# Архитектура подсистемы защиты ОС

Автор: Бастрыкин К.М.

# Основные функции подсистемы защиты ОС

- 1. *Идентификация и аутентификация*. Ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоставив системе аутентифицирующую информацию, подтверждающую, что пользователь действительно является тем, кем он себя заявляет.
- 2. *Разграничение доступа*. Каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности.
- 3. *Аудит*. ОС регистрирует в специальном журнале события, потенциально опасные для поддержания безопасности системы.

# Основные функции подсистемы защиты ОС

- 4. *Управление политикой безопасности*. Политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна гибко реагировать на изменения условий функционирования ОС. Управление политикой безопасности осуществляется администраторами системы с использованием соответствующих средств, встроенных в ОС.
- 5. *Криптографические функции*. Защита информации немыслима без использования криптографических средств защиты. Шифрование используется в ОС при хранении и передаче по каналам связи паролей пользователей и некоторых других данных, критичных для безопасности системы.
- 6. *Сетевые функции*. Современные ОС, как правило, работают не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе и задач, имеющих прямое отношение к защите информации.

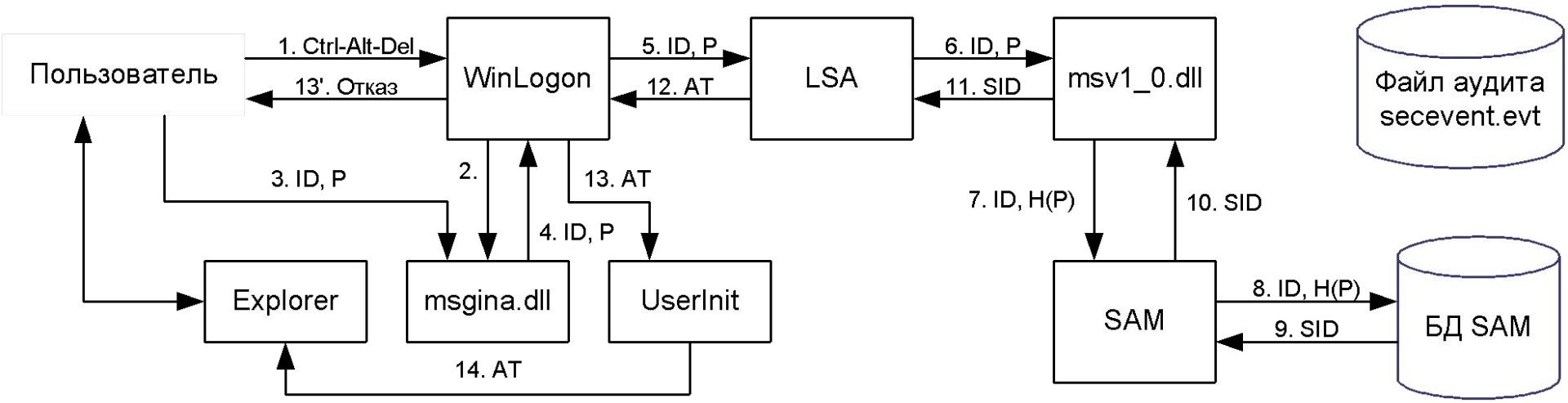
# Идентификация, аутентификация и авторизация

- В защищенной ОС любой пользователь (субъект доступа), перед тем как начать работу с системой, должен пройти идентификацию, аутентификацию и авторизацию.

# Идентификация, аутентификация и авторизация

- *Идентификация* субъекта доступа заключается в том, что субъект сообщает ОС *идентифицирующую информацию о себе*(имя, учетный номер и т. д.) и таким образом идентифицирует себя.
- *Аутентификация* субъекта доступа заключается в том, что субъект предоставляет ОС помимо идентифицирующей информации еще и аутентифицирующую информацию,подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация.
- *Авторизация* субъекта доступа происходит после успешной идентификации и аутентификации. При авторизации субъекта ОС выполняет действия, необходимые для того, чтобы субъект мог начать работу в системе.

# Аутентификация



# Разграничение доступа к объектам ОС

Основными понятиями процесса разграничения доступа к объектам ОС являются

-объект доступа,

-метод доступа к объекту и

-субъект доступа.

