Операционные системы
Автор: Серков В.А.

Пример вирусной атаки с использованием средств операционной системы

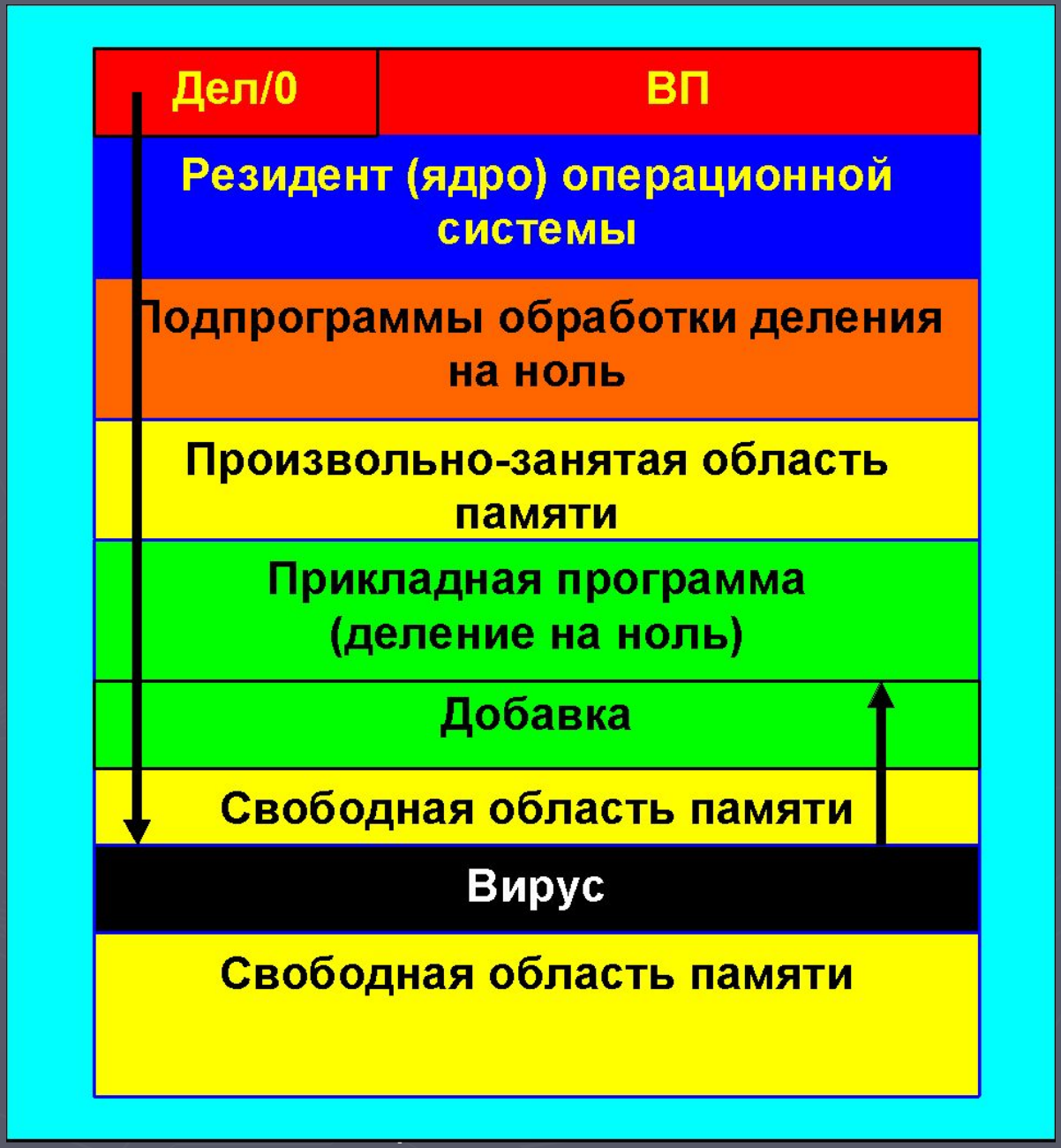
"Операционные

"Операционные

"Операционные

"Операционные

"Операционные



"Операционные

Угрозы безопасности операционных систем

По типу реализованной злоумышленником уязвимости

1. Ошибки при проектировании и программировании ОС, а также недокументированные возможности установленного программного обеспечения. Сюда следует отнести и так называемые "люки" - специально или непреднамеренно встроенные в систему "служебные входы", позволяющие миновать систему безопасности.
2. Неправильная политика безопасности. Чаще всего под этим понятием подразумевают ошибки системного администратора.

