13 Средства безопасности в вычислительных системах

Средства обеспечения безопасности занимают особое положение среди компонентов системы: они взаимодействуют с большинством других подсистем и влияют на их работу. Подсистема безопасности рассматривается обычно как обособленная, но обращения к ней должны быть встроены в систему начиная с низших уровней.

13.1 Угрозы, защищаемые объекты, задачи подсистемы безопасности

Так или иначе, защита в вычислительной системе относится к информации в широком смысле.

К ***защищаемым объектам*** (видам защищаемой информации) в первую очередь относятся:

– программы – защита от несанкционированного использования, т.е. выполнения

– данные – защита он несанкционированного считывания и/или изменения; здесь в роли данных могут выступать также и программы в виде выполняемых файлов.

Субъектами подсистемы безопасности выступают ***пользователи*** системы, однако они всегда представлены ***процессами***, выполняющимися от их имени. Субъекты могут осуществлять легальный (санкционированный) доступ к объектам либо быть источниками ***угроз***.

В качестве ***угроз*** защищаемым объектам рассматриваются:

– несанкционированное использование (программ)

– утечка или хищение (несанкционированное использование данных)

– несанкционированное изменение или искажение (данных)

– уничтожение

Понятие несанкционированного доступа (***НСД***) считается устаревшим ввиду излишней обобщенности.

Угрозы могут исходить не только от субъектов, но и от иных внешних факторов, например физических (особенно искажение и уничтожение данных).

В рамках системы безопасности имеется в виду обычно защита от ущерба при сознательных (не обязательно умышленных) действий пользователя или программного обеспечения. Защита от случайных повреждений относится к обеспечению надежности, хотя «побочным эффектом» системы безопасности может быть и повышение надежности.

Функции подсистемы безопасности могут быть разделены на три основные группы:

– ***Идентификация*** пользователей

– ***Управление доступом***, в первую очередь ограничение доступа

– ***Аудит***: документирование (протоколирование) действий пользователя или программ пользователя.

Уровни действия средств обеспечения безопасности:

– Физическая защита информации на носителях и в средах передачи

– Криптографическая защита информации

– Защита от несанкционированного использования и/или изменения на уровне ***прав доступа***

– Общая защита от проникновения нежелательных пользователей в систему

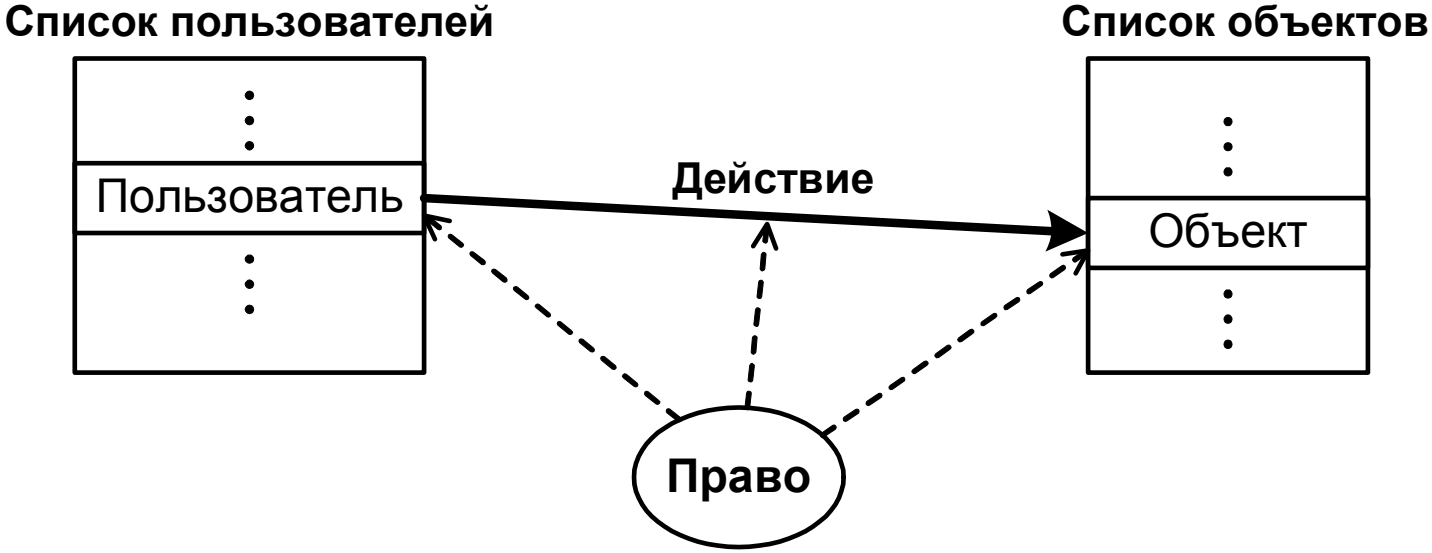
– Организационные меры ограничения доступа

