**Реферат на тему «Система безопасности ОС»**

# **Требования к безопасности**

Требования к безопасности определяются на основе международных стандартов по оценке защищенности – ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation – Общие критерии оценки безопасности ИТ. В этом стандарте определены 7 уровней безопасности (EAL1 – EAL7).

Выделяют следующие 9 требований к безопасности.

# **Обязательная идентификация и аутентификация**

Пользователь до выполнения действий должен пройти

* *идентификацию* – представится системе (логин и пароль);
  + процесс Winlogon.exe;
* *аутентификацию* – подтвердить, что он является тем, кем представился;
  + Процесс Lsass.exe.

# **Управляемый доступ к объектам**

*Пользователь-владелец* должен иметь возможность предоставлять доступ к объекту определенным пользователям/группам пользователей.

Безопасный доступ – Security Reference Monitor – монитор контроля без-сти.

# **Аудит**

Система должна отслеживать и записывать все события, связанные с доступом к объектам – SRM и Lsass.exe.

# **Защита при повторном использовании объектов**

Если область памяти выделялась какому-либо пользователю, а затем была освобождена – данные в этой области памяти должны быть стерты.

В Windows освобожденная память очищается системным потоком обнуления страниц, который работает во время простоя системы.

# **Организация управляемого доступа к объектам. Принцип организации доступа**

Принцип организации управляемого доступа: у каждого пользователя имеется свой *маркер доступа*, в котором есть уникальный id пользователя. Процессы, которые создаются пользователем, наследуют его маркер.

Попытка доступа => сравнение с id, которые содержатся в дескрипторе защиты => доступ либо разрешается, либо запрещается.

Все объекты системы имеют *дескриптор защиты*, который состоит из :

* списка id пользователей
  + могут получить доступ к объекту
  + не могут получить доступ к объекту
* вида доступа
  + только чтение
  + чтение и запись
  + только запись
  + полный доступ и т.д.

# **Идентификаторы защиты**

*Идентификатор защиты* – SID (Security Identifier) – идентификатор для однозначного определения пользователя в системе.

Имеется у пользователей, групп пользователей, пк, доменов и членов доменов. Указывается случайным образом => вероятность совпадения у разных пользователей близка к нулю. Состоит из:

* номера версии – поле Reversion;
* кода агента идентификатора – поле IdentifierAuthority;
* кодов субагентов – поле SubAuthority;
  + количество субагентов – поле SubAuthorityCount;
  + последний код субагента – *относительный идентификатор* – т.к. все учетные записи пользователей могут иметь одинаковые коды, кроме RID (RID=500 => локальный администратор)

# **Маркер доступа**

*Маркер доступа* создается во время входа пользователя в систему процессом Lsass.exe и хранится в поле *Token* структуры *EPROCESS* и имеет следующие поля:

* TokenId – id маркера;
* UserAndGroups – SID учетной записи;

При проверке возможности доступа к ресурсу система проверяет, входит ли SID учетной записи в список доступа файла.

# **Дескриптор защиты**

*Дескриптор защиты* – атрибут объектов, к которым могут получать доступ различные процессы и который содержит информацию о пользователях, которым либо запрещен, либо разрешен доступ к объекту. Дескриптор защиты состоит из:

* Owner – SID владельца
* Dacl – список управления избирательным доступом – определяет пользователей, которые могут получить доступ к объекту, а также указывает тип доступа
* Sacl – системный список управления доступом – перечислены пользователи и операции, которые должны учитываться в журнале аудита безопасности.

**Списки управления доступом** представлены:

* + заголовок ACL Header

описывается структурой ACL, в которой хранятся количество элементов списка ACL и общий размер списка без заголовка;

* + посл-сть элементов списка (Access-Control Entry), который состоит из
    - заголовок ACE Header – указывает тип ACE
      * доступ разрешен
      * доступ запрещен
    - маску доступа – описывает виды доступа к объектам и права
      * право на удаление объекта
      * право на просмотр информации о дескрипторе защиты объекта
      * право на использование объекта для синхронизации
      * право на изменение списка DACL
      * право на смену владельца объекта
    - идентификатор

*Функция SeAccessCheck* отвечает за проверку возможности доступа процесса к объекту и может вернуть 1 из двух возможных результатов:

* true – если процессу возможно предоставить доступ к объекту и маску предварительного доступа;
* false – если доступ запрещен;

# **Права и привилегии**

*Права учетных записей и привилегии* – предназначены для управления действиями, которые не связаны с доступом к конкретным объектам.

*Право учетной записи* – разрешение или запрет на определенный вид входа в систему.

Виды входа:

* локальный вход;
* вход из сети;
* вход через службу удаленных рабочих столов;
* вход в качестве службы;
* вход в качестве пакетного задания.

*Привилегия* – разрешение или запрет определенных действий в системе. Например, включение или выключение пк, загрузка драйверов.

Список всех привилегий: панель управления – администрирование – оснастка MMC «локальная политика безопасности» – локальные политики – назначение прав пользователей.

# **Программа «создание дескриптора безопасности ОС»**

*Дескриптор безопасности* создается для ресурса и связывает ресурс с пользователем или процессом при помощи SID. При обращении к ресурсу проверяется, содержится ли данный процесс в дескрипторе безопасности.

Пользователь, который создает ресурс, в свою очередь идентифицируется с помощью SID и определяет права доступа и ограничения. И когда пользователь запускает процесс, процесс наследует SID данного пользователя. Если процесс будет работать с файлом/каталогом => его SID должен содержаться в дескрипторе безопасности этот файла/каталога.

* инициализация дескриптора безопасности – InitializeSecurityDescriptor
* установка SID владельца объекта – SetSecurityDescriptor
* установка SID первичной группы владельца – SetSecurityDescritporGroup
* проверяем валидность созданной структуры дескриптора – IsValidSecurityDescriptor
* создаем каталог – CreateDirectory