Лекция 9. Средства защиты информации в ОС Windows

1. Мандатное и ролевое разграничение доступа к объектам.
2. Подсистема безопасности ОС Windows.
3. Разграничение доступа к объектам в ОС Windows.

Мандатное разграничение доступа

- Все субъекты и объекты компьютерной системы должны быть однозначно идентифицированы;
- имеется линейно упорядоченный набор меток конфиденциальности и соответствующих им степеней допуска (нулевая метка или степень соответствуют общедоступному объекту и степени допуска к работе только с общедоступными объектами);
- каждому объекту информационной системы присвоена метка конфиденциальности;
- каждому субъекту информационной системы присваивается степень допуска;

Мандатное разграничение доступа

- в процессе своего существования каждый субъект имеет свой уровень конфиденциальности, равный максимуму из меток конфиденциальности объектов, к которым данный субъект получил доступ;
- понизить метку конфиденциальности объекта может только субъект, имеющий доступ к данному объекту и обладающий специальной привилегией;
- право на чтение информации из объекта получает только тот субъект, чья степень допуска не меньше метки конфиденциальности данного объекта (правило «не читать выше»);

Мандатное разграничение доступа

- право на запись информации в объект получает только тот субъект, чей уровень конфиденциальности не больше метки конфиденциальности данного объекта (правило «не записывать ниже»).

Мандатное разграничение доступа

- Основной целью является предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности (противодействие созданию каналов передачи информации «сверху вниз»).
- Формально доказано следующее важное утверждение: если начальное состояние компьютерной системы безопасно и все переходы из одного состояния системы в другое не нарушают правил разграничения доступа, то любое состояние информационной системы также безопасно.

Мандатное разграничение доступа

Другие достоинства :

- более высокая надежность работы самой компьютерной системы (при разграничении доступа к объектам контролируется и состояние самой системы);
- большая простота определения правил разграничения доступа по сравнению с дискреционным (эти правила более ясны для разработчиков и пользователей компьютерной системы).

Недостатки;

- сложность программной реализации;
- снижение эффективности работы компьютерной системы;
- создание дополнительных неудобств работе пользователей компьютерной системы (особенно с высокой степенью допуска).

Ролевое разграничение доступа

Основано на том, что в реальной жизни организации ее сотрудники выполняют определенные функциональные обязанности не от своего имени, а в рамках некоторой занимаемой ими должности (или роли). Реализация ролевого разграничения доступа к объектам компьютерной системы требует разработки набора (библиотеки) ролей, определяемых как набор прав доступа к объектам информационной системы (прав на выполнение над ними определенного набора действий). Этот набор прав должен соответствовать выполняемой работником трудовой функции.

Ролевое разграничение доступа

Основные понятия:

- привилегии (операции) – минимально возможные действия пользователя, требующие разрешения или запрещения этого действия;
- правила (задачи) – объединение привилегии, подмножества объектов, для которых может быть определена такая привилегия, и признака разрешения или запрещения этой привилегии;
- роль – набор правил, определяющих какими привилегиями по отношению к каким объектам будет обладать пользователь, которому будет назначена эта роль;
- сессия – подмножество ролей, которые активировал пользователь после своего входа в систему в течение определенного интервала времени.

Ролевое разграничение доступа

Реализация сводится к следующим шагам:

- разработчики приложенийсовместно с администратором и конструктором ролей составляют список привилегий и множество правил;
- конструктор ролей разрабатывает библиотеку ролей для данной системы;
- диспетчер ролей каждому пользователю системы статическим образом присваивает набор возможных для данного пользователя ролей (при этом могут использоваться статические ограничения на назначение ролей);
- после авторизации пользователя в системе для него создается сессия (при этом могут использоваться динамические ограничения на использование ролей).

