СЕССИОННЫЙ КОНТРОЛЬ ДОСТУПА - ЭФФЕКТИВНАЯ АЛЬТЕРНАТИВА DLP - РЕШЕНИЯМ

Введение.

В последнее время активно развиваются, так называемые, DLP - решения (DataLossPrevention или DataLeakPrevention, защита от утечек данных). DLPсистемы, реализующие подобные решения часто называют “системы защиты конфиденциальных данных от внутренних угроз”. При этом под внутренними угрозами понимаются несанкционированные (не предусмотренные политикой безопасности предприятия) действия (намеренные или случайные) со стороны сотрудников предприятия, имеющих легальные права доступа к соответствующим данным, связанные с выдачей конфиденциальной информации за контуры информационной системы.Сотрудников, осуществляющих подобные действия намеренно, с целью получения какой-либо выгоды, еще называют "инсайдерами".

DLP - решения реализуют контроль по ряду признаков покидающих информационную систему данных с целью предотвращения утечки конфиденциальной информации. Не будем детально останавливаться на описании подобных признаков и на вопросах построении DLP систем (эти вопросы хорошо представлены в литературе), остановимся лишь на следующем важном моменте. Решение основано на реализации функций контроля, в любом случае сильно подверженного ошибкам первого и второго рода, что сказывается на его эффективности. Если при появлении данной технологии подобные системы позиционировались для защиты от инсайдерских атак (от намеренных несанкционированных воздействий на систему легальных пользователей, осуществляемых с целью хищения конфиденциальной информации), то в последние годы отношение к подобным системам кардинально поменялось - сегодня DLP системы позиционируются, как эффективные решения от случайных, осуществляемых по халатности, действий легальных пользователей,

потенциально приводящих к утечке конфиденциальной информации. Принципиальное отличие постановки задачи защиты в этом случае состоит в том, что контролируемая системой защиты информация умышленно не маскируется (не преобразуется) каким-либо образом пользователем перед ее отправкой за пределы информационной системы, что, естественно, принципиально упрощает задачу контроля и позволяет в этом случае говорить об эффективности защиты. Актуальность же подобной задачи защиты обосновывается тем, что более 70% утечек связано именно с халатностью сотрудников.

Однако это ни в коей мере не снижает актуальности задачи защиты от намеренных несанкционированных воздействий на систему легальных пользователей - инсайдеров, кстати, и так думают многие потребители средств защиты. Например, в проведенном исследовании [1], проиллюстрированном на рис.1, сделан вывод о том, что наибольшую опасность для компаний сегодня представляют именно собственные сотрудники (легальные пользователи).

Рис.1. Наиболее актуальные ИБ угрозы

Естественно, что эту актуальнейшую задачу защиты - защиты от намеренных несанкционированных воздействий (преднамеренных атак) на

систему легальных пользователей - инсайдеров, также необходимо каким-либо образом эффективно решать.

1. Идея сессионного контроля доступа.

Естественно, что основой для реализации DLP-решения является следующее:

1. Возможность классификации (категорирования) обрабатываемой в информационной системе информации, проводимой с целью определения признаков конфиденциальной информации.

2. Возможность определения санкционированных режимов обработки конфиденциальной информации, в том числе санкционированных способов отправки конфиденциальной информации за пределы информационной системы (кому и/или куда и каким образом).

Без выполнения данных условий какой-либо контроль информации, покидающей информационную систему, невозможен, т.к. отсутствуют признаки (параметры), по которым может осуществляться подобный контроль.

Таким образом, реализация защиты предполагает полное понимание того, что такое конфиденциальная информация на предприятии, каким образом она создается и каков режим ее обработки, в частности, каким образом, в том числе, с использованием каких устройств и кому, например, по каким сетевым адресам, она может передаваться, т.е. понимание того, каким образом конфиденциальная информация может покинуть информационную систему.

