НОВЫЙ ПОДХОД К ЗАЩИТЕ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Введение

Решение задачи защиты информации от несанкционированного доступа в любой информационной системе основано на реализации контроля и разграничений прав доступа субъектов к защищаемым ресурсам (далее контроля доступа), 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. Первичным при назначении правил (разграничений прав) доступа субъектов к объектам в известных методах контроля доступа является объект, например, файловый объект. При этом различные объекты файлы, идентифицируемые своими именами в файловой системе, назначаются администратором для сохранения в них различного рода информации, обрабатываемой пользователями, в том числе, информации различных категорий конфиденциальности. Именно это и определяет известную применяемую на практике технологию защиты данных в информационных системах – конкретный файл, с учетом специфики разрешенной для сохранения в нем информации, является объектом защиты – именно к конкретным файлам должны назначаться права доступа субъектов, конкретные файлы должны гарантированно удаляться, шифроваться и т.д.

Остановимся на ключевом недостатке данного подхода к реализации контроля 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 права доступа субъектов, если их еще нет? А ведь это именно те объекты (файлы), которые, в первую очередь, и нуждаются в защите от несанкционированного доступа, поскольку именно в них хранятся обрабатываемые на компьютере данные. Это противоречие не только иллюстрирует всю нелогичность известной схемы контроля доступа, но и сказывается на возможности ее эффективного использования в современных условиях. Другой недостаток известных подходов состоит в том, 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, например, 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, нежели чем запущен порождающий его процесс, субъект 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 объекту. Естественно, что выполнение данного требования качественно усложняет задачу администрирования средства защиты.

В [4] рассмотрен метод контроля доступа, в значительной мере упрощающий эту задачу, за счет назначения прав доступа не к объектам субъектов, а субъектов к объектам. Упрощение задачи администрирования при этом достигается в результате использования масок при задании субъектов и объектов доступа в разграничительной политике, что кроме того позволяет получить достаточно важные новые свойства защиты [5]. Соответствующие технические решения для различных способов идентификации субъекта доступа запатентованы [6,7], реализованы и апробированы в программном средстве защиты информации "Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows" (далее КСЗИ «Панцирь+»). Однако, не смотря на эффективность данного решения, изложенная выше проблема, обусловливаемая рассмотренным противоречием известной схемы контроля доступа, не снимается и, как следствие, его целесообразно применять для реализации контроля 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 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 информационной системе, формируя принципиально иные требования к решению множества задач защиты информации. При этом отметим, что рассматриваемые в работе методы реализованы и апробированы при построении КСЗИ «Панцирь+». Далее для иллюстрации будем рассматривать интерфейсы этого программного средства защиты информации.

1. Принципы контроля доступа к создаваемым объектам.

Предлагаемые принципы контроля доступа к создаваемым объектам [8], основанные на их автоматической разметке при создании или модификации объекта, позволяют исключить сущность «объект доступа» из разграничительной политики доступа. Состоят они в следующем:

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 (модификации) субъектом объекта, объектом наследуется учетная информация субъекта доступа, создавшего этот объект - объект размечается (учетная информация субъекта сохраняется в атрибутах созданного им объекта).

4. При запросе доступа к любому объекту, диспетчер доступа (решающий элемент) получает разметку этого объекта, считывая его атрибуты, и анализирует запрос на непротиворечивость заданным правилам доступа, в результате чего предоставляет запрошенный субъектом доступ к объекту, либо отказывает в нем.

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

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.

Поскольку в работе рассматривается задача защиты данных, обрабатываемых в информационной системе, далее рассмотрим реализацию контроля доступа к файловым объектам и к буферу обмена, как к создаваемым объектам, используемым в системе для хранения данных.

2. Методы контроля доступа к создаваемым файлам.

Техническое решение, реализующее рассматриваемые далее методы контроля доступа к создаваемым файлам, запатентовано [9].

Мандатный метод контроля доступа.

