутов разрешает или запрещает пользователям просматривать атрибуты папки или файла, такие как «только чтение» или «скрытый». Атрибуты определяются файловой системой NTFS.
- Чтение дополнительных атрибутов разрешает или запрещает пользователям просматривать дополнительные атрибуты папки или файла. Дополнительные атрибуты определяются программами и могут варьироваться в зависимости от используемой программы.

Создание файлов/Запись данных

- Создание файлов применяется только к папкам и разрешает или запрещает пользователям создавать файлы в папке.
- Запись данных применяется только к файлам и разрешает или запрещает пользователям изменять файл или переписывать существующее содержание с помощью NTFS.

Создание папок/Дозапись данных

- Создание папок применяется только к папкам и разрешает или запрещает пользователям создавать папки в папке.
- Дозапись данных применяется только к файлам и позволяет или запрещает пользователям вносить изменения в конце файла. Это разрешение не касается изменения, удаления или перезаписи существующих данных.

Запись атрибутов

- Запись атрибутов позволяет или запрещает пользователям изменять атрибуты папок или файлов, такие как «только чтение» или «скрытый». Атрибуты определяются файловой системой NTFS.
- Запись атрибутов не подразумевает наличие прав на создание и удаление файлов или папок. Это разрешение включает только право на внесение изменений в атрибуты файла или папки.

Запись дополнительных атрибутов

- Запись дополнительных атрибутов позволяет или запрещает пользователям изменять дополнительные атрибуты папки или файла. Дополнительные атрибуты определяются программами и могут варьироваться в зависимости от используемой программы.
- Запись дополнительных атрибутов не подразумевает наличие прав на создание или удаление файлов или папок. Это разрешение позволяет только вносить изменения в атрибуты файла или папки.

Удаление подпапок и файлов и удаление

- Удаление подпапок и файлов распространяется только на папки и позволяет или запрещает пользователям удалять вложенные папки или файлы, даже если папке или файлу не назначено разрешение на удаление.
- Удаление разрешает или запрещает пользователям удалять папку или файл. Если разрешение на удаление файла или папки отсутствует, то их можно удалить в том случае, если вы имеете разрешение на удаление подпапок и файлов для родительской папки.

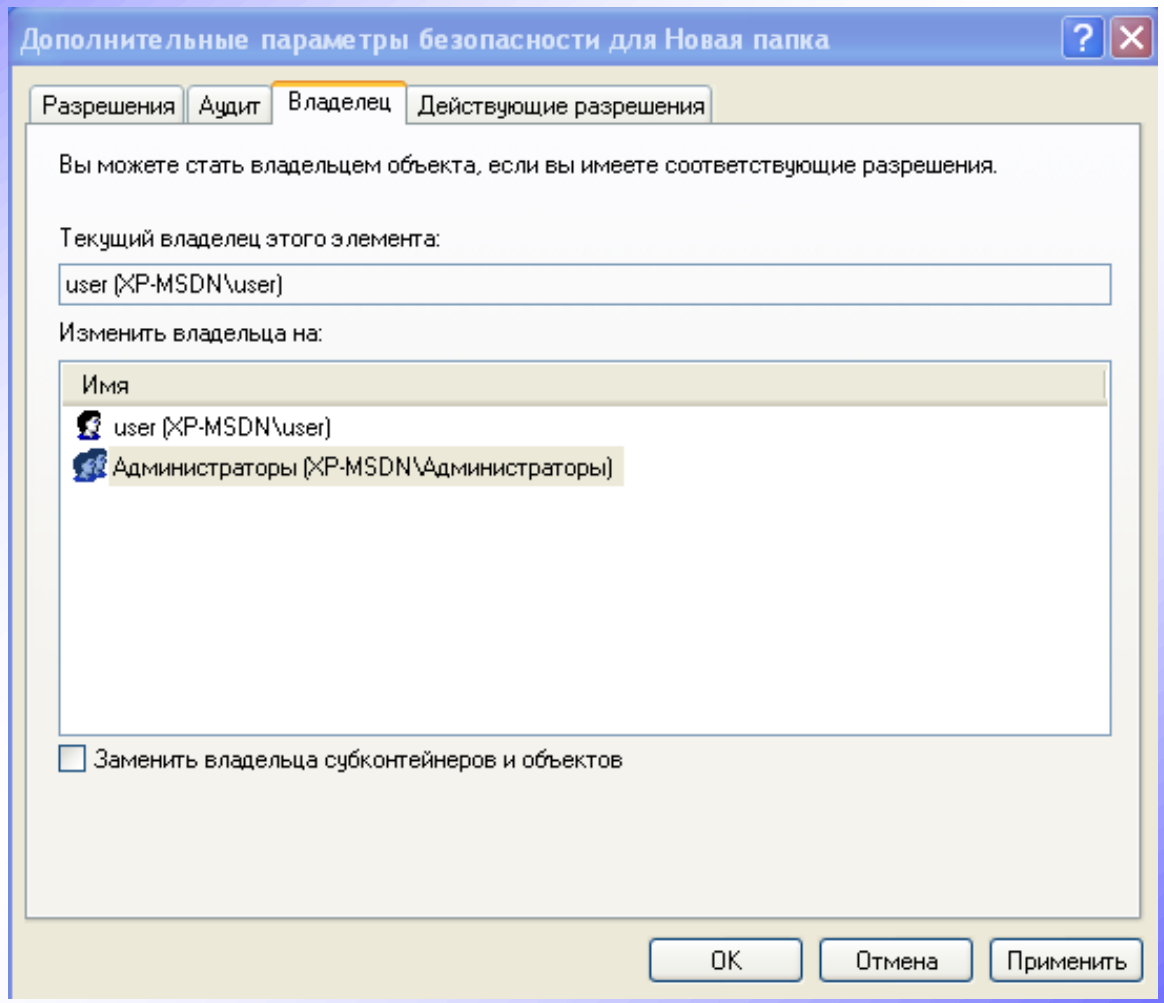
Чтение, изменение разрешений, смена владельца