В общем случае на одном компьютере могут быть различные способы обработки корпоративной информации - только открытой (в этих приложениях рассматриваемая задача защиты не имеет смысла); только конфиденциальной; и открытой, и конфиденциальной различными сотрудниками; и открытой, и конфиденциальной одним и тем же сотрудником.

Наиболее часто используемым на практике и при этом наиболее сложным для реализации защиты является случай обработки на одном и том же компьютере и открытой, и конфиденциальной информации одним и тем же сотрудником, который мы и будем далее рассматривать, как постановку задачи защиты в наиболее общем случае. Угроза утечки конфиденциальной информации при этом создается тем, что при обработке открытой информации пользователю должны предоставляться каналы выдачи (передачи) информации из компьютера, являющиеся несанкционированными при обработке им же конфиденциальной информации. Естественно, что без дополнительной защиты в этих условиях инсайдер имеет все возможности похитить конфиденциальную информацию.

В работе [2] нами было введено понятие и предложен метод сессионного контроля доступа, направленный на решение подобной задачи защиты, основу которого составляет реализация разделительной политики доступа к режимам обработки информации (сессиям), основанной на реализации разграничительных политики доступа к компьютерным ресурсам, образующим сессии. Под сессией [2] нами понимается режим обработки информации определенного уровня конфиденциальности. Соответственно сессия может быть открытой, конфиденциальной и т.д.

Идея метода защиты, в отличие от его практической реализации, требующей для эффективной реализации инновационных решений, крайне проста.Состоит она в создании на одном компьютере для одного сотрудника различных режимов (сессий) обработки информациираз личных категорий (уровней) конфиденциальности - в простейшем случае, открытая и конфиденциальная сессии, с полной изоляцией сессий по обрабатываемым в них данных (в этом и состоит разделительная политика доступа между сессиями), в чем и состоит максимальная сложность реализации сессионного контроля доступа.Говорить об эффективности сессионного контроля доступа возможно только в том случае, если в системе отсутствует объект (файловый объект, буфер обмена и т.д.), позволяющий осуществить обмен данными

между сессиями. Поскольку мы говорим о защите от инсайдерских атак, а не о халатности пользователя, то подобный "канал" обмена данными между сессиями рано или поздно злоумышленником будет выявлен и использован для хищения конфиденциальных данных. Для каждой же сессии реализуется разграничительная политика доступа к ресурсам (к локальным устройствам, внешним накопителям, объектам реестра ОС, к программам на запуск - замкнутость программной среды [2], к сетевым объектам, принтерам и т.д.), реализующая требуемый (регламентируемый политикой безопасности предприятия) режим обработки информации соответствующей категории. В итоге получаем, что конфиденциальная информация может обрабатываться только в регламентируемом режиме, а ее утечка становится невозможной, как в результате халатности, так от намеренных несанкционированных воздействий на систему легальных пользователей, задача же контроля, решаемая DLP системой в этом случае становится вырожденной - в ней уже нет необходимости.

В [3] проведено исследование возможных способов задания сущности "сессия" в разделительной политике доступа, в результате которого сделан вывод о том, что корректное задание сессии обеспечивается заданием ее учетной записью - для каждого сотрудника создается несколько учетных записей, каждая для работы в соответствующей сессии. Для каждой учетной записи создается разграничительная политика доступа к ресурсам, формирующая режим обработки информации соответствующего уровня конфиденциальности, сессии изолируются - реализуются необходимые меры, предотвращающие обмен данными между сессиями. Для смены сессии необходимо штатными средствами ОС сменить пользователя - сотруднику необходимо войти в систему под соответствующей учетной записью, при этом для входа в систему под различными учетными записями одному сотруднику может предоставляться один и тот же пароль.

