Типовая архитектура подсистемы защиты операционной системы Windows

Компоненты системы защиты ОС Windows. Разграничение доступа. Объекты, субъекты доступа. Пользователи и группы пользователей. Идентификатор безопасности. Дескриптор безопасности, список контроля доступа. Маркер доступа. Проверка прав доступа. Права и привилегии учетных записей. Аутентификация пользователя. Аудит в ОС Windows.

1. Классы безопасности
2. Компоненты системы защиты
3. Аутентификация пользователей
4. Разграничение доступа к объектам операционной системы
5. Контроль целостности
6. Аудит

Trusted Computer System Evaluation Criteria

Оценочный уровень	Описание
A1	Verified Design (проверенная конструкция)
B3	Security Domains (домены безопасности)
B2	Structured Protection (структурированная защита)
B1	Labeled Security Protection (защита с использованием грифа секретности)
C2	Controlled Access Protection (защита управляемого доступа)
C1	Discretionary Access Protection (устаревший уровень) (защита избирательного доступа)
D	Minimal Protection (минимальная защита)

Windows NT 3.5 с Service Pack 3 - уровень C2
Windows NT 4 с Service Pack 6a - уровень C2 для сетевой и автономной конфигураций

Trusted Computer System Evaluation Criteria

Основные требования предъявляемые к уровню безопасности C2:

- Механизм безопасной регистрации
- Управление избирательным доступом
- Аудит безопасности
- Защита при повторном использовании объектов

Требования уровня безопасности B:

- Функциональность пути доверительных отношений (trusted path functionality)
- Управление доверительными отношениями (trusted facility management)

Common Criteria for Information Technology Security Evaluation (CCITSE) (Общие критерии оценки безопасности информационных систем)

Windows 2000

Основные требования

- функции управления избирательным доступом (Discretinary Access Control Functions), основанные на применении криптографии
- политика управления избирательным доступом (Discretinary Access Control Policy) для дополнительных пользовательских объектов данных (User Data Object)
- внутренняя репликация (Internal Replication) для гарантированной синхронизации элементов данных, связанных с защитой, между физически раздельными частями распределенной операционной системы
- утилизация ресурсов (Resource Utilization) для физических пространств дисков
- блокировка интерактивного сеанса (Interactive Sessin Locking) и путь доверительных отношений (Trusted Path) для первоначального входа пользователя (initial user logging on)
- защита внутренней передачи данных (Internal Data Transfer Protection), чтобы обезопасить данные от раскрытия и несанкционированной модификации при передаче между физически раздельными частями распределенной операционной системы
- систематическое устранение обнаруживаемых недостатков в системе защиты (Systematic Flaw Remediation).

Common Criteria

Windows XP Professional
Windows Server 2003

- распределенной операционной системы;
- защиты конфиденциальных данных;
- управления сетью;
- службы каталогов;
- брандмауэра;
- VPN (Virtal Private Network);
- управления рабочим столом;
- инфраструктуры открытого ключа (Public Key Infrastructure, PKI);
- выдачи и управления сертификатами открытого ключа;
- встраиваемой операционной системы.

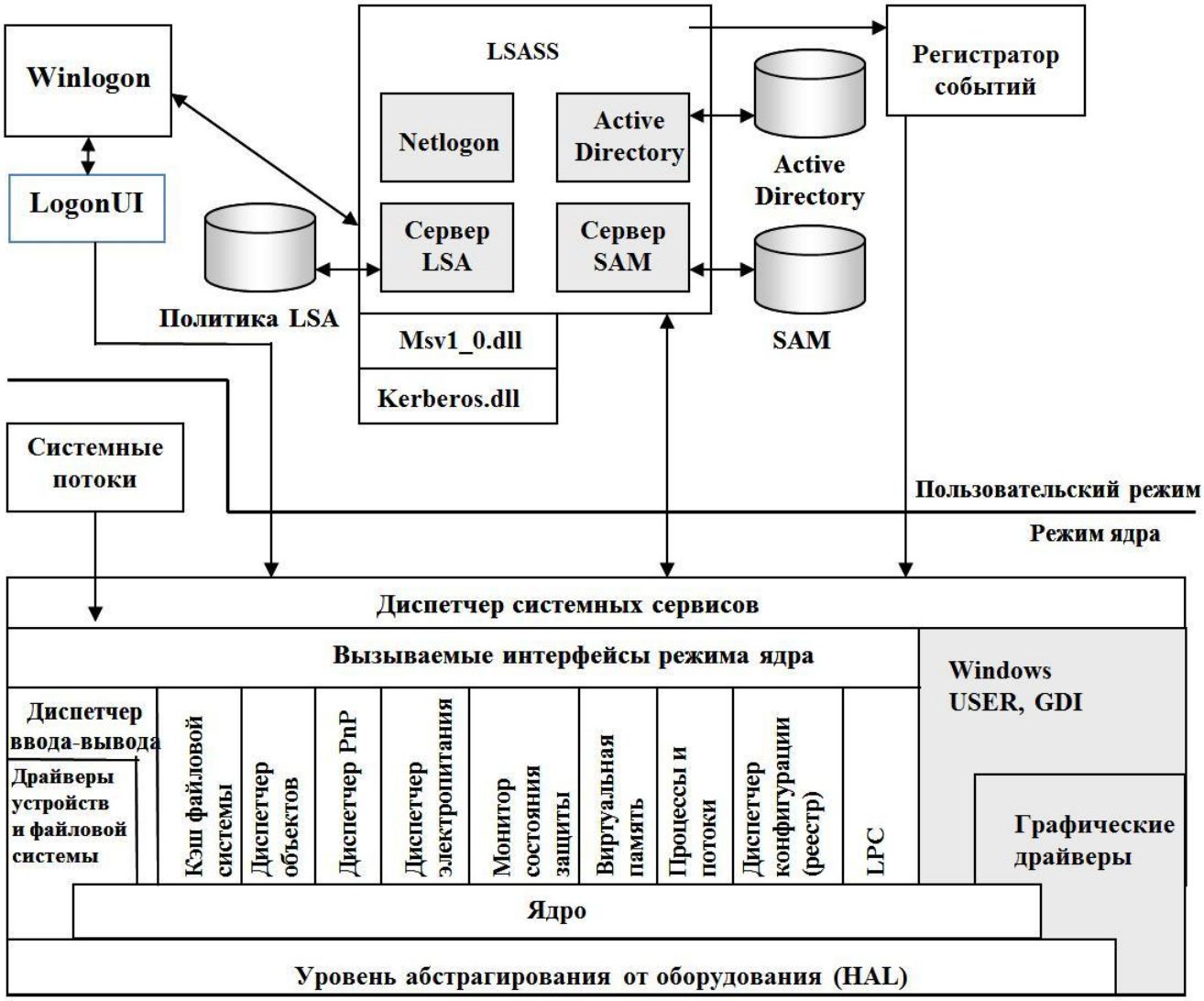
Windows Vista Enterprise
Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition
март 2011 года Windows 7 и Windows Server 2008 R2
2015-01-09 Microsoft Windows 8 and Windows Server 2012

http://www.commoncriteriaportal.org/

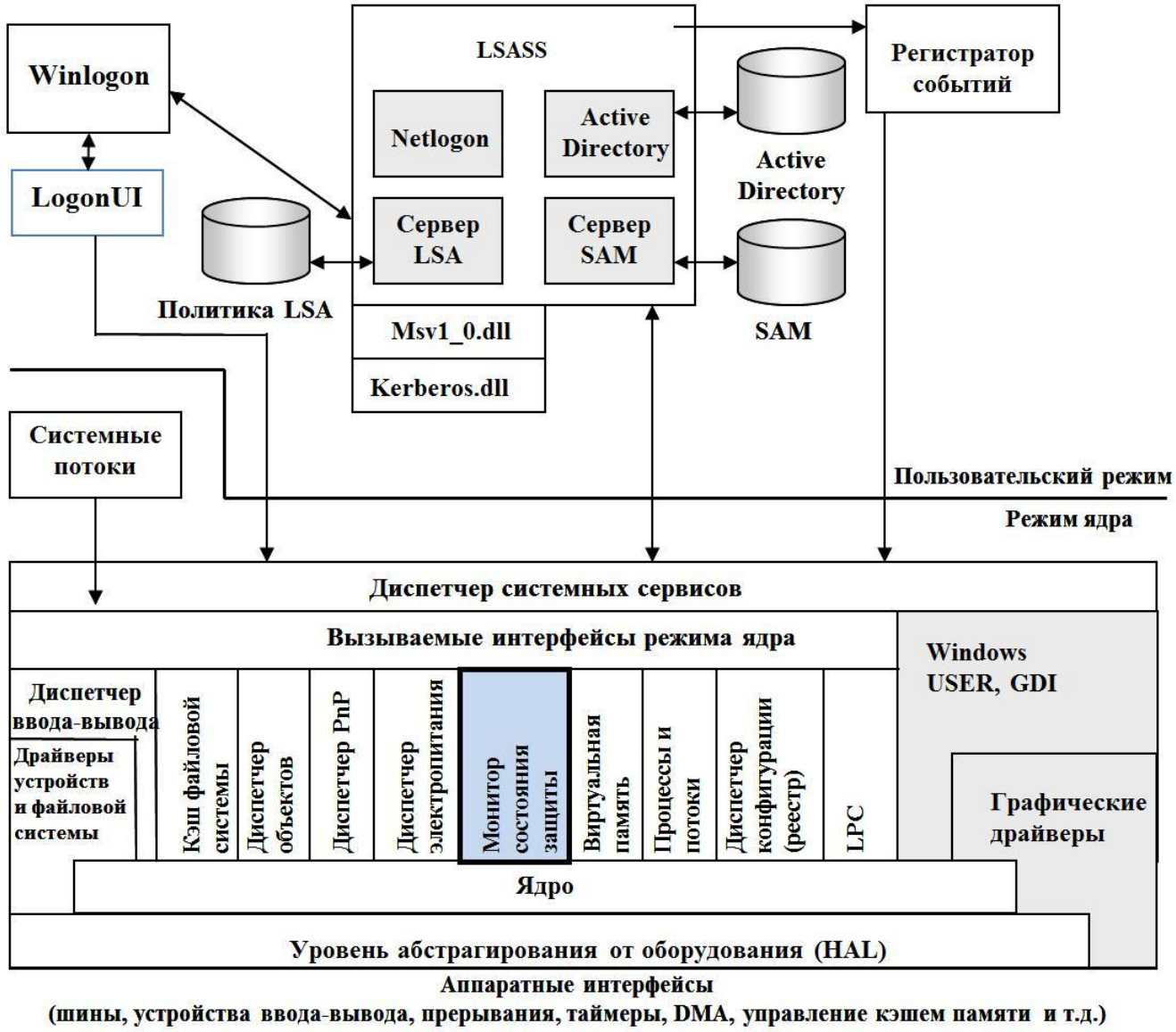
Главные компоненты и базы данных, на основе которых реализуется защита в Windows

- Монитор состояния защиты (Security Reference Monitor, SRM) (%SystemRoot%\System32\Ntoskrnl.exe)
- Подсистема локальной аутентификации (local security authentication subsystem, LSASS) (%SystemRoot%\System32\Lsass.exe)
- База данных политики LSASS (HKLM\SECURITY)
- Диспетчер учетных записей безопасности (Security Accounts Manager, SAM) (%SystemRoot%\System32\Samsrv.dll)
- База данных SAM (HKLM\SAM)
- Active Directory
- Сервер Active Directory (%SystemRoot%\System32\Ntdsa.dll)
- Пакеты аутентификации
- Процесс входа (Winlogon) (%SystemRoot%\System32\Winlogon.exe)
- Пользовательский интерфейс входа в систему Logon user interface (LogonUI) (%SystemRoot%\System32\\LogonUI.exe)
- Служба сетевого входа (Netlogon) (\Windows\System32\Netlogon.dll)
- Kernel Security Device Driver (KSecDD) (%SystemRoot%\System32\Ksecdd.sys)

