НОВАЯ ТЕХНОЛОГИЯ КОНТРОЛЯ И РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К ДАННЫМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

К.А. Щеглов, А.Ю. Щеглов, д.т.н., профессор

"Научно-производственное предприятие "Информационные технологии в бизнесе"

info@npp-itb.spb.ru

Введение

Решение задачи защиты информации от несанкционированного доступа в любой информационной системе основано на реализации контроля и разграничения прав доступа субъектов к защищаемым ресурсам, прежде всего, к файловым объектам, поскольку именно они предназначены для хранения обрабатываемых данных. При этом субъектами доступа в разграничительной политике выступают пользователи, идентифицируемые учетными записями. Правила доступа субъектов к объектам задаются, как правило, в виде матрицы доступа (матричное представление целесообразно с точки зрения возможности транспонирования матрицы, позволяющего представлять два способа задания разграничительной политики - субъектов к объектам или, наоборот, к объектам субъектов). Первичным при назначении разграничений прав доступа в известных методах контроля доступа является объект, например, файловый объект. Различные объекты (файлы), идентифицируемые своими именами в файловой системе, назначаются администратором для сохранения различного рода информации, обрабатываемой пользователями, в том числе информации различных категорий конфиденциальности. Именно это и определяет известную применяемую на практике технологию защиты информации в информационных системах – конкретный файл, с учетом специфики разрешенной для сохранения в нем информации, является объектом защиты обрабатываемых данных – именно конкретные файлы должны гарантированно удаляться, шифроваться и т.д.

Остановимся на ключевом недостатке данного подхода к реализации контроля и разграничения прав доступа, применительно к защите данных, обрабатываемых в информационных системах. Файлы принципиально различаются своим функциональным назначением в системе. Они могут быть подразделены на статичные (в первую очередь, это системные) и создаваемые пользователями в процессе работы. Принципиальная разница между этими группами файловых объектов, в части задания разграничительной политики доступа к ним, огромна, и состоит она в том, что системные объекты

присутствуют на компьютере на момент назначения администратором правил доступа субъектов к объектам, а создаваемых еще попросту нет. Резонно возникает вопрос: как же к ним разграничивать доступ, если их еще нет? А ведь это те объекты (файлы), которые, в первую очередь, и нуждаются в защите от несанкционированного доступа, поскольку именно в них хранятся обрабатываемые на компьютере данные, и, к слову сказать, именно в них могут создаваться вредоносные программы и иной вредоносный код, например, скрипты в процессе работы системы. Рассмотрим, к чему приводит практическая реализации подобного широкого используемого подхода к защите информации. Поскольку на момент задания разграничительной политики доступа - назначения правил доступа, создаваемых в процессе работы пользователями файлов еще не существует в системе, администратором заранее создаются хранилища (своего рода «контейнеры») для последующего сохранения в них создаваемых в процессе работы файлов. Т.е. администратором создаются папки-контейнеры, к которым впоследствии и разграничивается доступ субъектов. Объект доступа «файл» при этом исчезает из разграничительной политики в отношении создаваемых файлов -пользователи «принуждаются» создавать свои файлы только в определенных созданных администратором папках-контейнерах, поскольку, в противном случае, невозможно установить какие-либо разграничения к создаваемым файлам. Включение же в схему контроля доступа возможности назначения правил доступа к создаваемому файлу, создавшим его пользователем - «владельцем» в современных условиях, когда санкционированный пользователь выступает в качестве наиболее вероятного потенциального нарушителя, рассматривать не имеет смысла. Созданные файлы наследуют разграничения прав доступа, установленные администратором для папок-контейнеров. Посредством же реализации разграничительной политики доступа к папкам-контейнерам для пользователей соответствующим образом разграничивается доступ и к созданным пользователями в процессе функционирования системы файлам. Данное противоречие не только иллюстрирует всю нелогичность известной схемы контроля доступа, но и сказывается на возможности эффективного применения контроля и разграничения прав доступа в современных условиях. Это обусловливается тем, что сегодня в схеме контроля доступа принципиально должны изменяться требования к субъекту доступа. По различным причинам [1,2] в современных условиях процесс (приложение) несет в себе не меньшую, если не большую, угрозу несанкционированного доступа к обрабатываемой информации, чем пользователь. Как следствие, равноправными сущностями, определяющими субъект доступа в современно разграничительной

политике, должны выступать, как пользователь (учетная запись), так и процесс (полнопутевое имя исполняемого файла процесса), т.е. в разграничительной политике доступа субъект должен определяться, как «пользователь, процесс» (какой пользователь, каким процессом запрашивает доступ к объекту). С целью же защиты от обхода разграничительной политики доступа за счет использования сервисов олицетворения - штатной возможности современных универсальных ОС, позволяющей запросить у ОС и получить от нее право потоку выполнять действия под другой учетной записью, чем запущен порождающий его процесс, субъекта в современной разграничительной политике доступа уже имеет смысл идентифицировать тремя сущностями "исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс" [3], где исходный идентификатор пользователя - учетная запись, под которой запущен процесс, эффективный идентификатор - учетная запись, под которой процесс (соответствующий поток) запрашивает доступ к ресурсу, в том числе, и к файловому объекту. Выполнение данного требования качественно усложняет задачу задания администратором разграничительной политики доступа, что сказывается на эффективности использования контроля и разграничения прав доступа к ресурсам, в первую очередь, к файловым объектам, в современных информационных системах.

В [4] предложен метод контроля и разграничения прав доступа, в значительной мере упрощающий задачу администрирования, за счет назначения прав доступа не к объектам субъектов, а субъектов к объектам. Упрощение задачи администрирования при этом достигается за счет использования масок при задании объектов доступа в разграничительной политике, что в том числе, позволяет получить достаточно важные новые свойства защиты [5]. Эти решения для различных способов идентификации субъекта доступа нами запатентованы [6,7] и реализованы в программном средстве защиты информации "Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows" далее КСЗИ «Панцирь+» (новая разработка компании, находящаяся на сегодняшний день на сертификации). Не смотря на эффективность данного технического решения, изложенная проблема, обусловливаемая рассмотренным противоречием известной схемы контроля доступа, не снимается и соответствующий метод защиты позиционируется в модели защиты КСЗИ «Панцирь+» для реализации контроля и разграничения прав доступа к статичным объектам - к ресурсам, присутствующим в системе на момент задания администратором разграничительной политики доступа субъектов к объектам (системные файлы, объекты реестра ОС, сетевые объекты, внешние накопители и т.д.).

В работе рассмотрим методы контроля и разграничения прав доступа к создаваемым объектам, позволяющие исключить из разграничительной политики доступа сущность "объект доступа", за счет реализации автоматической разметки создаваемых объектов. Рассмотрим, как использование данных методов контроля доступа изменяет собственно технологию защиты данных в информационных системах, формируя принципиально новые требования к решению множества иных задач защиты обрабатываемых данных. При этом отметим, что рассматриваемые в работе методы защиты реализованы и апробированы при построении КСЗИ «Панцирь+», иллюстрируя далее технические решения, будем рассматривать интерфейсы данного программного средства защиты информации.