Необходимость исследования, проведенного в [3], была обусловлена появлением коммерческих средств защиты, использующих виртуальную

сущность "сессия".В этих решениях для работы в различных режимах создается одна учетная запись, а при регистрации пользователя в системе ему предлагается выбрать соответствующую сессию. Различные режимы формируются реализацией разграничительной политики доступа уже не между учетными записями, а между сессиями, т.е. в качестве субъекта доступа в разграничительной политике в них выступает не пользователь, а сессия. Мало того, что данный подход требует реализации в полном объеме механизмов контроля доступа ко всем потенциально защищаемым компьютерным ресурсам, где в качестве субъекта доступа уже должна выступать сущность сессия - к файловым объектам, к объектам реестра ОС, к устройствам, к принтерам, к сетевым объектам, к буферу обмена и т.д. - встроенные возможности защиты ОС при этом полностью отвергаются, но, что гораздо хуже, он не позволяет в общем случае реализовать корректную разделительную политику доступа между сессиями, т.е. всегда будут оставаться "каналы" обмена данными между сессиями. Проиллюстрируем сказанное примером. Вся разграничительная политика доступа к файловым объектам базируется в современных ОС на разграничении прав доступа для пользователей (учетных записей). При этом любое приложение создает конфигурационные файлы - свои для каждой учетной записи (по умолчанию эти файлы разделены системой между учетными записями). Таких файлов в системе масса, даже на их выявление потребуется не мало времени, и нет гарантии, что все их удастся выявить. В эти файлы приложение может осуществлять запись (с последующим чтением) данных с правами текущего пользователя, т.е. пользователь может туда записывать данные и читать от туда данные, причем далеко не всегда этим же приложением. Если различные режимы обработки создаются для одной учетной записи, то для корректного решения рассматриваемой задачи необходимо все конфигурационные файлы длявсех приложений, создаваемые одним и тем же пользователем, каким-то образом разделить между сессиями. Не говоря уже о возможности технического решения подобной задачи, можно представить

себе трудоемкость ее решения. Таким образом, как и DLP-решения, подобные реализации сессионного контроля доступа можно рассматривать, как средства защиты от утечек конфиденциальной информации, обусловливаемых исключительно халатностью сотрудников предприятия.

В порядке замечания отметим, что на практике сегодня широкое применение нашла ролевая модель контроля доступа (англ.*RoleBasedAccessControl, RBAC*), предполагающая реализацию разграничительной политики доступа к ресурсам для сущности "роль". Под ролью понимается режим обработки информации, реализующий формализуемые в информационной системе функциональные задачи пользователей (видим, совсем иное определение, чем сессия). Данный метод призван упростить задачу администрирования за счет реализации разграничительной политики доступа для виртуальной сущности "роль" с возможностью включения/исключения пользователей в/из роль (и). Видим, что, как и при сессионном контроле, здесь речь идет о задании режимов обработки, однако совсем с другой целью, как следствие, при ролевом контроле доступа понятным причинам не ставится и не решается задача изоляции данных между ролями для одного и того же пользователя (что, кстати говоря, и позволяет включать в качестве субъекта доступа виртуальную сущность "роль", что, как отмечали ранее, в части включения некой виртуальной сущности для задания субъекта доступа, не допустимо для сессионного контроля доступа). Как следствие, не смотря на то, что у ролевого контроля и у сессионного контроля доступа есть нечто общее - в обоих случаях формируются режимы обработки информации пользователями, они принципиально различаются, как в части постановки задачи защиты, так и в части ее решения - ролевой контроль доступа корректно (в части решения задачи защиты от утечки конфиденциальной информации - задачи защиты, решаемой сессионным контролем доступа) может использоваться в предположении, что различные роли, в которые включается один и тот же пользователь, предполагают обработку

информации одного и того же уровня конфиденциальности, что для сессионного контроля доступа означает работу в одной сессии (сессия формируется под уровень конфиденциальности информации).

2. Основные методы и механизмы защиты, реализующие сессионный контроль доступа.

Как отмечали, основу сессионного контроля доступа составляет формирование и разделение между собою режимов обработки информации различных категорий конфиденциальности. Две ключевые задачи защиты, которые должны решаться при реализации сессионного контроля доступа - разграничение прав доступа к обрабатываемым данным, в том числе, с целью их разделения между сессиями, и управление монтированием к системе устройств, локализующим наборы устройств, которые могут использоваться в различных сессиях. Применительно же к разрешенным, для использования в сессии устройствам затем уже, при необходимости, может реализовываться разграничительная политика доступа для соответствующих сессий.