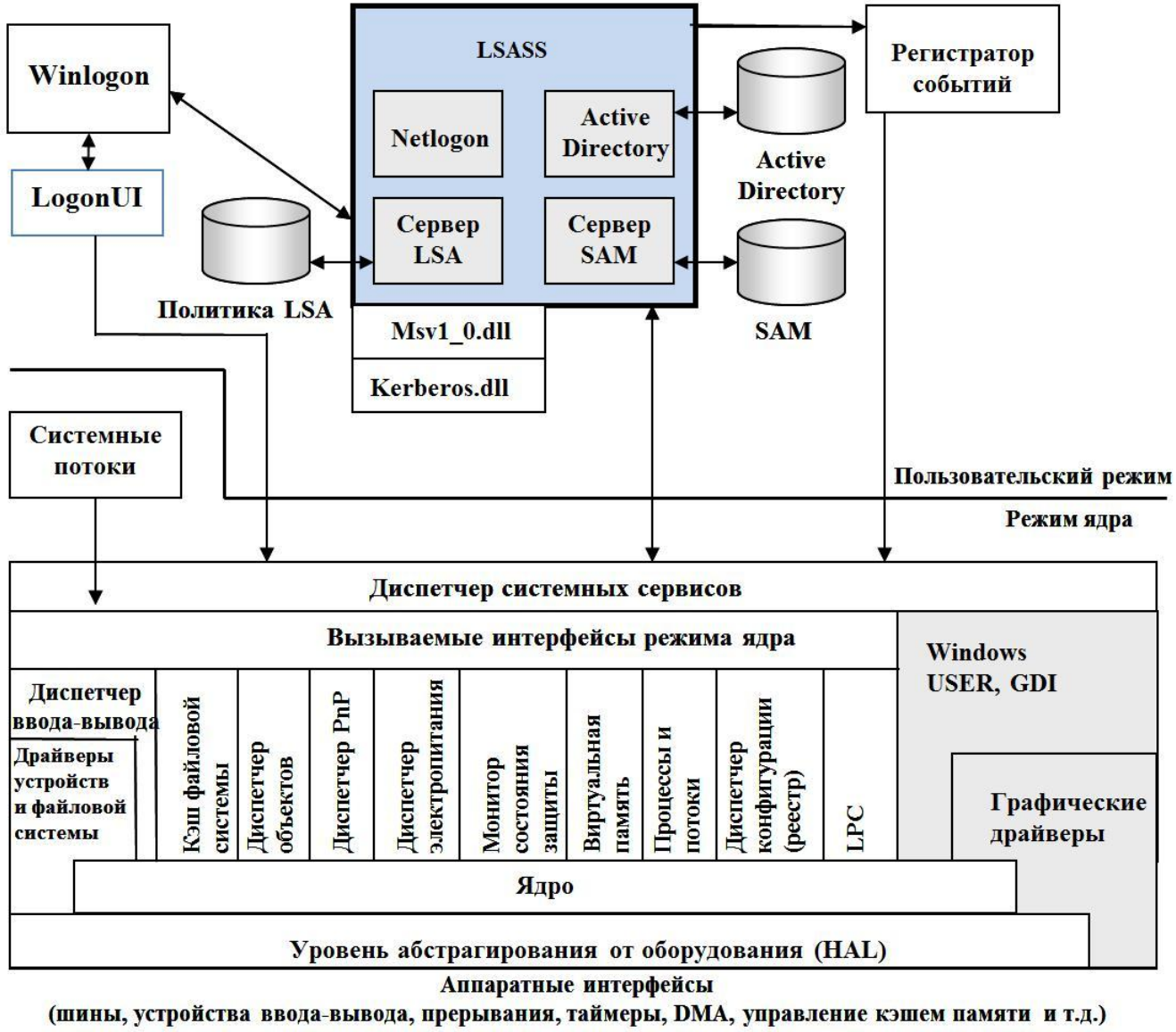
Компоненты системы защиты



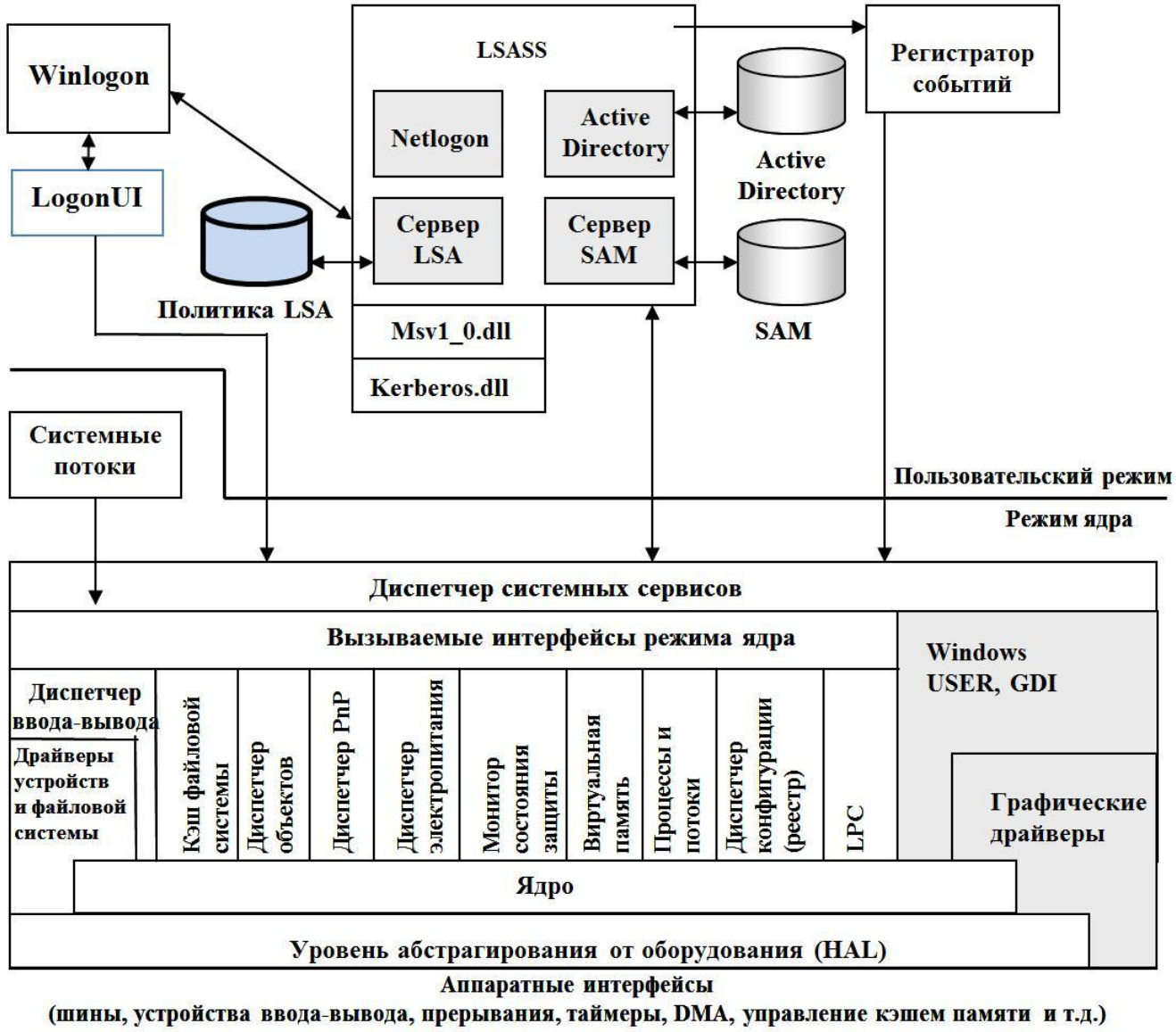
- Монитор состояния защиты (Security Reference Monitor, SRM) (%SystemRoot%\System32\Ntoskrnl.exe)



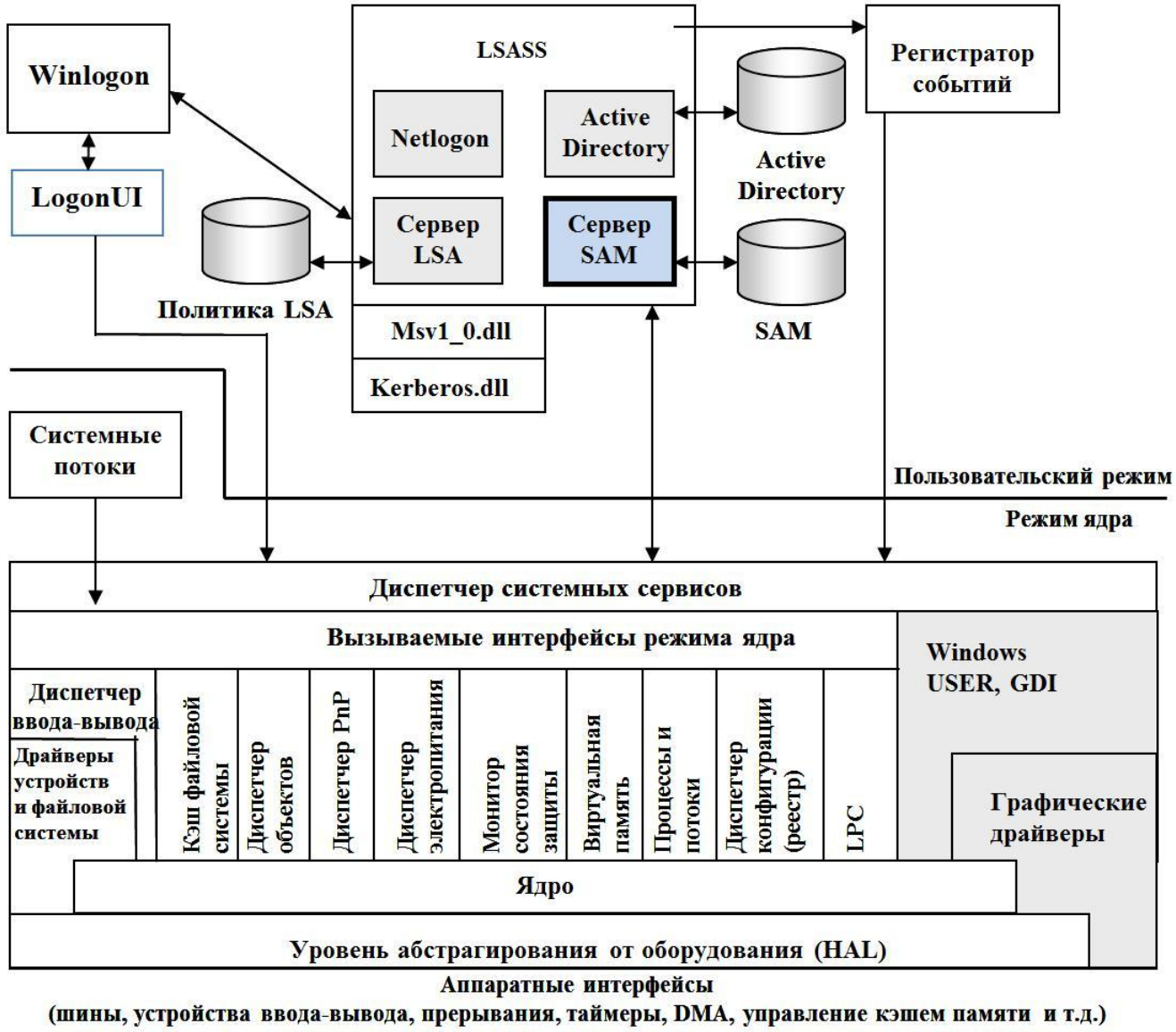
- Подсистема локальной аутентификации (local security authentication subsystem, LSASS) (%SystemRoot%\System32\Lsass.exe)



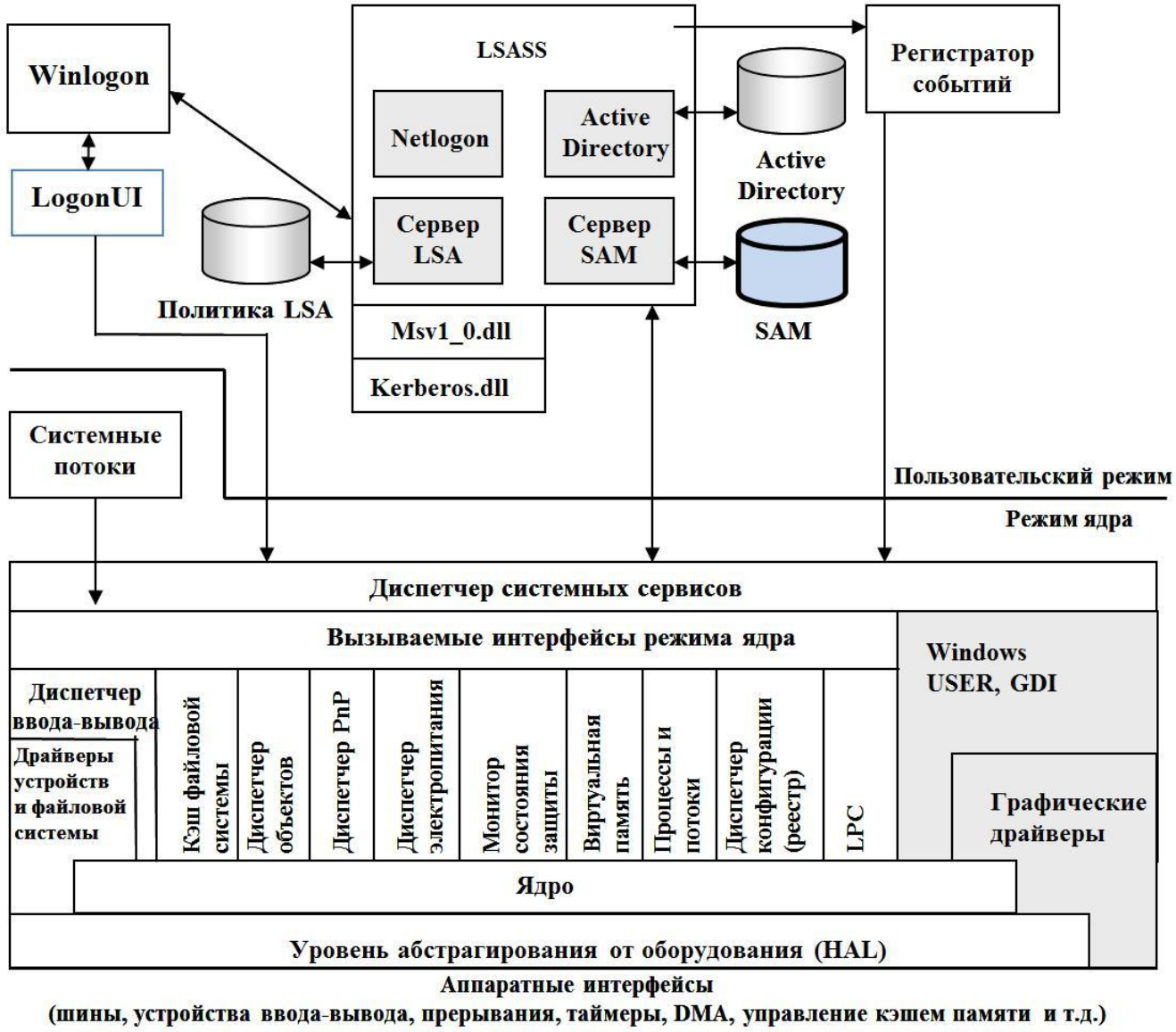
- База данных политики LSASS (HKLM\SECURITY)



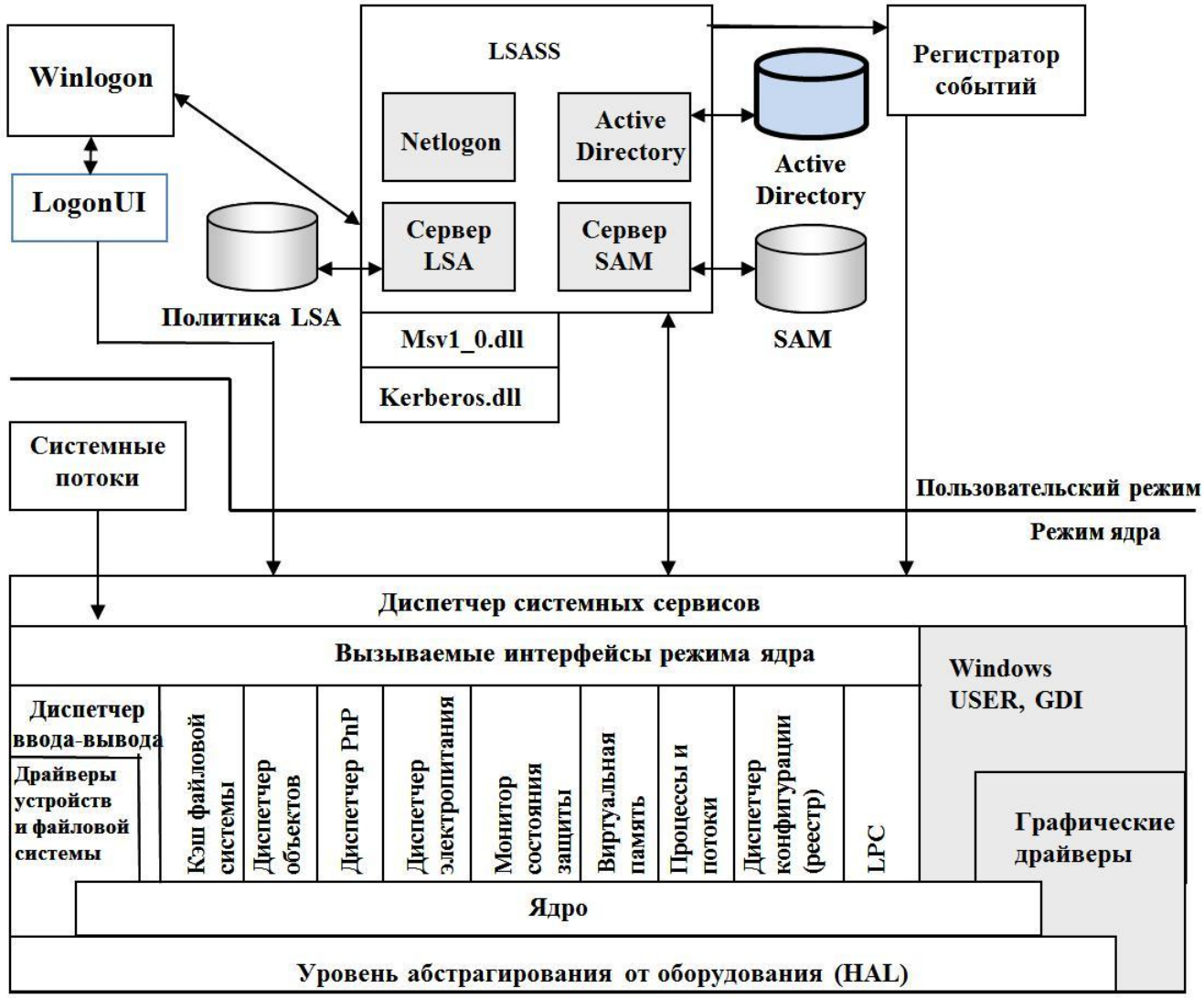
- Диспетчер учетных записей безопасности (Security Accounts Manager, SAM) (%SystemRoot%\System32\Samsrv.dll)



