МЕТОД РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ЛОКАЛЬНЫМ УСТРОЙСТВАМ РЕАЛИЗАЦИЕЙ УПРАВЛЕНИЯ МОНТИРОВАНИЕМ К СИСТЕМЕ УСТРОЙСТВ ПО ПОЛЬЗОВАТЕЛЯМ

Введение.

Ключевой задачей защиты информации в современных условиях является формирование защищаемого объекта в части локализации подключаемых к системе устройств (локальных устройств). Эффективная защита реализуется разграничительной политикой доступа субъектов к защищаемым объектам, но до тех пор, пока возможности подключения к системе устройств не локализованы невозможно определить перечень защищаемых объектов в системе - объектов, к которым необходимо разграничить права доступа. Например, чтобы утверждать, что защищаемый компьютер автономный, при этом не требуется реализации разграничительной политики доступа субъектов к сетевым ресурсам, необходимо предотвратить возможность подключения к системе (и отключить присутствующие в системе) всех устройств (сетевых адаптеров, модемов и т.д.), обеспечивающих доступ к сети. Данная задача защиты решается управлением монтирования устройств к системе, в том числе, с целью исключения возможности монтирования устройств, использование которых, по каким-либо причинам, несет в себе угрозу несанкционированного доступа к информации (например, смартфоны некоторых производителей не являются файловыми накопителями ОС Microsoft Windows - к ним невозможно разграничить права доступа как к файловым объектам).

В современных ОС Windows реализовано управление монтированием устройств к системе без учета работающих в системе пользователей, т.е. те устройства, которые администратором будет разрешено подключать (монтировать), разрешается подключать всем пользователям. Естественно,

что при этом не могут разграничиваться права доступа пользователей к разрешенным для монтирования к системе устройствам, как следствие, к каждому подобному устройству необходимо каким-то образом еще и разграничивать права доступа пользователей. Особенно это критично при реализации сессионного контроля доступа [1], который в современных условиях может рассматриваться в качестве эффективной альтернативы, так называемым, DLP - решениям (защита от утечки с компьютера конфиденциальной информации, угроза которой возникает при необходимости обработки на одном и том же компьютере одним и тем же пользователем, как открытой, так и конфиденциальной информации [2]). Важным является и тот аспект, что для многих устройств, например, локальный принтер, сканер и т.д., при реализации разграничительной политики может задаваться только один тип прав доступа - разрешено использовать, либо нет (это не файловый объект, где можно для различных пользователей задавать различные права доступа - чтение, запись, исполнение, удаление, переименование и т.д.). Все это обусловливает важность и целесообразность реализации разграничительной политики прав доступа пользователей к локальным устройствам управлением монтированием устройств к системе по пользователям.

1. Метод динамического монтирования к системе устройств по пользователям.

Особенность реализации разграничительной политики доступа к устройствам в данном случае состоит в том, что не перехватываются и не анализируются непосредственно запросы доступа пользователей к устройствам (в противном случае для каждого типа устройств пришлось бы делать соответствующий механизм защиты, решающий данные задачи). Для каждого пользователя задаются устройства, с которыми он может, либо, наоборот, не должен работать. При входе пользователя в систему монтируются и ему разрешается монтирование (например, внешние накопители) определенные в разграничительной политике устройства. С

учетом же того, что ОС многопользовательская (в системе одновременно может присутствовать несколько интерактивных пользователей), решается задача динамического примонтирования/отмонтирования устройств. При этом если в системе будет одновременно зарегистрировано несколько пользователей, то примонтированы к ней будут и будут разрешаться для примонтирования пользователями (например, внешние накопители) только те устройства, которые разрешено использовать всем этим зарегистрированным пользователям (остальные устройства будут автоматически отмонтированы от системы, либо их будет запрещено примонтировать).

Отметим, что для общности решаемой задачи защиты под подобную разграничительную политику подпадают все возможные устройства в системе и подключаемые к системе, что накладывает некоторые ограничения на возможность их автоматического примонтирования после отмонтирования от системы. Не все системные устройства могут автоматически примонтироваться к системе после их отмонтирования без полной перезагрузки системы. Однако это ограничение имеет скорее теоретический характер, т.к. в отношении устройств, монтируемых пользователями в процессе работы (что, в первую очередь, и требуется разграничивать), подобных ограничений не возникает.