Классификация по принципу оказываемого на операционную систему воздействия

1. Использование легальных каналов доступа к информации - доступ к файлу со стороны пользователя, не имеющего права на его чтение. Данная ситуация возможна при неправильной установке прав доступа пользователей. То есть, в том случае, если пользователь получает права, которых, согласно политике безопасности иметь не должен.
2. Использование скрытых каналов доступа к информации - ситуация возможна, когда злоумышленник использует недокументированные возможности операционной системы.
3. Создание новых каналов получения информации - использование специализированного ПО, заранее установленного в систему.

Классификация по характеру воздействия на операционную систему

1. Пассивное воздействие - наблюдение атакующего за процессами, происходящими в системе.
2. Активное воздействие - непосредственное воздействие злоумышленника на процессы, происходящие в операционной системе (удаление файлов, изменение прав доступа и т.д.).

Классификация по цели, осуществляемой атаки

1. Деструктивные действия по отношению к операционной системе - полное разрушение, либо уничтожение отдельных частей.

2. Несанкционированное чтение информации.

3. Несанкционированное изменение информации.

4. Несанкционированное уничтожение информации.

Идентификация и аутентификация

Идентификация субъекта доступа заключается в том, что субъект сообщает операционной системе идентифицирующую информацию о себе (имя, учетный номер и т.д.) и таким образом идентифицирует себя.

Аутентификация субъекта доступа заключается в том, что субъект предоставляет операционной системе помимо идентифицирующей информации еще и аутентифицирующую информацию, подтверждающую, что он действительно является тем субъектом доступа, к которому относится идентифицирующая информация.

Аутентификация с помощью пароля

Обычно для шифрования паролей в списке пользователей используют одну из известных криптографически стойких **хеш-функций** – легко вычисляемую функцию F, для которой обратная функция (возможно, неоднозначная) не может быть вычислена за приемлемое время.

В списке пользователей хранится не сам пароль, а образ пароля, являющийся результатом применения к паролю хеш-функции.

Пример хэш-функции

$$F(пароль) = \sum_{i=1}^{n} S_i$$

S_i – коды символов текста пароля.

Пример

Пароль – PROBA

Символы пароля:

80 + 82 + 79 + 66 + 65 = 372

F = 372

В процедуре генерации образа пароля обязательно должен участвовать маркант - число или строка, генерируемая случайным образом и хранящаяся в открытом виде вместе с образом пароля. Это необходимо для того, чтобы одинаковым паролям соответствовали разные образы

Методы подбора паролей

1. Тотальный перебор.
2. Тотальный перебор, оптимизированный по статистике встречаемости символов.
3. Тотальный перебор. оптимизированный с помощью словарей.
4. Подбор пароля с использованием знаний о пользователе.
5. Подбор образа пароля.

Аутентификация с помощью внешних носителей ключевой информации

Идентифицирующая и аутентифицирующая информация пользователя, хранится на внешнем носителе информации, который может представлять собой электронный USB-ключ, пластиковую смарт-карту и т. д.

При входе в систему пользователь подключает к компьютеру носитель ключевой информации, и операционная система считывает с него идентификатор пользователя и соответствующий ему ключ.

Аутентификация с помощью биометрических характеристик пользователей

Каждый человек обладает своим неповторимым набором биометрических характеристик, к которым относятся:

- отпечатки пальцев,
- рисунок сетчатки,
- рукописный и клавиатурный почерк и т.д.

Эти характеристики могут быть использованы для аутентификации пользователя.

Разграничение доступа к объектам ОС

Объект доступа

Любой элемент операционной системы, доступ к которому пользователей и других субъектов доступа может быть **произвольно** ограничен.