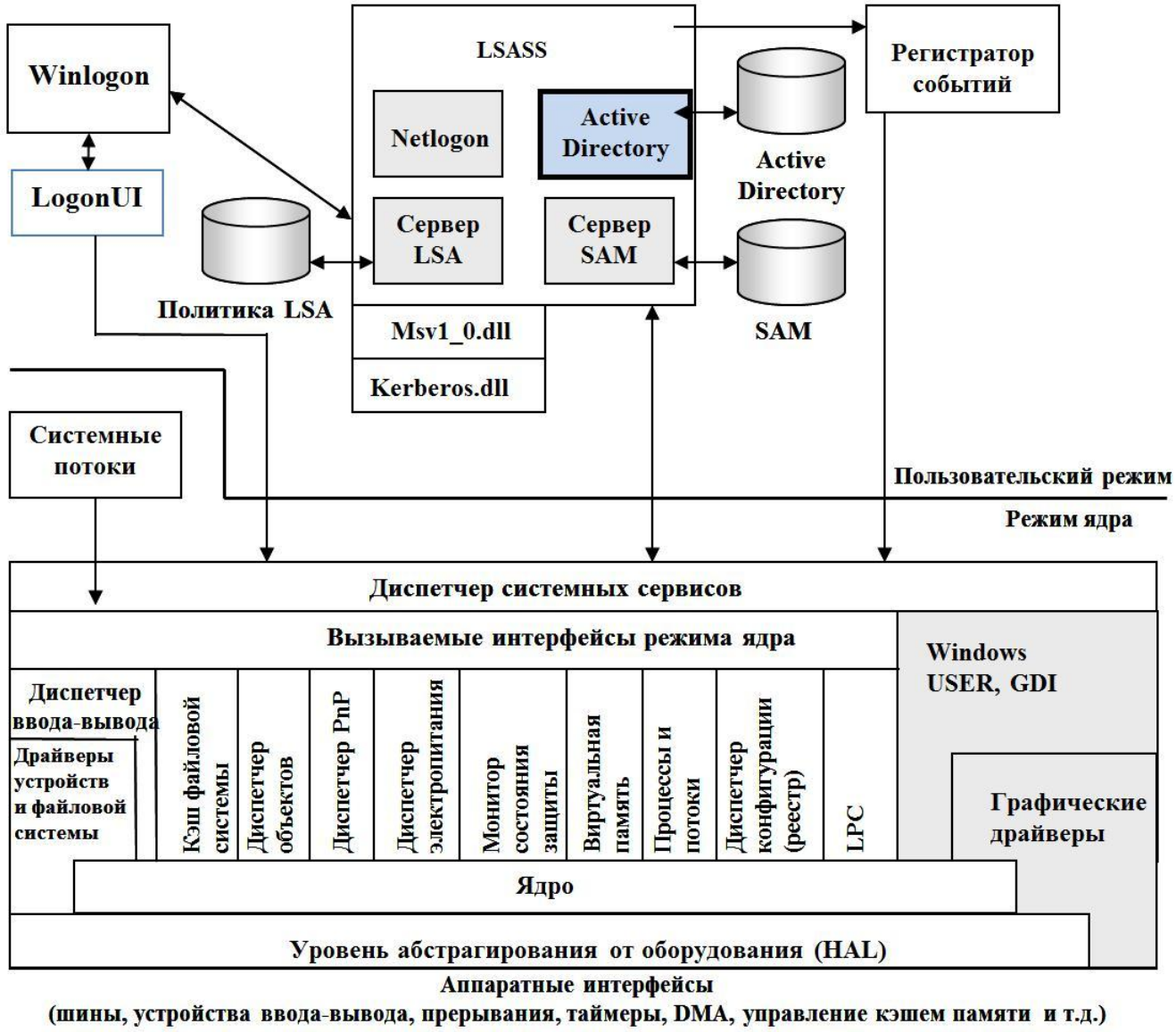
- База данных SAM (HKLM\SAM)



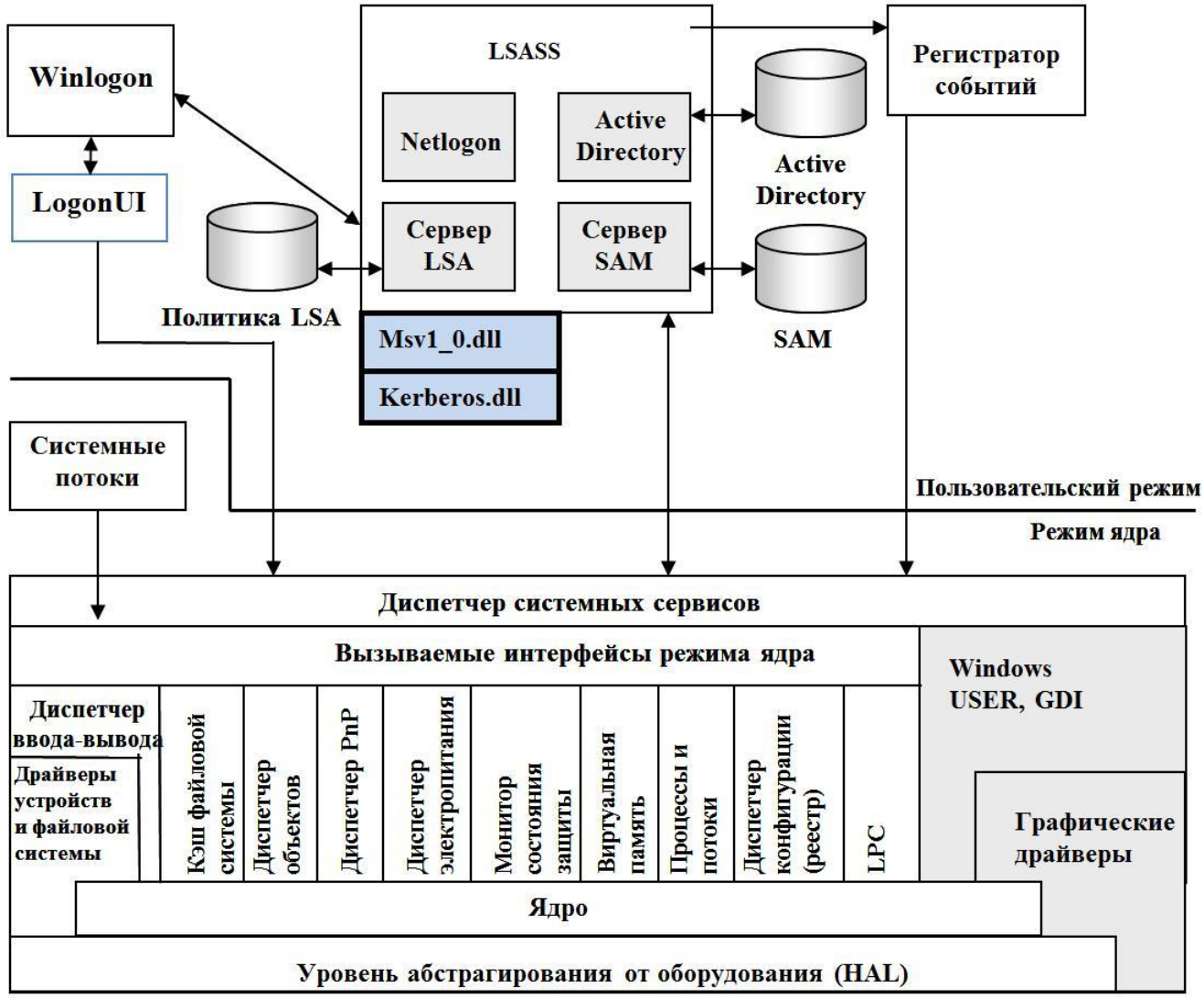
• Active Directory



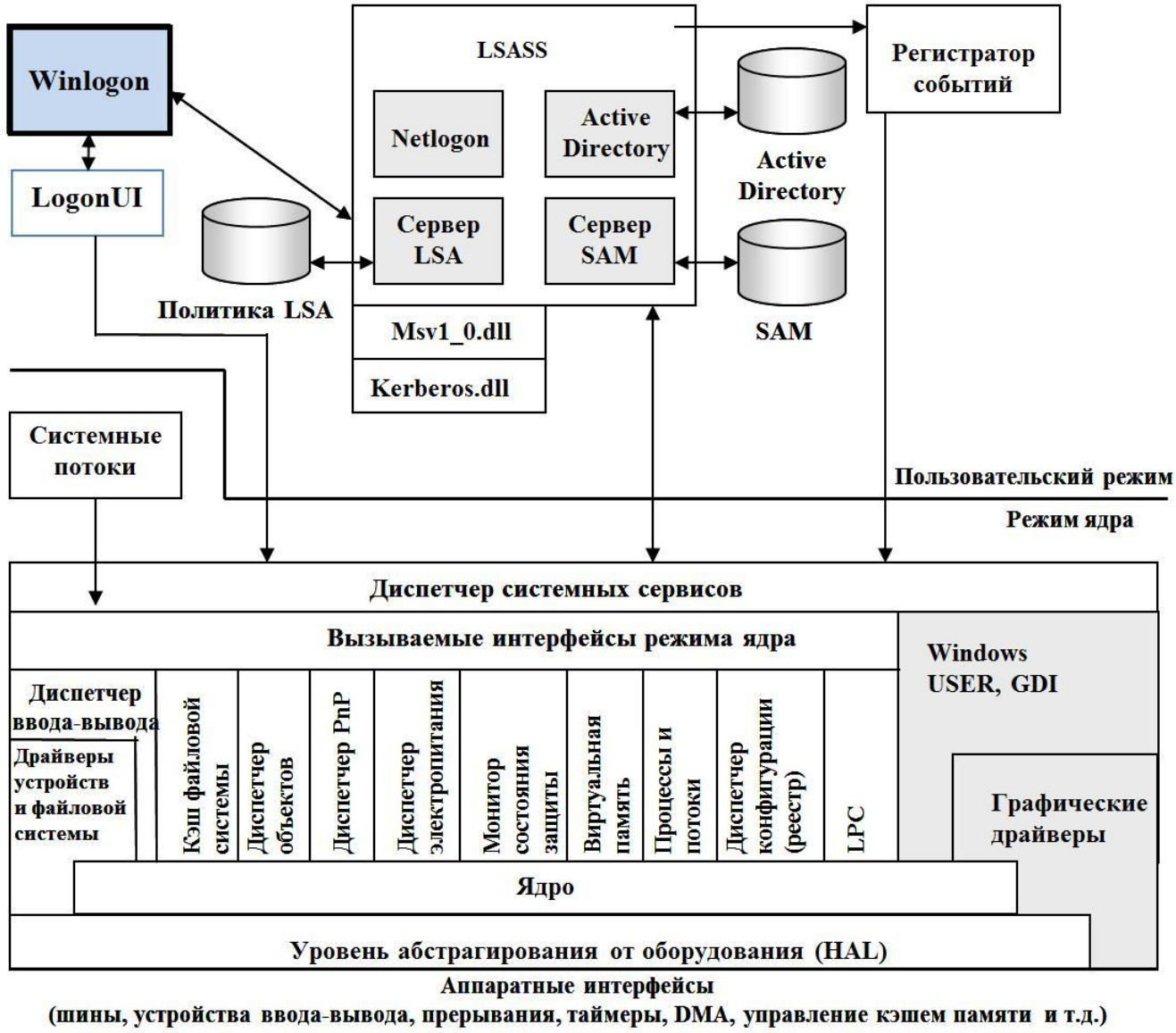
• Сервер Active Directory (%SystemRoot%\System32\Ntdsa.dll)



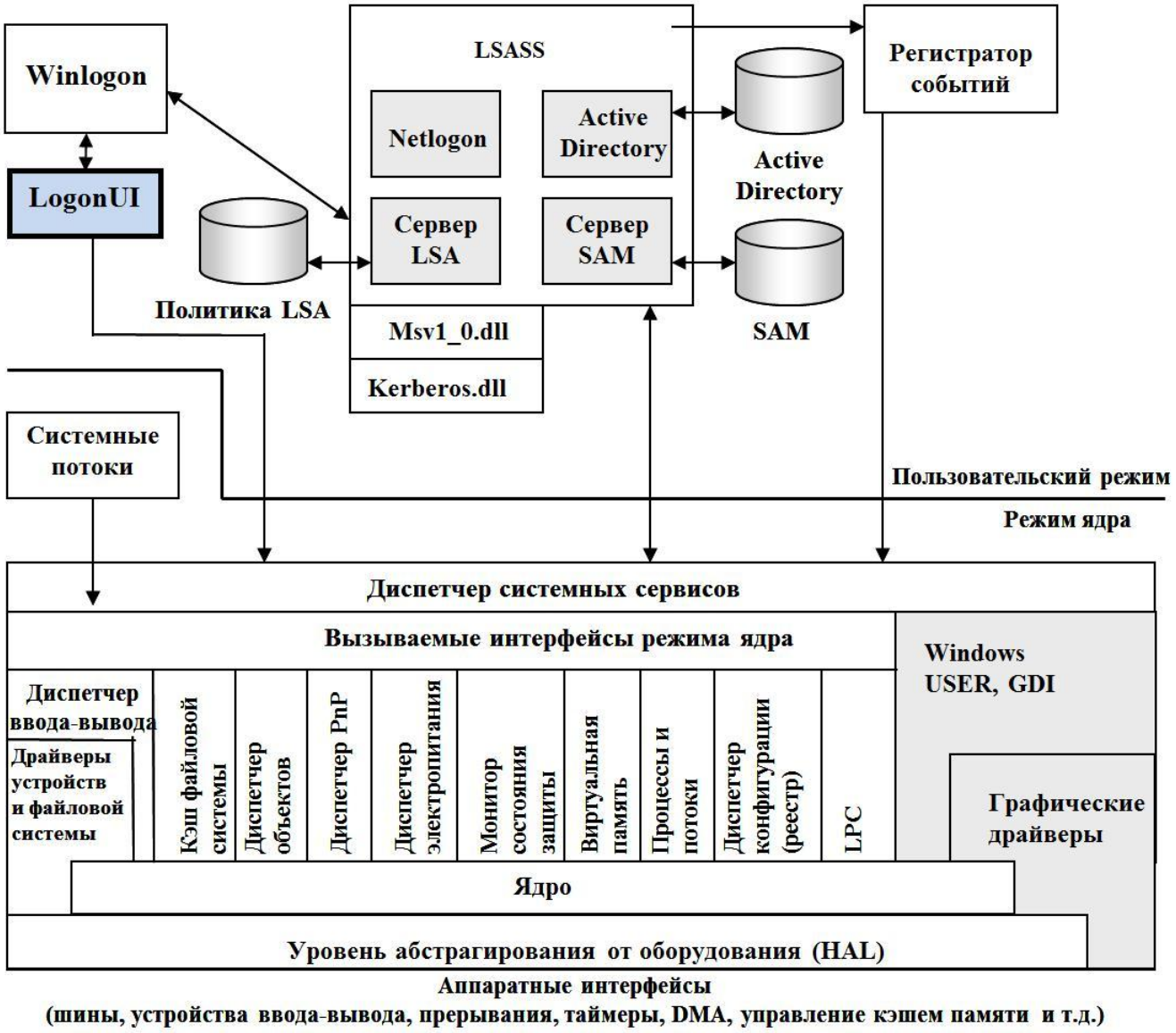
• Пакеты аутентификации



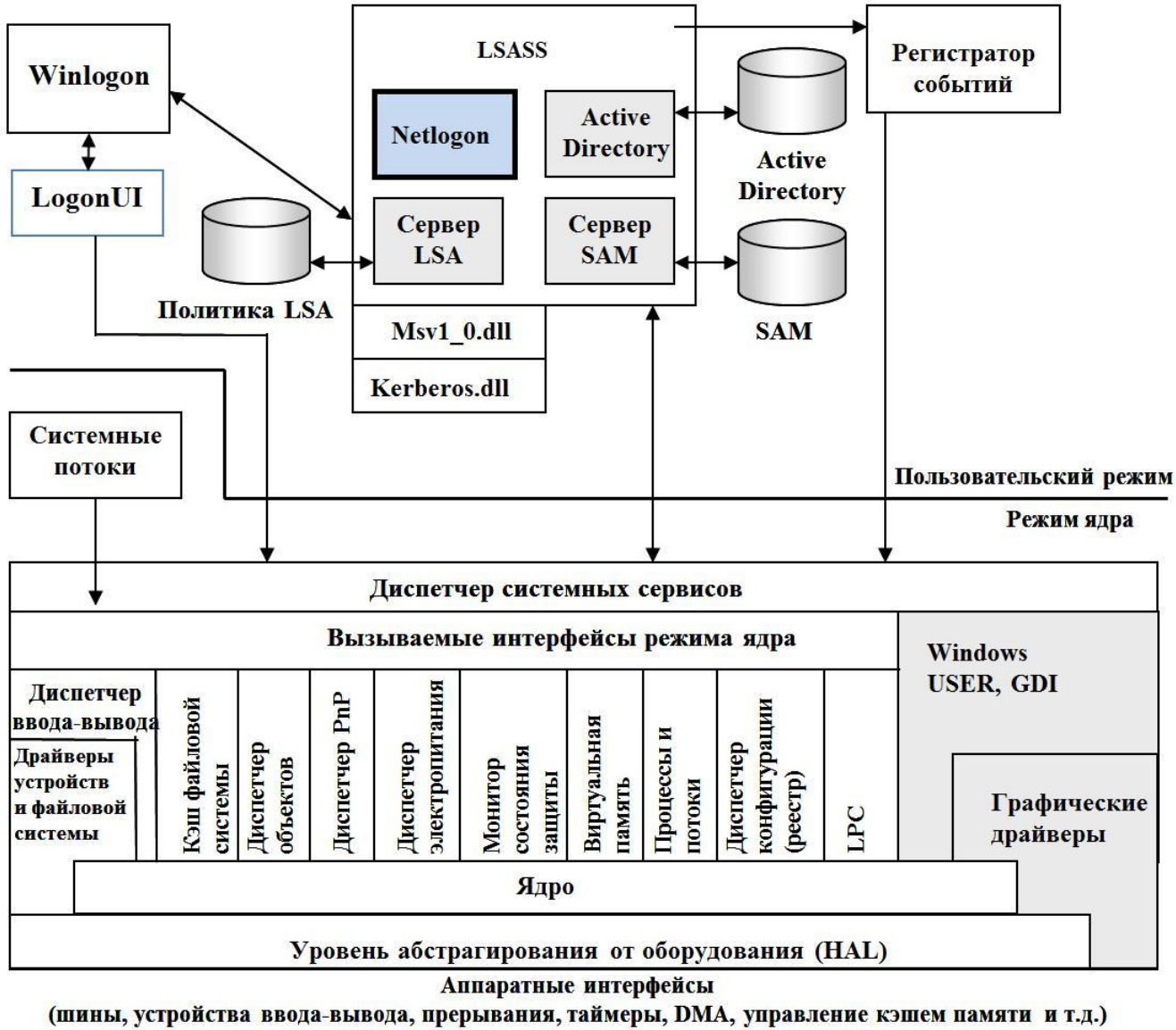
- Процесс входа (Winlogon) (%SystemRoot%\System32\Winlogon.exe)