2. Реализация метода динамического монтирования к системе устройств по пользователям.

Рассмотрим реализацию метода динамического монтирования устройств по пользователям на примере апробированного технического решения, реализованного в КСЗИ «Панцирь+» для ОС Microsot Windows [3].

Интерфейс просмотра списка устройств и класса устройств в системе представлен на рис.1.

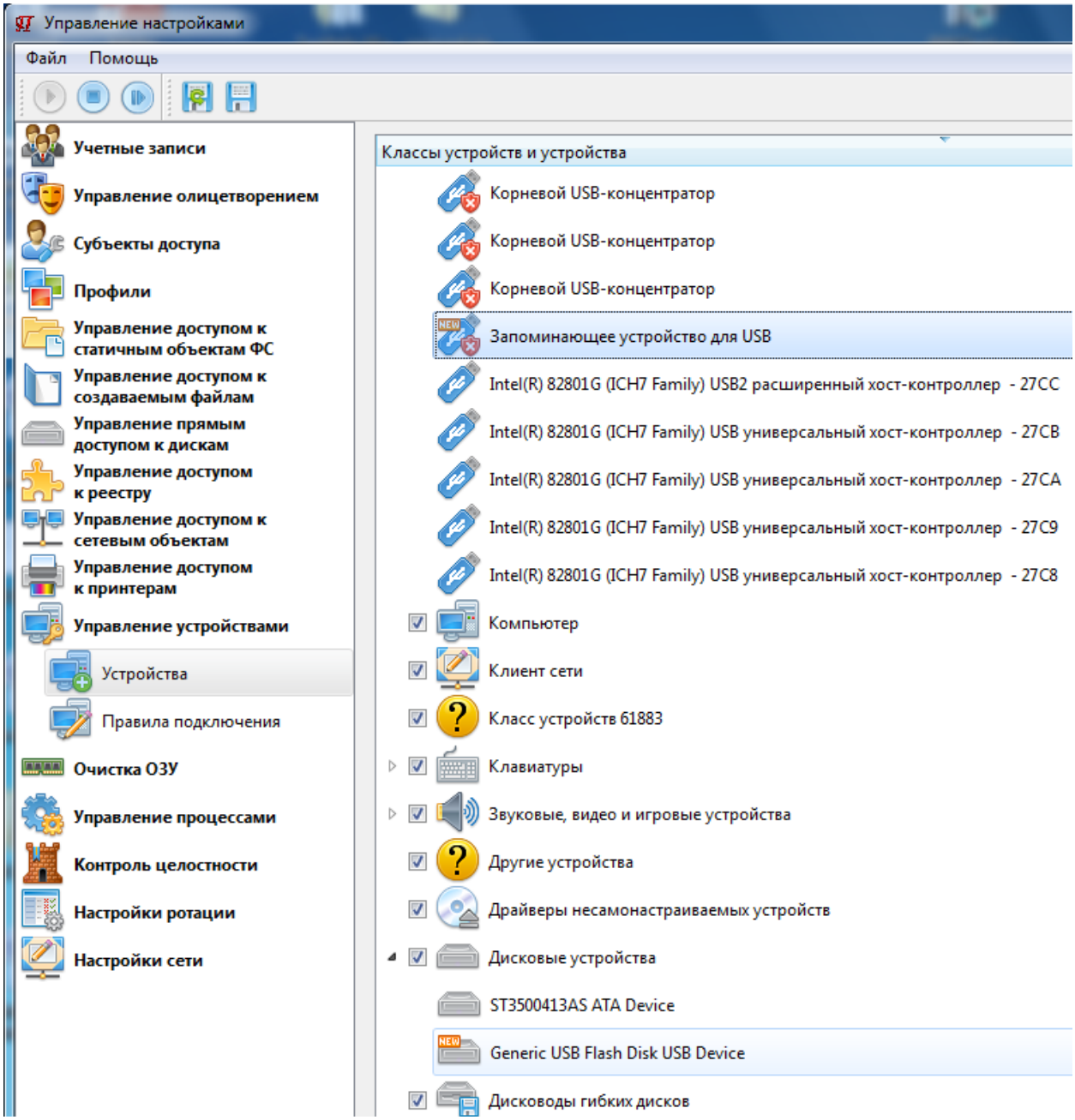

Рис.1. Интерфейс просмотра списка устройств и классов устройств

Конкретные устройства идентифицируются в разграничительной политике серийными номерами.