Мандатный метод контроля доступа на практике, как правило, используется для реализации контроля доступа к категорируемой по уровням конфиденциальности информации, с целью предотвращения понижения ее категории в процессе обработки, в предположении, что информация различных уровней конфиденциальности должна обрабатываться на компьютере в различных режимах. Особенностью реализации данного метода контроля доступа является назначение пользователям (в качестве субъекта доступа здесь выступает пользователь – учетная запись, т.к. процессы в общем случае не подпадают под соответствующую схему категорирования) и файловым объектам меток безопасности (в данном случае – уровней доступа). При запросе доступа арифметически (на больше, меньше, равно) в соответствии с заданным правилом сравниваются метка субъекта и метка объекта, к которому субъектом запрошен доступ, на основании чего принимается решение о корректности (непротиворечивости) запроса доступа. На практике, как правило, используется (задается по умолчанию) следующее правило мандатного доступа – запись в объект разрешается при условии совпадения значений меток субъекта и объекта (уровни доступа) совпадают, чтение объекта субъектом разрешается в том случае, если уровень доступа субъекта не ниже, чем требуемый уровень доступа к объекту.

Применительно к предлагаемому мандатному методу контроля доступа к создаваемым файлам метки безопасности (уровни доступа) или мандаты присваиваются исключительно пользователям (интерактивным пользователям) [10]. Уровни (список уровней) доступа для системы создаются заданием их числовых значений и смысловой транскрипцией из интерфейса (меню), представленного на рис.1. Число создаваемых меток не ограничено. Сравнению

диспетчером доступа подлежат числовые значения, смысловая же транскрипция метки используется для удобства администратора.

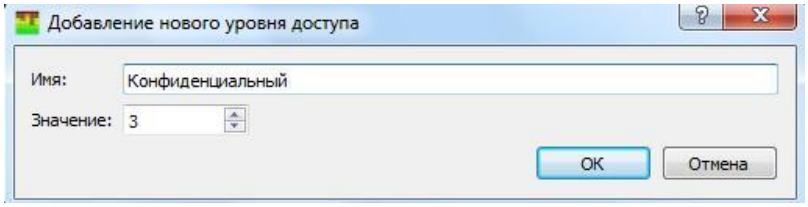

Рис.1. Меню задания уровней доступа (мандатных уровней)

Для любого заведенного в системе защиты пользователя может быть задан (выбран) уровень доступа. При этом метки безопасности могут назначаться не всем пользователям, а только тем, доступ к файлам, создаваемым которыми, будет контролироваться и разграничиваться (обрабатываемые этими пользователями данные требуется защищать). Назначенные администратором настройки мандатного контроля доступа отображаются в интерфейсе, приведенном на рис.2.

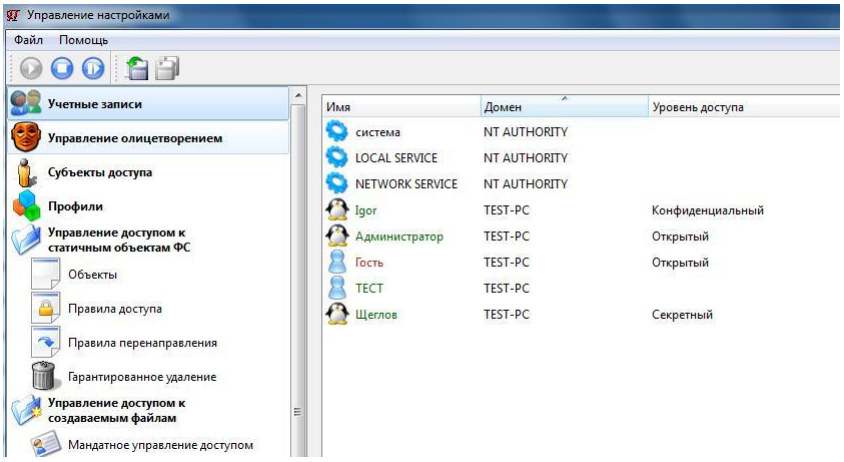

Рис.2. Отображение заведенных в системе пользователей с заданными для них мандатными уровнями

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 (в данном случае его уровень доступа), 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 [11] (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.3.

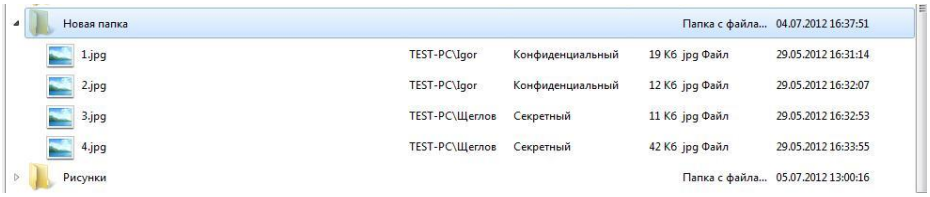

Рис.3. Отображение разметки созданных контролируемыми пользователями файлов при мандатном контроле доступа