Ролевое разграничение доступа

- Примеры статических ограничений на назначение ролей пользователям системы – возможность назначения роли главного администратора (суперпользователя) только одному пользователю, ограничение количества пользователей, которым может быть назначена определенная роль, запрет совмещения одним пользователем определенных ролей (например, роли конструктора и диспетчера ролей)
- Пример динамического ограничения на использование ролей – ограничение количества пользователей, одновременно выполняющих определенную роль (например, администратора).

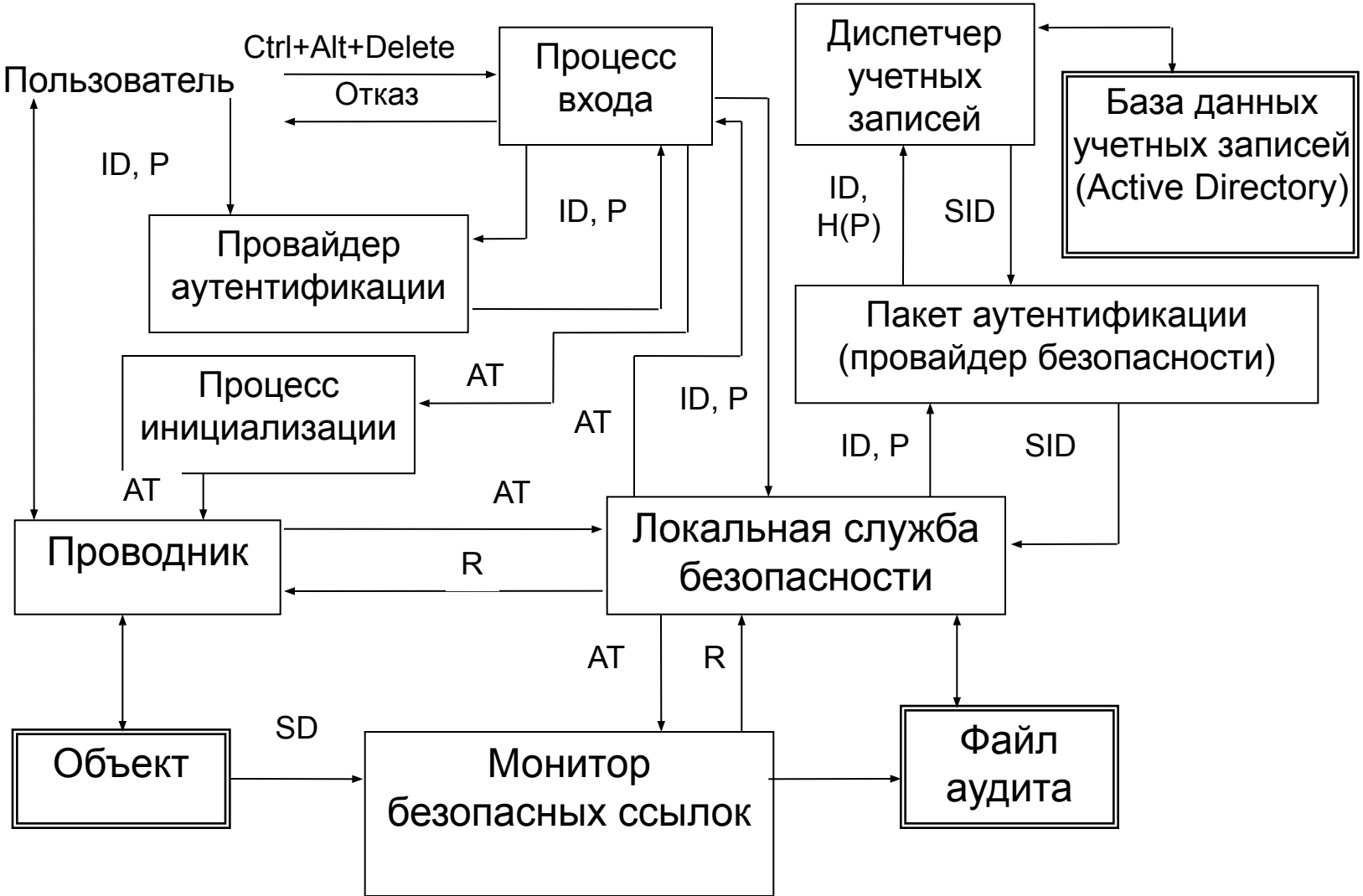
Ролевое разграничение доступа

- Сочетает элементы мандатного разграничения (объединение субъектов и объектов доступа в одном правиле) и дискреционного разграничения (назначение ролей отдельным субъектам). Этим обеспечивается жесткость правил разграничения доступа и гибкость настройки механизма разграничения на конкретные условия применения. Преимущества ролевого разграничения доступа к объектам проявляются при организации коллективного доступа к ресурсам сложных компьютерных систем с большим количеством пользователей и объектов.

Ролевое разграничение доступа

- К недостаткам ролевого разграничения доступа относится отсутствие формальных доказательств безопасности компьютерной системы, возможность внесения дублирования и избыточности при предоставлении пользователям прав доступа, сложность конструирования ролей.

Подсистема безопасности ОС Windows



Подсистема безопасности ОС Windows

- Ядром подсистемы безопасности является локальная служба безопасности (Local Security Authority, LSA), размещающаяся в файле lsass.exe.
- После загрузки операционной системы автоматически запускается процесс входа (winlogon.exe), который остается активным до перезагрузки операционной системы или выключения питания компьютера, а его аварийное завершение приводит аварийному завершению и всей операционной системы. Этим обеспечивается практическая невозможность подмены процесса входа при функционировании системы.

Подсистема безопасности ОС Windows