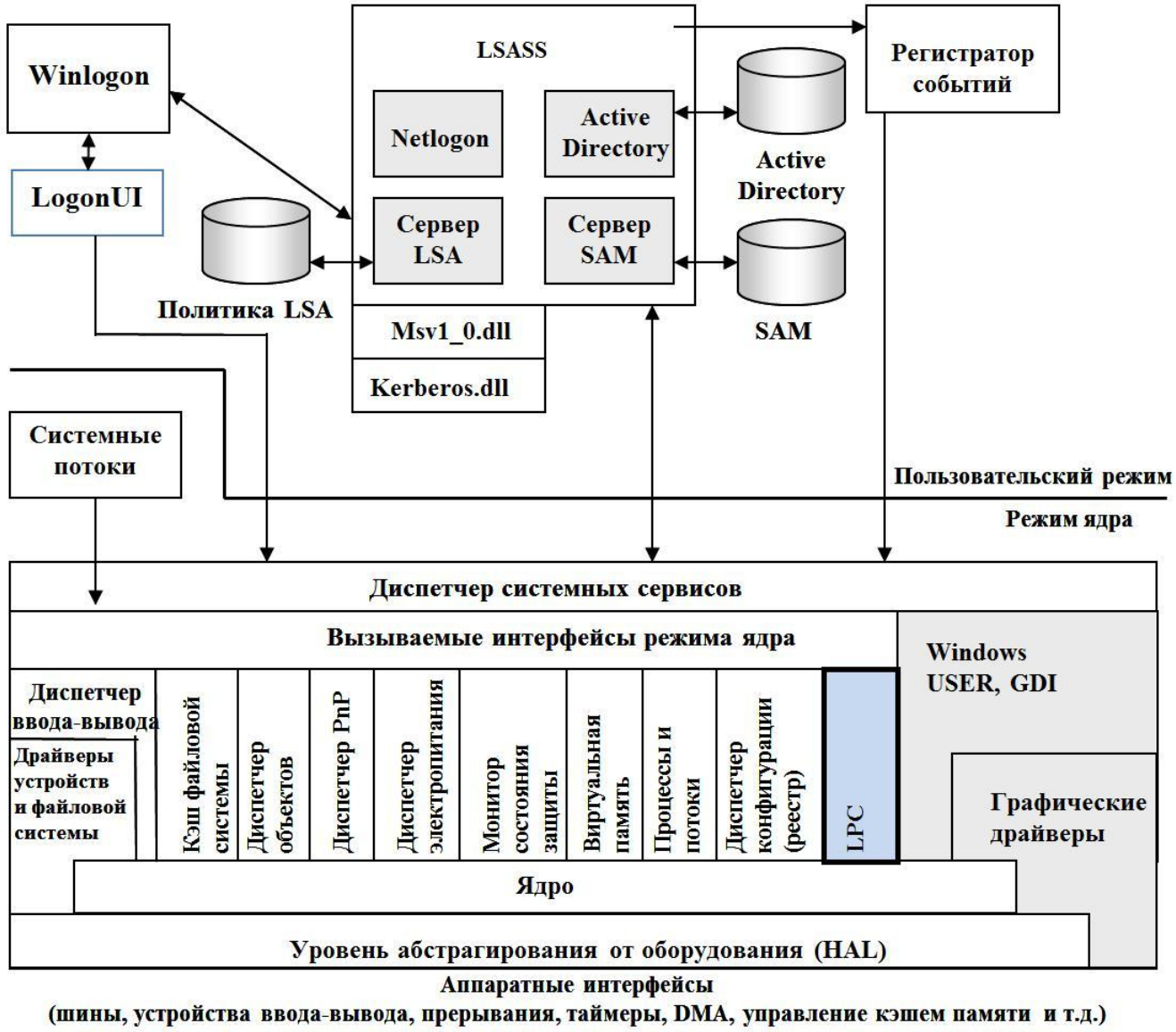
- Пользовательский интерфейс входа в систему Logon user interface (LogonUI) (%SystemRoot%\System32\\LogonUI.exe)



- Служба сетевого входа (Netlogon) (%SystemRoot%\System32\Netlogon.dll)



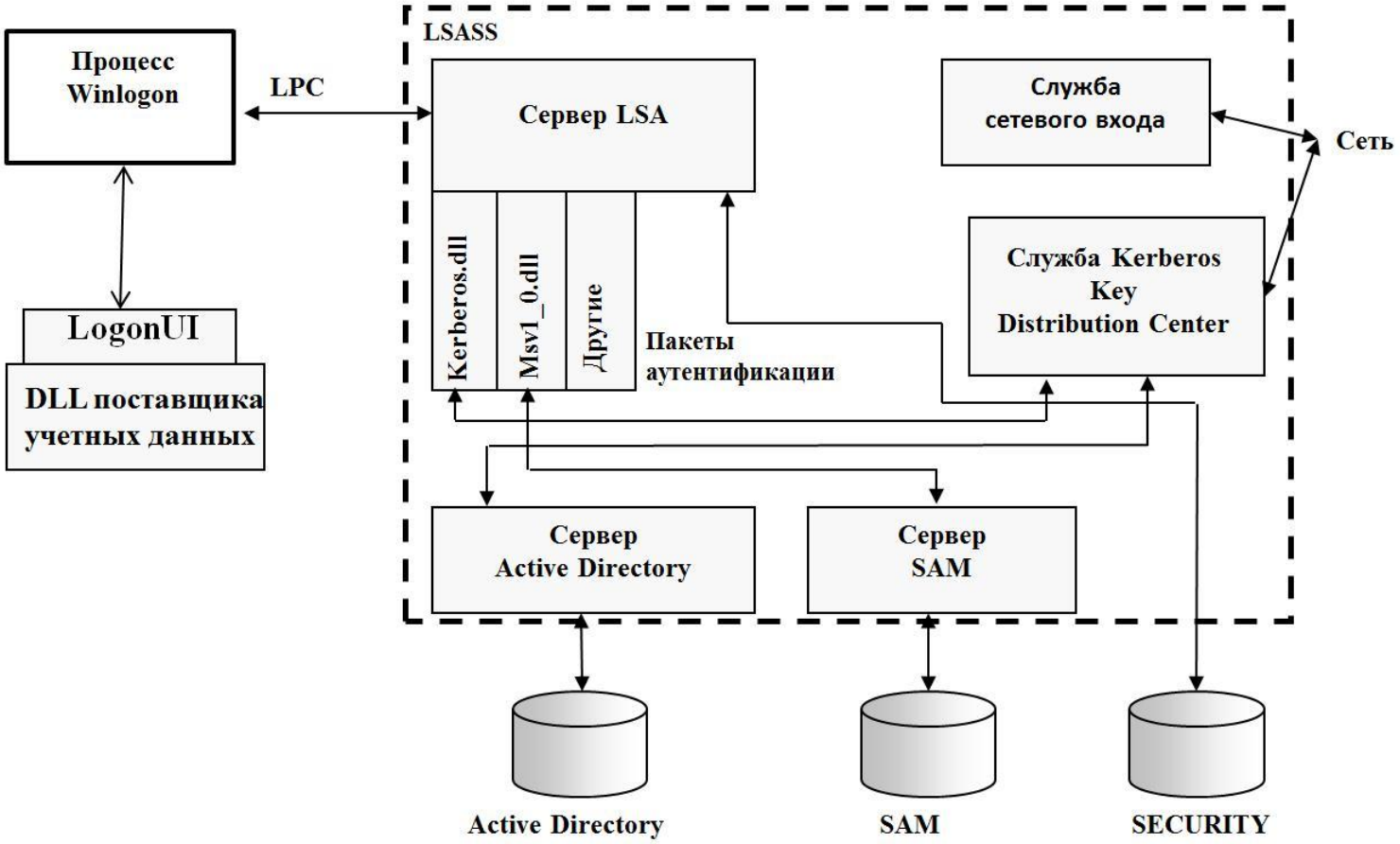
- Kernel Security Device Driver (KSecDD) (%SystemRoot%\System32\Ksecdd.sys)



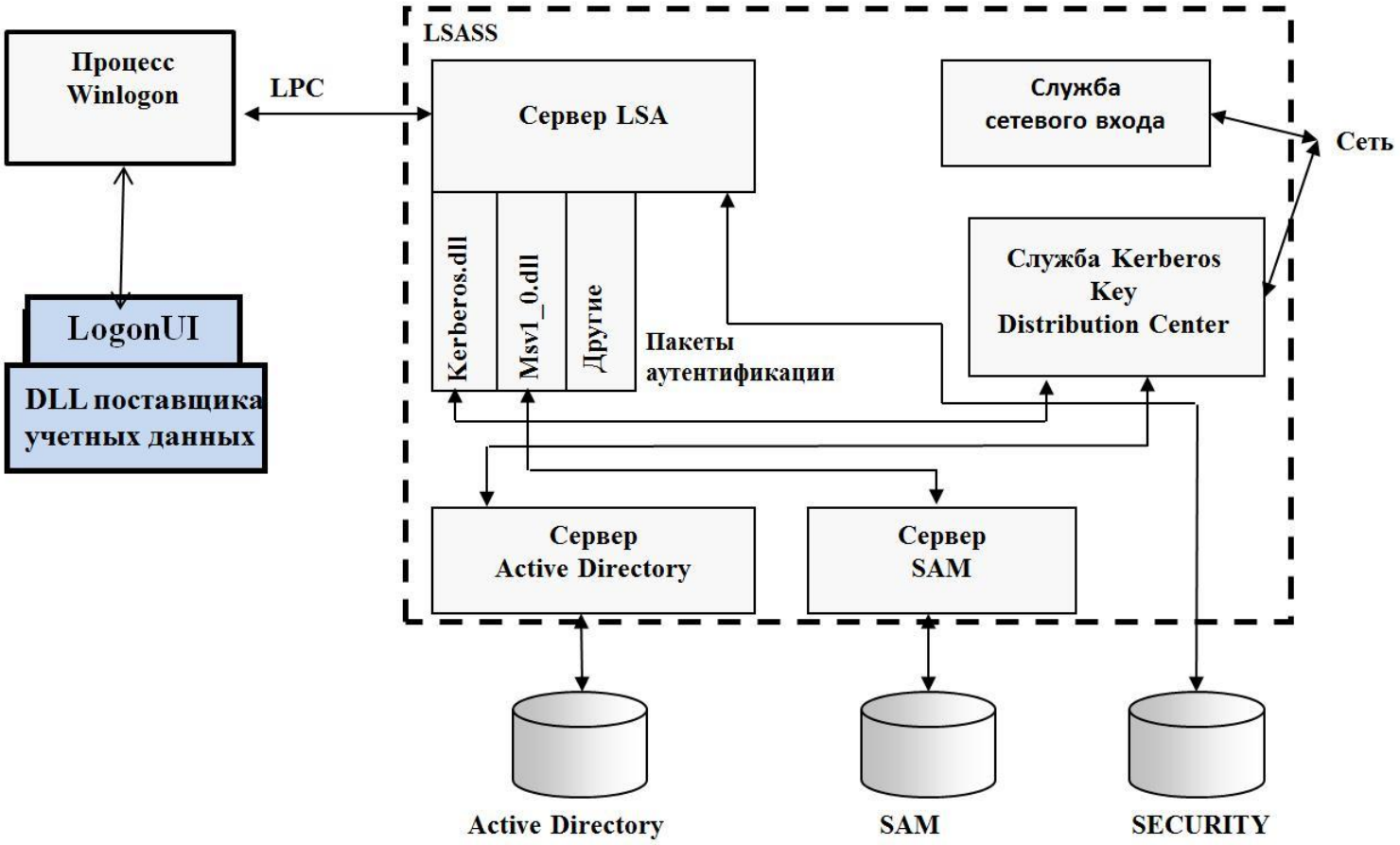
Идентификация, аутентификация и авторизация пользователей

