Егоров Валерий Юрьевич
vec@mail.ru
тел. +79603251632

Контроль доступа к аппаратным устройствам компьютера на основе управления политикой питания

В настоящее время в современных операционных системах (ОС) осуществляется контроль доступа к логическим объектам, таким как файлы, объекты синхронизации, процессы (нити), а также к физическим объектам, таким как устройства ввода-вывода, сканеры, принтеры и т.д. на основе политики безопасности, принятой на уровне компьютера или домена. Над этими объектами осуществляется дискреционный или мандатный контроль доступа. Указанный перечень может быть расширен с использованием контроля доступа к устройствам на основе управления политикой питания. К шинам, которые поддерживают управление политикой питания, относятся, в том числе, шины PCI Express и USB.

Например, рассмотрим работу контроллеров USB в составе автоматизированного рабочего места (АРМ). Сегодня имеются решения, которые позволяют администратору безопасности управлять доступом пользователя к накопителям, подключенным к шине USB. Однако, администратор не имеет возможности определять перечень разъёмов, к которым возможно подключение того или иного устройства.

Возможность управления и контроля доступа к разъёмам USB может предоставить контроль доступа на основе управления политикой питания. Для этого необходимо расширить политику безопасности не только на перечень устройств, в отношении которых осуществляется разделение прав доступа, но также и на перечень разъёмов, к которым данные устройства могут быть подключены. При таком подходе возможности администрирования политики безопасности существенным образом расширяются. Например, в разъёмы на передней панели компьютера можно подключать только накопители MassStorage, в то время как к тыловым

разъёмам возможно подключение каких-либо токенов и оргтехники. При этом настройки прав доступа меняются в зависимости от того, какой именно пользователь осуществил вход в систему. Кроме того, возможна реализация запрета на подключение к компьютеру устройств до входа пользователя в систему.

На физическом уровне реализация подобной политики безопасности потребует управление режимами питания устройств со стороны менеджера безопасности. Если пользователю запрещен доступ к фронтальным USB разъёмам до достаточно перевести нужные разъёмы в режим D3hot. Кроме того, данным способом можно запрещать использование USB разветвителей, включать и выключать поддержку зарядки мобильных устройств, а также скорость их зарядки.

Подобное расширение перечня механизмов контроля доступа может быть введено в состав политики безопасности в информационных системах, основанных на отечественных ОС. Внедрение такого механизма расширит возможности по администрированию информационных систем.