1. Реализация разграничения прав доступа к обрабатываемым данным.

Поскольку в данном случае речь идет о защите информации, категорируемой по уровням конфиденциальности, целесообразно рассматривать реализацию мандатного контроля доступа - контроля доступа на основе меток безопасности (мандатов) или уровней доступа.

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 очевидного противоречия данного правила, применительно к решению задачи реализации разделительной политики в целом, реализуемой для изолированной (в различных режимах) обработки информации различных уровней конфиденциальности [3], 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); использование данного правила связано с некорректностью реализации сессионного контроля доступа в общем виде.

Отметим, что в работе рассматривается задача защиты от утечек конфиденциальной информации - угроза нарушения конфиденциальности информации (исследуется возможность рассмотрения сессионного контроля доступа в качестве альтернативны DLP-решениям), в то время, как в общем случае сессионный контроль доступа должен использоваться и для решения не менее актуальной задачи защиты - защиты от несанкционированной модификации или удаления конфиденциальной информации на защищаемом компьютере в результате обеспечения возможности обработки на этом же компьютере открытой информации. Такая проблема обусловливается внесениемв рассматриваемом случае дополнительной угрозы обрабатываемым конфиденциальным данным (угрозы нарушения целостности и доступности информации), поскольку вероятность наделения вредоносными свойствами открытых документов, получаемых, например, из сети интернет, на порядки выше, чем конфиденциальных (различные режимы обработки), то же можно сказать и об использовании выявленных в приложениях уязвимостей, а приложение при прочтении открытого документа (потенциально зараженного) будет иметь доступ на

запись/модификацию конфиденциальных документов. Эта проблема исследована нами в [5].

К основным недостаткам известного метода мандатного контроля доступа можно отнести следующее. Во-первых, высокую сложность администрирования, поскольку метки безопасности должны присваиваться как субъектам (пользователям - учетным записям), так и объектам (на практике, как правило, папкам) - именно на основании арифметического сравнения меток субъекта и объекта принимается решение о непротиворечивости запроса доступа заданным правилам контроля доступа. При этом, поскольку невозможно назначить метку создаваемому файлу (файлу, которого еще нет в системе), разграничительная политика реализуется, посредством разрешения записи данных соответствующих категорий в папки соответствующих категорий, а не по средством разрешения чтения созданного файла, в котором хранятся данные соответствующей категории, что собственно противоречит логике [6]. Во-вторых, в системе присутствуют не только файлы, используемые для хранения данных, но и системные файлы и конфигурационные файлы пользователей, им также каким-то образом назначить метки безопасности для обеспечения возможности к ним доступа, а хранящиеся в этих файлах данные никак не вписываются в категорирование по уровням конфиденциальности. И, в-третьих, в системе присутствуют не разделяемые между пользователями системой и приложениями каталоги, например, используемые для хранения временных файлов. Для таких каталогов задание метки безопасности невозможно, эти каталоги необходимо разделять между учетными записями (с этой цель, например, может применяться техническое решение [7]).

В работе [8] нами предложен альтернативный метод мандатного контроля доступа - мандатного контроля доступа к создаваемым файлам, техническое решение, реализующее данный метод защиты запатентовано [9]. Принципиальное отличие данного метода состоит в том, что метки

безопасности (уровни доступа) назначаются только интерактивным пользователям, причем только тем из них, доступ к создаваемым файлам которыми следует разграничивать. При этом не разграничиваются права доступа по созданию файлов. При создании файла пользователем, которому присвоена метка безопасности (в том числе, и конфигурационных файлов, создаваемых под учетной записью пользователя), эта метка наследуется файлом – автоматически размещается в его атрибутах, то же реализуется при модификации соответствующим пользователем не размеченного ранее файла. При последующем доступе к размеченному рассмотренным способом файлу реализуется контроль доступа в соответствии с исходно заданными правилами контроля. Если пользователь, не имеющий метки, обращается к размеченному файлу, его запрос доступа отклоняется, если же пользователь, имеющий метку, запрашивает доступ к размеченному файлу (имеющему метку) проводится арифметическое сравнение этих меток.

