ПУБЛИКАЦИЯ РАЗРЕШЕНИЯ НА ДОСТУП К РАЗЛИЧНЫМ КОМПОНЕНТАМ ОПЕРАЦИОННОЙ СИСТЕМЫ НА БАЗЕ WINDOWS NT

Сотников С.В.[1], Мухаметханов Р.Р.[2]

[1]Сотников Сергей Викторович – кандидат технических наук, доцент;
[2]Мухаметханов Равиль Рамилевич – магистрант,
кафедра прикладной математики и информатики,
Казанский национальный исследовательский технический университет имени А.Н. Туполева – КАИ,
г. Казань

Аннотация: *в данной статье анализируется работа системного администратора в компаниях, которые используют информационные технологии, а в частности компьютерные сети. Целью нашего исследования является поиск способа автоматизации, некоторых задач системного администрирования, для облегчения рабочего процесса системного администратора. Рассматривается задача обеспечения информационной безопасности в компьютерной сети компании. Процесс решения данной задачи, является одним из трудоемких и сложных, в профессии системного администратора.*
Ключевые слова: *системный администратор, компьютерная сеть, информационная безопасность, Windows NT.*

Одной из основной задачей системного администрирования является, ответственность за обеспечение информационной безопасности в компании. Системный администратор должен обезопасить сеть не только от преднамеренных атак злоумышленников, но и от самих сотрудников, являющиеся пользователями сети компании. Необходимо ограничить возможность влияния на работоспособность сети некомпетентными действиями пользователей данной сети. Ограничив доступ к некоторым ресурсам сети компании, системный администратор обеспечит безопасность, тем самым уменьшив риск потери информации и сбоев в работе сети.

Рассмотрим одноранговую сеть на основе модели клиент-сервер, при которой клиенты обращаются к центральному узлу сети (серверу) [1].

Контроллер доменов (сервер) должен содержать всю информацию о каждом клиенте, а именно: версия операционной системы, файлы и папки данных, производительность системы, информация обо всех доступных директориях. Ниже представлены защищённые объекты операционной системы клиента на базе Windows, имеющие список доступа DACL, о которых контроллер доменов должен иметь полную информацию:

SE_UNKNOWN_OBJECT_TYPE – Неизвестный тип объекта.
SE_FILE_OBJECT – Указывает файл или каталог.
SE_SERVICE – Указывает службу Windows.
SE_PRINTER – Указывает принтер.
SE_REGISTRY_KEY – Указывает ключ реестра.
SE_LMSHARE – Указывает сетевой ресурс.
SE_KERNEL_OBJECT – Указывает локальный объект ядра.
SE_WINDOW_OBJECT - Указывает станцию окна или объект рабочего стола на локальном компьютере.
SE_DS_OBJECT – Указывает объект службы каталогов или набор свойств или свойство объекта службы каталогов.
SE_DS_OBJECT_ALL – Указывает объект службы каталогов и все его наборы свойств и свойства.
SE_PROVIDER_DEFINED_OBJECT – Указывает определенный с помощью провайдера объект.
SE_WMIGUID_OBJECT – Указывает объект WMI.
SE_REGISTRY_WOW64_32KEY – Указывает объект для ключа реестра под WOW64.

Всего в операционной системе клиента может быть 13 объектов, информацию о которых необходимо занести на сервер [2].

Занесение информации, о представленных выше объектах операционной системы клиента, в контроллер доменов достаточно трудоемкий процесс, который выполняется вручную системным администратором. Хотелось бы автоматизировать этот процесс. Предлагается разработать программное обеспечение (ПО), удовлетворяющее следующим требованиям:

1) Разрабатываемое ПО должно иметь графический интерфейс, с возможностью отображения в нем доступных компьютеров-клиентов в сети и отображение ресурсов (объектов) операционной системы клиента.
2) При запуске ПО на клиенте или сервере происходит обнаружение сети. Вся сеть представляется как дерево объектов, где главным объектом является сервер – контроллер доменов. Так же при не

обнаружении какого-либо компьютера в сети, должна быть возможность его поиска по IP адресу или названию данного компьютера. При выборе компьютера-клиента в списке дерева

3) Главной возможностью разрабатываемого ПО является публикация всех ресурсов клиента на контроллере домена. Публикация производится путем создания групп безопасностей в контроллере доменов для каждого объекта операционной системы, которых может быть 13, они представлены выше в постановке задачи.

4) После создания групп безопасности на контроллере доменов для существующих объектов клиента, данные группы заносятся в DACL список этих же объектов на самом клиенте.

На современном рынке программного обеспечения не существует подобной программы, удовлетворяющей вышеописанным требованиям. Разработка такого ПО является актуальной и востребованной в наше время.

Список литературы

1. *Таненбаум Э., Уэзеролл Д.* Компьютерные сети, изд. Питер, 2012. 960 с.
2. Microsoft Developer Network // SE_OBJECT_TYPE enumeration. [Электронный ресурс]. Режим доступа: https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa379593/ (дата обращения: 08.05.2017).