Дисциплина «Защита в операционных системах»

Лабораторная работа № 4

Тема: Концептуальная модель безопасности ОС семейства Windows

Цель: изучить концептуальную модель безопасности операционных систем семейства Windows, получить навыки практического использования ее средств обеспечения безопасности.

Время выполнения лабораторной работы (аудиторные часы) – 4 часов.

Оборудование и программное обеспечение: работа выполняется на ПЭВМ типа IBM PC с использованием стандартных функций ОС.

1. Теоретические сведения

1.1 Классификация защиты семейства ОС Windows

Разработчики операционной системы Windows уделили серьезное внимание обеспечению безопасности работы пользователей. Это подтверждается категориями, присвоенными различным версиям данной операционной системы по тем или иным международным и национальным критериям оценки безопасности. Так, по классификации «Оранжевой книги» ОС Windows NT 4 еще в 1999 году получила класс безопасности C2, по стандарту ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation (Общие критерии оценки безопасности информационных технологий) клиентские и серверные версии от Windows 2000 до Windows 10, от Windows Server 2008 до Windows Server 2013 получили уровень безопасности EAL4+, а операционные системы Windows 8, Windows Server 2012 Standard соответствуют требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) по 5 классу защищенности.

Какие средства безопасности предоставляют операционные семейства можно представить, если, например, познакомиться с требованиями оценки безопасности C2 «Оранжевой книги». Согласно им, система должна обеспечивать:

- средство безопасного входа в систему, которое обеспечивают точную идентификацию пользователей и предоставляют им возможности доступа к ресурсам компьютера только после прохождения процедуры аутентификации. В Windows за идентификацию и аутентификацию пользователей отвечают процессы Winlogon.exe и Lsass.exe.
- управление доступом, позволяющее владельцу ресурса (файла, раздела реестра, объекта ядра и др.) определить, кто имеет права на доступ к ресурсу, а также уточнить суть этих прав (чтение, изменение, запуск и т.п.). При

использовании дискреционной модели доступа для уплотнения матрицы доступа владелец может наделять правами, разрешающими различные виды доступа к объекту, как отдельного пользователя, так группу пользователей. Безопасный доступ реализуется в Windows компонентом Security Reference Monitor (SRM, монитор контроля безопасности) исполнительной системы Ntoskrnl.exe.

- аудит безопасности, позволяющий регистрировать события, относящиеся к вопросам безопасности. Идентификация пользователей при входе в систему позволяет привязывать все события безопасности в системе к конкретному пользователю. В Windows аудит поддерживается SRM и Lsass.exe.
- защита от повторного использования объекта, которая не позволяет пользователям просматривать данные, удаленные другим пользователем, или не позволяет обращаться к памяти, которая ранее была использована, а затем освобождена другим пользователем. В Windows освобожденная память очищается системным потоком обнуления страниц, работающим во время простоя системы (с нулевым приоритетом).

1.2 Идентификация пользователей

Для защиты данных Windows использует следующие основные механизмы:

- ✓ аутентификация и авторизация пользователей,
- ✓ аудит событий в системе,
- ✓ шифрование данных,
- ✓ поддержка инфраструктуры открытых ключей,
- ✓ встроенные средства сетевой защиты.

Эти механизмы поддерживаются такими подсистемами Windows как LSASS (Local Security Authority Subsystem Service, подсистема локальной аутентификации), SAM (Security Account Manager, диспетчер локальных записей безопасности), SRM (Security reference Monitor, монитор состояния защиты), Active Directory (служба каталогов), EFS (Encrypting File System, шифрующая файловая система) и др.

Защита объектов и аудит действий с ними в ОС Windows организованы на основе избирательного (дискреционного) доступа, когда права доступа (чтение, запись, удаление, изменение атрибутов) субъекта к объекту задается явно в специальной матрице доступа. Для укрупнения матрицы пользователи могут объединяться в группы. При попытке субъекта (одного из потоков процесса, запущенного от его имени) получить доступ к объекту указываются, какие операции пользователь собирается выполнять с объектом. Если подобный тип доступа разрешен, поток получает описатель (дескриптор) объекта и все потоки процесса могут выполнять операции с ним. Подобная схема доступа, очевидно, требует аутентификации каждого пользователя, получающего доступ к ресурсам и его надежную идентификацию в системе, а также механизмов описания прав пользователей и групп пользователей в системе, описания и проверки дискреционных прав доступа пользователей к объектам. Рассмотрим, как в ОС Windows организована аутентификация и авторизация пользователей.

Все действующие в системе объекты (пользователи, группы, локальные компьютеры, домены) идентифицируются в Windows не по именам, уникальность

которых не всегда удается достичь, а по идентификаторам защиты (Security Identifiers, SID). SID представляет собой числовое значение переменной длины:

S - R - I - SO - S1 - ... - Sn - RID

S - неизменный идентификатор строкового представления SID;

R - уровень ревизии (версия). На сегодня 1.

I - (identifier-authority) идентификатор полномочий. Представляет собой 48 битную строку, идентифицирующую компьютер или сеть, который(ая) выдал SID объекту. Возможные значения:

- 0 (SECURITY_NULL_SID_AUTHORITY) — используются для сравнений, когда неизвестны полномочия идентификатора;
- 1 (SECURITY_WORLD_SID_AUTHORITY) — применяются для конструирования идентификаторов SID, которые представляют всех пользователей. Например, идентификатор SID для группы *Everyone* (Все пользователи) — это *S-1-1-0;*
- 2 (SECURITY_LOCAL_SID_AUTHORITY) — используются для построения идентификаторов SID, представляющих пользователей, которые входят на локальный терминал;
- 5 (SECURITY_NT_AUTHORITY) — сама операционная система. То есть, данный идентификатор выпущен компьютером или доменом.