1. Принципы контроля доступа к создаваемым файлам. Техническое решение

Предлагаемые принципы контроля доступа к создаваемым файловым объектам основаны на исключении сущности «объект доступа» из разграничительной политики доступа к файловым объектам, как таковой (ввиду ее отсутствия на момент задания прав доступа администратором), и состоят они в следующем [8]:

1. Сущность "объект" исключается из схемы контроля доступа - при реализации разграничительной политики используются две сущности: идентификатор (учетная информация) субъекта, создавшего объект, и идентификатор субъекта, запрашивающего доступ к созданному объекту.

2. Правила доступа устанавливаются между сущностями: «субъект доступа (учетная информация), запрашивающий доступ к объекту» и «субъект доступа (учетная информация), создавший этот объект».

3. При создании субъектом нового файла, файлом наследуется учетная информация субъекта доступа, создавшего этот файл.

4. При запросе доступа к любому файлу, диспетчер доступа (решающий элемент) анализирует наличие, а при наличии, содержимое унаследованной файлом учетной информации создавшего его субъекта доступа. При наличии, анализирует заданные правила доступа, в результате чего предоставляет запрошенный субъектом доступ, либо отказывает в нем. При отсутствии – анализирует правило контроля доступа к неразмеченным (не унаследовавшим учетную информацию субъекта) объектам.

Таким образом реализуется разграничительная политика (задаются правила доступа) не для субъектов к объектам, а между субъектами доступа к создаваемым ими файлам.

Замечание. Уточним, что, естественно, и в этом случае реализуется доступ субъектов к объектам, но вот в разграничительной политике (в правилах доступа) объекты отсутствуют - присутствуют только субъекты доступа.

Рассмотрим запатентованное техническое решение [8], которое распространяется на реализацию методов контроля доступа к создаваемым файлам, излагаемых далее. Приведем и опишем его именно в том виде, как это сделано в [8], см. рис.1.

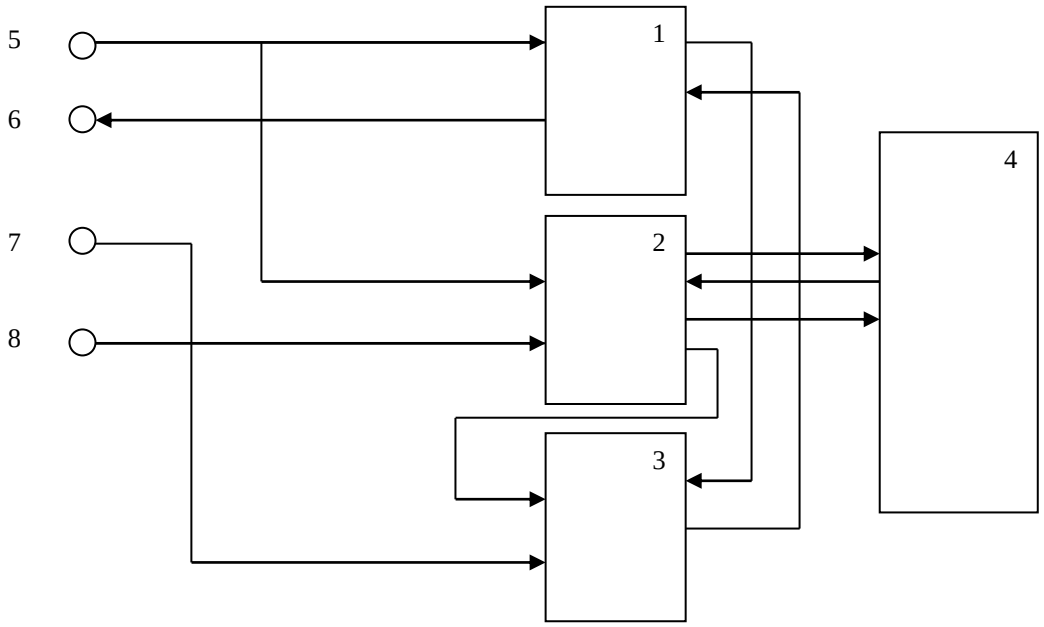

Рис.1. Система контроля доступа к создаваемым файлам на основе их автоматической разметки

Система содержит: решающий блок 1, блок автоматической разметки файлов 2, блок хранения правил доступа к файлам 3, блок хранения атрибутов файлов 4.

Со входа системы 8 администратором задаются идентификаторы субъекта, файлы создаваемые которым будут автоматически размечаться (если должны размечаться все создаваемые файлы, то подобная настройка может быть установлена по умолчанию), со входа 7 задаются правила доступа (соответственно мандатного, либо дискреционного или одновременно и того, и другого, если реализуются оба метода контроля доступа).запрос доступа поступает на вход системы 5, попадая в решающий блок 1 и в блок автоматической разметки файлов 2.Блоком 1 из блока 3 запрашивается соответствующее правило в отношении анализируемого запроса доступа. Если запрос не противоречит правилу, блоком 1 будет выдано на выход системы 6 разрешение анализируемого запроса доступа, в

противно случае, запрет. Блоком 2 осуществляется считывание из блока хранения атрибутов файлов 4, разметки (атрибутов) файла, к которому запрошен доступ, эти данные им передаются в блок 3 для выбора правила доступа. Если запрос состоит в создании нового файла, то блоком 2 создаются в блоке 4 атрибуты вновь создаваемого файла. В отношении файла, к которому осуществляется запрос доступа (по его атрибутам, хранящим учетные данные, либо метка безопасности субъекта доступа, создавшего этот файл), блоком 3 выбирается соответствующее правило доступа и передается в решающий блок 1, которые уже и осуществляет анализ непротиворечивости запроса правилу.

2. Методы и средства контроля доступа к создаваемым файлам.

Мандатный метод контроля доступа.

Метки безопасности (уровни доступа) или мандаты присваиваются исключительно пользователям (интерактивным пользователям) [9]. Уровни (список уровней) доступа для системы создаются заданием их числовых значений и смысловой транскрипцией из интерфейса (меню), представленного на рис.2. Число создаваемых меток не ограничено. Сравнению диспетчером доступа подлежат числовые значения, смысловая же транскрипция метки используется для удобства администратора.

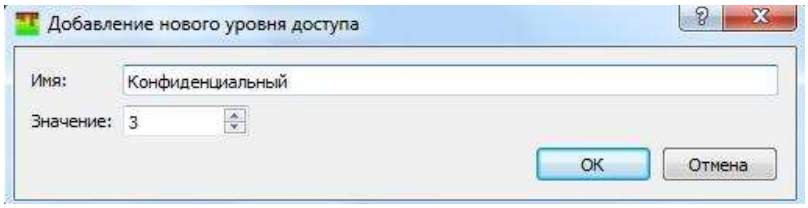

Рис.2. Меню задания уровней доступа (мандатных уровней)

Для любого заведенного в системе защиты пользователя может быть задан (выбран) любой, из заданных в системе защиты, уровень доступа. При этом метки безопасности могут назначаться не всем пользователям, а только тем, доступ к файлам, создаваемым которыми, контролируется. Назначенные администратором настройки мандатного контроля доступа отображаются в интерфейсе, приведенном на рис.3.