- Архитектура подсистемы аутентификации
- Параметры аутентификации

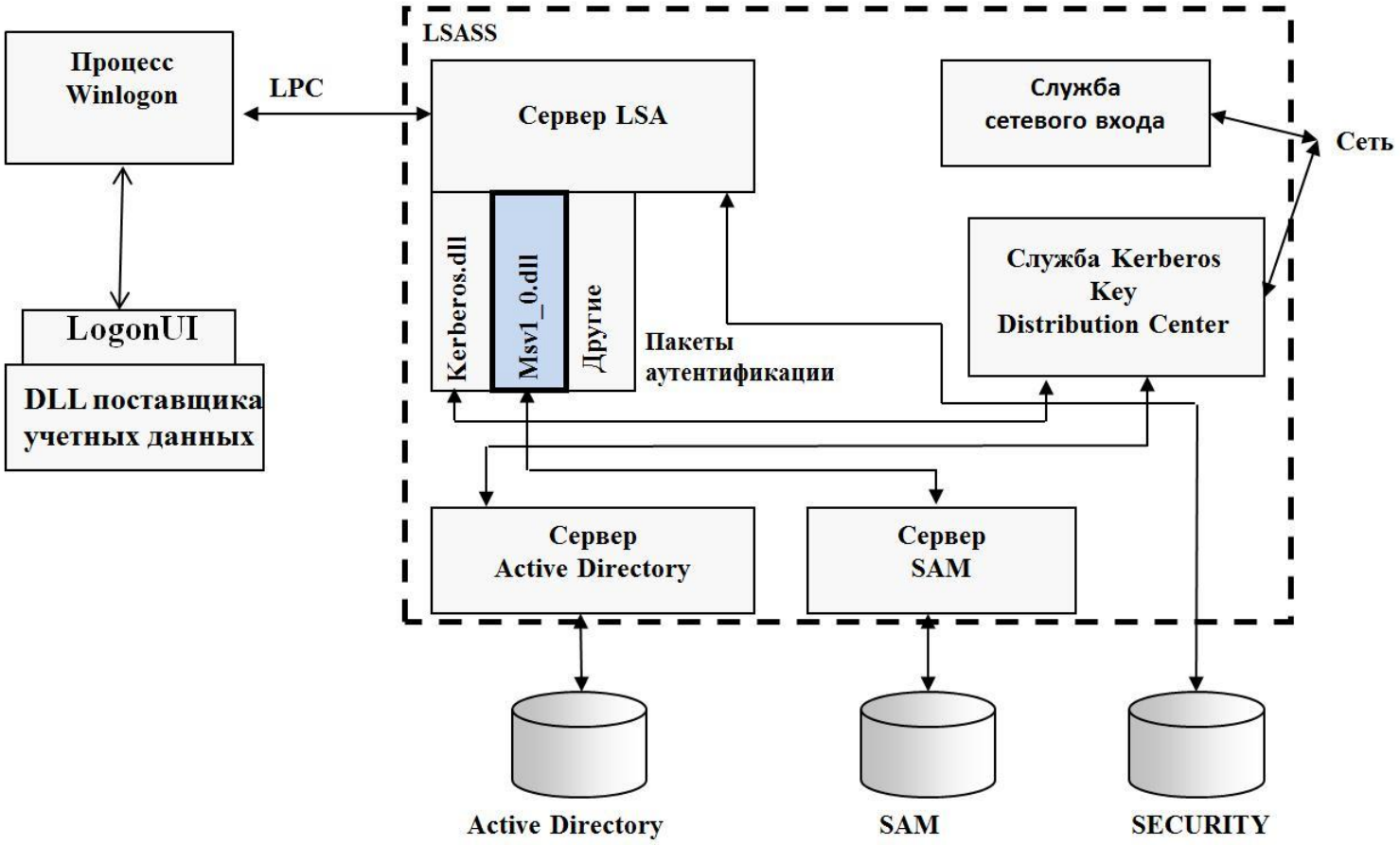
Архитектура подсистемы аутентификации



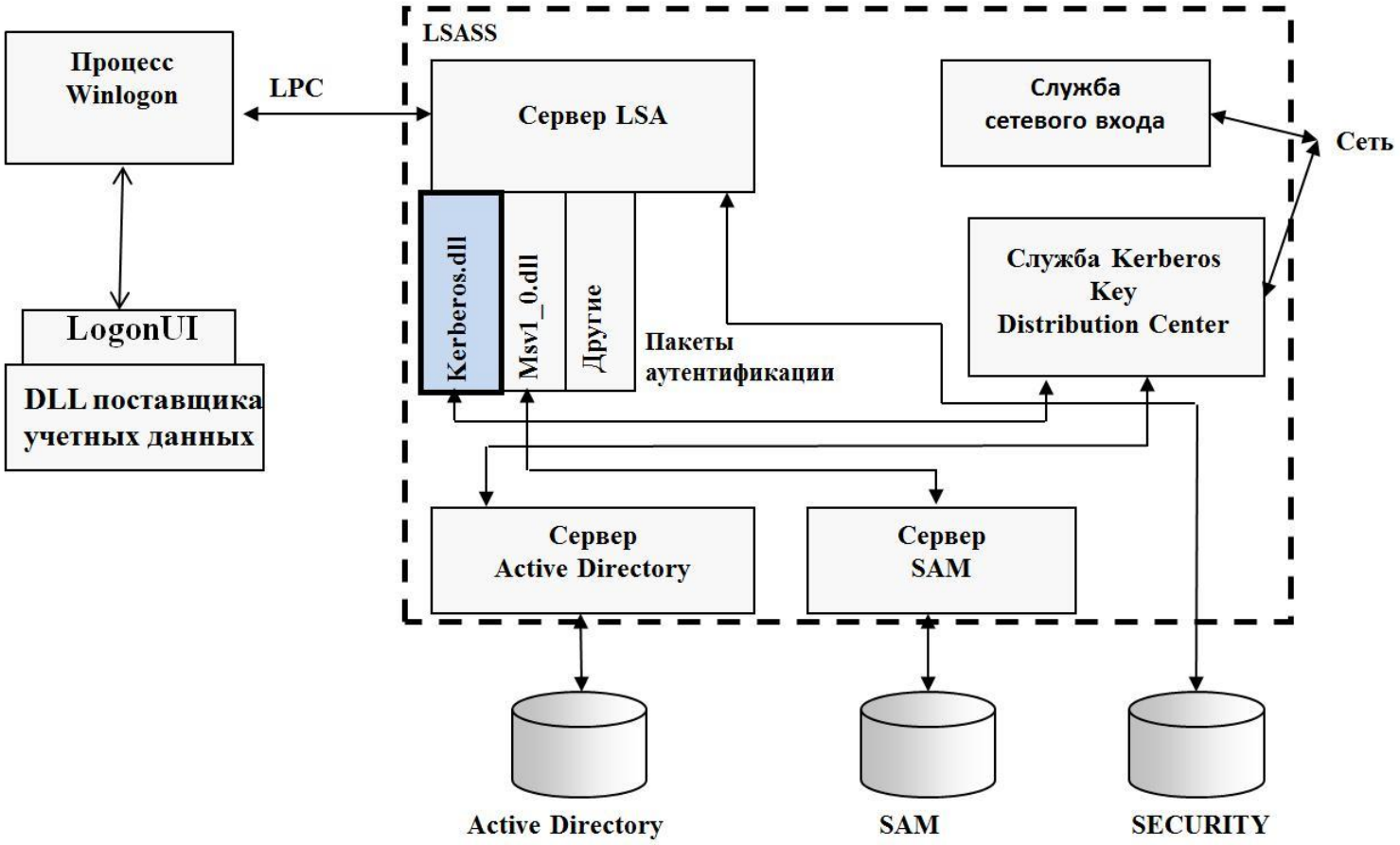
Архитектура подсистемы аутентификации



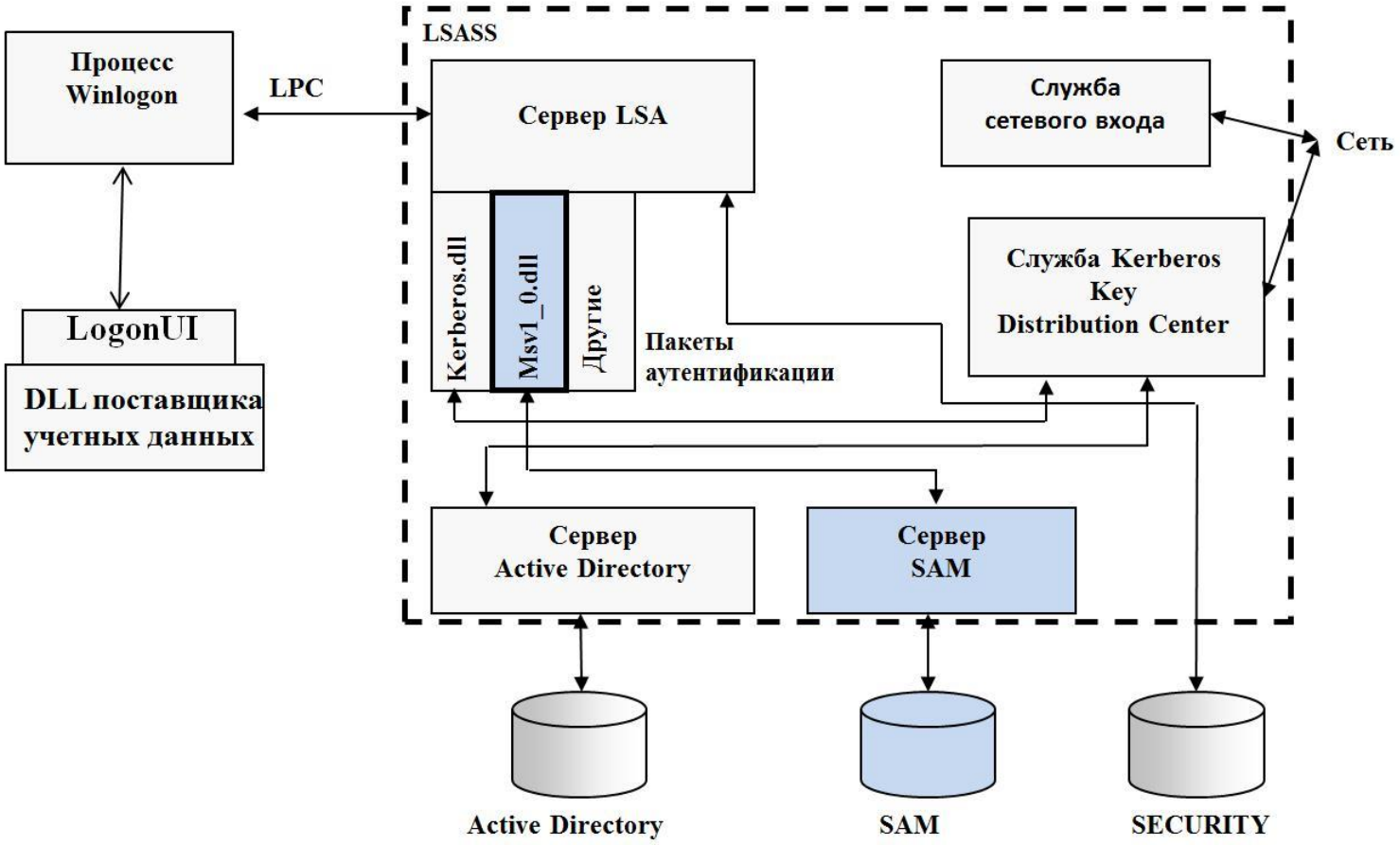
Архитектура подсистемы аутентификации



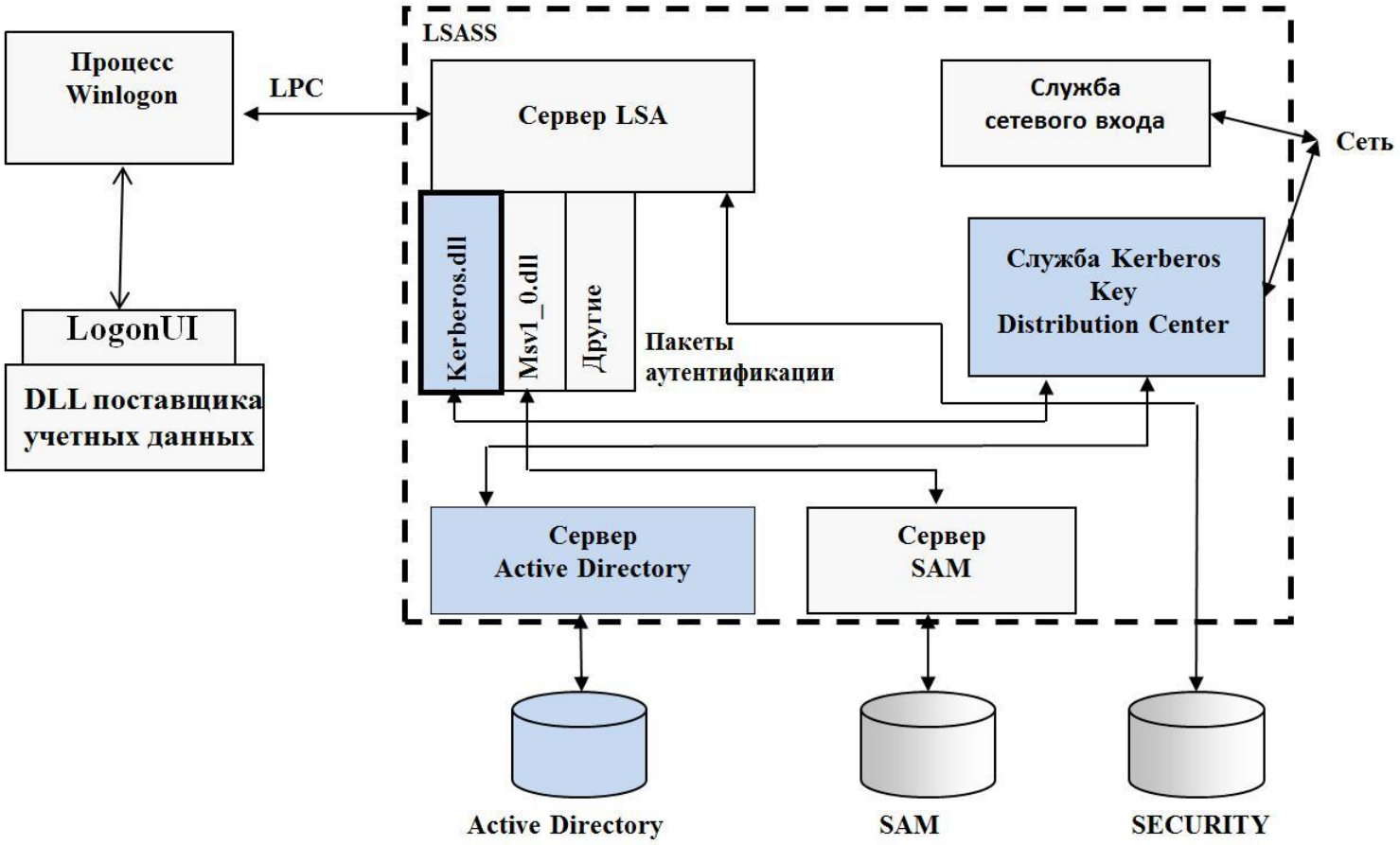
Архитектура подсистемы аутентификации



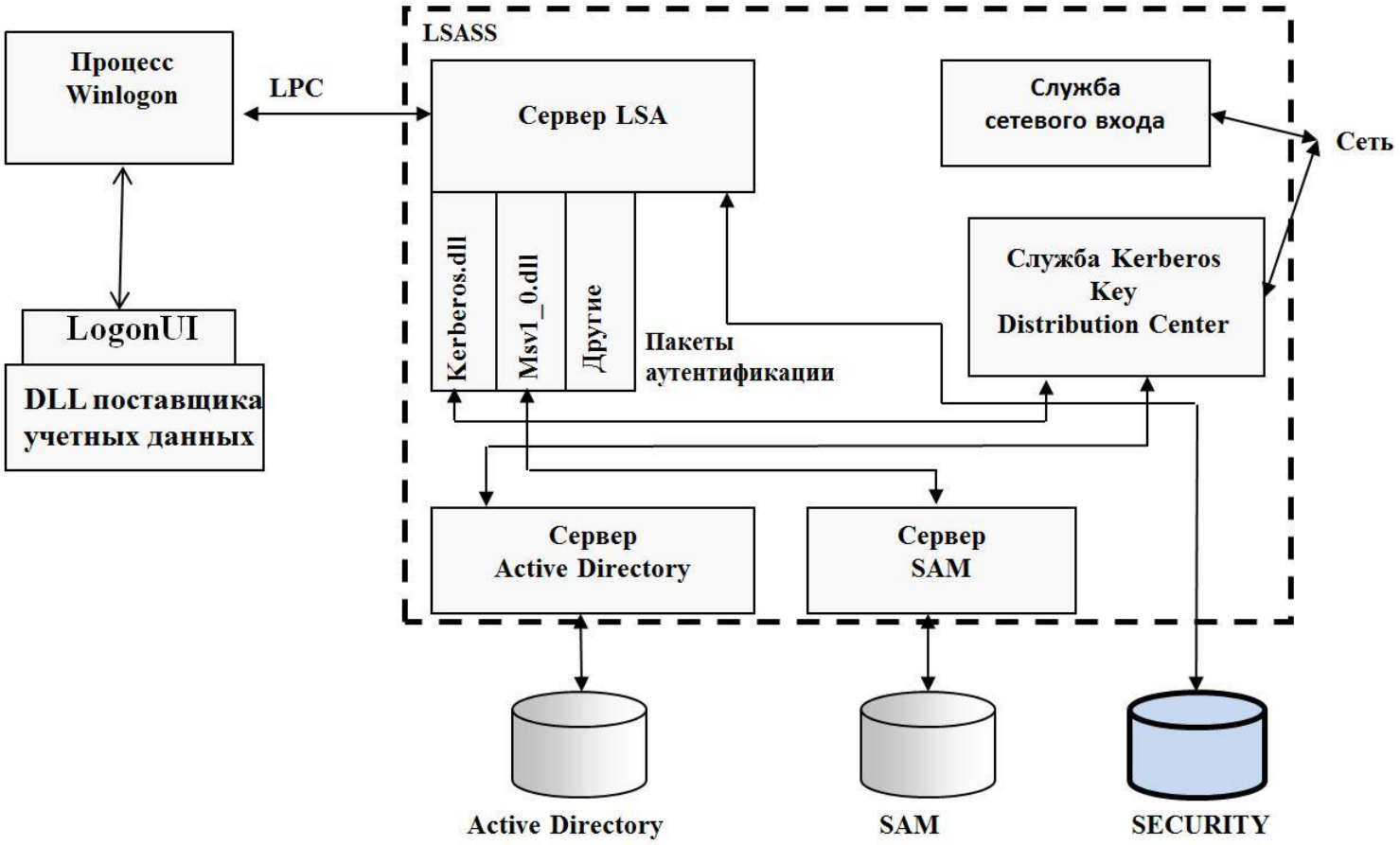
Архитектура подсистемы аутентификации



Архитектура подсистемы аутентификации



Архитектура подсистемы аутентификации



Формат паролей и хранилище паролей

- хешированные пароли для локальных учетных записей хранятся в локальной базе данных SAM
- хешированные пароли для учетных записей домена хранятся в базе данных Active Directory.