- Чтение разрешений позволяет или запрещает пользователям читать разрешения для папки или файла, такие как Полный доступ, Чтение и Запись.
- Изменение разрешений позволяет или запрещает пользователям изменять разрешения для папки или файла, такие как Полный доступ, Чтение и Запись.
- Смена владельца разрешает или запрещает пользователю изменять владельца файла или папки. Владелец файла или папки может изменять их разрешения, несмотря на любые существующие разрешения, которые защищают файл или папку.

Проблема «Владельца» файла

- Возможность изменять права доступа к файлу, кроме администратора, предоставляется владельцу этого файла (пользователю, создавшему данный файл).
- Угроза от владельца файла: пользователь, имеющий право чтения файла с конфиденциальной информацией, может скопировать эту информацию в созданный файл и предоставить доступ к новому файлу пользователям без доступа к конфиденциальной информации.

Назначение «владельца» файла в Windows



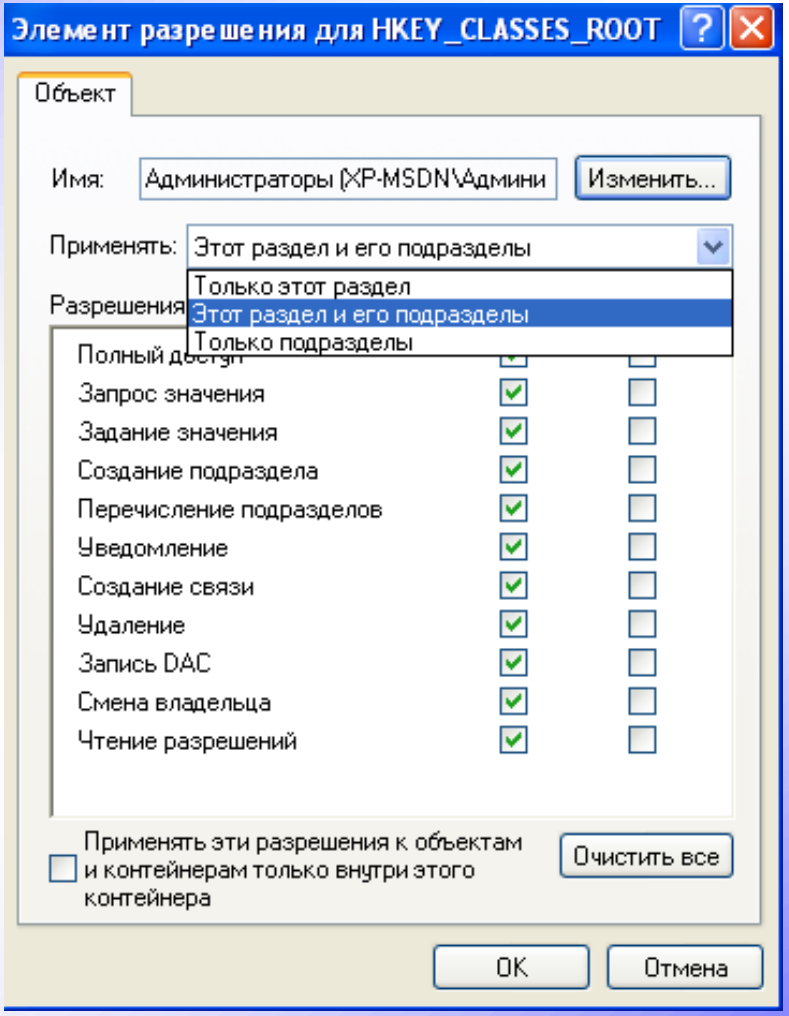
Управление доступом к реестру в Windows XP

- Действия с ключами – запрос и задание значения.
- Действия с вложенными разделами – перечисление и создание подразделов.
- Действия с разрешениями – чтение разрешений, запись DAC, смена владельца.
- Действия с текущим разделом – удаление, создание связи (аналогично связи между Users и CurrentUser).

Управление доступом к реестру в Windows XP

- Разграничение доступа возможно только к разделам (к ключам невозможно).
- Базовое разрешение «Чтение» включает в себя: запрос значения; перечисление подразделов; чтение разрешений; уведомление.

Управление доступом к реестру в Windows XP



Рассмотренные вопросы

- Требования к разграничению доступа, входящие в руководящие документы.
- Дискреционная и мандатная модели управления доступом.
- Типы доступа в UNIX-системах.
- Типы доступа в Windows.

Всем спасибо – все свободны,

если нет вопросов