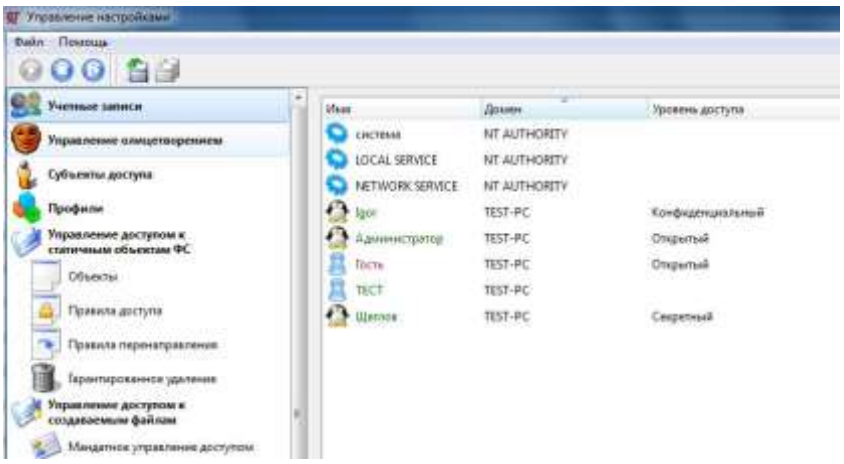

Рис.3. Отображение заведенных в системе пользователей с заданными для них мандатными уровнями

Вот и все настройки разграничительной политики доступа! Больше ничего не требуется, а главное, не требуется каким-либо образом размечать файловые объекты (назначать им метки безопасности).

Рассмотрим, как работает диспетчер доступа.

Как отмечали, метки безопасности назначаются контролируемым пользователям - тем пользователям, к файлам, создаваемым которыми, требуется разграничивать права доступа. При создании файла любым (не только тем, которому назначена метка безопасности) пользователем, создаваемый файл диспетчером доступа автоматически размечается - диспетчером доступа в его атрибуты автоматически помещаются учетные данные субъекта, создавшего этот файл. Подобным образом будет размечаться и неразмеченный ранее файл, при его модификации.

Размечать все создаваемые файлы имеет смысл для защиты от запуска вредоносных программ. Очевидно, что эффективная защита от подобной угрозы реализуется в том случае, если исполнение создаваемых в процессе работы системы файла, в том числе, и с системными правами, запрещено [10] (устанавливать программное обеспечение на защищаемый компьютер - это прерогатива исключительно администратора, который должен решать подобную задачу при отключенном средстве защиты).

Замечание. Предотвращение запуска создаваемого файла (вредоносной программы) с системными правами, за счет эксплуатации уязвимостей системных процессов и драйверов, является эффективным средством защиты от атак на повышение привилегий.

При последующем обращении к любому файлу, диспетчером доступа анализируется наличие у него разметки. Если файл не размечен, к нему будет разрешен запрашиваемый доступ, в случае модификации

файла, он будет автоматически размечаться. Если же файл размечен, и запрошен доступ на исполнение, данный запрос доступа отклоняется. Если запрашивается иной тип доступа к файлу, то анализируется, имеет ли метку безопасности пользователь, запросивший доступ к этому файлу. Если не имеет, анализируемый диспетчером запрос доступа отклоняется. Если же имеет, диспетчером анализируется соответствие запроса мандатным правилам доступа, посредством арифметического сравнения соответствующих меток безопасности (мандатов). С этой целью диспетчером определяются (по соответствующим учетным записям) мандаты - числовые значения назначенных им уровней доступа, пользователя, запросившего доступ к размеченному файлу, и пользователя, создавшего этот файл, и далее эти значения сравниваются между собою. В результате проведенного сравнения, запрошенный доступ диспетчером либо разрешается (если запрос не противоречит заданным правилам мандатного контроля доступа), либо отклоняется.

Разметка созданных в процессе работы системы файлов отображается в системе защиты с использованием специальной утилиты, в том виде, как это представлено на рис.4.

Рис.4. Отображение разметки созданных контролируемыми пользователями файлов при мандатном контроле доступа

Рассмотрим достоинства предложенного метода контроля доступа.

1. Как известно, мандатная схема контроля доступа предполагает применение именно для реализации разграничительной политики доступа к обрабатываемым данным, т.к. именно обрабатываемая информация может быть категорирована по уровням конфиденциальности. системные объекты (файловые) не подпадают под подобное категорирование, как следствие, их включение в данную схему контроля доступа (назначение меток безопасности системным объектам) противоречит самому принципу мандатного контроля доступа. Предлагаемое решение реализует именно такой подход - контролируются и разграничиваются права доступа к создаваемым файлам, используемым для хранения обрабатываемых в информационной системе данных.

2. Принципиальное упрощение задачи администрирования, а это, в том числе, также вопрос безопасности, обусловливаемый потенциальными ошибками администрирования. Как отмечали, известный метод мандатного контроля доступа предполагает назначение меток безопасности и субъектам, и объектам. При этом метки должны присваиваться всем файловым объектам - папкам, поскольку права доступа к файлу наследуются именно от папки-контейнера, в которой сохранен этот файл. Возникает проблема разметки системных папок, они никак не укладываются в схему категорирования обрабатываемой информации по уровню конфиденциальности, проблема разметки иерархических файловых объектов (вложенных папок) и т.д. В рассматриваемом случае, предполагающем автоматическую разметку именно создаваемых файлов, подобных проблем не возникает.

3. Корректная реализация разграничительной политики доступа в общем случае. Вопросы корректности реализации разграничительной политики доступа при реализации известного метода обусловливаются наличием неразделяемых ОС и приложениями папок (так называемых, папок общего или коллективного доступа), например, каталогов хранения временных файлов. В подобных папках временные файлы создаются в процессе работы системы, на момент задания администратором правил доступа (назначения меток безопасности объектам) их не существует, а сохранять файлы в этих папках для корректной работы системы и приложений должны все пользователи. Какую метку безопасности присвоить подобной папке? Если же подобный объект исключить из схемы контроля доступа - разрешить доступ всех пользователей, собственно теряет смысл мандатная схема контроля доступа! В рассматриваемом же случае и эта проблема решена - любой временный создаваемый файл в папке коллективного доступа будет автоматически размечаться, при этом система и приложения будут работать корректно (доступ к папке будет разрешен), а правила доступа будут действовать и в отношении этих папок. Эти вопросы исследованы в [9].

Замечание. В работе [11] дано обоснование того, что корректная разграничительная политика доступа, реализуемая мандатным методом контроля доступа к категорированной по уровням конфиденциальности информации, реализуется при использовании неиерархических меток безопасности. Поэтому в КСЗИ «Панцирь +» предусмотрена возможность задания правила сравнения меток.

Дискреционный метод контроля доступа.