Кроме достигаемого принципиального упрощения администрирования средства защиты, рассмотренный метод характеризуется еще одним, куда более значимым достоинством. Он обеспечивает корректное решение задачи контроля и разграничений прав доступа в общем случае, по двум причинам. Во-первых, не только непосредственно пользователями, но и приложениями «от лица» пользователей создается и модифицируется в процессе работы масса файлов в различных каталогах. Для корректной реализации схемы контроля доступа известным методом все эти файлы (либо соответствующие папки) должны быть определены и им должна быть присвоена метка безопасности, что несет в себе весьма большую вероятность допущения ошибки при администрировании. Вторая причина еще более существенна. Системой и приложениями создаются папки коллективного доступа, например, для временного хранения файлов, в которые для корректной работы программных средств необходимо разрешить полный доступ всем пользователям. Это противоречит самой идее мандатной схемы контроля доступа. Эти вопросы исследованы в [10]. При реализации же контроля доступа к создаваемым

файлам, любой создаваемый файл в любой папке будет принудительно размечаться, к нему будут разграничиваться права доступа.

Замечание. В работе [12] 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 (не установлено по умолчанию) 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, где, как ранее отмечали, субъект доступа должен идентифицироваться тремя сущностями "исходный идентификатор пользователя, эффективный идентификатор пользователя, процесс".

Интерфейс создания и отображения созданных подобным образом субъектов доступа в системе защиты проиллюстрирован на рис.4 [13].

При задании идентификатора пользователя (как исходного (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.

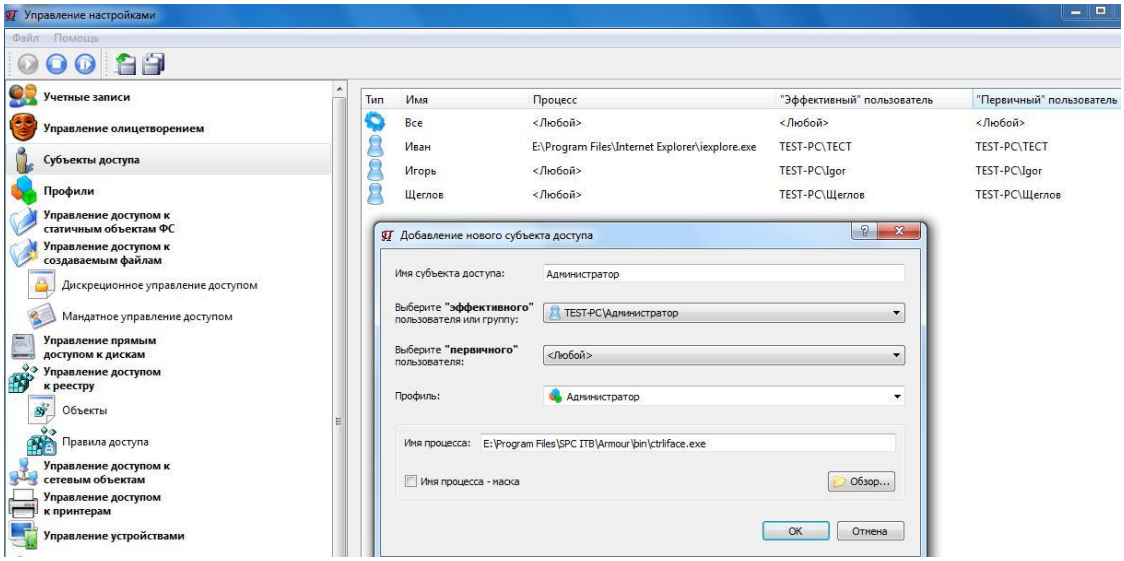

Рис.4. Создание и отображение в интерфейсе созданных субъектов доступа

Правила доступа задаются администратором из интерфейса и отображаются в интерфейсе, приведенном на рис.5 (субъекты доступа здесь отображаются присвоенными им при создании именами, см. рис.4).