Sn - 32-битные коды (количеством 0 и более) субагентов, которым было передано право выдать SID. Значение первых подчиненных полномочий общеизвестно. Они могут иметь значение:

- 5 — идентификаторы SID присваиваются сеансам регистрации для выдачи прав любому приложению, запускаемому во время определенного сеанса регистрации. У таких идентификаторов SID первые подчиненные полномочия установлены как 5 и принимают форму *S-1-5-5-x-y;*
- 6 — когда процесс регистрируется как служба, он получает специальный идентификатор SID в свой маркер для обозначения данного действия. Этот идентификатор SID имеет подчиненные полномочия 6 и всегда будет *S-1- 5-6;*
- 21 (SECURITY_NT_NON_UNIQUE) — обозначают идентификатор SID пользователя и идентификатор SID компьютера, которые не являются уникальными в глобальном масштабе;
- 32 (SECURITY_BUILTIN_DOMAIN_RID) — обозначают встроенные идентификаторы SID. Например, известный идентификатор SID для встроенной группы администраторов *S-1-5-32-544;*
- 80 (SECURITY_SERVICE_ID_BASE_RID) — обозначают идентификатор SID, который принадлежит службе.

Остальные подчиненные полномочия идентификатора совместно обозначают домен или компьютер, который издал идентификатор SID.

RID - 32-битный относительный идентификатор. Он является идентификатором уникального объекта безопасности в области, для которой был определен SID. Например, 500 — обозначает встроенную учетную запись *Administrator*, 501 — обозначает встроенную учетную запись *Guest, а* 502 — RID для билета на получение билетов протокола Kerberos .

При генерации SID Windows использует генератор случайных чисел, чтобы обеспечить уникальность SID для каждого пользователя. Для некоторого

произвольного пользователя SID может выглядеть так:

S-1-5-21-789336058-484763869-725345543-1003

Предопределенным пользователям и группам Windows выдает характерные SID, состоящие из SID компьютера или домена и предопределенного RID. В таблице 1 приведен перечень некоторых общеизвестных SID.

Таблица 1. Общеизвестные SID Windows

SID	Название	Описание
S-1-1-0	Все	Группа, в которую входят все пользователи
S-1-5-2	Сеть	Группа, в которую входят все пользователи, зарегистрировавшиеся в системе из сети
S-1-5-7	Анонимный вход	Группа, в которую входят все пользователи, вошедшие в систему анонимно
S-1-5-*домен* -500	Администратор	Учетная запись администратора системы. По умолчанию только эта запись обеспечивает полный контроль системы
S-1-5-домен-501	Гость	Учетная запись пользователя-гостя

Полный список общеизвестных SID можно посмотреть в документации Platform SDK. Узнать SID конкретного пользователя в системе, а также SID групп, в которые он включен, можно, используя консольную команду **whoami**:

whoami /user

Соответствие имени пользователя и его SID можно отследить также в ключе реестра HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ ProfileList.

После аутентификации пользователя процессом Winlogon, все процессы, запущенные от имени этого пользователя будут идентифицироваться специальным объектом, называемым маркером доступа (access token). Если процесс пользователя запускает дочерний процесс, то его маркер наследуются, поэтому маркер доступа олицетворяет пользователя для системы в каждом запущенном от его имени процессе. Основные элементы маркера представлены на рис. 5.1.

SID пользователя	**SID1 . SIDn Идентификаторы групп пользователя**	**DACL по умолчанию**	**Привилегии**	**Прочие параметры**

Рис. 5.1 Обобщенная структура маркера доступа.

Маркер доступа содержит идентификатор доступа самого пользователя и всех групп, в которые он включен. В маркер включен также DACL по умолчанию - первоначальный список прав доступа, который присоединяется к создаваемым пользователем объектам. Еще одна важная для определения прав пользователя в системе часть маркера - список его привилегий. Привилегии - это права доверенного объекта на совершение каких-либо действий по отношению ко всей системе. В таблице 5.2 перечислены некоторые привилегии, которые могут быть

предоставлены пользователю.

Таблица 5.2. Привилегии, которыми могут быть наделены пользователи

Имя и идентификатор привилегии	**Описание привилегии**
Увеличение приоритета диспетчирования **SeIncreaseBasePriorityPrivilege**	Пользователь, обладающий данной привилегией может изменять приоритет диспетчирования процесса с помощью интерфейса Диспетчера задач
Закрепление страниц в памяти **SeLockMemoryPrivilege**	Процесс получает возможность хранить данные в физической памяти, не прибегая к кэшированию данных в виртуальной памяти на диске.
Управление аудитом и журналом безопасности **SeAuditPrivilege**	Пользователь получает возможность указывать параметры аудита доступа к объекту для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра.
Овладение файлами или иными объектами **SeTakeOwnershipPrivilege**	Пользователь получает возможность становиться владельцем любых объектов безопасности системы, включая объекты Active Directory, файлы и папки NTFS, принтеры, разделы реестра, службы, процессы и потоки
Завершение работы системы **SeShutdownPrivilege**	Пользователь получает возможность завершать работу операционной системы на локальном компьютере
Обход перекрестной проверки **SeChangeNotifyPrivilege**	Используется для обхода проверки разрешений для промежуточных каталогов при проходе многоуровневых каталогов

Управление привилегиями пользователей осуществляется в оснастке **«Групповая политика»**, раздел **Конфигурация Windows/Локальные политики/Назначение прав пользователя**.