Применительно к реализации дискреционного метода контроля доступа задача упрощения администрирования системы защиты стоит еще острее. Это обусловливается современными требованиями к функциональным возможностям реализующего этот метод средства защиты информации. Сегодня говорить о какой-либо эффективной защите без реализации разграничительной политики доступа для субъекта "процесс" не приходится, поскольку именно процесс (приложение), в первую очередь, и подвержен атакам. Вместе с тем, в современных ОС права доступа процесса наследуются от запустившего его пользователя, т.е. все процессы (приложения), вне зависимо от решаемых ими задач, запускаемые пользователем, имеют одинаковые права доступа. Кроме того, при задании субъекта доступа целесообразен одновременно двух идентификаторов пользователя - первичного и эффективного, что необходимо для защиты от обхода разграничительной политики. Первичный идентификатор - это идентификатор пользователя, от "лица" которого запускается процесс. Однако при работе, процессом может быть запущен поток, функционирующий от "лица" другой учетной записи, например, для этого могут быть использованы сервисы олицетворения - штатная возможность современных ОС [3], и уже от "лица" этой учетной записи процесс может осуществить доступ к объекту (возможны и иные несанкционированные способы смены идентификатора пользователя при доступе к объекту). Эффективный идентификатор - это идентификатор пользователя, от "лица" которого процесс непосредственно и запрашивает доступ к объекту. Идентифицируя в субъекте доступа пользователя парой сущностей - первичный и эффективный идентификаторы, можно решать задачу предотвращения доступа к защищаемым объектам при заимствовании прав другого пользователя.

Пример (интерфейс) создания и отображения созданных субъектов доступа в системе защиты проиллюстрирован на рис.5. При задании администратором разграничительной политики доступа, субъекты доступа назначаются (тремя сущностями): первичный (или исходный) идентификатор пользователя, полнопутевое имя процесса, эффективный идентификатор пользователя [12].

При задании идентификатора пользователя (как первичного, так и эффективного) может использоваться маска "*" - "Любой" (в этом случае заданные правила будут распространяться на всех пользователей. Имя процесса, может задаваться либо полнопутевым именем его исполняемого файла, либо маской (возможно также использование переменных среды окружения). Например, маской C:\ProgramFile* покрываются все исполняемые файлы из данного каталога, маской "*" задается, что правило будет применимо к любому процессу. Поскольку один и тот же реальный субъект доступа в

разграничительной политике может "покрываться" одновременно несколькими масками, при анализе запроса доступа диспетчером принимаются разграничения по матрице доступа для субъекта, наиболее точно соответствующего своим описателем в разграничительной политике субъекту, запросившему доступ.

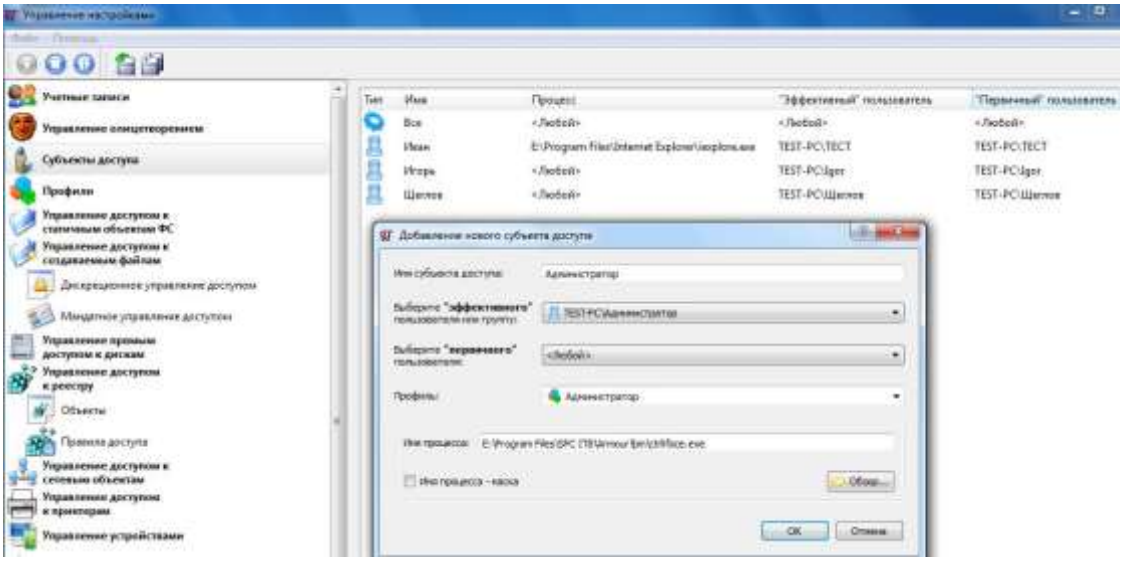

Рис.5. Создание и отображение в интерфейсе созданных субъектов доступа

Правила доступа создаются из интерфейса и отображаются в интерфейсе, приведенном на рис.6 (субъекты доступа здесь отображаются присвоенными им при создании именами, см. рис.5).

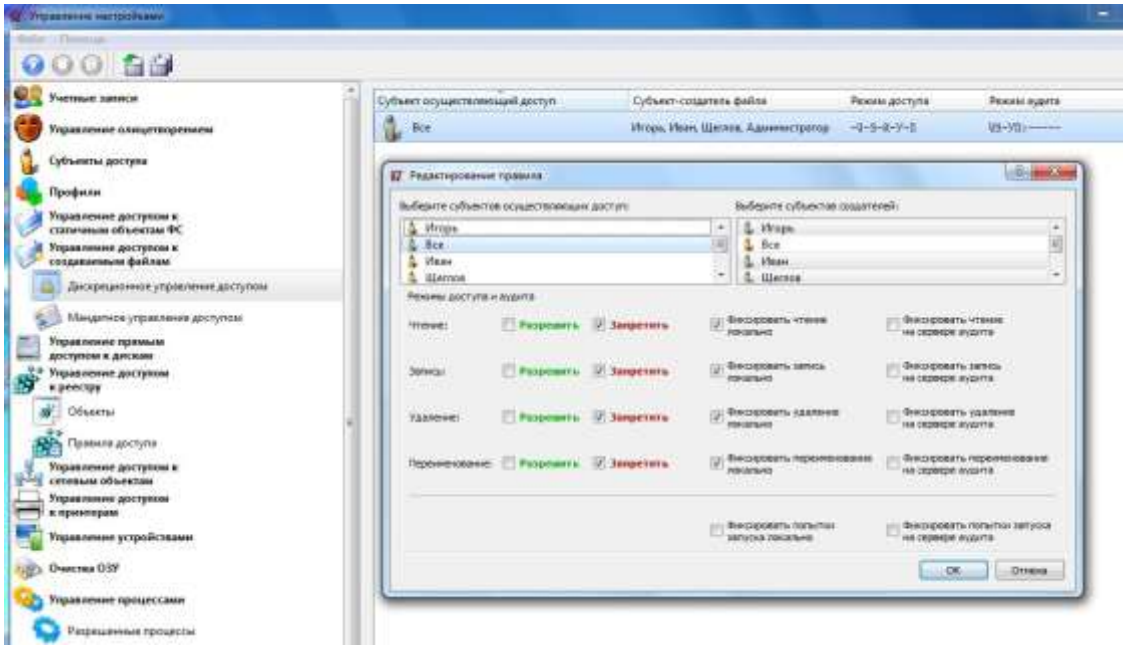

Рис.6. Создание и отображение в интерфейсе созданных правил доступа

Отметим, что в назначаемые права доступа, см. рис.6, не внесено право "исполнение", т.к., как отмечали ранее, запрет исполнения по умолчанию должен быть установлен для всех создаваемых файлов.