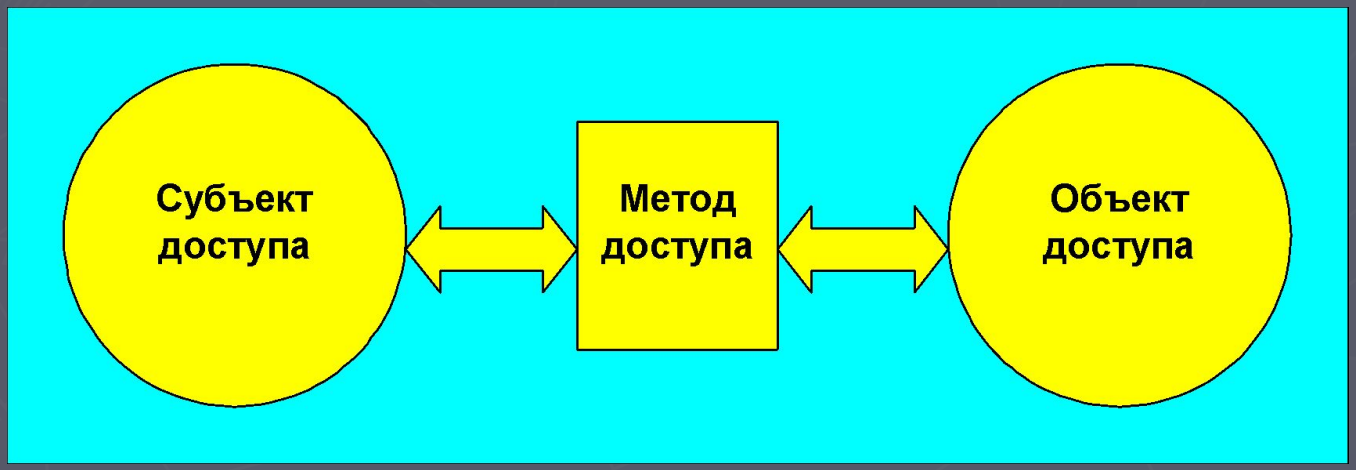
Если правила, ограничивающие доступ субъектов к некоторому элементу операционной системы, определены жестко и не допускают изменения с течением времени, этот элемент операционной системы мы не будем считать объектом.

Метод доступа

Методом доступа к объекту называется операция, определенная для некоторого объекта. Например, для файлов могут быть определены методы доступа "чтение", "запись" и "добавление" (дописывание информации в конец файла).

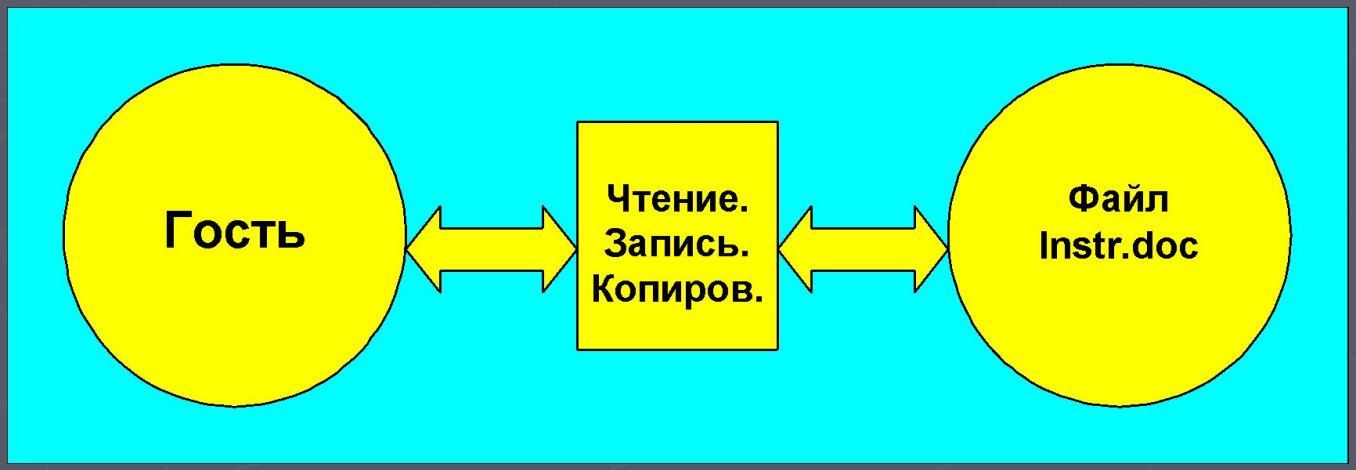
Субъект доступа

Любая сущность, способная инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Например, пользователи являются субъектами доступа.