Интерфейс настройки механизма управления монтированием устройств по пользователям приведен на рис.2.

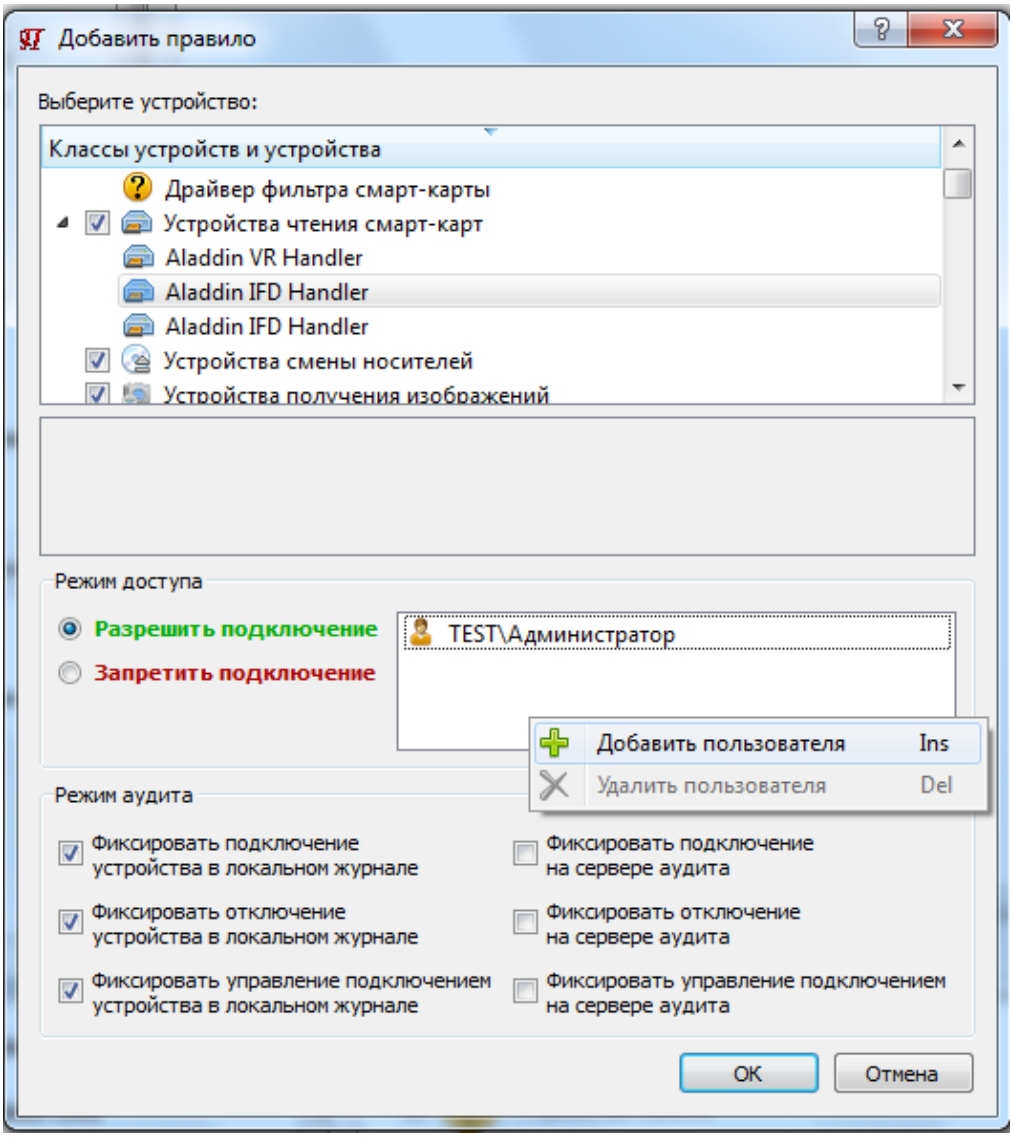

Рис.2. Интерфейс настройки механизма управления монтированием устройств по пользователям

Для любого устройства, в том числе, с учетом его серийного номера, можно задать пользователей (учетные записи), для которых данное устройство разрешается/запрещается монтировать к системе, в том числе монтировать конкретными пользователями в процессе их работы. Это относится и к системным устройствам, например, сетевые адаптеры. Если пользователю разрешено работать с таким устройством, оно будет автоматически примонтировано к системе, если нет, то после регистрации пользователя в системе, устройство будет автоматически отмонтировано.