Задание разграничительной политики доступа осуществляется следующим образом. Из списка заданных субъектов доступа, отображаемого в интерфейсе настройки правил доступа именами, см. рис.6, в поле "Выберите субъектов создателей", см. рис.6, задаются контролируемые субъекты доступа - те субъекты, к файлам, созданным которыми, будут разграничиваться права доступа других субъектов.

Применительно к выбранному (в поле "Выберите субъектов создателей") контролируемому субъекту создателю файла назначаются права доступа к создаваемым им файлам других субъектов. Это осуществляется следующим образом. Субъект, которому назначаются права доступа, выбирается (из списка имен созданных субъектов) в поле "Выберите субъектов осуществляющих доступ", см. рис.6. Для выбранной пары субъектов (в левом и в правом полях интерфейса), см. рис.6, соответствующим образом разрешаются, либо запрещаются соответствующие права доступа (чтение, запись, удаление, переименование). Заданное правило отображается соответствующей строкой в интерфейсе, см. рис.6.

Замечание. Требования к правилам доступа, выполнение которых позволяет построить безопасную систему, сформулированы и обоснованы в [12].

Рассмотрим, как работает диспетчер доступа.

При создании файла любым пользователем, создаваемый файл диспетчером доступа автоматически размечается - диспетчером доступа в его атрибуты автоматически помещаются учетные данные субъекта, создавшего этот файл. Подобным образом будет размечаться и неразмеченный ранее файл, при его модификации.

При последующем обращении (обработка запроса на исполнение была нами рассмотрена ранее) к любому файлу, диспетчером доступа анализируется наличие у него разметки. Если файл не размечен, к нему будет разрешен запрашиваемый доступ, в случае модификации файла, он будет автоматически размечаться. Если файл размечен - создан контролируемым субъектом доступа (был задан в поле интерфейса "Выберите субъектов создателей", см. рис.6), то диспетчером анализируются заданные правила доступа к файлу, созданные этим субъектом - анализируется соответствие запроса заданным дискреционным правилам доступа. В результате проведенного сравнения, запрошенный доступ

диспетчером либо разрешается, если запрос не противоречит заданным правилам дискреционного контроля доступа, либо отклоняется.

Для удобства администратора в состав средства защиты включена утилита, позволяющая администратору просмотреть разметку созданных контролируемыми субъектами файлов (отображаются учетные данные субъекта доступа, создавших файлы - учетная запись пользователя и полнопутевое имя процесса) из окна интерфейса, представленного на рис.7.

Рис.7. Отображение разметки созданных контролируемыми пользователями файлов при дискреционном контроле доступа

Отметим, что при реализации разграничительной политики доступа к создаваемым файлам мандатный и дискреционный механизмы контроля доступа могут использоваться совместно. При этом запрос доступа будет считаться санкционированным в том случае, если он не будит противоречить ни мандатным, ни дискреционным правилам доступа. При этом диспетчером доступа сначала анализируются мандатные правила доступа, затем дискреционные.

Проиллюстрируем принципиально упрощение задачи администрирования на примере. В качестве примера рассмотрим реализацию (разграничительную политику доступа) защиты от атак на интернет-браузеры, эксплуатирующих уязвимости, обнаруживаемые в этих приложениях Разграничительную политику доступа проиллюстрируем на примере защиты от атак на интернет-браузер InternetExplorer (далее IE).

Отметим, что при защите от атак на приложения методами контроля доступа к создаваемым файлам, реализуются одни и те же принципы защиты:

– предоставить возможность доступа процесса (приложения), на который может быть осуществлена атака, только к необходимым ему для корректного функционирования в системе файлам;

– обеспечить максимальное снижение последствий от успешной атаки, в случае ее неминуемости на процесс (приложение), с учетом возможных (актуальных) целей потенциальных атак.

Для реализации защиты создадим двух субъектов доступа - "Все" и "IE", см. рис.8, и зададим для них правила доступа, представленные на рис.9.

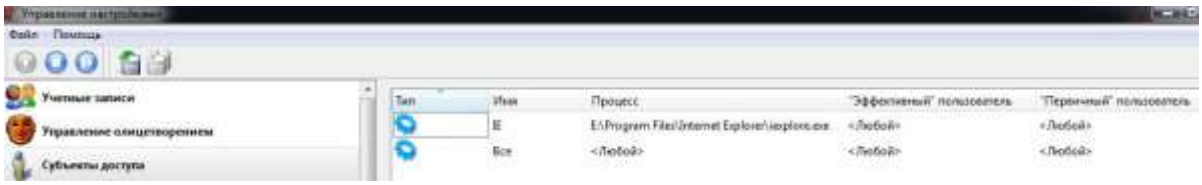

Рис.8. Отображение созданных субъектов доступа

Субъект осуществляющий доступ	Субъект-создатель файла	Режим доступа	Режим аудита
Все	IE	+Ч+З-И+У+П	ЧЗИУП:-----
IE	Все	-Ч-З-И-У-П	ЧЗИУП:-----

Рис.9. Отображение заданных правил доступа

Рассмотрим, что мы получим в результате реализации данной простейшей разграничительной политики. Интернет-браузер, вне зависимости от того, какими несанкционированными свойствами и каким образом он будет наделен (в том числе, и при повышении привилегий - пользователи (первичный и эффективный) заданы маской "*" - Любой), не получит доступ к конфиденциальной информации, обрабатываемой на компьютере - к создаваемым иными приложениями файлам (его работа в информационной системе в этой части полностью изолирована), не сможет запустить созданный им файл. Предотвращается возможность нарушения конфиденциальности, целостности и доступности (в части защиты от удаления) обрабатываемой на компьютере информации, в результате реализации любой известной и потенциально возможной атаки на интернет-браузер.

Иные же приложения при данной разграничительной политике имеют доступ (кроме исполнения) к файлам, создаваемым IE. На этом моменте следует акцентировать внимание. Уязвимый интернет-браузер может создать вредоносный файл (например, скриптовый файл и файл, содержащий макро-вирус), при чтении которого иным приложением, данное приложение будет наделено вредоносными свойствами. Из этого следует, что целесообразно не только запретить полный доступ браузеру к файлам, создаваемым иными приложениями, но и наоборот - полный доступ иных приложений к файлам, создаваемым браузером, по крайней мере тех приложений, которые при прочтении вредоносного файла могут быть наделены вредоносными свойствами. Другими словами, в этом смысле, работу интернет-браузера имеет смысл полностью изолировать.

Замечание. Для защиты системных ресурсов (системных файлов и объектов реестра) от атак со стороны интернет-браузера уже должен использоваться метод дискреционного контроля доступа в статичным объектам (как он реализован в КСЗИ «Панцирь+» кратко описано в [4]), основанный на

использовании решения [7], для которого субъекты доступа также задаются из интерфейса, представленного на рис.5.

3. Метод и средство контроля доступа к буферу обмена.