Данное решение реализовано и апробированов КСЗИ «Панцирь+»для ОС MicrosotWindows.Все иллюстрации далее в работе будем приводить с использованием реализованных в данной системе защиты информации интерфейсов и меню.

Таким образом, вся настройка разграничительной политики доступа сводится к заданию меток безопасности (уровней доступа) из меню, приведенного на рис.2 (задается количественным значением для возможности последующего арифметического сравнения, которому для удобства сопоставляется соответствующее смысловое содержание, которое можно задать произвольно), и к назначению пользователям (учетным записям) требуемых уровней доступа (меток безопасности) из заданного списка, что реализуется из интерфейса, представленного на рис.3.

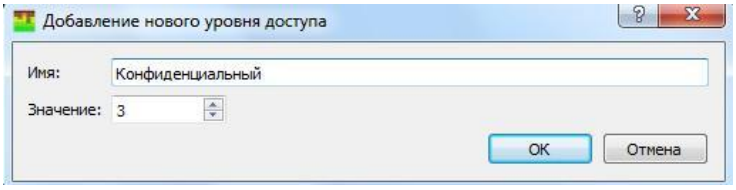

Рис.2. Меню задания уровней доступа (меток безопасности)

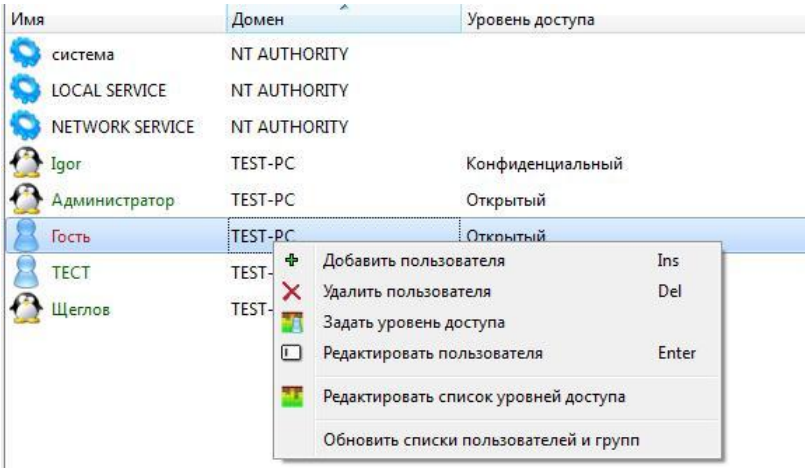

Рис.3. Задание пользователям уровней доступа (меток безопасности)

Для общности (возможности реализации сессионного контроля доступа как для защиты только от нарушения конфиденциальности информации, та к и для защиты в общем случае - от нарушения конфиденциальности, целостности и доступности информации) предусмотрена возможность задания правила арифметического сравнения меток безопасности, что реализуется из интерфейса, представленного на рис.4 (как отмечали, корректным в общем случае будет разрешение доступа при совпадении меток безопасности пользователя и размеченного файла - запрашиваемый доступ должен разрешаться исключительно в случае совпадения значений этих меток безопасности [5]).