Из интерфейса, см. рис.2, для каждого выбранного устройства может быть задан пользователь (список пользователей), которым разрешено, либо,

наоборот, запрещено (может использоваться, как разрешительная, так и запретительная политики, см. рис.2) монтировать данное устройство (либо при работе которого (которых) устройство может либо нет быть автоматически примонтировано системой). Если же устройство было санкционировано (при работе пользователя, которому разрешено монтирование этого устройства) подключено, при этом в системе регистрируется пользователь, для которого использование данного устройство определено, как несанкционированное, средство защиты автоматически отключит подобное устройство от системы, несанкционированно воспользоваться этим устройством не удастся. Если это системное устройство, то для его примонтирования может потребоваться перезагрузка системы с последующей регистрацией в системе санкционированного для этого устройства пользователя.

Результат настройки механизма защиты отображается в интерфейсе, приведенном на рис.3, в котором зеленым цветом отмечены заданные правила разрешения, красным - запретов.

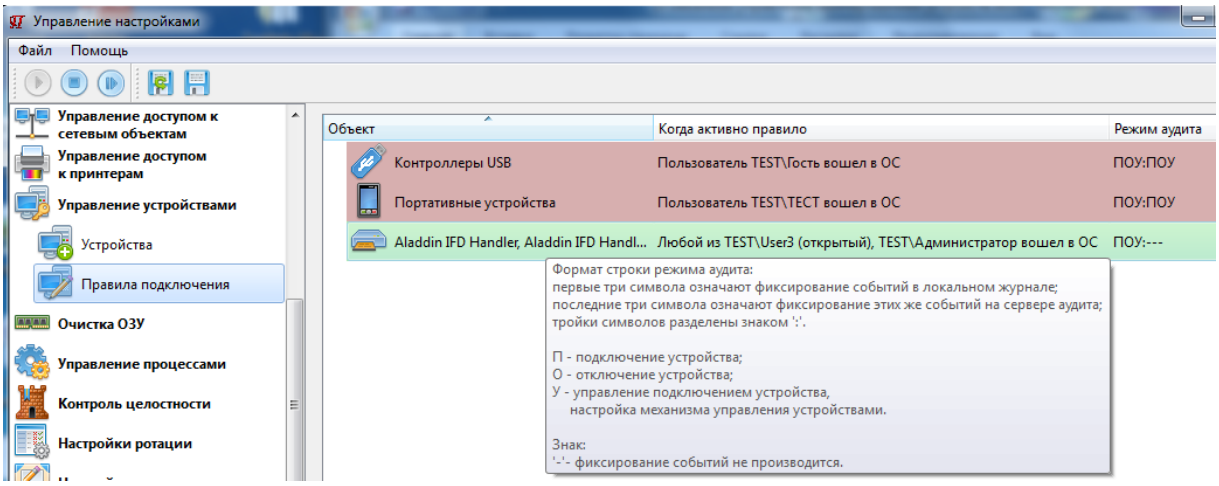

Рис.3. Интерфейс отображения настройки механизма управления динамическим монтированием устройств

Теперь рассмотрим, как реализуется управление монтированием устройств по пользователям при реализации в системе разграничительной политики доступа на основе меток безопасности (мандатов).

Отметим, что мандатный контроль доступа, в том виде, как он был изначально предложен [4], является некой абстракцией, применимой для реализации разграничительной политики доступа лишь в отношении файловых объектов, причем исключительно для управления потоками данных [2]. Однако и в этом случае он обладает серьезными противоречиями, связанными с разрешением доступа на чтение пользователем файлового объекта, характеризуемым большим уровнем допуска, чем уровень конфиденциальности соответствующего файлового объекта (например, пользователь, имеющий мандат (метку безопасности) "конфиденциальный", имеет право доступа на чтение к файловому объекту с меткой "открытый"). По сути именно это правило и позволяет говорить об иерархических метках, поскольку реализована иерархия их обработки при анализе запроса доступа субъекта к объекту. Однако, кроме очевидной бессмыслицы данного правила, применительно к решению задачи реализации разграничительной политики в целом, реализуемой для изолированной (в различных режимах) обработки информации различных уровней конфиденциальности [1], в том числе, и с возможность монтирования к системе в различных режимах различных устройств, когда пользователь, имеющий мандат "конфиденциальный" может сохранить обработанный им открытый документ только, как конфиденциальный - с меткой "конфиденциальный" (т.е. далее обрабатывать эти данные исключительно в режиме обработки конфиденциальных документов); данное правило не допустимо и ввиду внесения дополнительной угрозы обрабатываемым конфиденциальным документам, поскольку вероятность наделения вредоносными свойствами открытых документов на порядки выше, чем конфиденциальных (различные режимы обработки), а приложение при прочтении открытого документа (потенциально зараженного) будет иметь доступ на запись/модификацию конфиденциальных документов [5].