Организационные меры обеспечения безопасности принято отделять от технических.
Аналогично, при оценке технических средств безопасности агентурные методы проникновения обычно не учитывают.

Ключевые понятия для средств безопасности: ***права*** и ***привилегии***:

Право – разрешение конкретному пользователю выполнять конкретные действия над конкретным объектом

Привилегия – разрешение выполнять определенные действия в системе в целом



Применение прав

Основные ***требования*** к системе:

– Целостность и полнота (принцип «слабого звена»)

– Совместимость с действующими программными и аппаратными средствами (желательно прозрачность)

– Экономичность

– Удобство в использовании.

Последние два требования предполагают адекватность затрат на поддержание системы безопасности ожидаемым угрозам и потерям.

Пример конкретного набора формализованных требований к уровню безопасности ***C2*** министерства обороны США:

– Управление доступом к ресурсам: возможность разрешать или запрещать доступ к указанным ресурсам как отдельным пользователям, так и группам пользователей

– Защита памяти, в том числе и от возможного прочтения содержимого памяти даже после ее освобождения

– Регистрация всех пользователей в системе под уникальными идентификаторами и персонификация всех контролируемых системой действий пользователей

– Исключительное право системного администратора контролировать выполнение действий, относящихся к безопасности;

– Защита системы от вмешательства в нее – например, от модификации системного кода в памяти или системных файлов на диске.

В качестве количественных критериев оценки системы безопасности часто выступают:

– Время преодоления (также, возможно, время обнаружения нарушений и реагирования на них)

– Затраты на поддержание (в широком смысле)

Нередко применяется подход к оценке, основанный на моделях из теории игр: преодоление системы защиты и ее совершенствование рассматриваются как одновременно протекающие процессы в рамках стратегий противоборствующих сторон.

13.2 Подсистема безопасности Windows

13.2.1 Общая характеристика

Наличие системы безопасности свойственно ОС семейства Win NT, т.е. собственно NT, 2000, XP и последующим.
ОС Win 9x, будучи ориентированы на индивидуальное «настольное» использование, практически лишены средств поддержания безопасности, имеются лишь простейшие механизмы идентификации и ограничения подключения, которые несложно преодолеть.
Аналогично, файловые системы NTFS имеют встроенные средства защиты файлов (идентификация владельца), FAT – нет.

Windows NT считается удовлетворяющей уровню безопасности C2 Министерства обороны США, но лишь при выполнении ряда дополнительных условий

Действие подсистемы безопасности основано на использовании наборов привилегий и прав.

Объекты безопасности (защищаемые объекты) – объекты, которые требуют защиты от угроз и могут быть защищены от них, т.е. объекты, для которых предусмотрены хранение и контроль прав доступа (это большинство системных объектов):

– ***файлы*** и другие именованные объекты файловой системы

– «***пользователи***» (окна приложений – ***window station*** – и их меню)

– ***объекты ядра*** системы (память, ISO, процессы, потоки и т.д. и их дескрипторы)

– ***реестр*** (ключи реестра)

– ***службы*** (программы в режиме службы – ***service***)

– определяемые пользователем («частные» – ***private***).