# Разграничение доступа к объектам ОС

*Объектом доступа* называют любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой ОС, но и текущей политикой безопасности. Под объектами доступа понимают как ресурсы оборудования (процессор, сегменты памяти, принтер, диски и ленты), так и программные ресурсы (файлы, программы, семафоры), т. е. все то, доступ к чему контролируется.

# Разграничение доступа к объектам ОС

*Методом доступа* к объекту называется операция, определенная для объекта. Тип операции зависит от объектов.

# Разграничение доступа к объектам ОС

*Субъектом доступа* называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа).

# Разграничение доступа к объектам ОС

*Разграничением доступа* субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект—объект—метод, разрешен ли доступ данного субъекта к данному объекту по данному методу.

# Правила разграничения доступа

Правила разграничения доступа должны удовлетворять следующим требованиям:

- 1. Соответствовать аналогичным правилам, принятым в организации, в которой установлена ОС. Иными словами, если согласно правилам организации доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен.
- 2. Не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ОС.
- 3. Любой объект доступа должен иметь владельца. Недопустимо присутствие *ничейных объектов* — объектов, не имеющих владельца.
- 4. Не допускать присутствия *недоступных объектов* — объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа.
- 5. Не допускать утечки конфиденциальной информации.

# Правила разграничения доступа

Существуют две **основные модели разграничения доступа**:

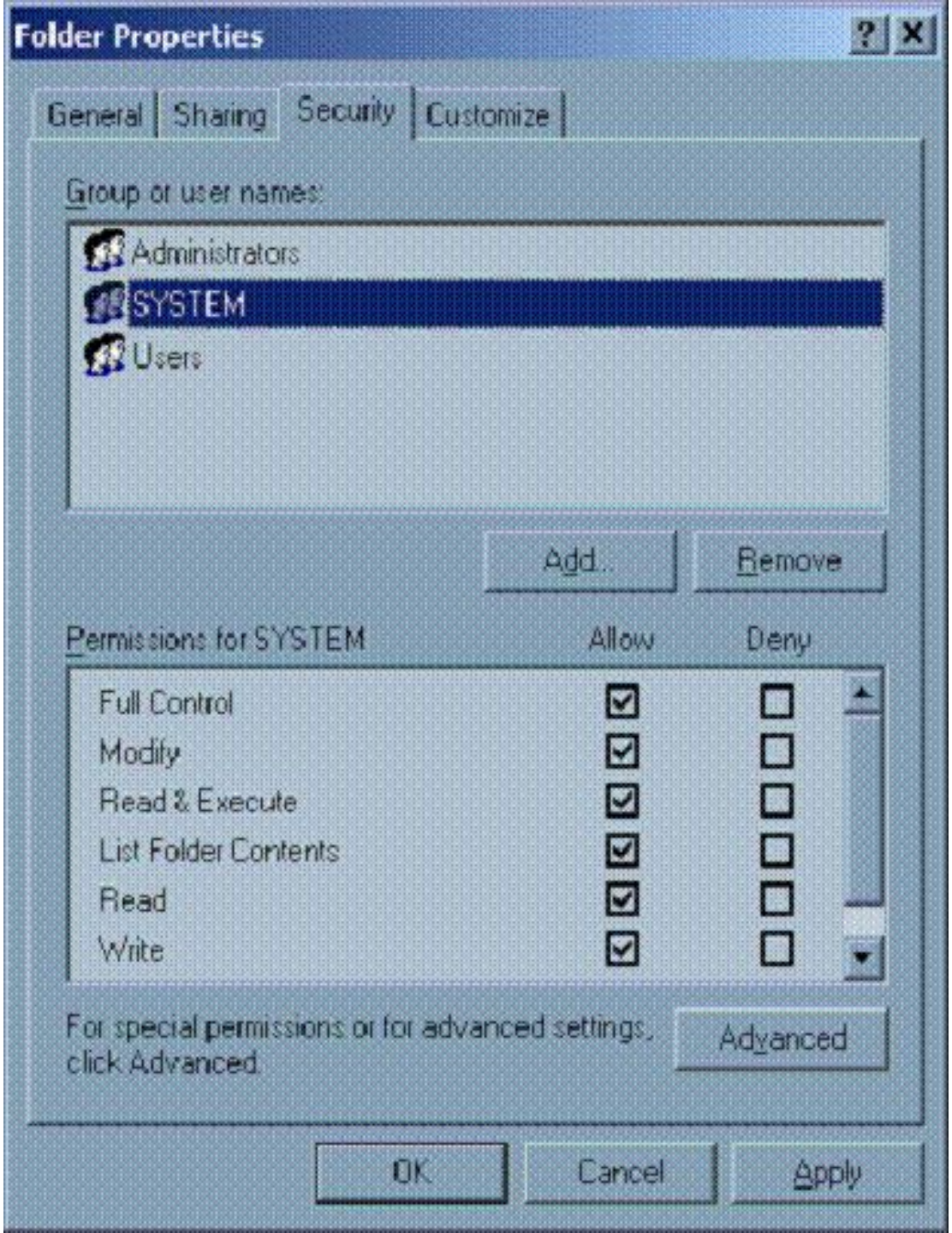
- избирательное (дискреционное) разграничение доступа;
- полномочное (мандатное) разграничение доступа.

