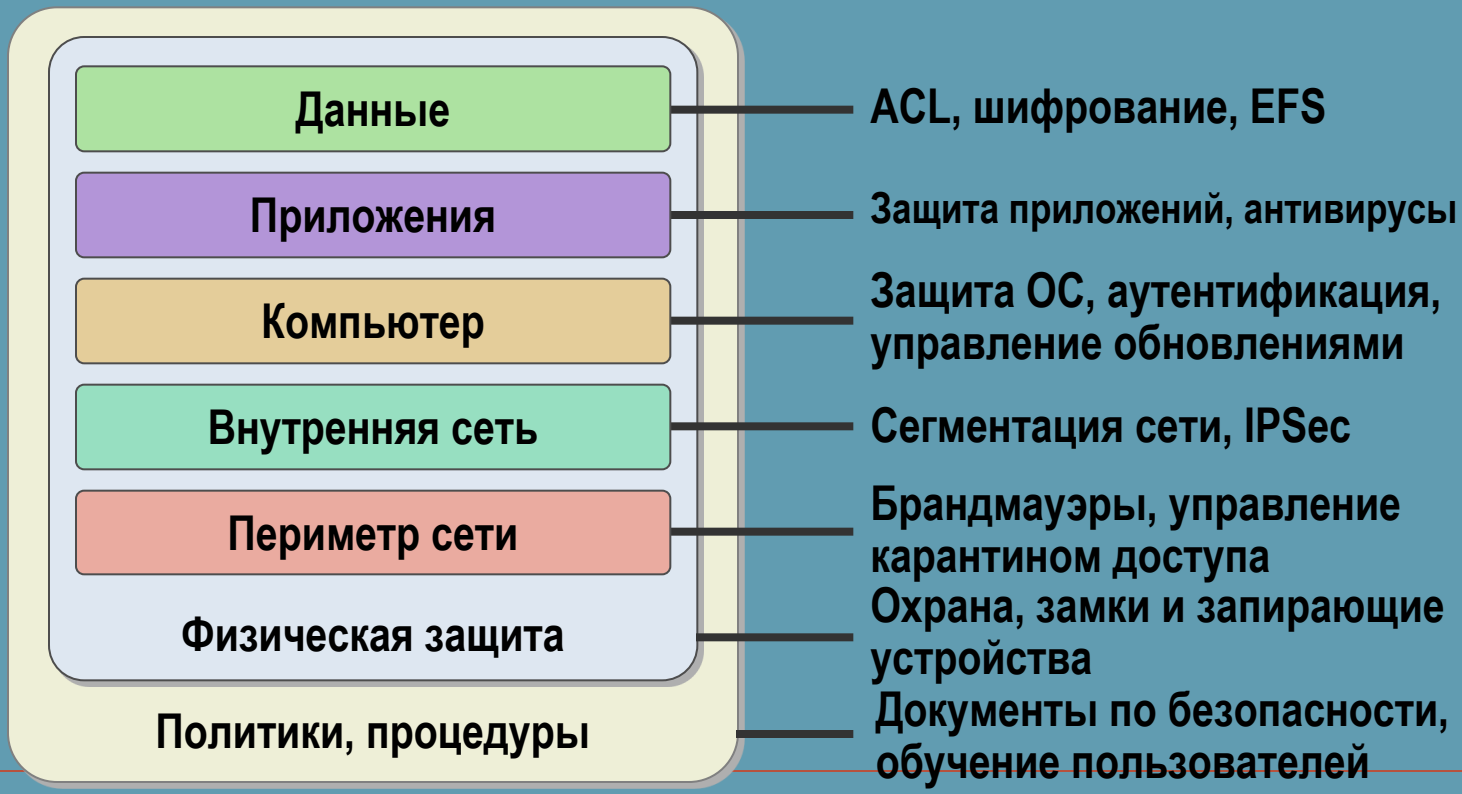
Администрирование информационных систем

Механизмы обеспечения безопасности данных

Модель многослойной защиты

Использование многослойной модели защиты позволяет:

- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**



Модель многослойной защиты

Использование многослойной модели защиты позволяет:

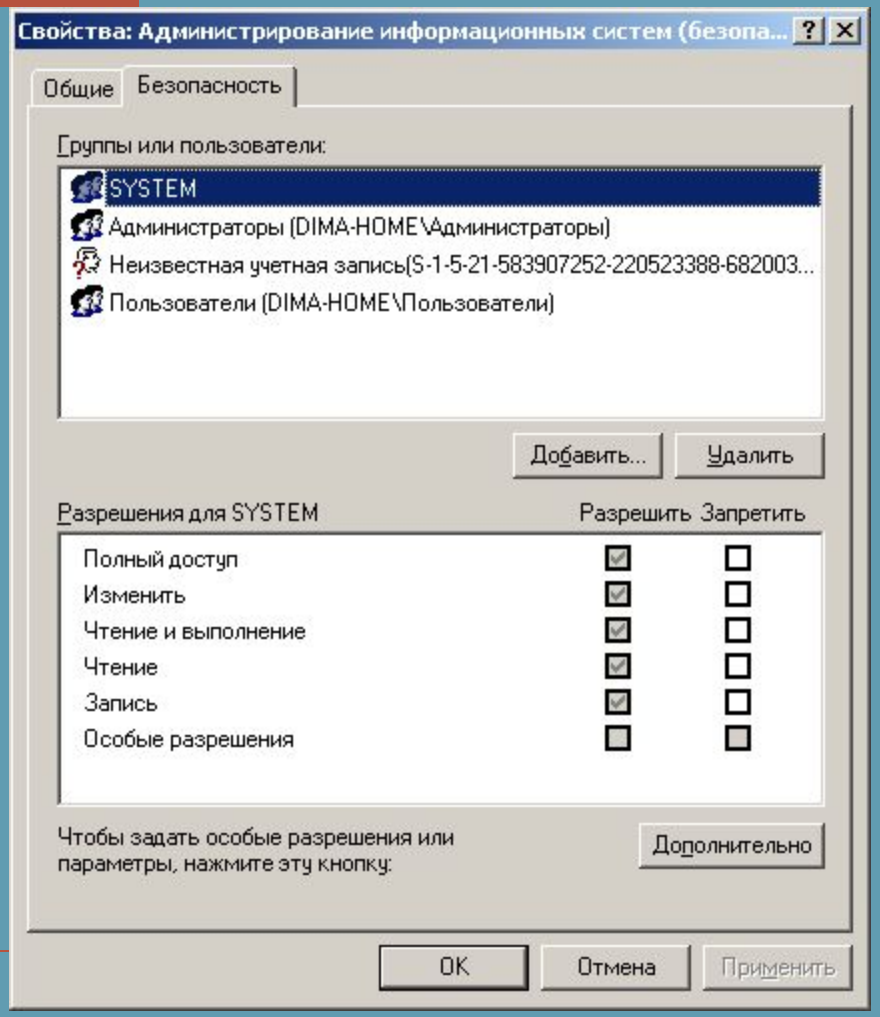
- **Уменьшить шанс успеха атаки**
- **Увеличить вероятность обнаружения атаки**

Управление доступом

- Одним из средств защиты данных является механизм управления доступом.
- Управление доступом на уровне данных в ОС Windows 2000/XP/2003 эффективно выполняется на носителях с файловой системой NTFS.
- Файловая система NTFS обеспечивает поддержку хранения списков прав доступа (ACL) и механизм их использования при выдаче разрешений и запретов на операции с файлами и каталогами.

Управление доступом

- Управление доступом к локальным папкам и каталогам на разделах NTFS выполняется с помощью специальной закладки **Безопасность** в окне **Свойство** папки или каталога.
- Управляющие кнопки **Добавить** и **Удалить** обеспечивают управление пользователями, нижнее окно позволяет устанавливать разрешения для выбранного объекта.
- Поддерживается групповое управление.



Управление доступом

- Для управления разрешениями в режиме командной строки используется команда cacls.
- **Синтаксис данной команды**:
  - **cacls** *имя_файла* [**/t**] [**/e** [**/r** *пользователь* [*…*]]] [**/c**] [**/g** *пользователь*:*разрешение*] [**/p** *пользователь*:*разрешение* [*…*]] [**/d** *пользователь* [*…*]]
- **Ключи команды**:
  - **/t** - Изменение таблиц контроля доступа (DACL) указанных файлов в текущем каталоге и всех подкаталогах
  - **/e** - Редактирование таблицы управления доступом (DACL) вместо ее замены
  - **/r** *пользователь* - Отмена прав доступа для указанного пользователя. Недопустим без параметра **/e**
  - **/c** - Продолжение внесения изменений в таблицы управления доступом (DACL) с игнорированием ошибок
  - **/g** *пользователь*:*разрешение* – Предоставление прав доступа указанному пользователю
  - **/p** *пользователь*:*разрешение* - Смена прав доступа для указанного пользователя
  - **/d** *пользователь* - Запрещение доступа для указанного пользователя