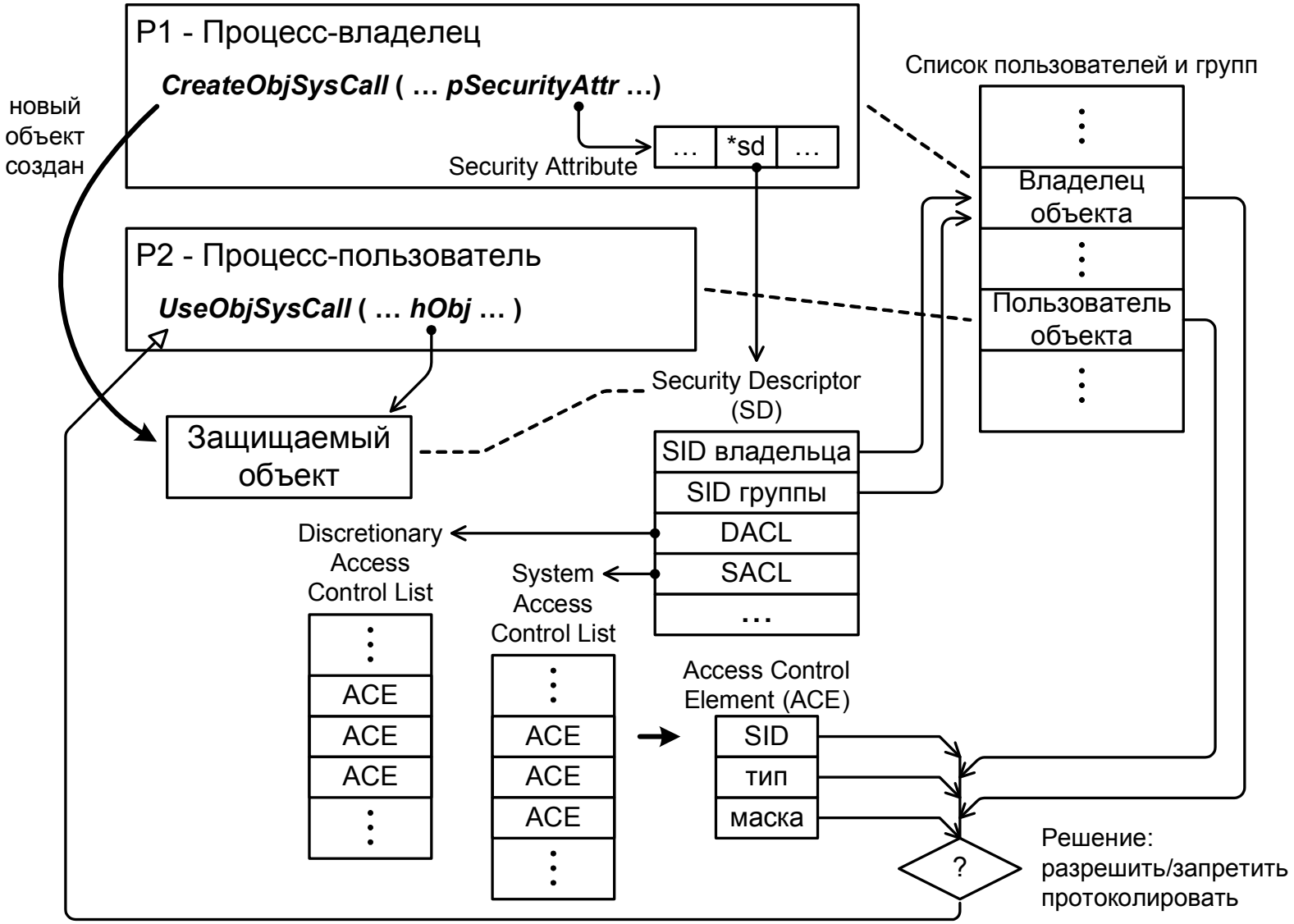
Механизмы обеспечения безопасности едины для всех типов объектов (при различных системных вызовах, инициирующих обращение к этим механизмам).