# Правила разграничения доступа

- При ***избирательном разграничении*** доступа определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам или группам субъектов. Большинство ОС реализуют именно избирательное разграничение доступа

# Правила разграничения доступа

Контроль является дискреционным в том смысле, что владелец объекта сам определяет тех, кто имеет доступ к объекту, а также вид их доступа.


Folder Properties
General
Sharing
Security
Customize
Group or user names:
Administrators
SYSTEM
Users
Add...
Remove
Permissions for SYSTEM
Allow
Deny
Full Control
Modify
Read & Execute
List Folder Contents
Read
Write
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

# Правила разграничения доступа

Недостатки:

1. Не предоставляет полной гарантии того, что информация не станет доступна субъектам не имеющим к ней доступа.
2. Система DAC не устанавливает никаких ограничений на распространение информации после того как субъект ее получил
3. В большинстве случаев данные в системе не принадлежат отдельным субъектам, а всей системе.

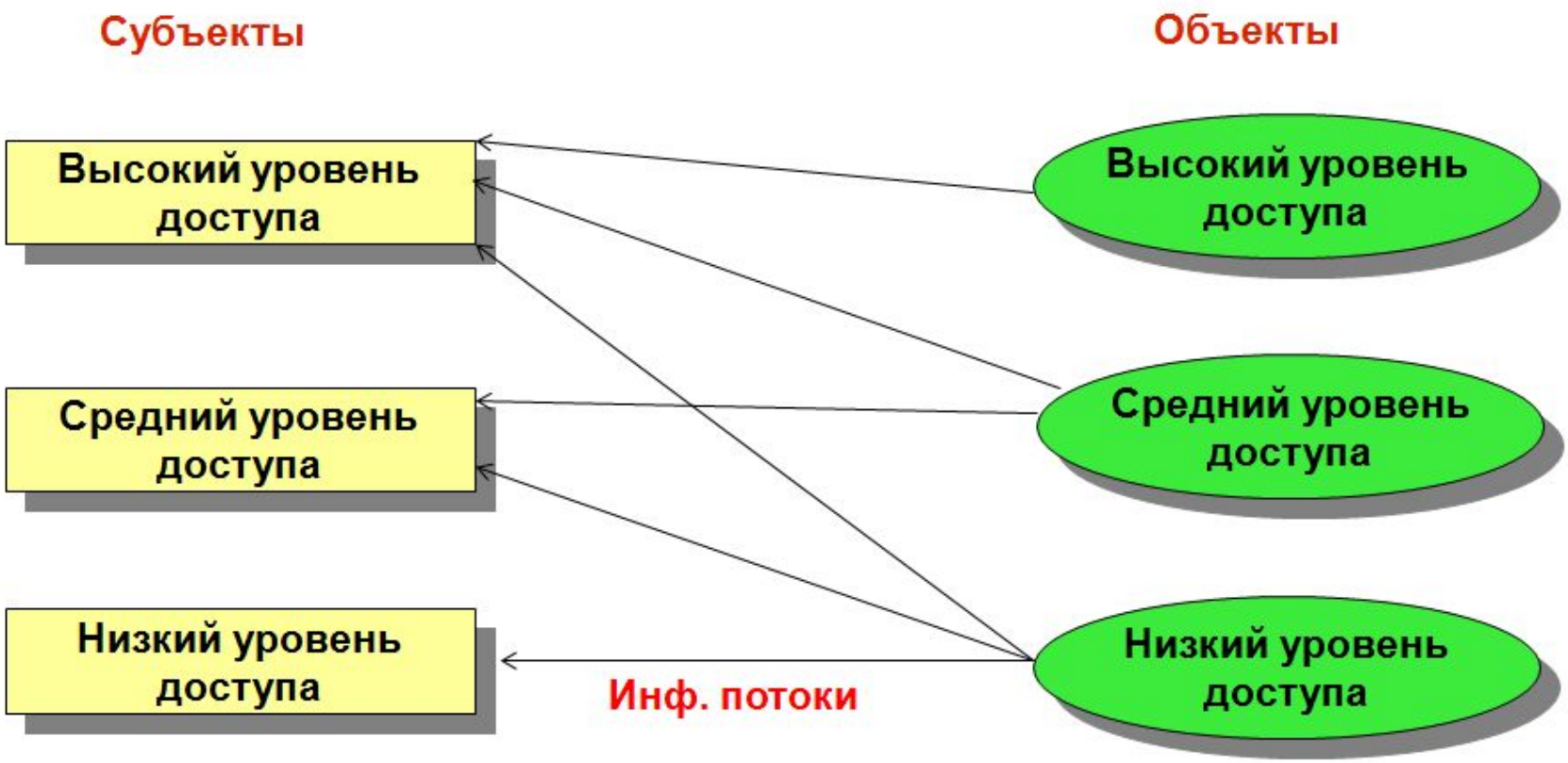
# Правила разграничения доступа

- ***Мандатное разграничение доступа*** заключается в том, что все объекты могут иметь уровни секретности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения секретов.

# Правила разграничения доступа

- Уровень конфиденциальности может принимать одно из строго упорядоченного ряда фиксированных значений, например: конфиденциально, секретно, для служебного пользования, не секретно и т.п.