Шифрование данных

- Шифрованная файловая система (Encrypting File System, EFS) позволяет безопасно хранить данные. EFS делает это возможным благодаря шифрованию данных в выбранных файлах и папках файловой системы NTFS.
- Файлы и папки на томах с файловой системой FAT не могут быть зашифрованы или расшифрованы.
- EFS разработана для безопасного хранения данных на локальных компьютерах. Поэтому она не поддерживает безопасную передачу файлов по сети.

Ключи шифрования

- *Шифрование* файлов происходит следующим образом:
  - Каждый файл имеет уникальный *ключ шифрования файла*, который позже используется для расшифровки данных файла.
  - Ключ шифрования файла сам по себе зашифрован — он защищен **открытым ключом** пользователя, соответствующим сертификату EFS.
  - Ключ шифрования файла также защищен открытым ключом каждого дополнительного пользователя EFS, уполномоченного расшифровывать файлы, и ключом каждого **агента восстановления**.
- Сертификат и закрытый ключ системы EFS могут быть выданы несколькими источниками. Сюда входит автоматическое создание сертификатов и выдача сертификатов центрами сертификации (ЦС) корпорации Майкрософт или сторонними центрами сертификации

Расшифровывание данных

- *Расшифровка* файлов происходит следующим образом:
  - Для расшифровки файла необходимо сначала расшифровать его ключ шифрования. Ключ шифрования файла расшифровывается, если **закрытый ключ** пользователя совпадает с открытым.
  - Не только пользователь может расшифровать ключ шифрования файла. Другие назначенные пользователи или агенты восстановления также могут расшифровать ключ шифрования файла, используя собственный закрытый ключ.
- Закрытые ключи содержатся в защищенном хранилище ключей, а не в диспетчере учетных записей безопасности (Security Account Manager, SAM) или в отдельном каталоге.

Хранение зашифрованных данных на удаленных серверах

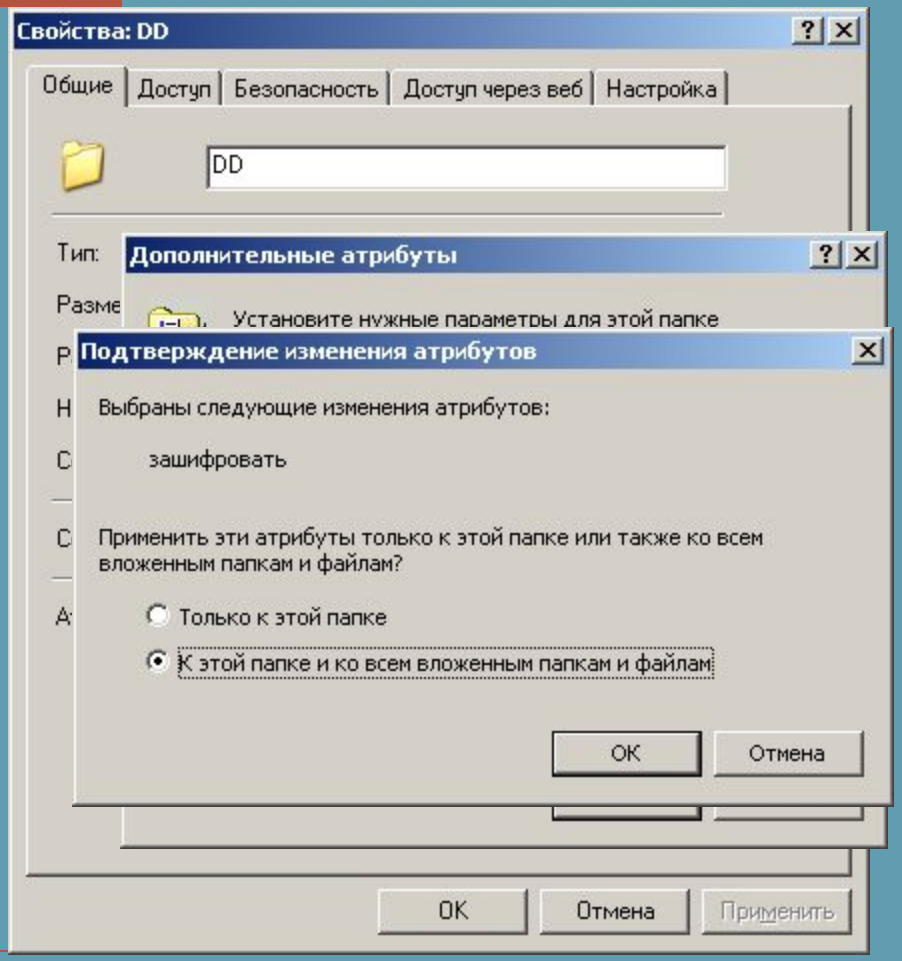
- Если пользователям рабочей среды семейства Windows Server 2003 или Windows XP нужно хранить зашифрованные файлы на удаленных серверах, необходимо помнить.
  - В семействе Windows Server 2003 и Windows XP поддерживается хранение зашифрованных файлов на удаленных серверах.
  - Пользователи могут удаленно применять шифрованную файловую систему только тогда, когда оба компьютера являются членами одного леса семейства Windows Server 2003.
  - Зашифрованные данные не шифруются при передаче по сети, а только при сохранении на диске. Исключения составляют случаи, когда система включает протокол IPSec или протокол WebDAV. IPSec шифрует данные при передаче по сети TCP/IP. Если файл был зашифрован перед копированием или перемещением в папку WebDAV на сервере, он останется зашифрованным при передаче и во время хранения на сервере.
  - Не поддерживается хранение сертификатов и закрытых ключей шифрованной файловой системы на смарт-картах.
  - Не поддерживается усиленная защита закрытых ключей для закрытых ключей EFS.