- После нажатия пользователем комбинации клавиш Ctrl+Alt+Delete процесс входа обращается к провайдеру аутентификации (динамически компонуемой библиотеке функций, DLL) для приема от пользователя его логического имени (ID) и аутентифицирующей информации (P).
- Стандартный провайдер аутентификации размещается в файле msgina.dll и в качестве аутентифицирующей информации использует пароли пользователей.

Подсистема безопасности ОС Windows

- Введенные пользователем логическое имя и пароль передаются процессом входа в LSA, которая обращается к пакету аутентификации (или провайдеру безопасности) для подтверждения подлинности пользователя. Если пользователь зарегистрирован на локальном компьютере, то пакет аутентификации вычисляет хеш-значение пароля H(P) и обращается к диспетчеру учетных записей (Security Account Manager, SAM) для проверки правильности введенного пароля и возможности для пользователя с введенным логическим именем начать работу в системе (не истек ли срок действия пароля, не заблокирована ли учетная запись пользователя и т.п.).

Подсистема безопасности ОС Windows

- Если пользователь зарегистрирован в домене, то провайдер безопасности (Secure Service Provider, SSP) отправляет запросы на начальный мандат и мандат на доступ к рабочей станции (по протоколу Kerberos) службе Active Directory для аутентификации пользователя на контроллере домена (сервере аутентификации группы компьютеров, разделяющих общую политику безопасности и информацию об учетных записях пользователей).

Подсистема безопасности ОС Windows

- Если хеш-значение введенного пользователем пароля не совпадает с эталоном, извлеченным из базы данных учетных записей, или работа пользователя в системе невозможна, то в LSA возвращается код ошибки, который локальная служба безопасности передает процессу входа для выдачи пользователю сообщения об отказе в доступе к системе.
- Если проверка подтвердила подлинность пользователя и отсутствие препятствий для начала его работы в КС, то в LSA передается уникальный идентификатор безопасности пользователя SID (security identifier).