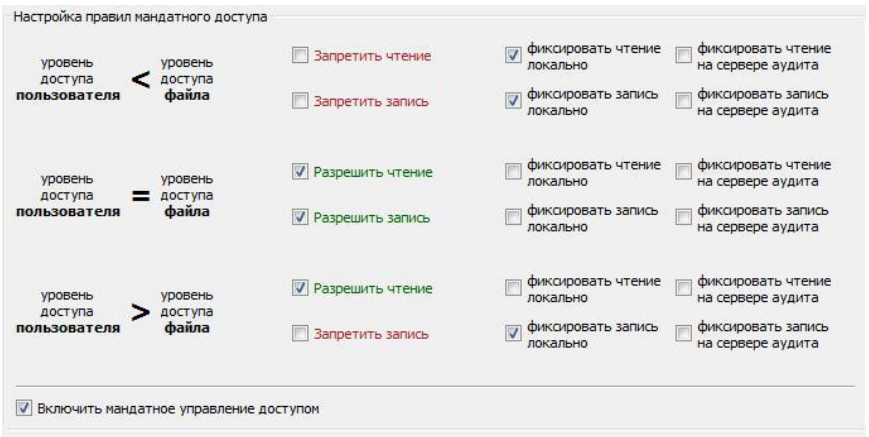

Рис.4. Интерфейс настройки правил мандатного контроля доступа

Кроме очевидного упрощения задачи администрирования механизма защиты, реализация данного метода обеспечивает корректность реализации разграничительной (в рассматриваемом случае - разделительной по обрабатываемым данным) политики доступа в общем случае, поскольку любой файл, создаваемый пользователем, которому назначается метка безопасности, где бы он не создавался, будет автоматически размечаться, в том числе и при сохранении его в неразделяемых системой и приложениями каталогах (каталогам здесь назначения меток не требуется – разграничение осуществляется не по средством задания правил по созданию файлов, а посредством задания правил последующего доступа к создаваемым (в данном случае, созданным и автоматически размеченным) файлам. Не возникает в этом случае и проблем, связанных с необходимостью назначения меток безопасности для системных файловых объектов - контролируется доступ к файлам, созданным интерактивными пользователями.

В порядке замечания отметим, что практическое использование данного метода контроля доступа собственно меняет технологию защиты данных, поскольку формирует принципиально иные требования к построению других механизмов защиты данных. В частности, гарантированно удалять уже требуется файлы, не сохраненные в определенных папках, а созданные определенными пользователями, в наше случае - в определенных сессиях, (например, под учетными записями, заведенными для работы в конфиденциальной сессии) [10]. То же можно сказать и в отношении шифрования – шифровать/расшифровывать опять же уже требуется файлы, не сохраненные в определенных папках, а созданные определенными пользователями – для определения ключа для расшифрования файла достаточно его разметки, содержащей информацию о том, в какой сессии создан этот файл. К слову сказать, данное техническое решение нами запатентовано [11].

Таким образом, использование рассмотренного метода позволяет реализовать корректное разделение сессий по обработке информации различных категорий конфиденциальности на уровне файловой системы.

В двух словах остановимся на контроле доступа к буферу обмена. В целом он разделяется системой между учетными записями. Однако существует режим запуска приложения с правами другого пользователя с использованием утилиты runas. Подобную возможность необходимо предотвратить, т.к. при этом буфер обмена является принадлежностью "рабочего стола" и между учетными записями не разграничивается.

2. Реализация управления монтированием устройств по пользователям (по учетным записям).

Другой важнейшей задачей защиты при реализации сессионного контроля доступа является локализация сессии по набору используемых (монтируемых к системе) устройств (разделение сессий - режимов обработки информации различных уровней конфиденциальности по устройствам).

В современных ОС Windows реализовано управление монтированием устройств к системе без учета работающих в системе пользователей, т.е. те устройства, которые автоматически подключаются к системе при загрузке ОС, как и все устройства, которые администратором будет разрешено подключать (монтировать), разрешается подключать для всех пользователей - для всех учетных записей, в нашем случае – для всех сессия, поскольку сессия формируется учетной записью. В рамках сессионного контроля доступа необходимо реализовать локализацию набора устройств не для системы в целом, а для конкретных пользователей - сессий. Важным является и тот момент, 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.). Т.е., разрешая/запрещая монтирование подобных

устройств по учетным записям, тем самым реализуется и разграничительная политика доступа к этим устройствам для сессий.