Методы хеширования пользовательских паролей

- LM (LanMan)
- NTLM

Разграничение доступа

- Объекты
- Субъекты
- Пользователи и группы пользователей
- Идентификатор безопасности
- Дескриптор безопасности
- Маркер доступа
- Порядок проверки прав доступа субъекта к объекту
- Права и привилегии учетных записей

Объекты доступа

1. Файловые объекты (файлы, дисковые директории, устройства, каналы, почтовые ящики (mailslots))
2. Объектовые директории
3. Ключи реестра (registry keys)
4. Процессы
5. Потоки или нити (threads)
6. Диспетчер сервисов (service control manager)
7. Сервисы (services)
8. Объекты управления окнами (window-management objects) (рабочие столы или рабочие поля (desktops), оконные станции (window stations))
9. Порты (ports)
10. Секции разделяемой памяти (shared memory sectons)
11. Символические связи (symbolic links)
12. Маркеры доступа (access tokens)
13. Объекты синхронизации (события (events) , пары событий (events pairs), семафоры (semaphores), мьютексы (mutexes))

Субъекты доступа

1. Пользователи (обычные и псевдопользователи)

псевдопользователи:

- SYSTEM - операционная система локального компьютера
- псевдопользователи с именами вида <имя_компьютера>$, где <имя_компьюгера> - сетевое имя компьютера

2. Группы пользователей

3. Специальные (временные) группы (INTERACTIVE, NETWORK и т.д.)

4. Относительные субъекты

CREATOR_OWNER - владелец объекта;

CREATOR_GROUP - первичная группа владельца объекта.

Предопределенные субъекты доступа:

- *Administrator* - администратор операционной системы
- *Guest* - гость операционной системы, пользователь с минимальными правами
- *Administrators* - группа администраторов операционной системы
- *Users* - группа пользователей операционной системы
- *Backup Operators* - группа операторов резервного копирования
- *Replicator* - субъект доступа, используемый при автоматической репликации файлов и ключей реестра между компьютерами домена.

На рабочих станциях Windows NT

Power Users

На серверах Windows NT

Account Operators - группа пользователей, которые могут работать с учетными записями непривилегированных субъектов доступа;
Print Operators - группа администраторов печати;
Server Operators - группа операторов сервера;

В доменах Windows NT :

Domain Admins - администраторы домена;
Domain Users - пользователи домена;
Domain Guests - гости домена.

Идентификатор безопасности (security identifiers, SID)

S-R-IA-SA-RID

S - идентификатор SID
R - номер редакции (revision).
IA - источник выдачи (issuing authority).
SA - уполномоченный центр (sub-authority).
RID - относительный идентификатор.

S-1-5-21-1463437245-1224812800-863842198-**1028**
S-1-5-21-1463437245-1224812800-863842198-**500**
S-1-5-21-1463437245-1224812800-863842198-**501**

Субъекты доступа которые имеют предопределенные идентификаторы

- SYSTEM;
- Everyone - группа, в которую входят все пользователи и псевдопользователи; S-1-1-0
- INTERACTIVE; S-1-5-4
- NETWORK; S-1-5-2
- DIAL_UP;
- CREATOR_OWNER;
- CREATOR_GROUP

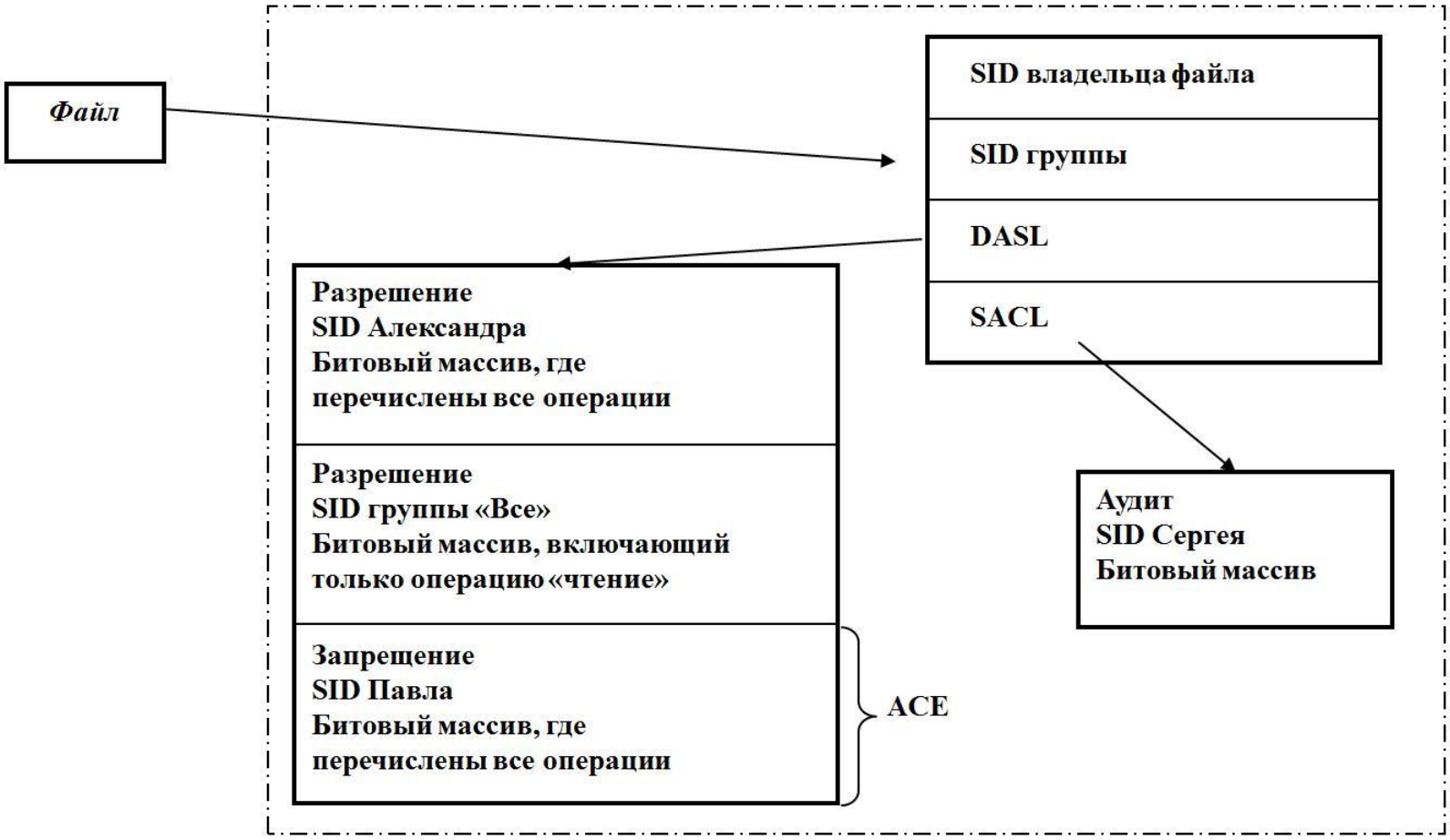
Дескриптор безопасности

- **Номер версии**. Версия модели защиты монитора состояния защиты, использованной для создания дескриптора.
- **Флаги.**
- **SID владельца**. Идентификатор безопасности владельца.
- **SID группы.** Идентификатор безопасности основной группы для данного объекта.
- **Список управления избирательным доступом** (discretinary access control list, DACL)
- **Системный список управления доступом** (system access control list, SACL)

ACL список - это набор *записей контроля доступа (Access Control Entry — ACE)*, каждая запись *состоит:*

- *идентификатор безопасности (SID), который представляет участника системы безопасности*
- *маска доступа (Access Mask), которая определяет разрешения для этого участника безопасности.*

Дескриптор безопасности

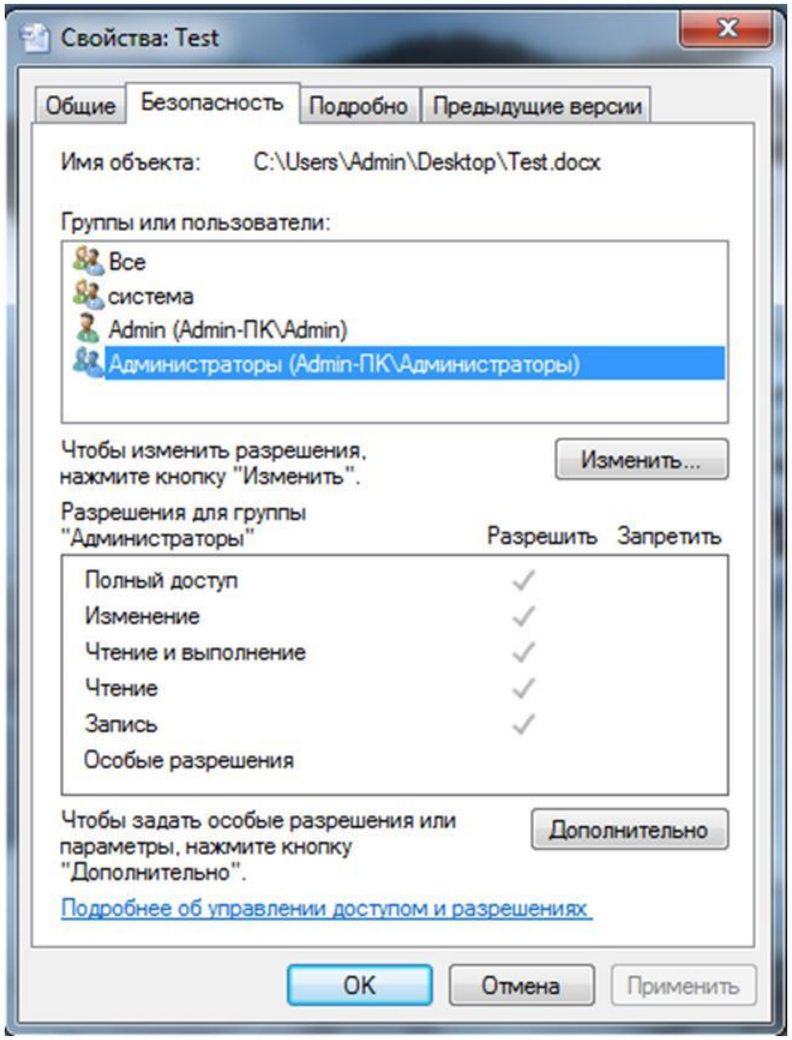


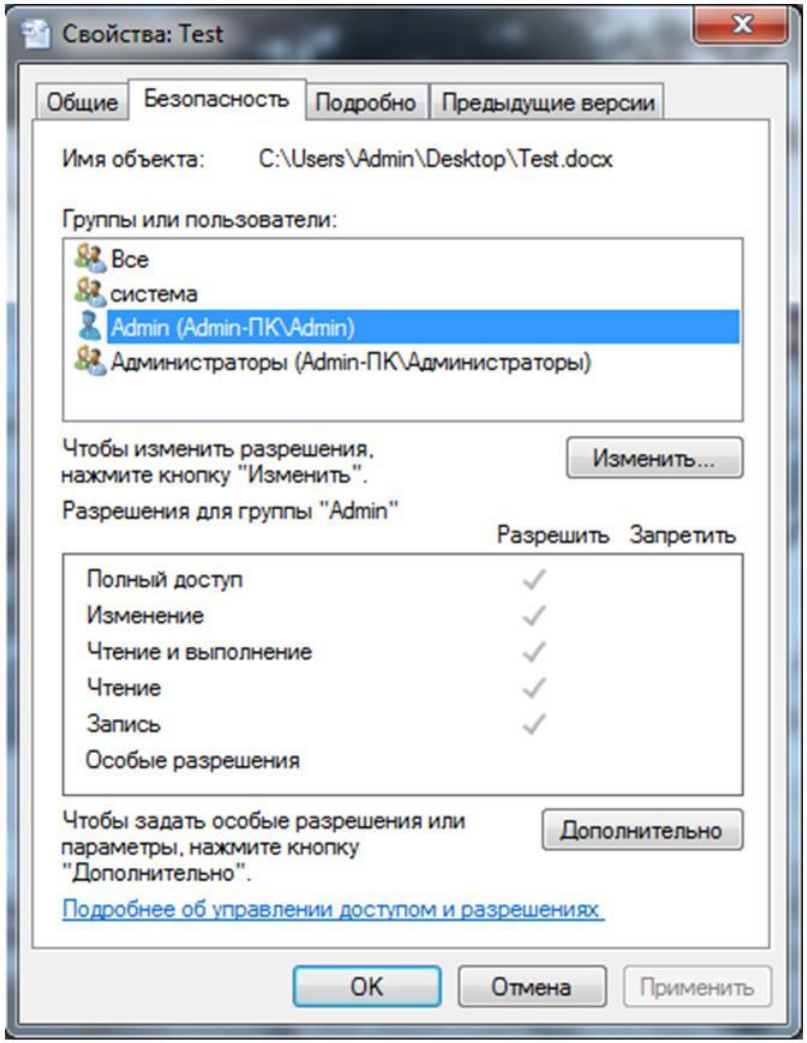
Порядок следования строк ACE в финальном списке

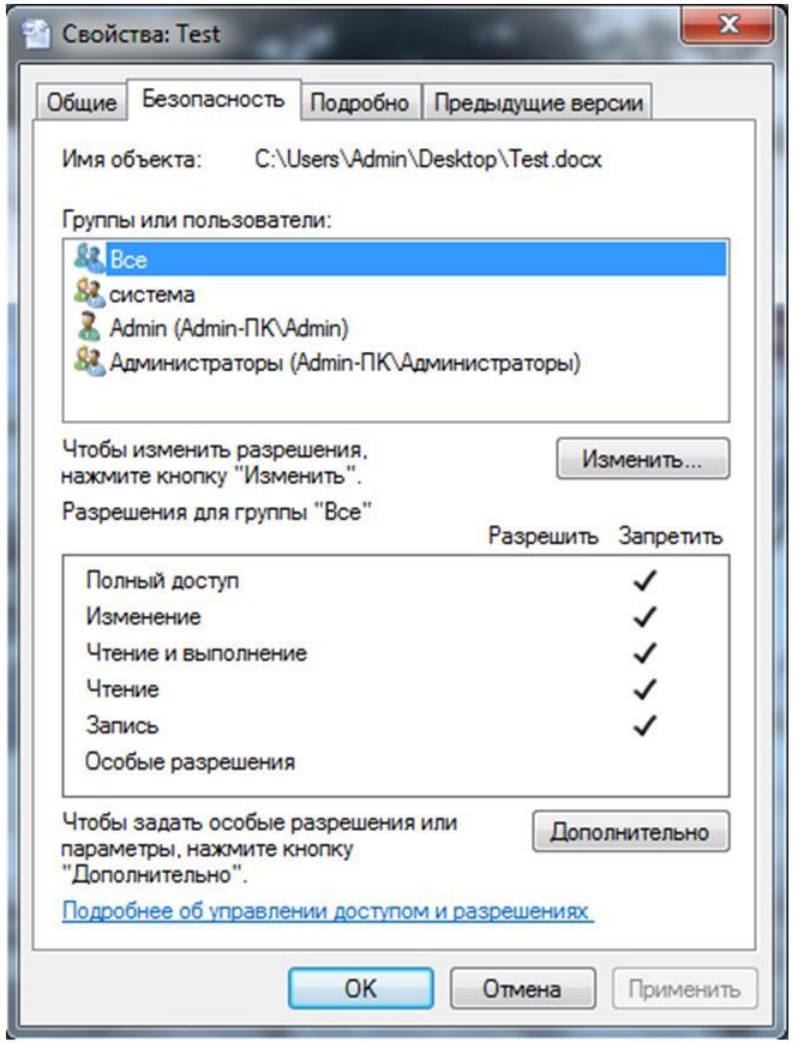
- явные запреты
- явные разрешения
- унаследованные запреты
- унаследованные разрешения

