Практическое задание по лекции №15

Каким сочетанием клавиш инициируется процедура аутентификации?

Что такое библиотека GINA?

Перечислите распространённые типы специальных событий для аудита безопасности

Гарантируется ли безопасность повторного использования областей физической памяти?

Что такое Windows File Protection?

Расскажите про маркер доступа

Можно ли добавить привилегию в маркер?

Как можно создать маркер перевоплощения?

Где можно посмотреть все действия пользователей?

Что согласно п4 политики безопасности должна делать ОС windows?

Процедурой аутентификации пользователя в системе управляет программа, WinLogon, представляющая собой начальную интерактивную процедуру, которая отображает начальный диалог с пользователем на экране.

Чтобы инициировать фиксацию событий, связанных с доступом к объекту, необходимо сформировать в дескрипторе безопасности этого объекта список SACL, в котором перечислены пользователи, чьи попытки доступа к данному объекту подлежат аудиту

Согласно п.4 политики безопасности, ОС должна защищать объекты от повторного использования.

В соответствии с политикой безопасности операционная система должна защищать себя от внешнего влияния или навязывания, такого, как модификация загруженной системы или системных файлов, хранимых на диске.

Наиболее важной характеристикой субъекта является маркер доступа

Для безопасной работы в духе принципа минимума привилегий ОС Windows поддерживает механизмы создания маркеров с ограниченными привилегиями и заимствования маркера

Другой способ выполнить код с заимствованным маркером - осуществить перевоплощение (impersonation)

Список SACL, входящий в состав дескриптора защиты объекта, можно формировать и модифицировать программными средствами

При формировании маркера используются ключи SECURITY и SAM реестра.

Библиотека GINA является заменяемым компонентом, интерфейс с ней хорошо документирован, поэтому иногда в приложениях, реализующих защиту, присутствует версия GINA, отличная от оригинальной.