Поскольку буфер обмена предназначен для временного хранения данных, используемых для обмена приложениями, и на момент задания администратором разграничительной политики доступа эти данные еще не созданы - здесь также можно говорить о контроле и разграничении прав доступа к создаваемым объектам (данным, временно записываемым в буфер обмена), как следствие, применить изложенные выше принципы контроля и разграничения прав доступа. Рассмотрим, как решена эта задача защиты в КСЗИ «Панцирь+» (решение патентуется). С учетом назначения буфера обмена - обмен данными осуществляется между приложениями, запускаемыми под одной учетной записью, основным субъектов к разграничительной политике является процесс.

Субъекты доступа, как и для механизма защиты, рассмотренного ранее, задаются из того же интерфейса (для данных механизмов защиты создается единый список субъектов доступа), представленного на рис.5, а правила доступа субъектов к буферу обмена (к данным, записанным в буфер обмена) – из интерфейса, представленного на рис.10. Настройка правил доступа и контроль доступа реализуются по полной аналогии с тем, как он реализован в отношении создаваемых файлов.

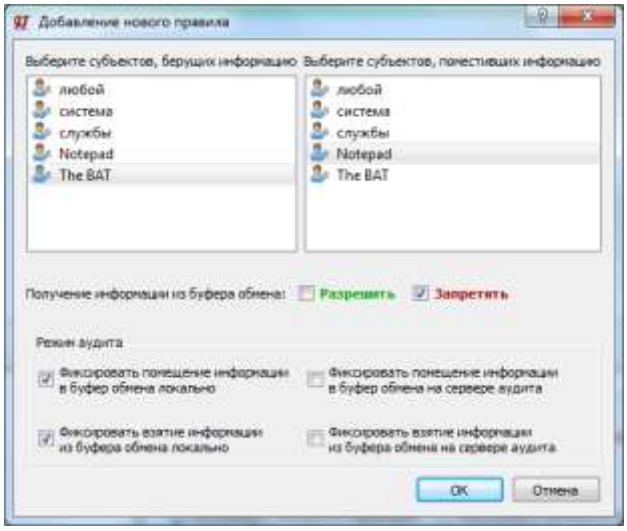

Рис.10. Задание правил доступа к буферу обмена

В правом столбце интерфейса, см. рис.10, задаются субъекты (контролируемые субъекты), к данным, записанным которыми в буфер обмена, будут разграничиваться права доступа остальных субъектов. В левом столбце для каждого выбранного субъекта из правого столбца, выбираются

субъекты и задаются правила доступа к данным, сохраненным в буфере обмена контролируемым субъектом. Естественно, что к задаваемым правилам доступа здесь относится разрешение или запрет получения доступа к данным, записанным (созданным) в буфере обмена каким-либо субъектом.

Если вернуться к примеру решения задачи защиты от атак на интернет-браузер IE, проиллюстрированному на рис.8, рис.9, то применительно к решению данной задачи защиты может быть реализована следующая разграничительная политика доступа к буферу обмена, задаваемая лишь одним правилом. Субъекту доступа "IE", см. рис.8, следует запретить доступ к данным, записываемым в буфер обмена субъектом доступа "Все", см. рис.8. В результате задания такого правила, браузер не сможет через буфер обмена получить доступ к данным, обрабатываемым иными приложениями, при этом сможет использовать буфер обмена для обработки собственных данных.

4. Изменение технологии защиты данных в информационной системе.

Рассмотрим, как практическое использование предложенных методов контроля и разграничения прав доступа к создаваемым файлам в целом сказывается на технологии защиты компьютерной информации, что проиллюстрируем на примере решения задачи гарантированного удаления файлов. Опять же рассмотрим реализацию соответствующего механизма защиты в КСЗИ «Панцирь+».

Прежде всего, рассмотрим соответствующую задачу защиты информации. Если говорить об информации, хранящейся на компьютере, в широком смысле, то далеко не все данные образуют файлы. Есть еще, так называемая, остаточная информация. Дело в том, что при удалении файла штатными средствами ОС, собственно данные не удаляются, осуществляется переразметка MFT-таблицы (на примере Windows). Другими словами, на жестком диске и на внешних накопителях всегда присутствует, так называемая остаточная информация, которую невозможно прочитать, обратившись к файлу (эта информация не образует файла), но достаточно просто получить к ней доступ с использованием сторонних программ прямого доступа к диску.

Поскольку остаточная информация не образует какого-либо объекта, подлежащего идентификации, она должна гарантированно удаляться при удалении файлова. Это реализуется отдельным механизмом гарантированного удаления остаточной информации, состоящем в следующем. Запрос на удаление и модификацию файла перехватывается средством защиты, после чего им осуществляется очистка освобождаемого дискового пространства (заданное число раз записывается исходно заданная

администратором информация), затем управление передается системе для «удаления» штатными средствами ОС.

При реализации контроля доступа к статичным объектам ключевой является сущность «объект доступа» - разграничиваются права доступа субъектов к объектам. Именно посредством разграничений прав доступа субъектов к объектом определяется то, в каком объекте насколько критичная информация должна сохраняться субъектами. Следовательно, правила гарантированного удаления должны устанавливаться в отношении объектов доступа – файловых объектов, см. рис.11.

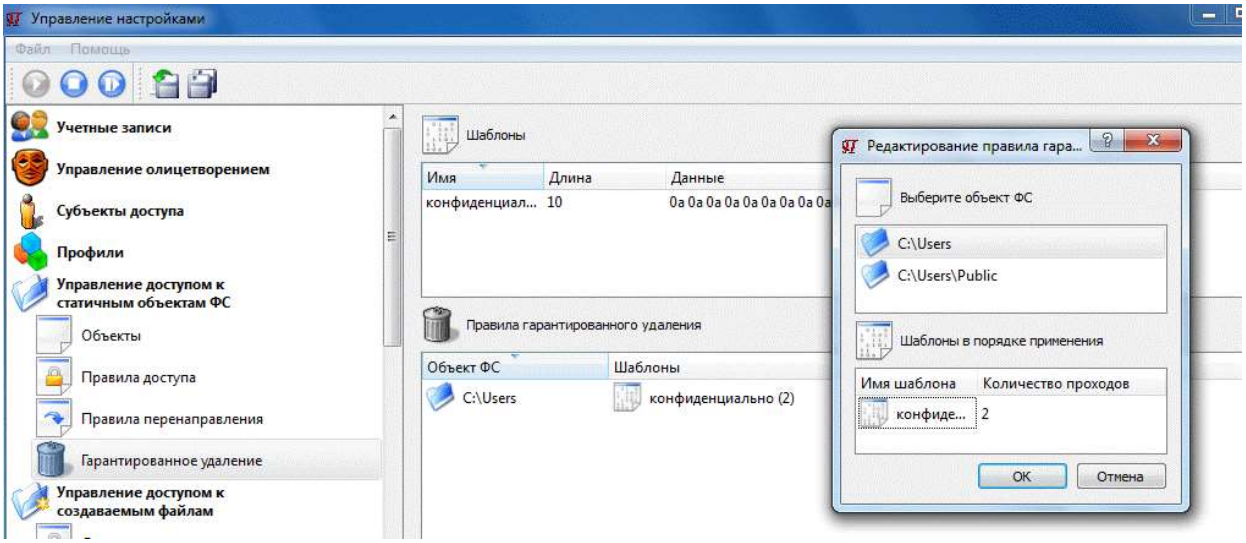

Рис.11. Интерфейс задания правил гарантированного удаления статичных файлов

При использовании подобного решения опять же встают вопросы корректности и сложности администрирования. Дело в том, что гарантированно удалять необходимо файлы не только из папок, предназначенных для хранения файлов с конфиденциальными данными, но и из временных файлов, которые создаются большинством приложений, и т.д. Ведь при удалении временного файла системой, данные также хранятся в виде остаточной информацией на диске.