Предлагаемое решение состоит в следующем. Для каждого пользователя (учетной записи, соответственно, сессии) задаются устройства, с которыми он может, либо, наоборот, не должен работать. При входе пользователя в систему монтируются и ему разрешается подключение (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 подключения/отключения устройств. При этом если в системе будет одновременно зарегистрировано несколько пользователей, то подключены к системе будут и будут разрешаться для подключенияпользователями только те устройства, которые разрешено использовать всем этим зарегистрированным пользователям (одновременно во всех соответствующих сессиях).Иные устройства будут автоматически отключены от системы, либо соответственно их будет запрещено подключать.

Как видим, данное решение предполагает реализацию динамического монтирования/отмонтирования устройств по пользователям.

Особенность реализации управления монтированием устройств по пользователям с использованием меток безопасности состоит в том, что какая-либо формализация отношения меток безопасности в отношении устройств в общем случае невозможна в принципе. Например, устройство может использоваться как для обработки информации категорий не ниже конфиденциальной, так и, наоборот, не выше конфиденциальной.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.5, 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 по причине, рассмотренной выше.

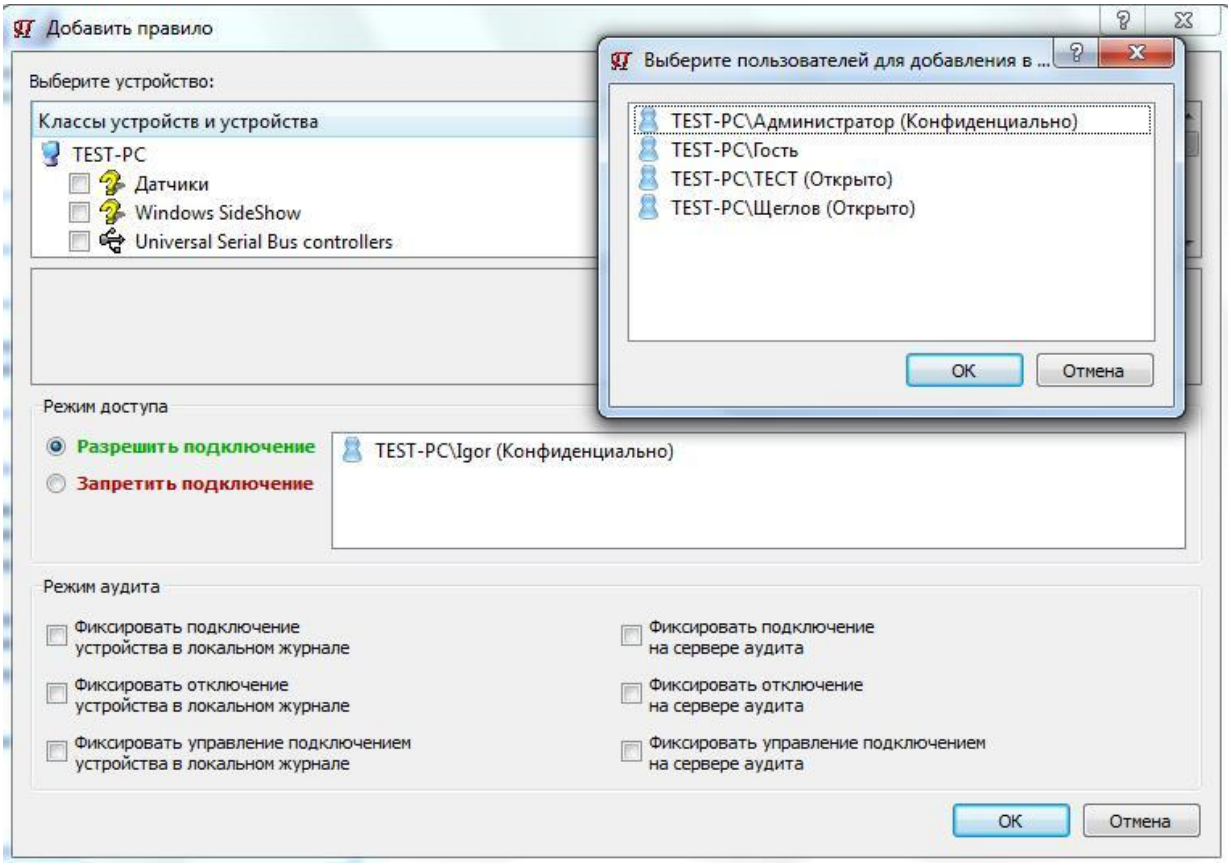

Рис.5. Интерфейс настройки механизма управления монтированием устройств по пользователям при реализации мандатного контроля доступа