Если параметры безопасности конкретного объекта не описаны, в действие вступают правила «по умолчанию»:

– принадлежащие ядру системные объекты – доступны всем пользователям

– объекты файловой системы и приравниваемые к ним ключи реестра – доступны владельцу (создателю), его потомкам и процессам его основной группы

При попытке выполнения контролируемого действия выполняется проверка на соответствие его либо правам пользователя в отношении данного объекта, либо привилегиям пользователя. В рамках принятых концепций средства обеспечения безопасности в большинстве случаев применяются автоматически. Реально вмешиваться в работу подсистемы приходится в основном при разработке специфического ПО, при программировании многопользовательских задач либо при необходимости защищать собственные (нестандартные) объекты.



Действие подсистемы безопасности Windows (схематично)

13.2.2 Используемые структуры данных

Общая организация подсистемы безопасности Windows сложная и многоуровневая

Идентификация пользователей и групп

Для идентификации пользователей и групп в рамках системы безопасности Win NT используется их ***Security Identifier*** (***SID***, не путать с ID сеанса в UNIX).

Элементы управления доступом

«Материальный носитель» прав доступа – ***элементы управления доступом*** (***Access Control Element/Entry*** – ***ACE***). Элементы ACE объединяются в списки ACL (см. ниже).

Каждый элемент ACE описывает однотипные права для одного пользователя или группы:

– ***SID*** – идентификатор пользователя (группы)
– ***тип*** элемента – характер прав
– ***маска*** прав – действия, на которые распространяются права.

Типы ACE:

– **`ACCESS_ALLOWED_ACE_TYPE`** – действие разрешено
– **`ACCESS_DENIED_ACE_TYPE`** – действие запрещено
– **`SYSTEM_AUDIT_ACE_TYPE`** – действие подвергается аудиту (протоколируется)

Маска прав – 32-разрядная, разряды показывают наличие (или блокировку, в зависимости от типа) соответствующих разрешений. Наборы прав различаются в зависимости от объектов, основные 4 флага едины для всех объектов:

– **GENERIC_READ**
– **GENERIC_WRITE**
– **GENERIC_EXECUTE**
– **GENERIC_ALL**

В соответствии с типами элементов ACE определены структуры для их представления:

– **ACL_HEADER** – заголовок
– **ACCESS_ALOWED_ACE** – разрешающая запись
– **ACCESS_DENIED_ACE** – запрещающая запись

Дескрипторы безопасности

Связь элементов управления доступом с конкретным объектом – ***дескриптор безопасности*** (***Security Descriptor***, ***SD***), содержащий ***SID*** владельца (индивидуального и основной группы) состоящие из ACE ***списки управления доступом*** (***Access Control List***, ***ACL***).

Дескрипторы безопасности поддерживаются только в Win NT начиная с версии 3.1 и в последующих ОС. В Win 9x поддержки не было.

Два списка в одном дескрипторе безопасности:

– ***дискреционный*** список управления доступом (***Discretionary Access Control List*** – ***DACL***) – управление правами

– ***системный*** список управления доступом (***System Access Control List*** – ***SACL***) – управление протоколированием

Соблюдаются условности:

– Полное отсутствие списка (пустой указатель на список) – права «по умолчанию»

– Пустой список – отсутствие прав доступа

– Запрещающие записи имеют приоритет перед разрешающими, но вплоть до версии Win NT 4.0 это обеспечивалось лишь размещением их в списке раньше разрешающих.

Таким образом, содержимое дескриптора безопасности:
– SID владельца
– SID основной группы владельца
– DACL
– SACL
– дополнительная информация.

Два формата дескриптора:

– ***абсолютный*** (***absolute***) – дескриптор содержит указатели на управляющую информацию.