Чтобы посмотреть привилегии пользователя, можно также использовать команду **whoami /all**

Остальные параметры маркера носят информационный характер и определяют, например, какая подсистема создала маркер, уникальный идентификатор маркера, время его действия. Необходимо также отметить возможность создания ограниченных маркеров (restricted token), которые отличаются от обычных тем, что из них удаляются некоторые привилегии и его SID-идентификаторы проверяются только на запрещающие правила. Создать ограниченный маркер можно программно, используя API-функцию **CreateRestrictedToken**, а можно запустить процесс с ограниченным маркером, используя пункт контекстного меню Windows “Запуск от имени другого пользователя” (рис. 5.2).

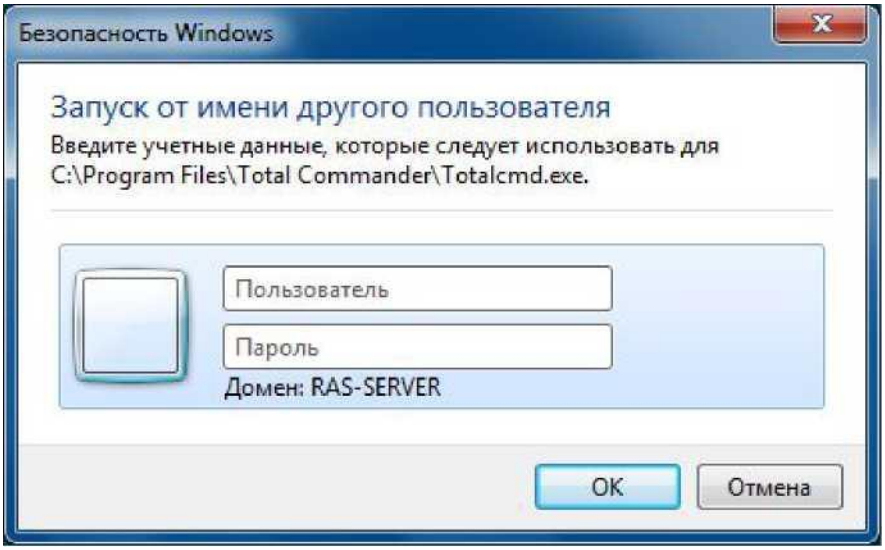

Рис. 5.2 Запуск процесса с ограниченным маркером

Ограниченные маркеры используются для процессов, подменяющих клиента и выполняющих небезопасный код.

Маркер доступа может быть создан не только при первоначальном входе пользователя в систему. Windows предоставляет возможность запуска процессов от имени других пользователей, создавая для этих процессов соответствующий маркер. Для этих целей можно использовать:

- API-функции **CreateProcessAsUser, CreateProcessWithLogon**;
- оконный интерфейс (рис.2), инициализирующийся при выборе пункта контекстного меню **“Запуск от имени другого пользователя”**;
- консольную команду **runas**:

runas ***/user:имя_пользователя program*** **,**

где: ***имя_пользователя*** - имя учетной записи пользователя, которая будет использована для запуска программы в формате *пользователь@домен* или *домен\пользователь;*

program - команда или программа, которая будет запущена с помощью учетной записи, указанной в параметре /user.

В любом варианте запуска процесса от имени другой учетной записи необходимо задать ее пароль.

1.3 Защита объектов системы.

Маркер доступа идентифицирует субъектов-пользователей системы. С другой стороны, каждый объект системы, требующий защиты, содержит описание прав доступа к нему пользователей. Для этих целей используется **дескриптор безопасности (Security Descriptor, SD)**. Каждому объекту системы, включая файлы, принтеры, сетевые службы, контейнеры Active Directory и другие, присваивается дескриптор безопасности, который определяет права доступа к объекту и содержит следующие основные атрибуты (рис. 5.3):

- SID владельца, идентифицирующий учетную запись пользователя-владельца объекта;
- пользовательский список управления доступом (Discretionary Access

Control List, DACL), который позволяет отслеживать права и ограничения, установленные владельцем данного объекта. DACL может быть изменен пользователем, который указан как текущий владелец объекта.

- системный список управления доступом (System Access Control List, SACL), определяющий перечень действий над объектом, подлежащих аудиту;
- флаги, задающие атрибуты объекта.

Авторизация Windows основана на сопоставлении маркера доступа субъекта с дескриптором безопасности объекта. Управляя свойствами объекта, администраторы могут устанавливать разрешения, назначать право владения и отслеживать доступ пользователей.