Как следствие, корректной можно считать следующую схему мандатного контроля доступа - пользователь имеет право доступа

(чтение/запись) только к объектам с одноименной меткой безопасности (мандатом), для обработки документов различных уровней конфиденциальности пользователь должен регистрироваться в системе под различными учетными записями, которым присвоены различные метки безопасности (мандаты) - корректность именно такого решения - задание режима обработки информации (сессии) учетной записью, обоснована в [1]. При этом метки безопасности уже могут использоваться для решения различных задач защищенной обработки информации, в частности для реализации ролевой модели, поскольку они уже не несут признаков иерархии в том смысле, что обработка в различных сессиях полностью изолируется. К слову сказать, вот и эффективная альтернатива DLP - решениям (защита от утечки с компьютера конфиденциальной информации, угроза которой возникает при необходимости обработки на одном и том же компьютере одним и тем же пользователем, как открытой, так и конфиденциальной информации). Достаточно создать на компьютере две сессии - открытую и конфиденциальную, разделить их [1], разграничить права доступа к ресурсам для каждой сессии, в результате чего (при соответствующей настройке разграничительной политики доступа - в данном случае уже разделительной [1,2]) утечка конфиденциальной информации с компьютера станет невозможной.

Особенность же реализации управления монтированием устройств по пользователям при реализации в системе разграничительной политики доступа на основе меток безопасности состоит в том, что какая-либо формализация отношения меток безопасности в общем случае невозможна в принципе. Например, устройство может использоваться как для обработки информации категорий не ниже конфиденциальной, так и, наоборот, не выше конфиденциальной. Кроме того, на практике может возникнуть и необходимость разграничений для пользователей одной категории (которым присвоена одна и та же метка) - одним из них разрешить монтирование того или иного устройства, другим нет.

Все это обусловливает целесообразность реализации следующего решения. При назначении мандатов (меток безопасности) пользователям, данные метки будут отображаться в окне выбора пользователей для которых устанавливаются правила монтирования выбранного устройства, см.рис.4. Т.е. метки безопасности в данном случае используются исключительно в целях информирования администратора при назначении им правил монтирования к системе устройств. Любая иная схема учета назначенных пользователем меток безопасности в мандатной схеме управления монтированием устройств не будет обладать необходимой универсальностью (как отмечали, отношения меток безопасности устройств в общем случае могут быть различными) и только усложнит настройку соответствующего механизма защиты.