– ***относительный*** (***self-relative***) – поля находятся непосредственно в дескрипторе, следуя друг за другом.

Все системные вызовы работают с дескрипторами SD в абсолютном формате. относительный формат служит для записи на диск и передачи между процессами (сериализация).

Внутренняя реализация структуры дескриптора безопасности по соображениям безопасности считается закрытой. Для работы с дескрипторами определены соответствующие системные функции.

Атрибут безопасности

Атрибут безопасности служит для связывания объектов с их наборами прав. Применим практически для всех системных объектов, а также пользовательских объектов.
Описывается структурой **`SECURITY_ATTRIBUTE`**:

– **`nLength`** – размер структуры;

– **`lpSecurityDescriptor`** – указатель на дескриптор (описатель) безопасности объекта;

– **`bInheritHandle`** – флаг разрешения наследования атрибута.

Сопоставление атрибута объекту происходит при его (объекта) создании или открытии. Передача осуществляется по указателю **`LPSECURITY_ATTRIBUTE`**, пустой указатель (**`NULL`**) – игнорирование параметра. Атрибуты безопасности поддерживаются начиная с версий Win 95 и Win NT 3.1 соответственно, но в Win 9x переданный атрибут безопасности игнорируется.

13.2.3 API подсистемы безопасности (фрагментарно)

Для формирования дескрипторов служат функция:

```
InitializeSecurityDescriptor();
```

Функция создает работоспособный, но фактически «пустой» дескриптор: без списков, все управляющие флаги **FALSE**.

Получение информации о SID:

```
LookupAccountName();
LookupAccountSid();
```

Создание, формирование, модификация SID:

```
BOOL AllocateAndInitializeSid();
BOOL InitializeSid();
FreeSid();
CopySid();
IsValidSid();
GetLengthSid();
EqualSid();
```

Списки ACL:

```
InitializeAcl()
AddAccessDeniedAce()
AddAccessAlowedAce()
SetSecurityDescriptorAacl() //привязка к SD
```

Пример:

```
SECURITY_ATTRIBUTES sa;
SECURITY_DESCRIPTOR sd;
InitializeSecurityDescriptor(&sd,
SECURITY_DESCRIPTOR_REVISION);
SetSecurityDescriptorDacl(&sd,TRUE,NULL,FALSE);
sa.nLength = sizeof(sa);
sa.bInheritHandle = TRUE;
sa.lpSecurityDescriptor = &sd;
```

Здесь список ACL отсутствует, объект будет общедоступным.

Явная проверка прав доступа:

```
BOOL AccessCheck();
```

Создание «частного» (private) защищаемого объекта

```
CreatePrivateObjectSecurity();
```

При регистрации пользователя его пароль сверяется с информацией, хранящейся в системной базе данных. В случае успеха на основании этой информации ему назначается т.н. ***маркер*** или ***токен доступа*** (***access token***), в данном случае это ***основной токен персонализации*** (***impersonation token***) Этот маркер в дальнейшем будет присваиваться каждому процессу, который запустит пользователь.

Маркер содержит информацию о пользователе, группе, привилегиях и правах доступа. При попытке обратиться к объекту выполняется поиск в списке ACL этого объекта элемента ACE, соответствующего обратившемуся процессу.

На основе сравнения маркера доступа и ACE принимается решение о разрешении или запрещении доступа процесса к объекту.

Помимо основного, можно получить т.н. ***специальный*** токен персонализации, который используется для выполнения действий от имени другого процесса и с его правами. Обычное («легальное») применение данного механизма – исполнение сервером действий от имени своего клиента, что включает контроль прав соответствующего рядового пользователя (сервер считается заведомо защищенным и пользующимся большим доверием, чем клиент).