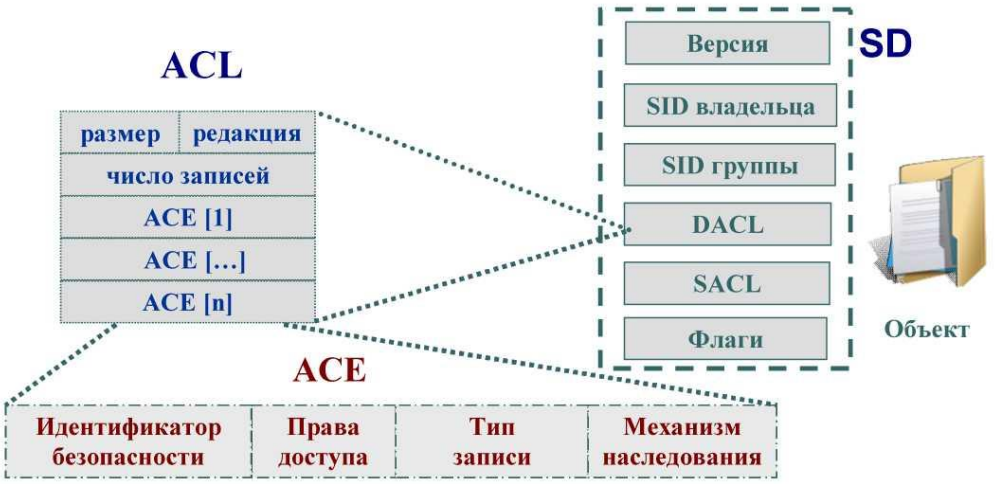

Рис.5.3 Структура дескриптора безопасности объекта Windows

Список управления доступом содержит набор элементов (Access Control Entries, ACE). В DACL каждый ACE состоит из четырех частей: в первой указываются пользователи или группы, к которым относится данная запись, во второй - права доступа, а третья информирует о том, предоставляются эти права или отбираются. Четвертая часть представляет собой набор флагов, определяющих, как данная запись будет наследоваться вложенными объектами (актуально, например, для папок файловой системы, разделов реестра).

Если список ACE в DACL пуст, к нему нет доступа ни у одного пользователя (только у владельца на изменение DACL). Если отсутствует сам DACL в SD объекта - полный доступ к нему имеют все пользователи.

Если какой-либо поток запросил доступ к объекту, подсистема SRM (Security reference Monitor, монитор состояния защиты) осуществляет проверку прав пользователя, запустившего поток, на данный объект, просматривая его список DACL. Проверка осуществляется до появления разрешающих прав **на все** запрошенные операции. Если встретится запрещающее правило хотя бы **на одну** запрошенную операцию, доступ не будет предоставлен.

Рассмотрим пример на рис.5.4. Процесс пытается получить доступ к объекту с заданным DACL. В маркере процесса указаны SID запустившего его пользователя, а также SID групп, в которые он входит. В списке DACL объекта присутствуют разрешающие правила на чтение для пользователя с SID=100, и на запись для группы с SID=205. Однако, в доступе пользователю будет отказано,

поскольку раньше встречается запрещающее запись правило для группы с SID=201.

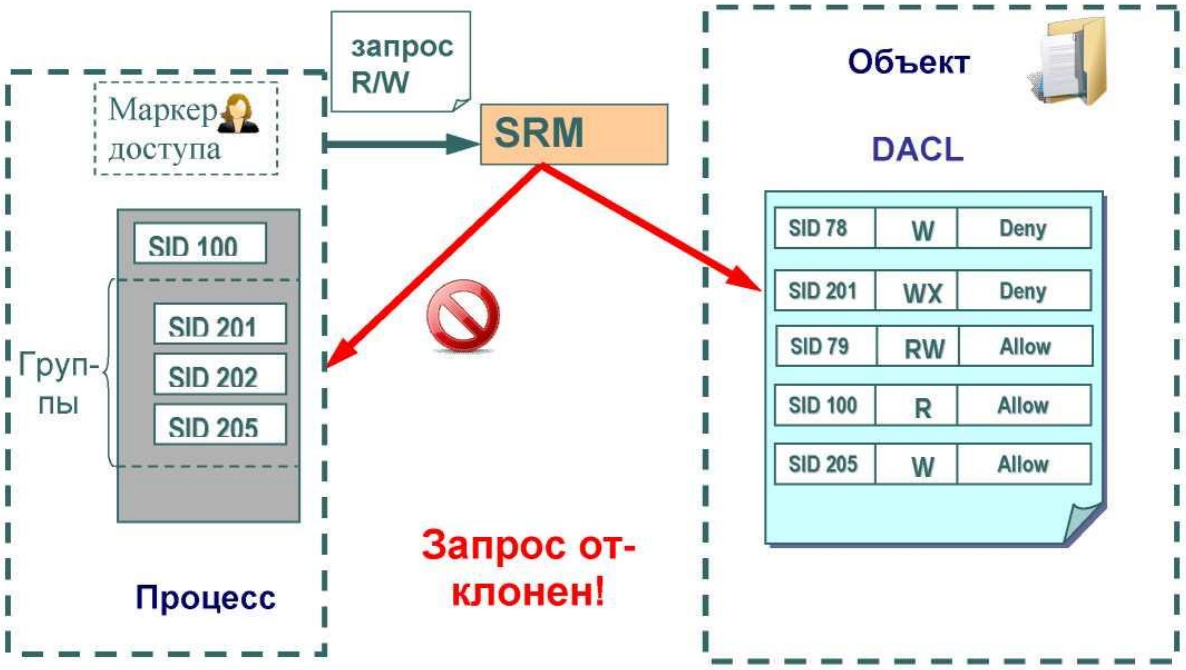

Рис. 5.4 Проверка прав доступа пользователя к объекту

Необходимо отметить, что запрещающее правило помещено в списке DACL на рисунке не случайно.

Запрещающие правила **всегда** размещаются перед разрешающими, то есть являются **доминирующими** при проверке прав доступа.

Для определения и просмотра прав доступа пользователей к ресурсам можно использовать как графические средства контроля, так и консольные команды. Стандартное окно свойств объекта файловой системы (диска, папки, файла) на вкладке **Безопасность** (рис. 5.5) позволяет просмотреть текущие разрешения для пользователей и групп пользователей, редактировать их, создавать новые или удалять существующие.

