Лабораторная работа № 20

Тема: Политика безопасности и ограничения программ в ОС Windows XP.

Цель работы**:** Цель работы: Изучить политику ограниченного использования программ.

Предварительная подготовка: спец. дисциплины «Операционные системы».

Количество часов: 2 часа

Оборудование: Персональный компьютер.

Краткие теоретические сведения

1Общие сведения

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения путем определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для хеша, правила дляcертификата, правила для пути и правила для зоны Интернета. Программное обеспечение может выполняться на двух уровнях: неограниченном и запрещенном.

Политики ограниченного использования программ регулируют использование неизвестных программ и программ, к которым нет доверия. В организациях используется набор хорошо известных и проверенных приложений. Администраторы и служба поддержки обучены для поддержки этих программ. Однако, при запуске пользователем других программ, они могут конфликтовать с установленным программным обеспечением, изменять важные данные настройки или, что ещё хуже, содержать вирусыили «троянские» программы для несанкционированного удаленного доступа.

При интенсивном использовании сетей, Интернета и электронной почты в бизнесе пользователи повсеместно сталкиваются с различными программами. Пользователям постоянно приходится принимать решения о запуске неизвестных программ, поскольку документы и веб-страницы содержат программный код —сценарии. Вирусы и «троянские» программы зачастую умышленно замаскированы для введения пользователей в заблуждение при запуске. При таком большом количестве и разнообразии программ отдельным пользователям трудно определить, какое программное обеспечение следует запускать.

Пользователем необходим эффективный механизм идентификации и разделения программ на безопасные и не заслуживающие доверия. После идентификации программы к ним может быть применена политика для определения, могут ли они быть запущены. Политики ограниченного использования программ предоставляют различные

способы идентификации программного обеспечения и средства определения, следует ли запускать данное приложение.

2Дополнительные правила и уровни безопасности

Дополнительные правила и уровни безопасности

При применении политик ограниченного использования программ идентификация программного обеспечения производится посредством следующих правил:

2.1Правило для сертификата

Политики ограниченного использования программ могут идентифицировать файл по его сертификату подписи. Правила для сертификатов не применяются к файлам с расширением .exe или .dll. Они используются для сценариев и пакетов установщика Windows. Имеется возможность создать правило для сертификата, идентифицирующее приложение и затем, в зависимости от уровня безопасности, позволяющее или не позволяющее его запустить. Например, администратор может использовать правила для сертификатов, чтобы автоматически доверять программам из проверенного источника в домене без запроса пользователя. Кроме того, правила для сертификатов могут использоваться в запрещенных областях операционной системы.

2.2Правило для пути

Правило для пути идентифицирует программы по пути к файлу. Например, если имеется компьютер с политикой запрета по умолчанию, имеется возможность, предоставить неограниченный доступ к указанной папке для каждого пользователя. Для данного типа правил могут быть использованы некоторые общие пути: %userprofile%, %windir%, %appdata%, %programfiles% и %temp%.

Поскольку данные правила определяются с использованием пути, при перемещении программы правило для пути применяться не будет.

2.3Правило для хеша

Хеш представляет собой серию байтов фиксированной длины, однозначно идентифицирующую программу или файл. Хеш рассчитывается с помощью алгоритма хеширования. Политики ограниченного использования программ могут идентифицировать файлы по их хешу с помощью алгоритмов хеширования SHA-1 (Secure Hash Algorithm) и MD5 hash algorithm.

Например, имеется возможность создать правило для хеша и задать уровень безопасности «Не разрешено», чтобы запретить запуск определенного файла. Хеш переименованного или перемещенного в другую

папку файла не изменяется. Однако, при любом изменении файла значение хеша изменяется, позволяя обойти ограничения.

Политики ограниченного использования программ распознают только хеши, рассчитанные с помощью политик ограниченного использования программ.

2.4Правило для зоны Интернета

Правила для зоны влияют только на пакеты установщика Windows.

Правило для зоны идентифицирует программное обеспечение из зоны, указанной посредством Internet Explorer. Такими зонами являются Интернет, локальный компьютер, местная интрасеть, ограниченные узлы и надежные сайты.

2.5Уровень безопасности

В политиках ограниченного использования программ используются следующие уровни безопасности:

- *Неограниченный*. Приложения запускаются со всеми правами пользователя, вошедшего в систему.
- *Не разрешено*. Приложения не могут быть запущены.
- *Обычный пользователь*. Приложения запускаются с правами обычного пользователя, даже если пользователь является членом группы администраторов.

Отчет должен содержать

1. Название, цель, задание лабораторной работы
2. Описание выполнение задания
3. Ответы на контрольные вопросы

Контрольные вопросы

1. Перечислите уровни безопасности.
2. Какая имеется возможность использования программ с помощью политик ограниченного доступа?
3. Программное обеспечение может выполняться на каких уровнях?