Управление сертификатами

- Шифрованная файловая система (EFS) с помощью криптографии открытого ключа шифрует содержимое файлов. В ней применяются ключи, полученные от сертификата пользователя и дополнительных пользователей, а также от назначенных агентов восстановления шифрованных данных, которые настроены. Поскольку в сертификатах могут также содержатся сведения о закрытом ключе, сертификаты требуют правильного управления.
- Сертификаты, используемые файловой системой EFS, могут быть получены в центре сертификации (ЦС) или же автоматически созданы компьютером. При получении EFS сертификата в центре сертификации необходима ссылка сертификата на поставщика службы криптографии (CSP) и соответствующий идентификатор объекта (OID). В EFS возможно использование основного или расширенного CSP. Если эти два атрибута не установлены правильно в сертификате, EFS не может его использовать.
- Сертификаты и закрытые ключи от всех назначенных агентов восстановления шифрованных данных нужно экспортировать на съемный диск или хранить в безопасности до тех пор, пока они не понадобятся.
- При экспортировании сертификата и закрытого ключа убедитесь, что выбранный сертификат содержит **Шифрованную файловую систему** в **Назначениях** и что имеется соответствующий закрытый ключ.

Шифрование файлов

- Для выполнения шифрования данных можно воспользоваться кнопкой **Другие** в закладке **Свойства** файла.
- Для удобства пользователя зашифрованные папки и файлы отображаются другим цветом.



Использование утилит командной строки

- Для просмотра информации о зашифрованных файлах можно воспользоваться утилитой efsinfo
- Синтаксис
  - **efsinfo**[**/u**] [**/r**] [**/c**] [**/i**] [**/y**] [**/k**] [**/s:каталог**] [*Путь*[**,***Путь***...**]][**/?**]
  - **efsinfo /t:** *каталог*

Использование утилит командной строки

- Отображение или изменение шифрование папок и файлов на томах NTFS.
- Использованная без параметров команда **cipher** отображает состояние шифрования текущей папки и всех файлов, находящихся в ней.
- **Синтаксис**
  - **cipher** [{**/e** | **/d**}] [**/s:***папка*] [**/a**] [**/i**] [**/f**] [**/q**] [**/h**] [**/k**] [**/u**[**/n**]] [{*путь* [...]] | **/r:***имя_файла_без_расширения* | **/w:***путь* | **/x**[**:***путь*] *имя_файла_без_расширения*}]