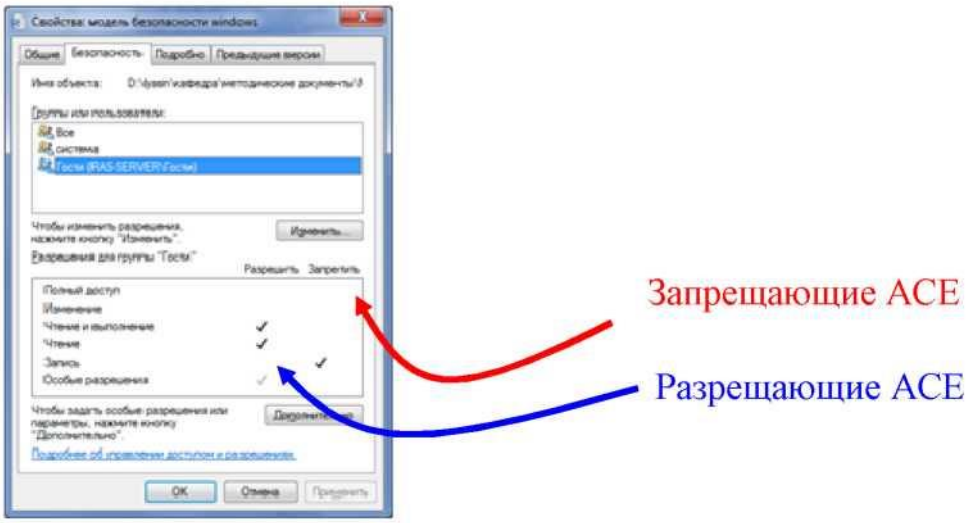

Рис. 5.5 GUI-интерфейс Windows для изменения прав доступа к объектам

При определении прав доступа к объектам можно задать правила их наследования в дочерних контейнерах. В окне дополнительных параметров безопасности на вкладке Разрешения при выборе опции «Добавлять разрешения, наследуемые от родительских объектов» (рис. 5.6) можно унаследовать разрешения и ограничения, заданные для родительского контейнера, текущему объекту.

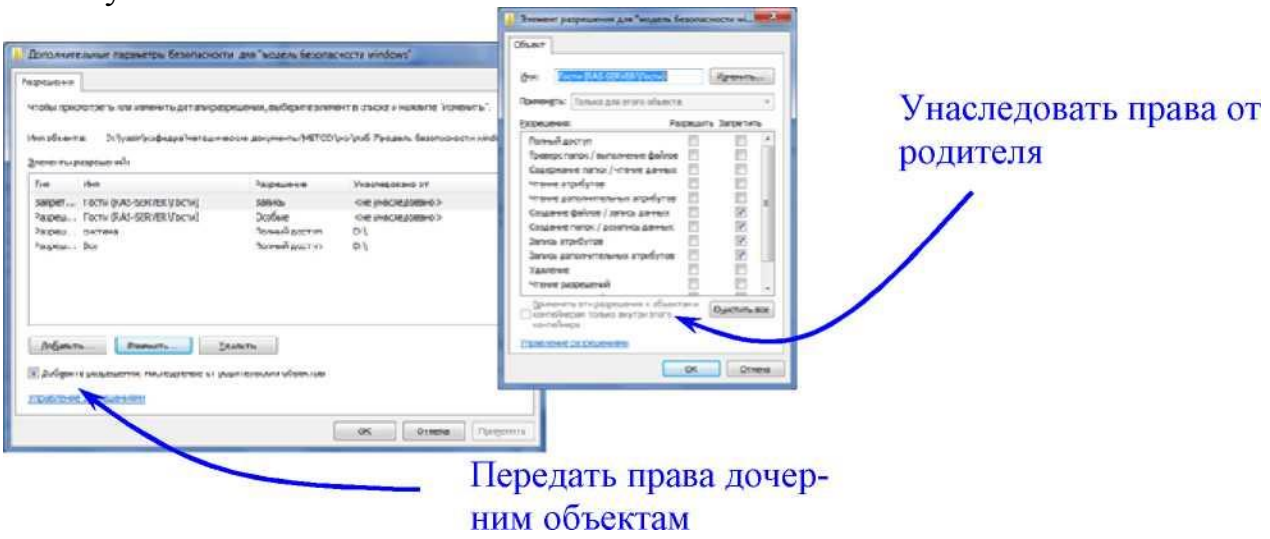

Рис.5.6 Определение параметров наследования прав доступа к объектам

При выборе опции «Применять эти разрешения к объектам и контейнерам только внутри этого контейнера» разрешается передача определенных для объекта-контейнера правил доступа его дочерним объектам.

В этом же окне на вкладке Владелец допустимо узнать владельца объекта и заменить его. Владелец объекта имеет право на изменение списка его DACL, даже если к нему запрещен любой тип доступа. Администратор имеет право становиться владельцем любого объекта.

С учетом возможности вхождения пользователя в различные группы и независимости определения прав доступа к объектам для групп и пользователей, зачастую бывает сложно определить конечные права пользователя на доступ к объекту: требуется просмотреть запрещающие правила, определенные для самого объекта, для всех групп, в которые он включен, затем то же проделать для разрешающих правил. Автоматизировать процесс определения разрешенных пользователю видов доступа к объекту можно с использованием вкладки «Действующие разрешения» окна дополнительных параметров безопасности объекта (рис. 5.7).