Разграничение доступа

Совокупность правил, определяющая для каждой тройки субъект-метод-объект, разрешен ли доступ данного субъекта к данному объекту по данному методу.



Модели разграничения доступа

Избирательное разграничение доступа

Система правил избирательного или дискреционного разграничения доступа (discretionary access control) формулируется следующим образом.

1. Для любого объекта операционной системы существует **владелец**.
2. **Владелец** объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект-метод-объект возможность доступа определена **однозначно**.

Избирательное разграничение доступа

Субъекты (домены)	Объекты			
	O1	O2	O3	O4
Админ.				
Группа 1		**Методы доступа**		
Группа 2				
Группа 3				

Избирательное разграничение доступа

При создании нового объекта владелец объекта должен определить права доступа различных субъектов к этому объекту. Если владелец объекта не сделал этого, то либо новому объекту назначаются атрибуты защиты по умолчанию, либо новый объект наследует атрибуты защиты от родительского объекта (каталога, контейнера и т.д.).

Избирательное разграничение доступа является наиболее распространенным механизмом разграничения доступа. Это обусловлено сравнительной простотой реализации этой модели.

Изолированная программная среда

Правила разграничения доступа формулируются следующим образом.

1. Для любого объекта операционной системы существует **владелец**.
2. **Владелец** объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой четверки

субъект-метод-процесс-объект

возможность доступа определена однозначно.

4. Существует хотя бы один привилегированный пользователь (**администратор**), имеющий возможность обратиться к любому объекту по любому методу.
5. Для каждого субъекта определен список программ, которые этот субъект может запускать.

Изолированная программная среда

Изолированная программная среда существенно повышает защищенность операционной системы от разрушающих программных воздействий, включая программные закладки и компьютерные вирусы.

Кроме того, при использовании данной модели повышается защищенность целостности данных, хранящихся в системе.

Полномочное разграничение доступа без контроля информационных потоков

1. Для любого объекта операционной системы существует владелец.
2. Владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту.
3. Для каждой тройки субъект-метод-объект возможность доступа определена однозначно.
4. Существует хотя бы один привилегированный пользователь (администратор), имеющий возможность удалить любой объект.

Полномочное разграничение доступа без контроля информационных потоков

5. В множестве объектов доступа операционной системы выделяется подмножество объектов полномочного разграничения доступа.

Каждый объект полномочного разграничения доступа имеет **гриф секретности (ГСО).** Чем выше числовое значение грифа секретности, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретен.

Если объект не является объектом полномочного разграничения доступа или если объект несекретен, администратор может обратиться к нему по любому методу, как и в предыдущей модели разграничения доступа.

Полномочное разграничение доступа без контроля информационных потоков

6. Каждый субъект доступа имеет **уровень допуска (УДС).** Чем выше числовое значение уровня допуска, тем больший допуск имеет субъект.

Нулевое значение уровня допуска означает, что субъект не имеет допуска.