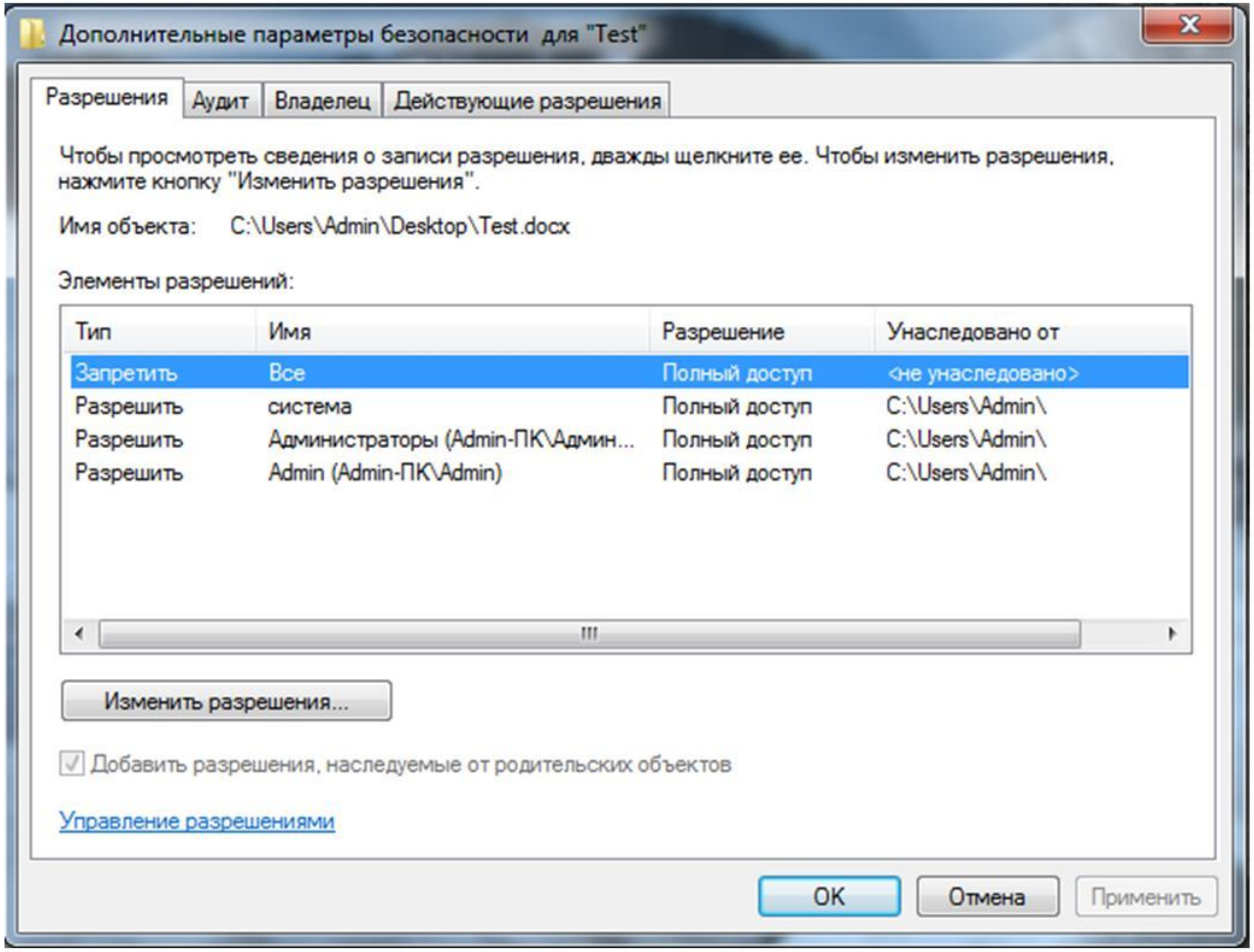
Проверка прав выполняется в порядке следования строк ACE

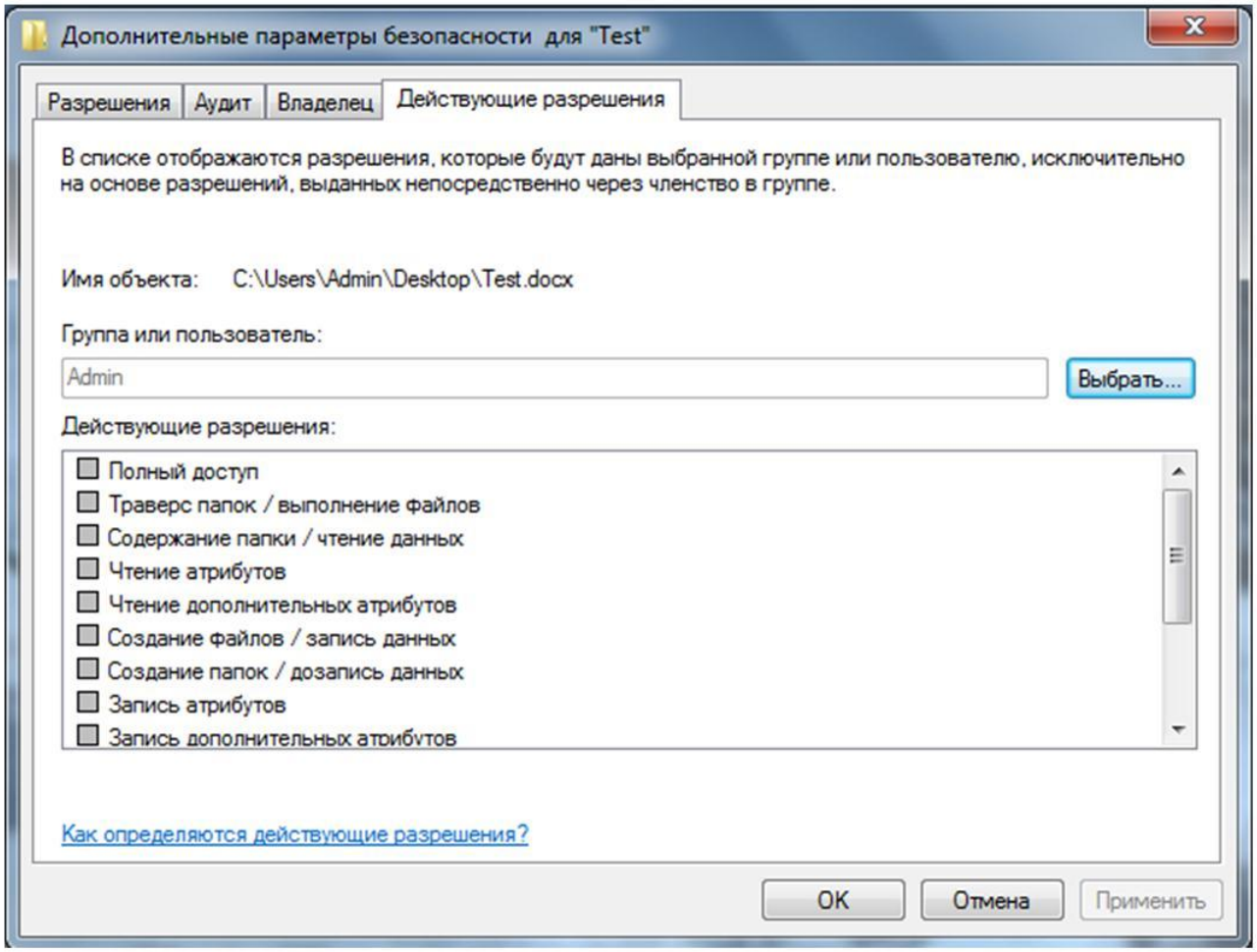
- до первого появления запрета на какую-либо операцию
- до явного разрешения всех запрошенных операций

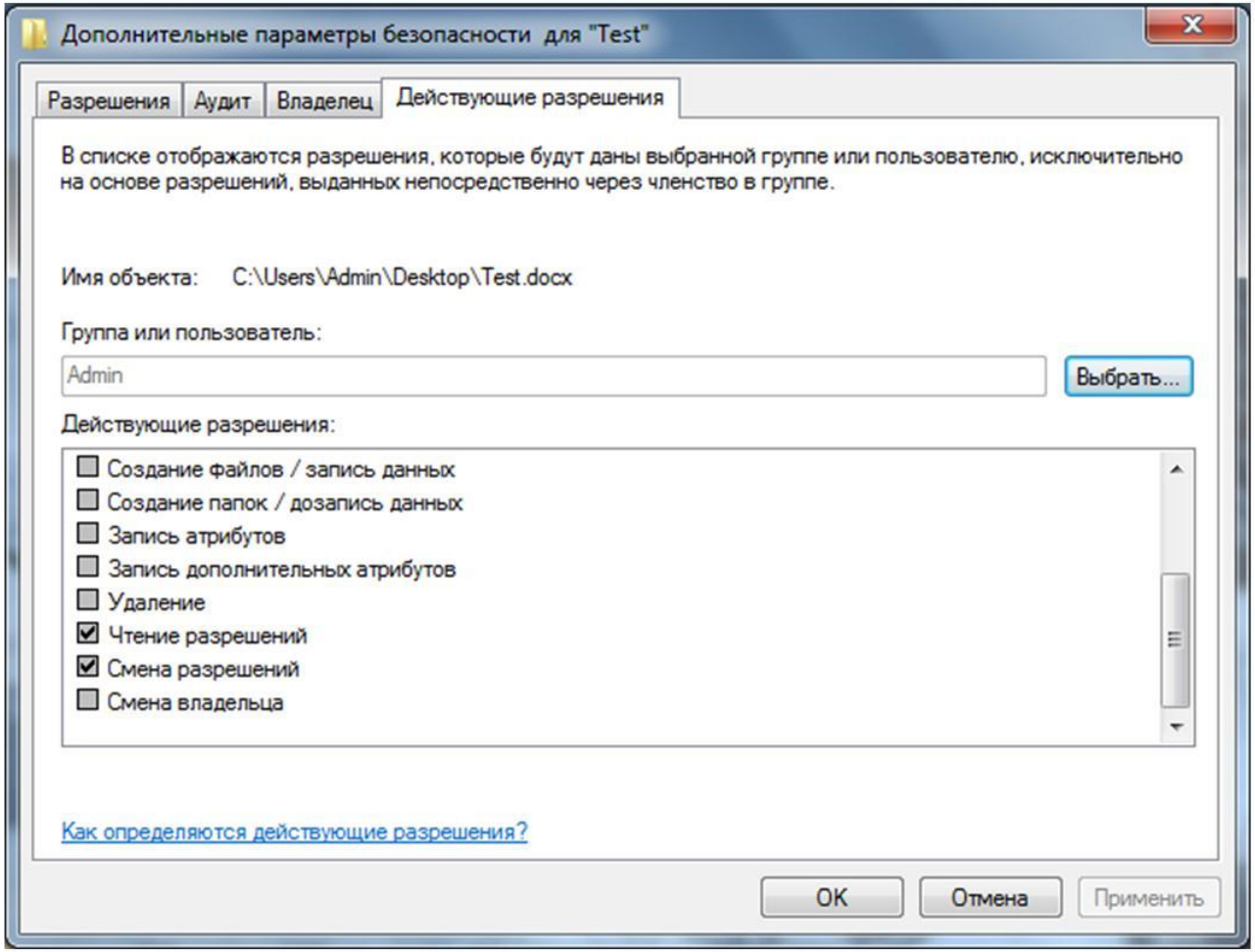

Свойства: Test
Общие
Безопасность
Подробно
Предыдущие версии
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Группы или пользователи:
Все
система
Admin (Admin-ПК\Admin)
Администраторы (Admin-ПК\Администраторы)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "Администраторы"
Разрешить
Запретить
Полный доступ
Изменение
Чтение и выполнение
Чтение
Запись
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
Подробнее об управлении доступом и разрешениях
OK
Отмена
Применить


Свойства: Test
Общие
Безопасность
Подробно
Предыдущие версии
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Группы или пользователи:
Все
система
Admin (Admin-ПК\Admin)
Администраторы (Admin-ПК\Администраторы)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "Admin"
Разрешить
Запретить
Полный доступ
Изменение
Чтение и выполнение
Чтение
Запись
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
Подробнее об управлении доступом и разрешениях
OK
Отмена
Применить


Свойства: Test
Общие
Безопасность
Подробно
Предыдущие версии
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Группы или пользователи:
Все
система
Admin (Admin-ПК\Admin)
Администраторы (Admin-ПК\Администраторы)
Чтобы изменить разрешения, нажмите кнопку "Изменить".
Изменить...
Разрешения для группы "Все"
Разрешить
Запретить
Полный доступ
Изменение
Чтение и выполнение
Чтение
Запись
Особые разрешения
Чтобы задать особые разрешения или параметры, нажмите кнопку "Дополнительно".
Дополнительно
Подробнее об управлении доступом и разрешениях
OK
Отмена
Применить


Дополнительные параметры безопасности для "Test"
Разрешения
Аудит
Владелец
Действующие разрешения
Чтобы просмотреть сведения о записи разрешения, дважды щелкните ее. Чтобы изменить разрешения, нажмите кнопку "Изменить разрешения".
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Элементы разрешений:
Тип
Имя
Разрешение
Унаследовано от
Запретить
Все
Полный доступ
<не унаследовано>
Разрешить
система
Полный доступ
C:\Users\Admin\
Разрешить
Администраторы (Admin-ПК\Админ...
Полный доступ
C:\Users\Admin\
Разрешить
Admin (Admin-ПК\Admin)
Полный доступ
C:\Users\Admin\
Изменить разрешения...
Добавить разрешения, наследуемые от родительских объектов
Управление разрешениями
OK
Отмена
Применить


Дополнительные параметры безопасности для "Test"
Разрешения
Аудит
Владелец
Действующие разрешения
В списке отображаются разрешения, которые будут даны выбранной группе или пользователю, исключительно на основе разрешений, выданных непосредственно через членство в группе.
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Группа или пользователь:
Admin
Выбрать...
Действующие разрешения:
Полный доступ
Траверс папок / выполнение файлов
Содержание папки / чтение данных
Чтение атрибутов
Чтение дополнительных атрибутов
Создание файлов / запись данных
Создание папок / дозапись данных
Запись атрибутов
Запись дополнительных атрибутов
Как определяются действующие разрешения?
OK
Отмена
Применить


Дополнительные параметры безопасности для "Test"
Разрешения
Аудит
Владелец
Действующие разрешения
В списке отображаются разрешения, которые будут даны выбранной группе или пользователю, исключительно на основе разрешений, выданных непосредственно через членство в группе.
Имя объекта: C:\Users\Admin\Desktop\Test.docx
Группа или пользователь:
Admin
Выбрать...
Действующие разрешения:
Создание файлов / запись данных
Создание папок / дозапись данных
Запись атрибутов
Запись дополнительных атрибутов
Удаление
Чтение разрешений
Смена разрешений
Смена владельца
Как определяются действующие разрешения?
OK
Отмена
Применить

Маркер доступа (access token)

- формируется для каждого субъекта
- ассоциируется с каждым потоком, исполняемым от имени пользователя

Основные компоненты маркера доступа

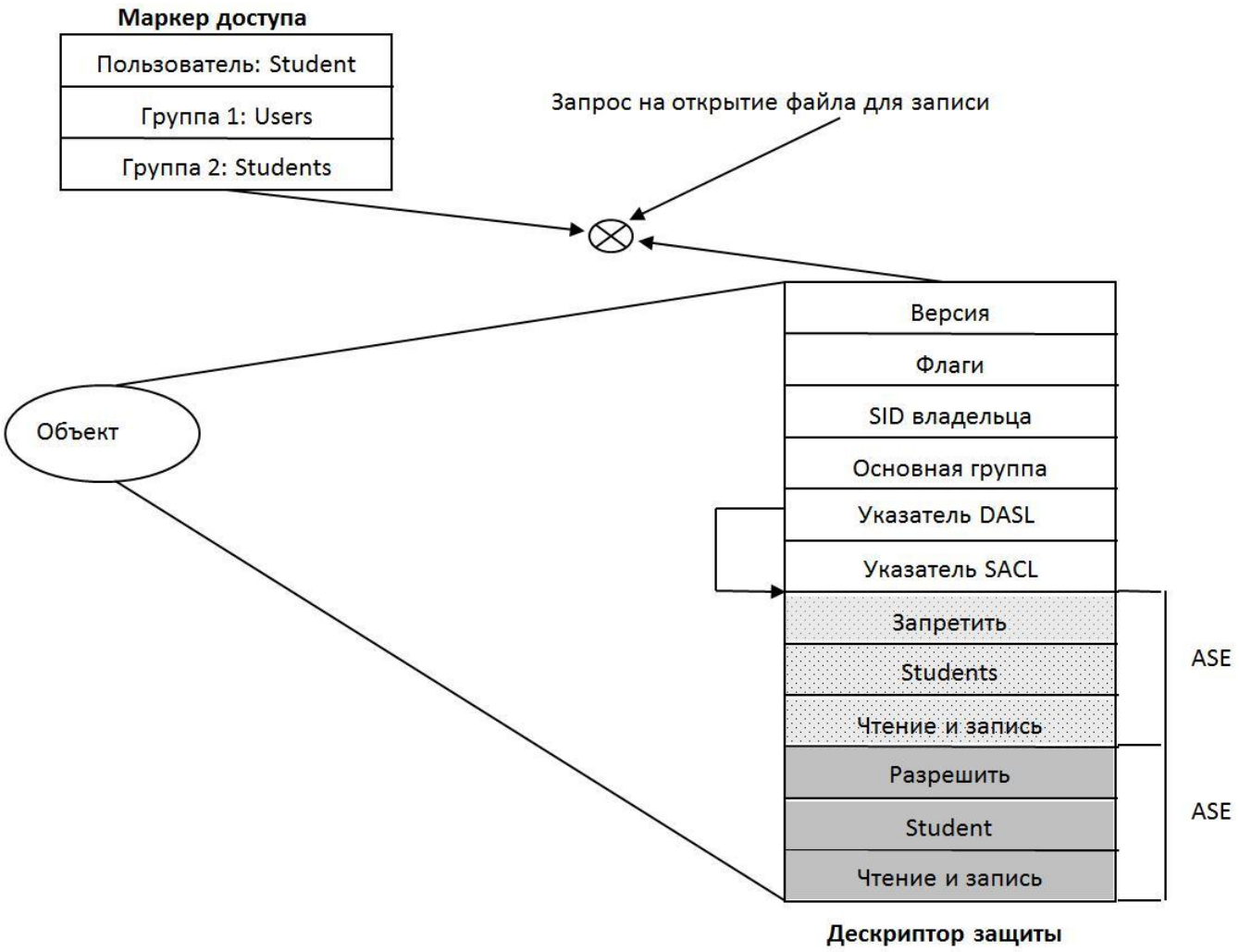
SID пользователя	SID_1,….. SID_n Идентификаторы групп пользователя	DACL по умолчанию	Привилегии	Другие параметры

• основной (primary token) (идентифицирует контекст защиты процесса)
• олицетворяющий (impersonation token) (применяется для временного заимствования потоком другого контекста защиты — обычно другого пользователя).