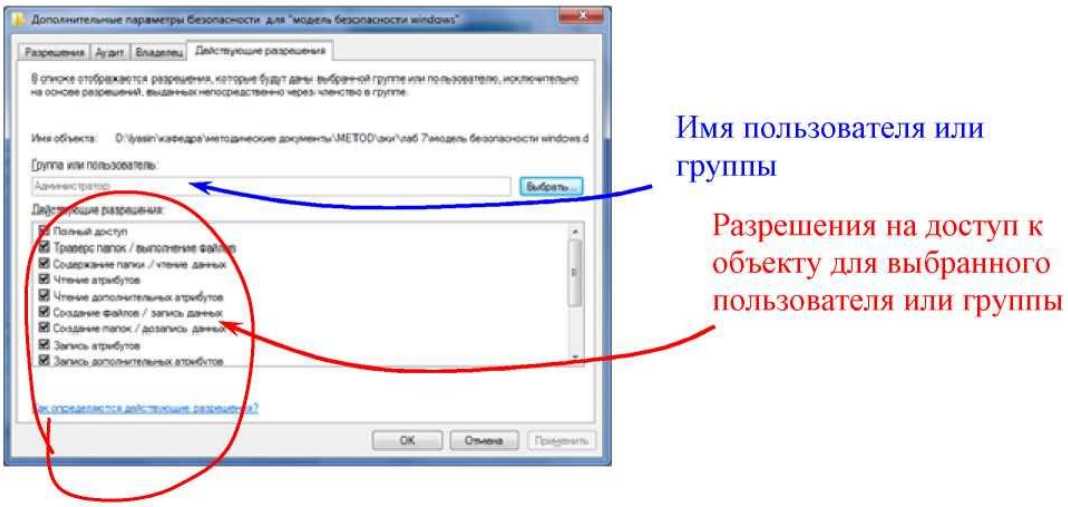

Рис. 5.7 Определение эффективных прав доступа пользователя (группы) к объекту

Для просмотра и изменения прав доступа к объектам в режиме командной строки предназначена команда **icacls** (**cacls** в Windows XP).

icacls *имяфайла* [**/t**] [**/e**] [**/c**] [**/g** *пользователь:разрешение]* [**/r** *пользователь* [...]] [**/p** *полъзователь:разрешение* [...]] [**/d** *пользователь* [...]].

Назначения параметров команды приведены в таблице 5.3.

Таблица 5.3 Параметры команды icacls

<имя файла>	Задаёт файл или папку, права доступа к которой необходимо просмотреть/изменить (допустимо использовать шаблоны с символами * и ?).
/t	Изменение избирательных таблиц контроля доступа (DACL) указанных файлов в текущем каталоге и всех подкаталогах
/e	Редактирование избирательной таблицы управления доступом (DACL) вместо ее замены
/c	Заставляет команду продолжить изменение прав доступа при возникновении ошибки, связанной с нарушениями прав доступа
/g <пользователь | группа: разрешение>	Предоставление прав доступа указанному пользователю
/r <пользователь | группа>	Отнимает права доступа указанного пользователя.
/p <пользователь | группа: разрешение>	Заменяет права доступа указанного пользователя
/d <пользователь | группа>	Отказывает в праве доступа указанному пользователю или группе

Для указания добавляемых или отнимаемых прав используются следующие значения:

F - полный доступ;

C - изменение (запись);
W - запись;
R - чтение;
N - нет доступа.
Рассмотрим несколько примеров.
icacls d:\test
Выдаст список DACL для папки test.
icacls d:\test /d ИмяКомпьютера\ИмяПользователя /e
Запретит доступ к объекту для указанного пользователя.
icacls d:\test /p ИмяКомпьютера\ИмяГруппы^ /e /t
Предоставит полный доступ к папке ***d:\test*** *и ее подпапках всем для членов указанной группы.*

Для программного просмотра и изменения списков **DACL** можно использовать API-функции **AddAccessAllowedAce, AddAccessDeniedAce, SetSecurityInfo.**

Подробнее с этими функциями и примерами их использования можно ознакомиться в [3].

1.4 Реализация мандатного механизма доступа

Рассмотренные способы работы с дискреционным списком доступа иллюстрируют реализацию в Windows модели произвольного доступа. Но начиная с Windows Vista фирма Microsoft реализовала элементы мандатного доступа для контроля доступа к объектам. За этот уровень обеспечения безопасности отвечает ***Windows Integrity Control (WIC)***. Концепция **WIC** вторит уже рассмотренным выше принципами принудительного (мандатного) управления доступом и основана на построении доверительных отношений между объектами и управлении действиями с ними пользователей на основе их уровня доверия. Базовым понятием WIC является уровень целостности (integrity level) объекта. WIC присваивает контролируемым объектам один из шести доступных уровней целостности:

- ***Untrusted*** — анонимные процессы автоматически попадают в эту категорию.
- ***Low*** — стандартный уровень при работе с Интернетом. Если браузер Internet Explorer запущен в защищенном режиме, все файлы и процессы, ассоциированные с ним, назначаются в эту категорию. Некоторые папки, такие как, например, Temporary Internet Folder, также по умолчанию наделяются *Низким уровнем доверия.*
- ***Medium*** — в данном контексте работает большинство объектов. Ординарные пользователи получают *Средний уровень,* всем объектам присваивается данный уровень доступа, если не указан какой-либо иной.
- ***High*** — уровень, ассоциированный в системе с *Администраторами.* Объекты *Высокого уровня* недоступны обычным пользователям.
- ***System*** — уровень для работы ядра операционной системы и его служб.
- ***Installer*** — вершина в иерархии уровней WIC. Его объекты могут изменять и удалять файлы всех предыдущих уровней.

