**Практическое задание по лекции 15**

**Вопросы лекция 15**

1. Что в первую очередь должен сделать пользователь для доступа к компьютеру, согласно политике безопасности?

2. Что представляет собой программа WinLogon?

3. Почему иногда в приложениях, реализующих защиту, присутствует версия GINA, отличная от оригинальной?

4. Что делает Winlogon в случае успешного входа в систему?

5. Какой инструмент является основным для выявления вторжений? Как это реализуется?

6. Какие операции влияют на состояние безопасности компьютерной системы?

7. Чем может быть сгенерировано событие аудита в ОС Windows?

8. От чего ОС должна защищать объекты? Для чего инициализируют объекты?

9. Каким образом в ОС Windows гарантируется безопасность повторного использования областей физической памяти?

10. От чего защищают встроенные в ОС Windows средства защиты файлов? Что лежит в основе этой защиты?

11. Что подлежит мониторингу и защите в составе ОС?

12. Как создаётся и что хранит маркер доступа?

13. Что поддерживает ОС Windows для безопасной работы по принципу минимума привилегий?

14. Почему в ОС Windows нельзя менять большую часть информации в маркере?

**Словарь лекция 15**

SAS (secure attention sequence) - это специальная клавиша или комбинация клавиш, которую пользователь должен нажать на клавиатуре компьютера перед входом в систему. Ядро операционной системы, взаимодействующие напрямую с компьютером, может обработать нажатие комбинации клавиш и начать вход в систему.

Программа входа в систему (WinLogon) - это компонент операционной системы Microsoft Windows, отвечающий за вход в систему.

GINA (Graphic Identification aNd Authentication) - это графическая библиотека идентификации и аутентификации.

Маркер доступа - программный объект операционных систем класса Microsoft Windows, содержит информацию по безопасности сеанса и идентифицирует пользователя, группу пользователей и пользовательские привилегии.

SACL (System Access Control List) - список управления доступом к объектам Microsoft Windows, используемый для аудита доступа к объекту.

SeSecurityPrivilege - это привилегия, которой должен обладать процесс для управления файлом журнала безопасности, а также для просмотра и изменения SACL объектов.

SeAuditPrivilege - это привилегия, которой должен обладать процесс, вызывающий системные записи аудита, чтобы успешно сгенерировать запись аудита в журнале безопасности.

PFN (Page Frame Number) - системная база данных, содержащая список страниц оперативной памяти системы и ускоряющая доступ и действия ядра ОС с оперативной памятью.

WFP (Windows File Protection) - это технология, позволяющая запретить программам изменять или удалять наиболее важные системные файлы операционных систем семейства Windows.

TrueType - это формат компьютерных шрифтов. Шрифты в данном формате используются во многих современных операционных системах. Файлы с такими шрифтами имеют расширение имени «ttf».

Каталог dllcache - это скрытый каталог, который хранит копии системных файлов, предназначенные для замены используемых системных файлов в случае их повреждения или незаконного изменения.

Sfc.exe (system file checker) - это утилита, предназначенная для проверки корректности версии всех системных файлов.

SigVerif.exe (Signature Verification) - это утилита, предназначенная для проверки подписи и выявления неподписанных файлов.

runas - это утилита, которая позволяет запускать приложения от имени другой учетной записи.

AdjustTokenPrivileges - это функция, предназначенная для включения и отключения определенных привилегий маркера доступа.

CreateProcessAsUser - это функция, предназначенная для запуска нового процесса с указанным маркером. Она является аналогом функции CreateProcess за исключением параметра hToken, который указывает на маркер, определяющий контекст пользователя нового процесса.

Перевоплощение (impersonation) - один из потоков процесса функционирует с маркером, отличным от маркера текущего процесса.

TokenImpersonationLevel - это параметр маркера, которым определяется уровень перевоплощения.

DuplicateTokenEx - это функция, с помощью которой создают маркер перевоплощения, путем дублирования существующего маркера и придания ему нужных прав доступа и уровня имперсонации.

ImpersonateLoggedOnUser и RevertToSelf - это функции, с помощью которых осуществляются перевоплощение и возврат в исходное состояние соответственно.