Теперь рассмотрим, насколько изменится реализация данного механизма защиты, в случае, если в системе защиты реализуется метод контроля доступа к создаваемым файлам. Описанный выше подход к реализации гарантированного удаления файлов здесь не применим, т.к. любой файл любым субъектом может быть создан в любом объекте (в любой папке), что априори не позволяет исходно задать правила гарантированного удаления через объекты.

Однако созданный файл однозначно описывается своей разметкой. Это позволяет реализовать метод гарантированного удаления, основанный на автоматической разметке файлов, состоящий в следующем. Из интерфейсов, представленных на рис.12, соответственно, на рис.13, в зависимости от

реализованного метода контроля доступа к создаваемым файлам - дискреционный, либо мандатный, задаются правила гарантированного удаления – задаются субъекты, задаваемые своими иенами (соответственно, уровни доступа – метки безопасности), файлы, созданные которыми, должны гарантированно удаляться. При запросе на удаление к любому файлу, средством защиты считывается разметка файла, анализируются заданные правила и принимается решение о необходимости гарантированного удаления этого файла.

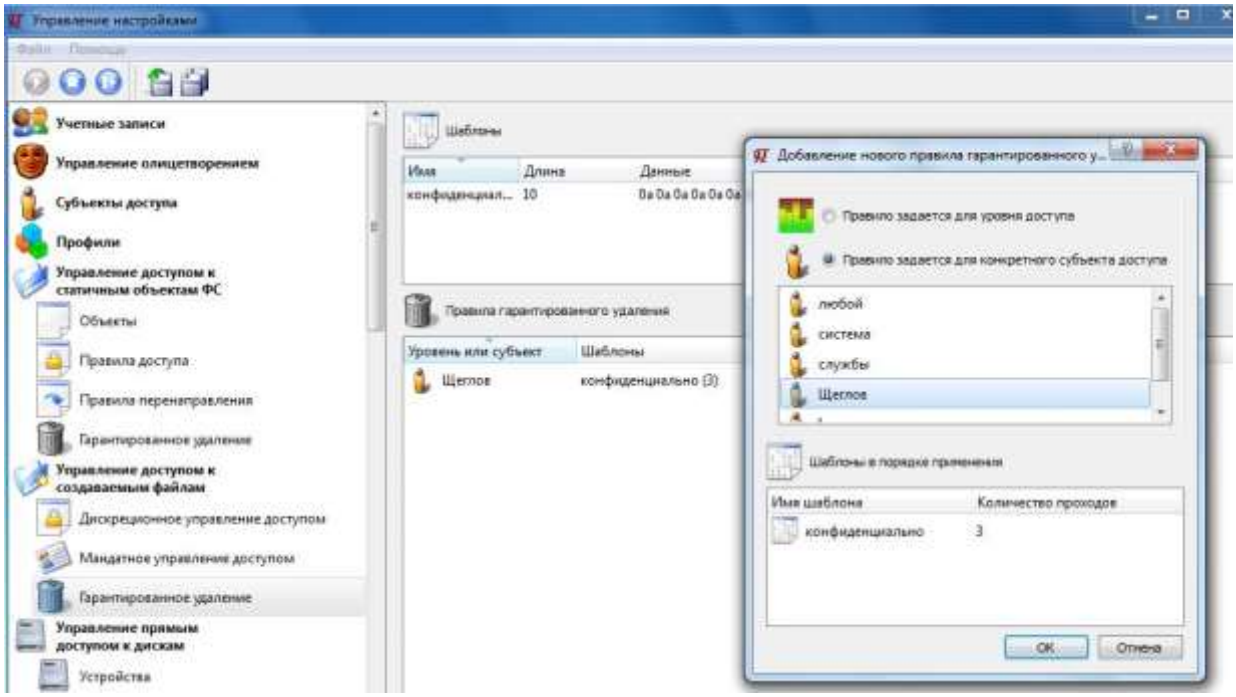

Рис.12. Интерфейс задания правил гарантированного удаления при дискреционном контроле доступа к создаваемым файлам

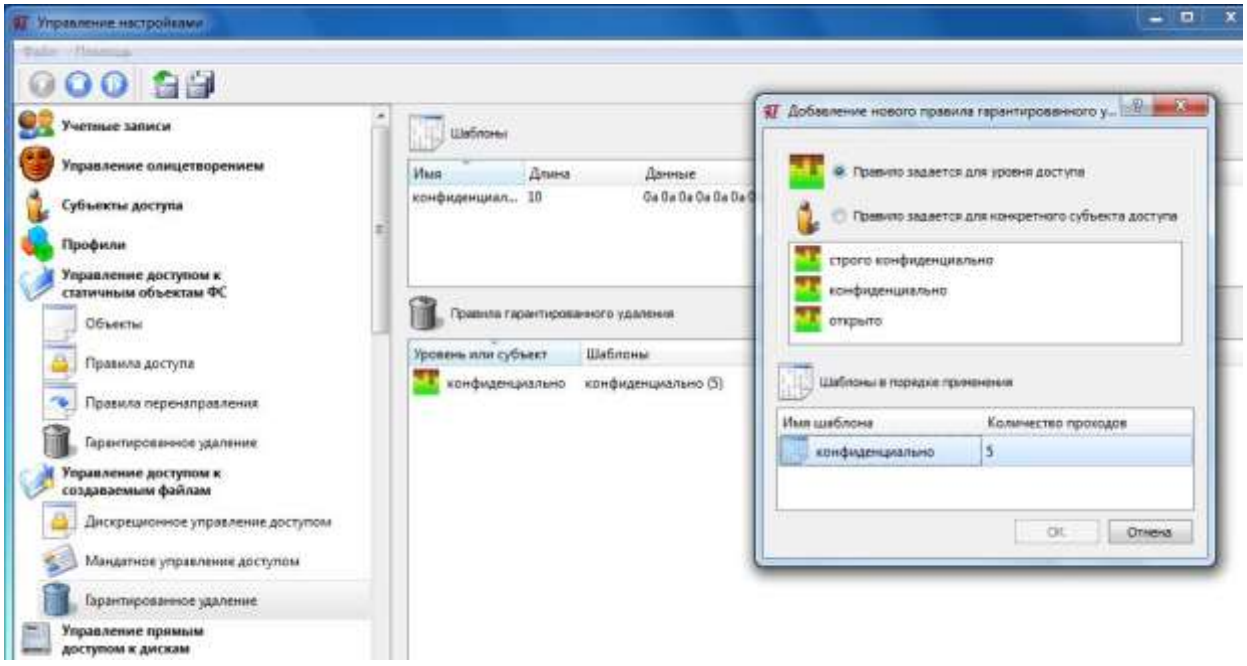

Рис.13. Интерфейс задания правил гарантированного удаления при мандатном контроле доступа к создаваемым файлам

В двух словах о реализации автоматического шифрования создаваемых файлов. Именно эти файлы, как файлы, используемые для хранения обрабатываемой на компьютере информации, и требуется хранить в зашифрованном виде.