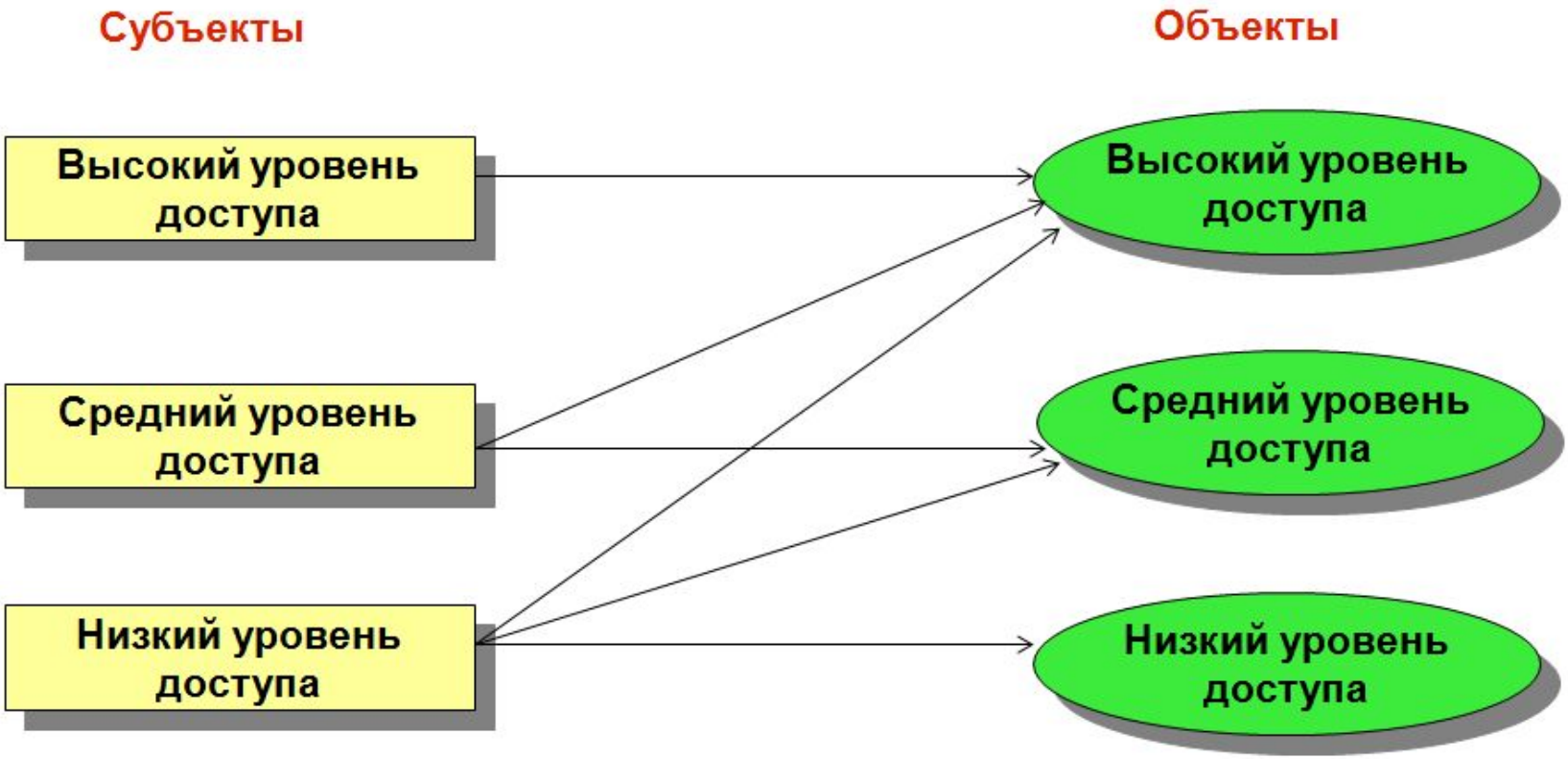
# Чтение информации



# Правила разграничения доступа

- Субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта.

# Запись информации



- Доступ на запись дается если УБ субъекта равняется УБ объекта

# Правила разграничения доступа

Достоинства:

1. Возможно существенное упрощение задачи администрирования
2. Пользователь не может полностью управлять доступом к ресурсам, которые он создаёт.
3. Система запрещает пользователю или процессу, обладающему определённым уровнем доверия, получать доступ к информации, процессам или устройствам более защищённого уровня.

Недостаток:

1. Отдельно взятые категории одного уровня равнозначны, что приводит в большинстве случаев к избыточности прав доступа для конкретных субъектов в пределах соответствующих уровней.

Недостаток

# Аудит

- Процедура *аудита* применительно к ОС заключается в регистрации в специальном журнале, называемом *журналом аудита* или *журналом безопасности*, событий, которые могут представлять опасность для ОС. Пользователи системы, обладающие правом чтения журнала аудита, называются *аудиторами*.

# Аудит

- **Требования к аудиту.**
- Подсистема аудита ОС должна удовлетворять следующим требованиям.
- 1. Добавлять записи в журнал аудита может только ОС. Если предоставить это право какому-то физическому пользователю, этот пользователь получит возможность компрометировать других пользователей, добавляя в журнал аудита соответствующие записи.
- 2. Редактировать или удалять отдельные записи в журнале аудита не может ни один субъект доступа, в том числе и сама ОС.
- 3. Просматривать журнал аудита могут только пользователи, обладающие соответствующей привилегией.
- 4. Очищать журнал аудита могут только пользователи-аудиторы. После очистки журнала в него автоматически вносится запись о том, что журнал аудита был очищен, с указанием времени очистки журнала и имени пользователя, очистившего журнал. ОС должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.
- 5. При переполнении журнала аудита ОС аварийно завершает работу («зависает»). После перезагрузки работать с системой могут только аудиторы. ОС переходит к обычному режиму работы только после очистки журнала аудита.
- Для ограничения доступа к журналу аудита должны применяться специальные средства защиты.

# Аудит

**Политика аудита** — это совокупность правил, определяющих, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты ОС в журнале аудита должны обязательно регистрироваться следующие события:

- попытки входа/выхода пользователей из системы;
- попытки изменения списка пользователей;
- попытки изменения политики безопасности, в том числе и политики аудита.