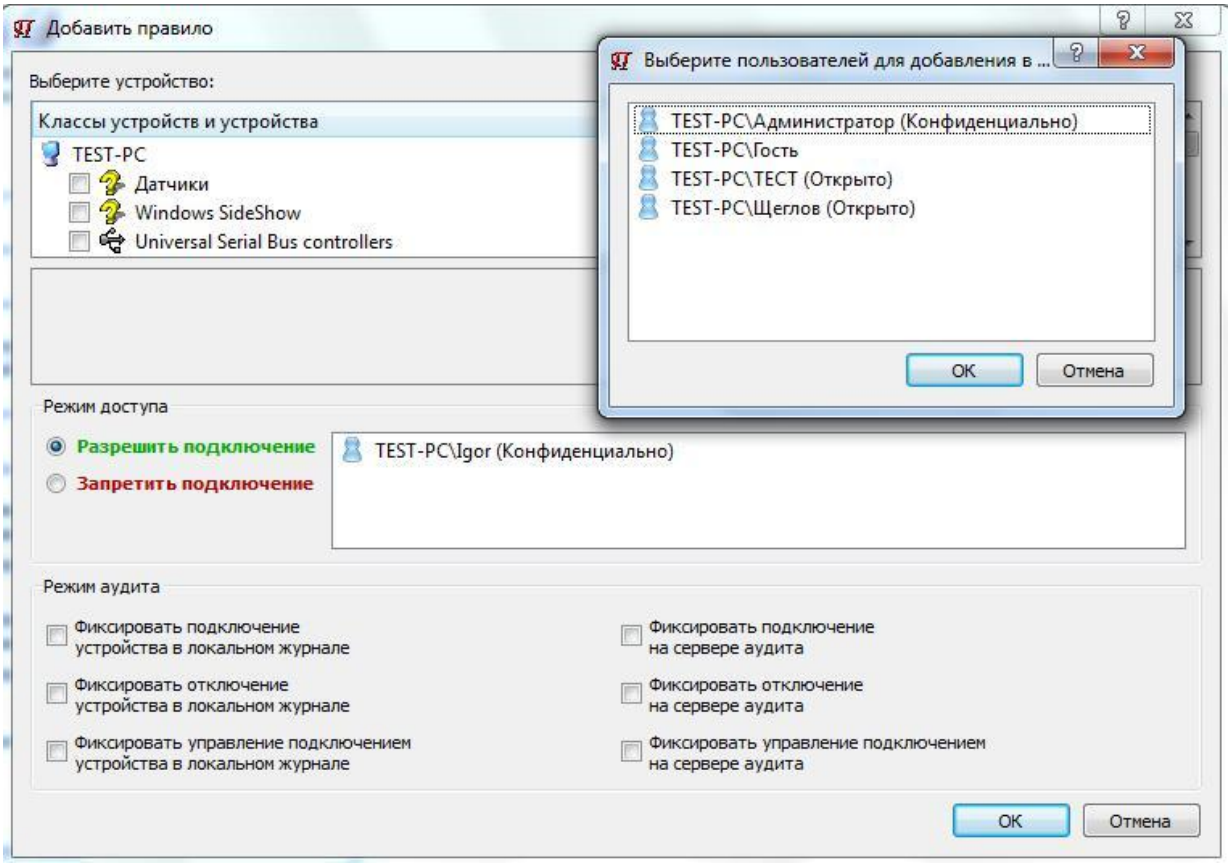

Рис.4. Интерфейс настройки механизма управления монтированием устройств по пользователям при реализации мандатного механизма контроля доступа

Заключение.

Задача управления монтированием устройств – это ключевая задача защиты, решаемая с целью формирования объекта защиты (локализации набора устройств объекта защиты). Естественно, что без решения данной задачи корректную разграничительную политику доступа пользователей к ресурсам информационной системы реализовать не представляется возможным. Предложенный же в работе метод позволяет управлять монтированием устройств к системе с учетом пользователей, работающих в системе, что обеспечивает возможность разграничивать возможность монтирования к системе устройств для различных пользователей (учетных записей), а для локальных устройств, для которых применимо задание только одного типа доступа (использовать, либо нет) данным решением реализуется и разграничительная политика доступа пользователей к подобным устройствам. Это принципиально расширяет возможности данного механизма защиты, которые необходимы для решения ряда важнейших современных задач защиты, в том числе, для реализации сессионного контроля доступа [1], являющегося эффективным методом защиты от утечек обрабатываемой конфиденциальной информации, и позволяет реализовать корректную разграничительную политику доступа к защищаемым ресурсам в общем случае, за счет локализации на защищаемом компьютере набора используемых локальных устройств.

Литература.

1. Щеглов К.А., Щеглов А.Ю. Метод сессионного контроля доступа к файловым объектам. Вопросы практической реализации // Вестник компьютерных и информационных технологий. - 2014. - № 8. - С. 54-60.
2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004, – 384 с.
3. Щеглов А.Ю. и др. Комплексная система защиты информации "Панцирь+" для ОС Microsoft Windows. Свидетельство регистрации программы для ЭВМ №2014660889 от 17.10.2014.

4. Bell D. E., LaPadula L. J. Security Computer Systems: Unified Exposition and MULTICS Interpretation, Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.
5. Щеглов К.А., Щеглов А.Ю. Модели и правила мандатного контроля доступа // Вестник компьютерных и информационных технологий. - 2014. - № 5. - С. 44-49.