Контроль по уровням целостности при доступе к объекту также

осуществляется на основе правил ACE. Но это специализированные ACE, которые начиная с Windows Vista хранятся в списке SACL дескриптора безопасности объекта наряду с правилами аудита. Уровень целостности пользователя (процесса, выполняющегося от его имени) хранится в его токене безопасности. При доступе процесса к объекту монитор безопасности сравнивает уровень целостности в токене с уровнем целостности в дескрипторе объекта (в SACL). Система выдает права доступа в зависимости от того выше или ниже уровень целостности субъекта по отношению к объекту, а также в зависимости от флагов политики целостности в соответствующей ACE объекта. Уровни целостности (IL) пользователя описываются в его идентификаторе безопасности, точнее - в его RID-части:

SID = S-1-16-0x0 - уровень Untrusted
SID = S-1-16-0x1000 - уровень Low
SID= S-1-16-0x2000 - уровень Medium
SID= S-1-16-0x3000 - уровень High
SID= S-1-16-0x4000 - уровень системы

Для изменения уровня целостности объектов можно использовать следующие инструменты:

- уже рассмотренную команду *icacls* с ключом /setintegitylevel. Например, вот так можно присвоить файлу низкий (l) уровень целостности:

icacls f:\temp /setintegritylevel l

- используя специальные утилиты *Chml* ("change mandatory label") для изменения уровня целостности файлов и папок, и *Regil* ("Registry integrity levels") для работы с уровнями целостности ключей реестра.

Изменить уровень целостности процесса можно, например, запустив его утилитой psexec.exe с соответствующим ключом. Вот как можно запустить блокнот с высоким уровнем целостности: psexec -h notepad.exe

Очевидно, что изменять уровень целостности запускаемых процессов потенциально небезопасная операция, поэтом ее могут запускать только процессы, у которых в маркере доступа установлена привилегия ***SeRelabelPrivilege*.**

Узнать, каким уровнем целостности обладает процесс можно, например, запустив утилиту ProcessExplorer из набора Sysinternals [6] (рис. 5.8).

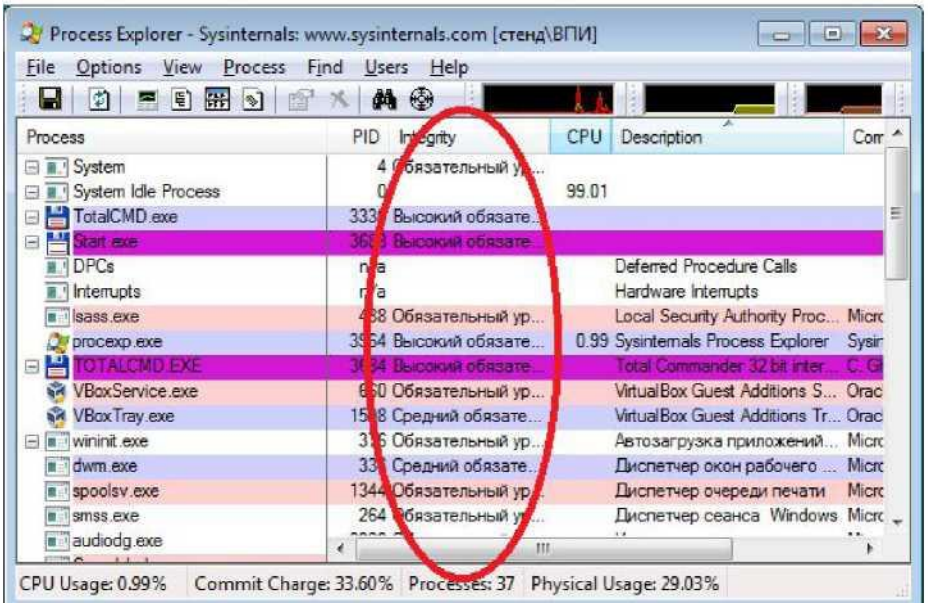

Рис. 5.8 Уровень целостности запущенных процессов в интерфейсе ProcessExplorer

Необходимо отметить, что контроль уровней целостности имеет ***более высокий приоритет*** при проверке прав доступа к объекту перед дискреционной таблицей.

2. Задание

2.1. Ознакомьтесь с теоретическими основами защиты информации в ОС семейства Windows в настоящих указаниях и конспектах лекций.

2.2. Выполните задания 2.2.1-2.2.6

2.2.1. При выполнении лабораторной работы на компьютерах в учебной лаборатории запустите в программе **Oracle VM Virtualbox** виртуальную машину Win 7. Войдите в систему под учетной записью администратора. Все действия в п.п. 2.2.1-2.2.6 выполняйте в системе, работающей на виртуальной машине.

2.2.2. Создайте учетную запись нового пользователя **testUser** в оснастке **«Управление компьютером» (compmgmt.msc)**. При создании новой учетной записи задайте произвольный пароль пользователя **testUser**, запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу ”**testGroup**” и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске **C:** папку **forTesting**. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).

2.2.3. С помощью команды **runas** запустите сеанс командной строки (**cmd.exe**) от имени вновь созданного пользователя. Командой **whoami** посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя.

Строку запуска и результат работы этой и всех следующих консольных команд копируйте в файл протокола лабораторной работы.

2.2.4. Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен

SID S-1-5-21-……-……-……-1002. (Используйте ключ реестра **HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList**).

2.2.5. Командой **whoami** определите перечень текущих привилегий пользователя testUser. В сеансе командной строки пользователя попробуйте изменить системное время командой time. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «Локальные параметры безопасности» (secpol.msc). Добавьте пользователя в список параметров политики «Изменение системного времени» **раздела Локальные политики -> Назначение прав пользователя**. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась SeSystemtimePriviege. Попробуйте изменить системное время командой time.

Убедитесь, что привилегия «Завершение работы системы» (SeShutdown - Privilege) предоставлена пользователю testUser . После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой shutdown -s. Добавть ему привилегию «Принудительное удаленное завершение» (SeRemoteShutdownPrivilege). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой shutdown -a).