Подсистема безопасности ОС Windows

LSA создает для пользователя маркер доступа AT (access token), который идентифицирует субъект во всех его действиях с объектами КС. В маркере доступа содержится следующая информация:

- SID пользователя;
- идентификаторы безопасности его групп;
- полномочия пользователя;
- идентификаторы безопасности пользователя и его первичной группы, дискреционный список контроля доступа, которые будут использованы при создании пользователем новых объектов в КС;
- источник выдачи маркера доступа;
- тип маркера доступа – первичный или используемый для олицетворения (см. далее);
- текущий уровень олицетворения и др.

Подсистема безопасности ОС Windows

- Созданный LSA маркер доступа АТ передается процессу входа, который с помощью провайдера аутентификации завершает процесс авторизации пользователя в КС, запуская процесс его инициализации (userinit.exe) и передавая ему АТ.
- Процесс инициализации на основе содержащегося в АТ идентификатора безопасности пользователя загружает из реестра Windows его профиль и загружает программную оболочку – Проводник Windows (explorer.exe), передавая ему маркер доступа пользователя. После этого процесс инициализации завершает свою работу.

Подсистема безопасности ОС Windows

- Только процессы, окна которых расположены на одном Рабочем столе, могут взаимодействовать между собой, используя средства графического интерфейса пользователя Windows (GUI).
- Процесс входа (winlogon) выполняется на отдельном Рабочем столе. Никакой другой процесс, в том числе и программная закладка для перехвата паролей, не имеет доступа к этому Рабочему столу.
- Переключение экрана компьютера с одного Рабочего стола на другой производится при нажатии комбинации клавиш Ctrl+Alt+Delete. В ОС Windows сообщение о нажатии Ctrl+Alt+Delete посылается только процессу входа. Для всех других процессов нажатие этой комбинации клавиш совершенно незаметно.

Механизм олицетворения

- При взаимодействии клиентов и серверов в операционной системе Windows может использоваться механизм олицетворения (impersonation). В этом случае при необходимости обратиться с запросом к серверу в процессе клиента создается поток (thread), которому назначается маркер доступа пользователя, инициировавшего этот запрос. Этот механизм позволяет серверу действовать от лица клиента при доступе к объектам, к которым сам сервер не имеет доступа.

Разграничение доступа к объектам

С объектом разграничения доступа связывается дескриптор безопасности SD (security descriptor), содержащий следующую информацию:

- идентификатор безопасности (SID) владельца объекта;
- идентификатор безопасности первичной группы владельца;
- дискреционный список контроля доступа (discretionary access control list, DACL);
- системный список контроля доступа (system access control list, SACL).

Списки управления доступом

1. Список SACL управляется администратором системы и предназначен для аудита безопасности.
2. Список DACL управляется владельцем объекта. Каждый элемент списка DACL (access control entry, ACE) определяет права доступа к объекту одному пользователю или группе. Каждый ACE содержит следующую информацию:

- идентификатор безопасности SID субъекта, для которого определяются права доступа;
- маска доступа (access mask, AM), которая специфицирует контролируемые данным ACE права доступа;
- тип ACE;
- признак наследования прав доступа к объекту, определенных для родительского объекта.

Разграничение доступа к объектам

- Элементы списка DACL могут быть двух типов – элементы, разрешающие специфицированные в них права доступа (Access-allowed ACE), и элементы, запрещающие определенные в них права доступа (Access-denied ACE). Элементы для запрещения субъектам использования определенных прав доступа должны размещаться в «голове» списка, до первого из элементов, разрешающих использование субъектом тех или иных прав доступа.

Права доступа

- В операционной системе Windows различаются специальные, стандартные и общие (generic) права доступа к объектам. Специальные права доступа определяют возможность обращения к объекту по свойственному только данной категории объектов методу – чтение данных из объекта, запись данных в объект, чтение атрибутов объекта, выполнение программного файла и т.д.
- Стандартные права доступа определяют возможность доступа к объекту по методу, применимому к любому объекту, – изменение владельца объекта, изменение списка DACL объекта, удаление объекта и т.д.