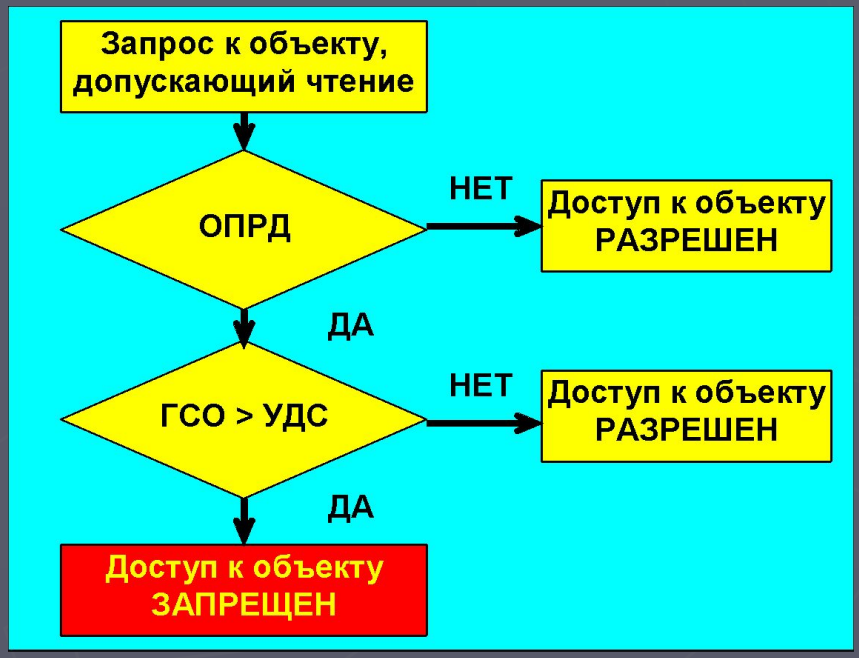
Обычно ненулевое значение допуска назначается только субъектам-пользователям и не назначается субъектам, от имени которых выполняются системные процессы.

Полномочное разграничение доступа без контроля информационных потоков

7. Если субъект открывает объект в режиме, допускающем чтение и:

- объект является объектом полномочного разграничения доступа (ОПРД)
- гриф секретности объекта (ГС) строго выше уровня допуска субъекта (УД), обращающегося к нему,

то доступ субъекта к объекту запрещен независимо от состояния матрицы доступа.



Полномочное разграничение доступа с контролем информационных потоков

1, 2 - аналогичны полномочному разграничению доступа без контроля информационных потоков.

3. Для каждой четверки **субъект-объект-метод-процесс** возможность доступа определена однозначно в каждый момент времени.

При изменении состояния процесса со временем возможность предоставления доступа также может измениться, т.е. если в некоторый момент времени к некоторому объекту разрешен доступ некоторого субъекта посредством некоторого процесса, это не означает, что в другой момент времени доступ тоже будет разрешен.

Вместе с тем в каждый момент времени возможность доступа определена однозначно - никаких случайных величин здесь нет. Поскольку права процесса на доступ к объекту меняются с течением времени, они должны проверяться не только при открытии объекта, но и перед выполнением над объектом таких операций, как чтение и запись.

Полномочное разграничение доступа с контролем информационных потоков

4, 5, 6, 7 аналогичны полномочному разграничению доступа без контроля информационных потоков.

8. Каждый процесс операционной системы имеет **уровень конфиденциальности (УКП),** равный максимуму из грифов секретности объектов, открытых процессом на протяжении своего существования.

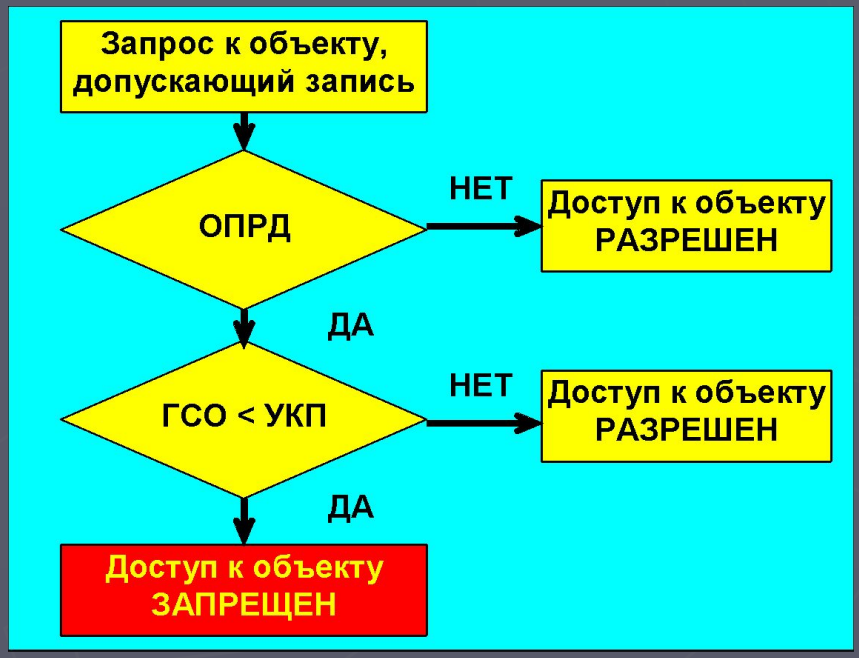
Уровень конфиденциальности фактически представляет собой гриф секретности информации, хранящейся в оперативной памяти процесса.

