Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Операционные системы и системное программирование**

Реферат

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Матюх А.А.

Минск 2020

**Система безопасности Windows**

Требования к системе безопасности операционной системы Windows описан в стандарте ISO/IEC 15408. В нем определены семь уровней безопасности от EAL1 до EAL7. Наличие у уровня в конце знака плюс означает Flaw Remediation – исправление ошибок, что говорит о постоянном выпуске ошибок. К примеру, Windows 7 был присвоен уровень EAL4+.

Рассмотрим основные требования к безопасности:

1. Обязательная идентификация и аутентификация;
2. Управляемый доступ к объектам;
3. Аудит;
4. Защита при повторном использовании объектов.

Для однозначного определения пользователя в системе используются идентификаторы защиты (SID – Security Identifier), которые генерируются случайным образом самой системой, дабы снизить вероятность совпадения идентификаторов к минимуму. Кроме пользователей, SID имеется у групп пользователей, компьютеров, доменов и членов доменов.

В WRK структура SID описывается в файле public\sdk\inc\ntseapi.h . SID состоит из следующих частей:

* номер версии – поле Revision (1 байт);
* код агента идентификатора (identifier authority) – поле IdentifierAuthority (6 байт);
* коды субагентов (subauthority values) – поле SubAuthority (от 1 до 15 кодов по 4 байта каждый). Количество кодов субагентов хранится в поле SubAuthorityCount.

Для входа и работы с процессами пользователю используется маркер доступа, который хранит в себе идентификаторы безопасности этого пользователя. Рассмотрим структуру токена

* TokenId – идентификатор маркера;
* UserAndGroups – SID учетной записи пользователя и групп, в которые данная учетная запись входит.;
* Privileges – список привилегий;
* DefaultDacl – список управления избирательным доступом по умолчанию (DACL, Discretionary Access-Control List).

Для управления различными действиями в системе используются права и привилегии.

Права представляют собой разрешения или запрет на определенный вид входа в учетную запись. Проверка прав осуществляется в процессах Winlogon.exe и Lsass.exe.

Привилегии же представляют собой разрешения или запреты на работу с системными объектами. Привилегии хранятся в поле Privileges структуры маркера доступа TOKEN.