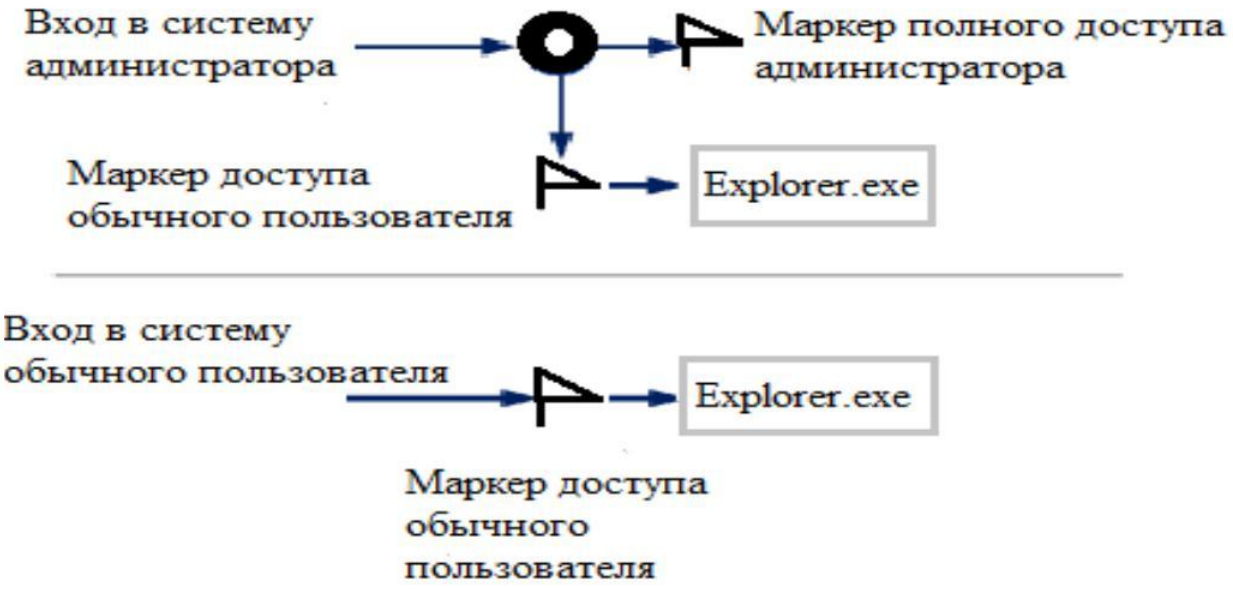
Проверка прав доступа

Основные этапы проверки прав доступа

1. В отсутствие DACL (DACL = null) объект является незащищенным, и система защиты предоставляет к нему полный доступ
2. Если у вызывающего потока имеется привилегия на захват объекта во владение (take-ownership privilege), система защиты предоставляет владельцу право на доступ для записи (write-owner access) до анализа DACL.
3. Если SID субъекта совпадает с SID владельца объекта и запрашиваются стандартные права доступа, то доступ предоставляется независимо от содержимого DACL.
4. Система последовательно сравнивает SID каждого ACE из DACL с SID маркера. Если обнаруживается соответствие, выполняется сравнение маски доступа с проверяемыми правами.


Маркер доступа
Пользователь: Student
Группа 1: Users
Группа 2: Students
Запрос на открытие файла для записи
Объект
Версия
Флаги
SID владельца
Основная группа
Указатель DASL
Указатель SACL
Запретить
Students
Чтение и запись
Разрешить
Student
Чтение и запись
ASE
ASE
Дескриптор защиты

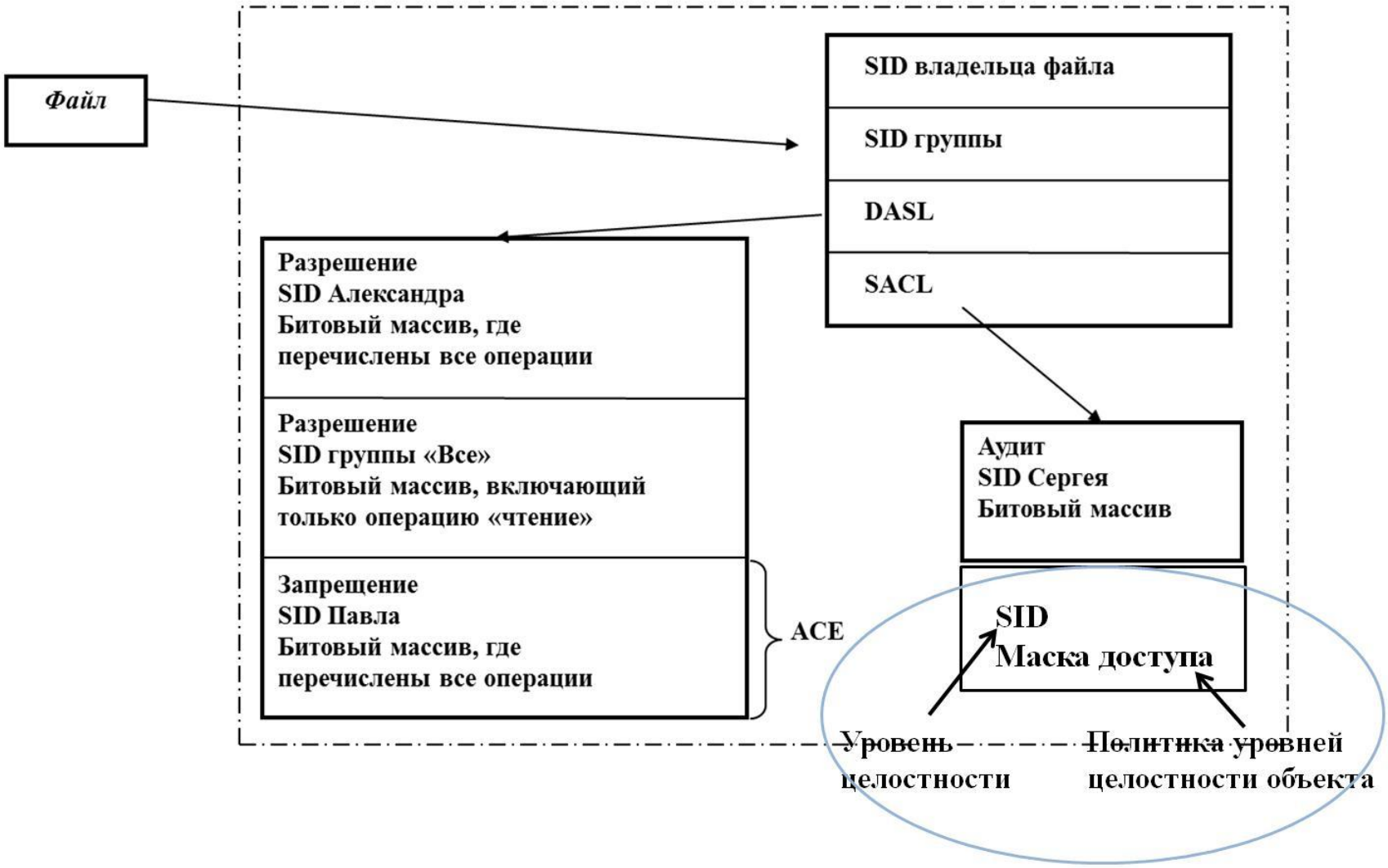
User Account Control (UAC)



Mandatory Integrity Control (MIC) (принудительный контроль целостности)

SID	Уровень целостности	Примеры процессов
S-1-16-0	Untrusted(0) (ненадежный)	Используется процессами, запущенными группой Anonymous. Он блокирует большинство доступов по записи
S-1-16-4096	Low (1) (низкий)	Используется защищенным режимом InternetExplorer. Он блокирует доступ по записи к большинству объектов системы (таких как файлы и разделы реестра)
S-1-16-8192	Medium (2) (средний)	Используется обычными приложениями, запущенными при включенной системеUAC (UserAccountControl)
S-1-16-12288	High(3) (высокий)	Используется административными приложениями, запущенными через повышение уровня полномочий при включенной системе UAC, или обычными приложениями при выключенной системе UAC и при наличии у пользователя прав администратора
S-1-16-16384	System(4) (системный)	Используется службами и другими приложениями системного уровня (например, Wininit, Winlogon, Smss и т.д.)

Дескриптор безопасности



Mandatory Integrity Control (MIC) (принудительный контроль целостности)

Политики уровней целостности

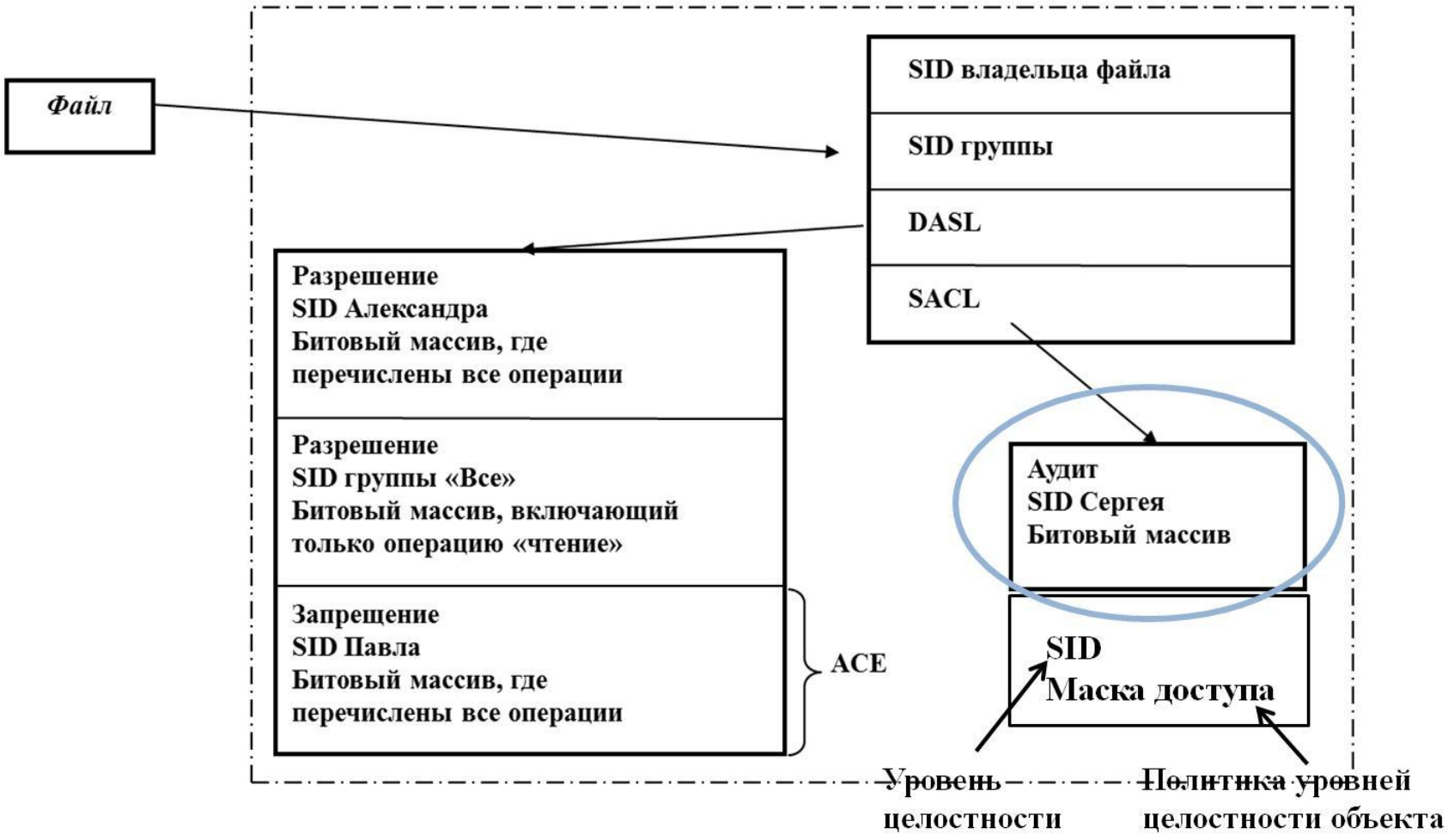
Политика	Объекты, в которых она присутствует по умолчанию	Описание
No- Write- Up (отказ в записи)	Подразумевается на всех объектах	Используется для ограничения доступа к объекту по записи со стороны процессов, имеющих более низкий уровень целостности
No- Read- Up (отказ в чтении)	Только на объектах процессов	Используется для ограничения доступа к объекту по чтению со стороны процессов, имеющих более низкий уровень целостности. Конкретное использование в отношении объектов процессов создает защиту от утечки информации путем блокирования чтения адресного пространства из внешнего процесса
No- Execute- Up (отказ в выполнении)	Только на двоичных реализациях COM-классов	Используется для ограничения доступа к объекту по выполнению со стороны процессов, имеющих более низкий уровень целостности. Конкретное использование в отношении COM-классов преследует цель ограничения прав на запуск и активацию COM- класса

Аудит

События аудита может генерировать

- диспетчер объектов в результате проверки прав доступа
- Windows-функции, доступные пользовательским приложениям
- код режима ядра

Дескриптор безопасности



Системный список контроля доступа (SACL)

регистрировать	идентификатор субъекта	права доступа	флаги и атрибуты

s (SUCCESSFUL_ACCESS_ACE_FLAG) - регистрация в журнале аудита всех *успешных* обращений к объекту субъекта, идентификатор которого записан в ACE, по любому из методов доступа, перечисленных в маске доступа ACE;

f (FAILED_ACCESS_ACE_FLAG) - регистрация в журнале аудита всех *неуспешных* обращений к объекту субъекта, идентификатор которого записан в ACE, по любому из методов доступа, перечисленных в маске доступа ACE.

i - при доступе субъектов к объекту ACE игнорируется.

Необходимые условия фиксации в журнале аудита события, связанного с доступом субъекта к объекту:

- политика аудита операционной системы допускает регистрацию в журнале аудита событий, связанных с успешным (или неуспешным) доступом субъектов к объектам;
- SACL объекта содержит хотя бы один ACE, в котором:
  - идентификатор субъекта относится к субъекту, открывающему объект;
  - установлен флаг s (или соответственно f) и не установлен флаг i;
  - маска доступа, содержащая права, запрашиваемые субъектом, не пуста.