Очевидно, что при использовании в системе методов контроля доступа к статичным файловым объектам, администратору требуется задавать файловые объекты, включая файловые накопители, при сохранении субъектом данных в которых, эти данные будут автоматически зашифровываться. Само по себе это трудоемкая задача, причем ошибка в администрировании здесь крайне критична, т.к. может привести к утечке конфиденциальной информации. Например, если рассматривать пользователя в качестве потенциального нарушителя, что необходимо в современных условиях, то в этом случае остается множество файловых объектов, в которые файлы и приложения осуществляют запись с правами текущего пользователя, которые позволят пользователю сохранить информацию в открытом виде, причем не обязательно непосредственно пользователем-нарушителем, данные могут быть сохранены под учетной записью пользователя уязвимым приложением. Чтобы предотвратить подобные потенциальные "каналы" утечки, администратору необходимо выявить все подобные файлы и задать применительно к ним режим записи с шифрованием. Возможность практической реализации, а уж тем более, корректного решения, предотвращающего возможность утечки информации при этом в общем случае, трудно считать реализуемой на практике.

В случае же использования метода (мандатного или дискреционного, или обоих одновременно) контроля доступа к создаваемым файлам, в системе защиты может быть решена задача принудительного для субъекта доступа хранения информации в зашифрованном виде. При этом, по аналогии с тем, как это показано на рис.12, рис.13, при настройке политики шифрования файлов уже потребуется задавать не объекты доступа, сохраняемая в которых информация будет автоматически зашифровываться, а субъекты доступа (при мандатном контроле - уровни доступа или метки безопасности), при сохранении которыми данных, они будут автоматически зашифровываться. Заметим, что учетной информации субъекта, сохраняемой в качестве атрибута создаваемого (модифицируемого) яайла в незашифрованном виде (не является секретной информацией), достаточно, чтобы выбрать клюк шифрования для расшифрования файла, где бы (вкакой папке) он не был бы созданю. Данное решение нами запатеновано

[13] и положено в основу разрабатываемого программного средства «Система защиты данных «Панцирь +». Получаем корректное решение задачи шифрования обрабатываемой информации в общем виде - где бы (в какой бы папке), в том числе, и на внешнем файловом накопителе, пользователь, в том числе, приложение с правами пользователя, не создал (модифицировал) файл, этот файл будет автоматически зашифровываться.

Как видим, применение методов контроля доступа к создаваемым файлам принципиально меняет требования к реализации многих иных механизмов защиты, решающих иные задачи защиты информации. Это позволяет говорить о предлагаемой новой технологии защиты данных, обрабатываемых в информационной системе.

Заключение.

В заключение отметим, что простота администрирования и эксплуатации средств защиты, реализующих предложенные методы, позволяет расширить область эффективного применения контроля и разграничения прав доступа. Примером тому может служить система защиты от вредоносных программ "Системы защиты «Панцирь+», описанная, например, в [14]. Данной системой не только осуществляется автоматическая разметка создаваемых файлов с последующим предотвращением их исполнения (запрещается также исполнение файлов с внешних накопителей), но и реализуется автоматическая разметка исполняемых статичных файлов (при первом их исполнении), с предотвращением последующей модификации, удаления подобных файлов. Отметим, что существует множество направлений развития данного антивирусного средства защиты, не требующего какого-либо сигнатурного либо поведенческого анализа, например, по аналогии с тем, как это было описано выше, достаточно просто реализовать изолированность обработки данных критичными процессами (например, сетевыми приложениями), либо приложениями, к которым по каким-либо причинам у пользователя отсутствует доверие, и т.д. Однако эти вопросы выходят за рамки настоящей работы.

Еще в заключении обратим внимание на следующее. В работе рассмотрены методы контроля доступа к создаваемым объектам, в том числе, файловым. Данными методами не решается задача разграничения прав доступа по созданию файлов - решается задача разграничения последующего к ним доступа. Эта задача, как и задача разграничения прав доступа к системным объектам должна решаться иными средствами. Вместе с тем, отметим, что сама по себе постановка задачи контроля в подобной постановке – задача контроля доступа по созданию файловых объектов, выдвигает совершенно новые

требования к решению, реализация которых позволяет получить принципиально новые возможности защиты, например, рассмотренные в [5]. Принципиально при этом меняются собственно методы контроля доступа и их практическая реализация, в частности это иллюстрируют запатентованные нами решения [6,7], реализованные в КСЗИ «Панцирь+». Эти вопросы авторы планируют рассмотреть в следующей работе.

Литература

1. 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.

2. 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.

3. Щеглов К.А., Щеглов А.Ю. Методы идентификации и аутентификации пользователя при доступе к файловым объектам // Вестник компьютерных и информационных технологий. - 2012. - № 10. - С. 47-51.

4. Щеглов К.А., Щеглов А.Ю. Контроль доступа к статичным файловым объектам // Вопросы защиты информации. - 2012. - Вып. 97. - № 2. - С. 12-20.

5. Маркина Т.А., Щеглов А.Ю. Метод защиты от атак типа drive-by загрузка. - Известия ВУЗзов. Приборостроение, 2014. - № 4. - С. 15-20.

6. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к ресурсам компьютерной системы с субъектом доступа «пользователь», «процесс». Положительное решение на выдачу патента на изобретение по заявке № 201320208/08(030001) от 30.04.2013.

7. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к ресурсам компьютерной системы с субъектом «исходный пользователь», «эффективный пользователь», «процесс». Положительное решение на выдачу патента на изобретение по заявке № 2013128215/08(041992) от 18.06.2013.

8. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к файлам на основе их автоматической разметки. Патент на изобретение № 2524566. Приоритет изобретения 18.03.2013.

9. Щеглов К.А., Щеглов А.Ю. Реализация метода мандатного доступа к создаваемым файловым объектам // Вопросы защиты информации. - 2013. - Вып. 103. - № 4. - С. 16-20.

10. Щеглов К.А., Щеглов А.Ю. Защита от вредоносных программ методом контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. -2012. - № 8. - С. 46-51.

11. Щеглов К.А., Щеглов А.Ю. Модели и правила мандатного контроля доступа // Вестник компьютерных и информационных технологий. - 2014. - № 5. - С. 44-49.

12. Щеглов К.А., Щеглов А.Ю. Практическая реализация дискреционного метода контроля доступа к создаваемым файловым объектам//Вестник компьютерных и информационных технологий. - 2013. - № 4. - С. 43-49.

13. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к шифруемым создаваемым файлам. Положительное решение на выдачу патента на изобретение по заявке № 2013129406/08(043781) от 26.06.2013.

14. Щеглов К.А., Щеглов А.Ю. Система защиты от запуска вредоносного ПО "Панцирь" // Вестник компьютерных и информационных технологий. - 2013. - № 5. - С. 38-43.