Уровни:

– **`SecurityAnonymous`** – нет идентификационной информации о клиенте

– **`SecurityIdentification`** – можно плучить идентификационную информацию

– **`SecurityImpersonation`** – разрешена персонификация (работа от имени данного процесса)

Вход пользователя и получение токена:

BOOL LogonUser()
BOOL OpenProcessToken(), OpenThreadToken()
ImpersonateLoggedOnUser() *//с токеном другого процесса*
ImpersonateSelf() *//смена уровня собственного токена*

13.3 Служба Kerberos

Механизм (сервис) ***Kerberos*** (***The Kerberos Network Authentication Service V5***) описан в RFC 1510 (дополнения в RFC 1964) и призван обеспечить безопасное взаимодействие между клиентами и серверами в распределенной системе.

В крупных сложных системах серьезной проблемой является потенциальное наличие «враждебных» серверов, в т.ч. и предоставляющих вполне «легальные» услуги, но при этом выполняющих деструктивные функции, например, собирающие пароли пользователей (клиентов).

Поскольку в большой системе количество серверов велико, и многие из их относятся к «малознакомым», вероятность данной угрозы достаточно высока. Обладая же паролем клиента, злоумышленник получает доступ к его ресурсам на других серверах, возможность исполнять действия от его имени и т.д.

Вариантом решения проблемы является сосредоточение функций идентификации (аутентификации) в немногих хорошо защищенных центрах, которые управляют процессом раздачи прав. Подобная схема «клиент – сервер – центр аутентификации» называется трехсторонней, или «с ***доверительной третьей стороной***» (***trusted third-party***).

Сам принцип аутентификации с точки зрения пользователя при этом не изменяется, однако общается он уже не непосредственно с сервером, а с «третьей стороной» – специальным ***сервером аутентификации***.

Согласно Kerberos, обмен между клиентом и сервером аутентификации (наиболее уязвимый отрезок) защищается криптографически – ***симметричным*** шифрованием с ***секретным ключом*** (***secret key*** или ***private key***), стандартно используется алгоритм ***DES***). Kerberos-сервер хранит информацию о своих клиентах, включая их секретный ключ.

Приняты следующие термины:

– ***Key Distribution Center*** (***KDC***) – центр распределения ключей, сервер системы аутентификации

– ***Ticket*** («***билет***») – разрешение, набор информации, пересылаемый "целевому" серверу вместо пароля пользователя

– ***Ticket-Granting Server*** (***TGS***) – сервер выдачи «билетов»

– ***Ticket-Granting Ticket*** (***TGT***) – «билет предоставления билетов».

Кроме постоянного секретного ключа в обмене участвует также ***сеансовый ключ*** (***session key***), которым защищаются передаваемые билеты. Дополнительным средством идентификации их подлинности служит ***временная метка*** (***time stamp***), играющая роль ***имитовставки*** и обеспечивающая уникальность каждой посылки и противодействие повторному использованию перехваченных данных.

Имея полученный от KDC билет, клиент пересылает его серверу вместо своего пароля. Сервер, поддерживающий Kerberos (т.е. способный распознать эту ситуацию) обращается к тому же KDC за подтверждением подлинности билета и выполняет запрос только после положительного ответа. Воспользоваться перехваченным билетом явным образом нельзя, т.к. он содержит временную метку и устаревает.

Рис – Трехсторонняя схема аутентификации

Таким образом:

– «базовый» секретный ключ клиента известен только клиенту и KDC;

– текущий обмен билетами защищен криптографически с временным ключом;

– имитовставки усложняют наблюдение за обменом и препятствуют использованию перехваченных посылок.

В рамках Kerberos описан ряд алгоритмов (протоколов) обмена между участниками взаимодействия. Для связи используются протоколы TCP и UDP, порт **88**. В виде, описанном в RFC, Kerberos рассчитан на использование в любых сетях вплоть до глобальных: варианты взаимного расположения участников обмена ограничено только их достижимостью посредством обычных сетевых протоколов.

Начиная с Windows 2000 декларируется соответствие спецификации Kerberos, причем механизм Kerberos включается в ее подсистему безопасности прозрачно. В состав «билета» включается идентификатор объекта безопасности (SID) пользователя.