Выбрав соответствующий класс устройств, либо конкретное устройство (конкретное устройство идентифицируется серийным номером), можно разрешить/запретить, см. рис.5, его монтирование к системе, как для всех, так и для отдельных пользователей - сессий.

В результате применения рассмотренных методов защиты реализуется разделение сессий по обрабатываемым данным и по возможности использования устройств (например, для открытой сессии беспроводное подключение к внешней сети, для конфиденциальной - проводное). Далее

соответствующими механизмами контроля и разграничение прав доступа, при необходимости, для соответствующих сессий реализуется разграничительная политика доступа к ресурсам (например, для конфиденциальной сессии разрешается доступ только к корпоративным хостам) - формируются режимы изолированной между сессиями обработки данных. В результате изолирования обработки данных между сессиями становится невозможным обработка данных одной категории конфиденциальности в режиме, предназначенном для обработки данных иной категории конфиденциальности, что обеспечивает невозможность их утечки.

Заключение.

В заключение отметим, что в данной работе исследуется задача защиты информации, решаемая в предположении, что угрозу несет в себе легальный пользователь. Предложенное решение основано на изолировании обработки данных между сессиями, поскольку сессия задается учетной записью - между учетными записями. Аналогичный подход с использованием технического решения[9] может быть реализован и для решения принципиально иной задачи защиты информации, заключающейся в предположении, что угрозу несет в себе не пользователь, а процесс [12,13]. В этом случае также создаются и изолируются режимы обработки данных, но режимы создаются и изолируются не применительно к учетным записям, а для критичных процессов [14].Естественно, что при построении эффективной защиты информационной системы, заданные задачи защиты должны решаться в комплексе. Однако рассмотрение этого вопроса выходит за рамки настоящей работы.

Литература.

1. Опрос «Кода Безопасности» выявил наиболее актуальные ИБ угрозы [Электронный ресурс] // URL:/ http://www.securitycode.ru/company/news/SC-analytic-2011.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004, - 384с.

3. 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.

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.

6. Щеглов К.А., Щеглов А.Ю. Непротиворечивая модель мандатного контроля доступа // Известия ВУЗзов. Приборостроение. - Санкт-Петербург, 2014. - № 4. - С. 12-15.

7. Щеглов А.Ю., Щеглов К.А. Система переформирования объекта в запросе доступа. Патент на изобретение №2538918.

8. Щеглов К.А., Щеглов А.Ю. Принцип и метод мандатного контроля доступа к создаваемым файловым объектам // Вопросы защиты информации. - 2012. - Вып. 96. - № 1. - С. 40-44.

9. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к файлам на основе их автоматической разметки. Патент на изобретение№2524566.

10. Щеглов К.А., Щеглов А.Ю. Принципы реализации дополнительной защиты информации при контроле доступа к создаваемым файловым объектам на основе их автоматической разметки // Вопросы защиты информации. - 2014. - Вып. 104. - № 1. - С. 29-34.

11. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к шифруемым создаваемым файлам. Патент на изобретение №2533061.

12. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. - 2013. - Вып. 101. - № 2. - С. 36-43.

13. Щеглов К.А., Щеглов А.Ю. Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. - 2012. - Вып. 99. - № 4. - С. 31-36.

14. Щеглов К.А., Щеглов А.Ю. Защита от атак на уязвимости приложений // Информационные технологии. - 2014. - № 9. - С. 34-39.