2.2.6. Ознакомьтесь со справкой по консольной команде icacls. Используя эту команду, просмотрите разрешения на папку c:\forTesting. Объясните все обозначения в описаниях прав пользователей и групп в выдаче команды.

а) Разрешите пользователю testUser запись в папку forTesting, но запретите запись для группы testGroup. Попробуйте записать файлы или папки в forTesting от имени пользователя testUser. Объясните результат. Посмотрите эффективные разрешения пользователя testUser к папке forTesting в окне свойств папки.

б) Используя стандартное окно свойств папки, задайте для пользователя testUser такие права доступа к папке, чтобы он мог записывать информацию в папку forTesting, но не мог просматривать ее содержимое. Проверьте, что папка forTesting является теперь для пользователя testUser “слепой”, запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки.

в) Для вложенной папки forTesting\Docs отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка forTesting\Docs перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

г) Снимите запрет на чтение папки forTesting для пользователя testUser. Используя команду icacls запретите этому пользователю доступ к файлам с расширением txt в папке forTesting. Убедитесь в недоступности файлов для пользователя.

д) Командой icacls запретите пользователю все права на доступ к папке forTesting и разреште полный доступ к вложенной папке forTesting\Docs. Убедитесь в доступности папки forTesting\Docs для пользователя. Удалите у пользователя testUser привилегию SeChangeNotifyPrivilege. Попробуйте получить доступ к папке forTesting\Docs. **Объясните результат, записать в выводы.**

е) Запустите файловый менеджер от имени пользователя testUser и создайте в нем папку newFolder на диске C. Для папки newFolder очистите весь

список ACL командой cacls. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

ж) С использованием команды whoami проверьте уровень целостности для пользователя testUser и администратора (учетная запись ВПИ). Запустите какое-нибудь приложение (калькулятор, блокнот) от имени testUser и администратора. С использованием утилиты ProcessExplorer (можно найти в папке c:\Utils на виртуальной машине) проверьте уровень целостности запущенных приложений. Объясните разницу. Верните пользователю testUser права на полный доступ к папке forTesting. От имени администратора создайте в папке forTesting текстовый файл someText.txt. Измените уровень целостности этого файла до высокого с использованием команды icacls. Запустите блокнот от имени пользователя testUser, откройте в нём файл someText.txt, измените содержимое файла и попробуйте сохранить изменения. Объясните причину отказа в доступе. Как можно предоставить пользователю testUset доступ к файлу?

2.2.7. После окончания работы восстановить исходное состояние системы: удалить созданные папки и файлы, разделы реестра, удалить учетную запись созданного пользователя и его группы.

2.2.8. Подготовьте и представьте отчёт по лабораторной работе преподавателю и отчитайтесь за работу.

3. Контрольные вопросы

1. К какому классу безопасности относится ОС Windows по различным критериям оценки?
2. Каким образом пользователи идентифицируются в ОС Windows?
3. Что такое списки DACL и SACL?
4. Перечислите, каким образом можно запустить процесс от имени другого пользователя.
5. Как происходит проверка прав доступа пользователя к ресурсам в ОС Windows?
6. Что такое маркер безопасности, и какова его роль в модели безопасности Windows?
7. Как с использованием команды icacls добавить права на запись для всех файлов заданной папки?
8. Что такое уровень целостности? Как он влияет на права доступа субъектов к объектам ОС? Как можно узнать и задать уровень целостности для объектов и субъектов?

4. Требования к отчёту

Отчёт выполняется каждым студентом индивидуально. Работа должна быть оформлена в электронном виде в формате .doc и распечатана на листах формата А4. На титульном листе указываются: наименование учебного учреждения, наименование дисциплины, название и номер работы, вариант, выполнил: фамилия, имя, отчество, группа, проверил: преподаватель ФИО (образец титульного листа представлен в приложении 1).

Отчет должен содержать:

- название и цель работы;
- краткие теоретические сведения, ответы на контрольные вопросы;
- протокол выполнения лабораторной работы, содержащий список консольных команд, составленных при выполнении работы, и результаты их выполнения (в виде скриншотов).
- выводы по результатам работы.

5. Литература

1. Соломон, Руссинович. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. 4-е издание, СПб.: Питер, 2008., 992 с.

2. А. Чекмарев, А. Вишневский, О. Кокорева Microsoft Windows Server 2003. Русская версия. Наиболее полное руководство., СПб.: БХВ-Петербург, 2008 г., 1120 с.

3. Лясин Д.Н., Саньков С.Г. Методы и средства защиты компьютерной информации (учебное пособие). - Волгоград, Издательство ВолгГТУ РПК "Политехник", 2005г.

4. Лясин Д.Н., Саньков С.Г. Методические указания к лабораторным работам по курсу «Защита информации», 2011.

5. У. Р. Станек. Командная строка Microsoft Windows. Справочник администратора. М.: Русская редакция, 2009., 480с.

6. Безопасность Windows Server 2003 в библиотеке Microsoft TechNet. http://technet.microsoft.com/ru-ru/library/dd548350%28WS.10%29.aspx

7. Набор утилит Sysinternals. Утилита ProcessExplorer. https://technet.microsoft.com/ru-RU/sysinternals/bb896653

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

Лабораторная работа № ____
на тему «_____»

Выполнил обучающийся гр._____

_____
(Фамилия, Имя, Отчество)

Проверил:

_____
(должность, Фамилия, Имя, Отчество)

Ростов-на-Дону
20____