Полномочное разграничение доступа с контролем информационных потоков

9. Если субъект открывает объект в режиме, допускающем запись и:

- объект является объектом полномочного разграничения доступа (ОПРД)
- гриф секретности объекта строго ниже уровня конфиденциальности процесса, обращающегося к нему, ,

то доступ субъекта к объекту запрещен независимо от состояния матрицы доступа.



Полномочное разграничение доступа с контролем информационных потоков

10. Понизить гриф секретности объекта полномочного разграничения доступа может только субъект, который:

- имеет доступ к объекту согласно правилу 7;

- обладает специальной привилегией, позволяющей ему понижать грифы секретности объектов.

При использовании данной модели разграничения доступа существенно страдает производительность операционной системы, поскольку права доступа к объекту должны проверяться не только при открытии объекта, но и при каждой операции чтения/записи.

Свойства моделей разграничения доступа

Свойства модели	Избиратель-ное разгра-ничение доступа	Изолиро-ванная програм-мная среда	Полномочное разграничение доступа	
			без контро-ля потоков	с контролем потоков
Защита от утечки информации	Отсутствует	Отсутствует	Отсутствует	Имеется
Защищенность от разрушающих воздействий	Низкая	Высокая	Низкая	Низкая
Сложность реализации	Низкая	Средняя	Средняя	Высокая
Сложность администриро-вания	Низкая	Средняя	Низкая	Высокая
Затраты ресур-сов компьютера	Низкие	Низкие	Низкие	Высокие
Использование программного обеспечения, разработанного для других систем	Возможно	Возможно	Возможно	Проблематич-но

Если для организации чрезвычайно важно обеспечение защищенности системы от несанкционированной утечки информации, без полномочного разграничения доступа с контролем информационных потоков просто не обойтись.

В остальных ситуациях применение этой модели нецелесообразно из-за резкого ухудшения эксплуатационных качеств операционной системы.

Что касается изолированной программной среды, то ее целесообразно использовать в случаях, когда очень важно обеспечивать целостность программ и данных операционной системы.

В остальных ситуациях простое избирательное разграничение доступа наиболее эффективно.

Аудит

Процедура **аудита** применительно к операционным системам заключается в регистрации в специальном журнале, называемом журналом аудита или журналом безопасности, событий, которые могут представлять опасность для операционной системы.

Пользователи системы, обладающие правом чтения этого журнала, называются **аудиторами.**

Подсистема аудита операционной системы **должна удовлетворять** следующим **требованиям**:

1. Только сама операционная система может добавлять записи в журнал аудита.

2. Ни один субъект доступа, в том числе и сама операционная система, не имеет возможности редактировать или удалять отдельные записи в журнале аудита.

3. Только пользователи-аудиторы, обладающие соответствующей привилегией, могут просматривать журнал аудита.

4. Только пользователи-аудиторы могут очищать журнал аудита. 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. Операционная система должна поддерживать возможность сохранения журнала аудита перед очисткой в другом файле.

5. При переполнении журнала аудита операционная система аварийно завершает работу ("зависает"). После перезагрузки работать с системой могут только аудиторы. Операционная система переходит к обычному режиму работы только после очистки журнала аудита.

Для обеспечения надежной защиты операционной системы 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.

Окончательный выбор того, какие события должны регистрироваться в журнале аудита, а какие не должны, возлагается на аудиторов с учетом специфики обрабатываемой информации.