Права доступа

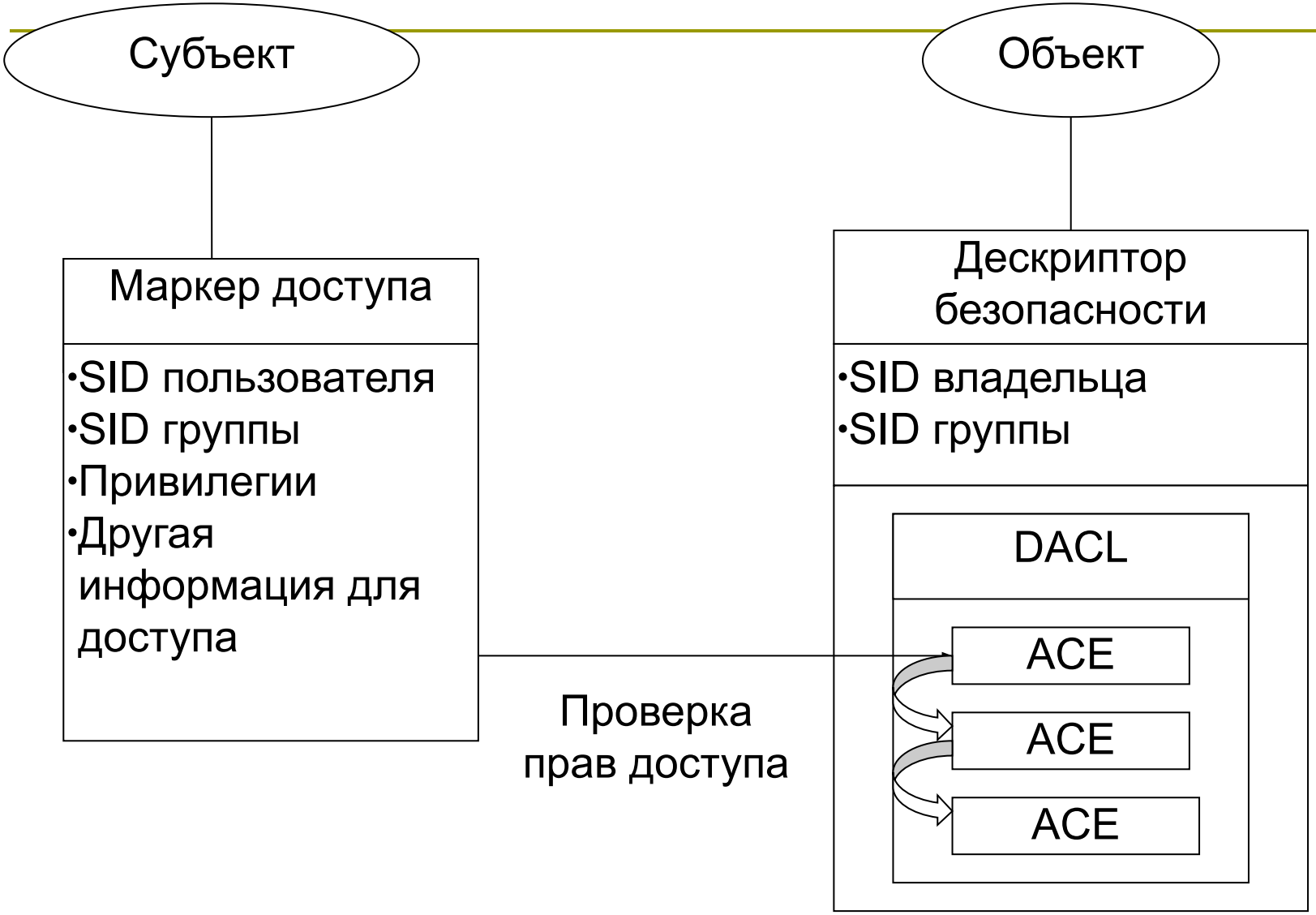
Каждое из общих прав доступа представляет собой комбинацию специальных и стандартных прав и предоставляет возможность обращения к объекту с помощью некоторого набора методов доступа. Примеры общих прав доступа:

- чтение, включающее в себя чтение DACL объекта, чтение данных из объекта, чтение его атрибутов и расширенных атрибутов, использование объекта для синхронизации;
- запись, включающая в себя чтение DACL объекта, запись и добавление данных в объект, запись его атрибутов и расширенных атрибутов, использование объекта для синхронизации;
- выполнение, включающее в себя чтение DACL объекта, чтение его атрибутов, выполнение программного файла и использование объекта для синхронизации.

Разграничение доступа к объектам

- Маркер доступа субъекта, обращающегося к некоторому объекту, поступает в локальную службу безопасности LSA. От LSA маркер доступа поступает к монитору безопасных ссылок (security reference monitor, SRM), который просматривает DACL из дескриптора безопасности SD соответствующего объекта и принимает решение R о предоставлении доступа субъекту или отказе в доступе. Получив от SRM результат R, LSA передает его субъекту, запросившему доступ к объекту.

Разграничение доступа к объектам



Алгоритм проверки прав доступа к объекту

1. Если SID из АТ субъекта не совпадает с SID в ACE списка контроля доступа к объекту, то переход к следующему ACE, иначе переход к п. 2.
2. Если в элементе ACE запрещается доступ к объекту для субъекта с данным SID, но этот субъект является владельцем объекта и запрашиваемая маска доступа содержит только попытку доступа к объекту для чтения или изменения дискреционного списка контроля доступа к объекту, то доступ субъекта к объекту разрешается, иначе осуществляется переход к п.3.
3. Если в элементе ACE запрещается доступ к объекту для субъекта с данным SID, то сравниваются запрашиваемая маска доступа и маска доступа в ACE. Если при сравнении находится хотя бы один общий метод доступа, то попытка доступа субъекта к объекту отклоняется, иначе происходит переход к следующему ACE.

Алгоритм проверки прав доступа к объекту

4. Если в элементе ACE разрешается доступ к объекту для субъекта с данным SID, то также сравниваются запрашиваемая маска доступа и маска доступа, определенная в ACE. Если при этом маски доступа полностью совпадают, то доступ субъекта к объекту разрешается, иначе происходит переход к следующему ACE.
5. Если достигнут конец списка DACL из дескриптора безопасности объекта, то попытка доступа субъекта к объекту отклоняется.

Алгоритм проверки прав доступа к объекту

- Если DACL объекта пуст, то любой доступ к нему запрещен всем субъектам, за исключением владельца объекта, которому разрешены чтение и (или) изменение списка контроля доступа к объекту.
- Если у объекта нет дескриптора безопасности (например, у папок и файлов, размещенных на дисках под управлением файловой системы FAT), то любые пользователи и группы могут получить любые права доступа к данному объекту.

Контейнерные и неконтейнерные объекты

Контейнерный объект, например папка, имеет логические связи с другими объектами (вложенными папками и файлами), которые могут наследовать определенные права доступа от своего родительского объекта.

По умолчанию, изменение прав доступа к папке автоматически распространяется на права доступа к файлам этой папки, но не на вложенные в нее другие папки. При наследовании права доступа, установленные для дочерних объектов, могут добавляться к правам доступа, установленным для родительского объекта, или полностью заменяться ими.

Назначение дескрипторов безопасности вновь создаваемым объектам

1. На основе явно заданного субъектом и корректного по форме дескриптора безопасности (например, при вызове системных функций CreateFile или CreateDirectory при создании файлов или папок, при вызове системной функции RegCreateKeyEx при создании раздела реестра и т.п.);
2. На основе механизма наследования (если при создании объекта дескриптор безопасности не задается);
3. Из маркера доступа субъекта, создающего объект (если наследование невозможно).