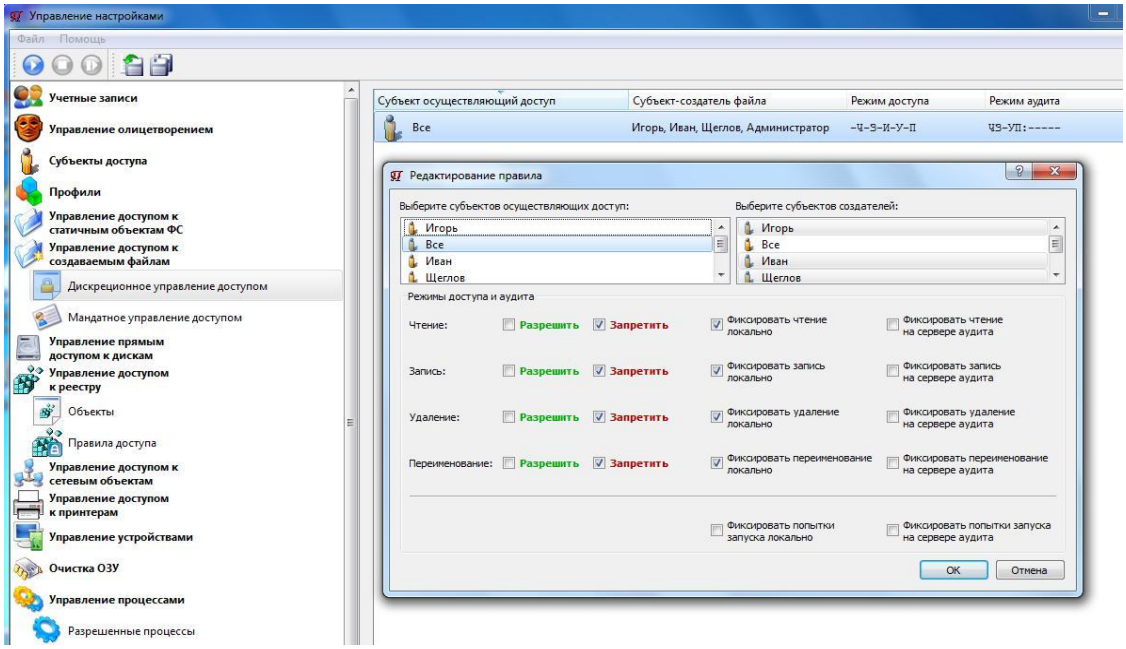

Рис.5. Создание и отображение в интерфейсе созданных правил доступа

Отметим, что в назначаемые права доступа, см. рис.5, 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.5, в поле "Выберите субъектов создателей", см. рис.5, 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.5. 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.5.

Замечание. Требования к правилам доступа, выполнение которых позволяет построить безопасную систему, сформулированы и обоснованы в [13].

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.5), 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.6.

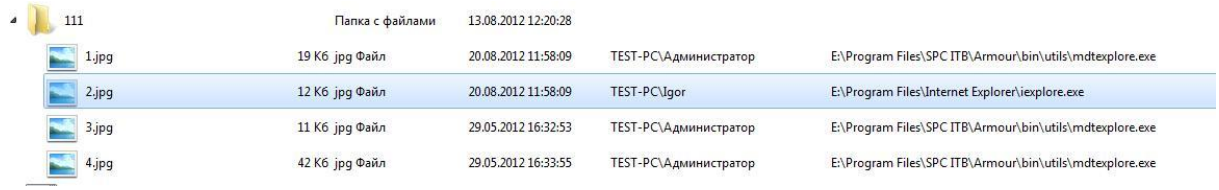

Рис.6. Отображение разметки созданных контролируемыми пользователями файлов при дискреционном контроле доступа

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.

Как видим, дискреционный метод контроля доступа к создаваемым файлам позволяет решать важнейшие современные задачи защиты информации от атак, эксплуатирующих уязвимости приложений. Например, всего несколькими

правилами в разграничительной политике доступа можно изолировать работу интернет-браузера (либо иных, по каким-либо соображениям, критичных приложений), предотвратив его доступ к данным, обрабатываемым иными приложениями.

Замечание. Для защиты же системных ресурсов (системных файлов и объектов реестра) от атак со стороны интернет-браузера, либо какого-либо иного критичного приложения, уже должен использоваться метод дискреционного контроля доступа к 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.4.

3. Метод контроля доступа к буферу обмена.

Поскольку буфер обмена предназначен для временного хранения данных, используемых для обмена данными 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 (к 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+». С учетом назначения буфера обмена - обмен данными осуществляется между приложениями, запускаемыми под одной учетной записью, основным субъектом доступа в 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.4, а правила доступа субъектов к буферу обмена (к данным, записанным в буфер обмена) – из интерфейса, представленного на рис.7. Настройка правил доступа и контроль доступа реализуются по полной аналогии с тем, как это реализовано в отношении создаваемых файлов.

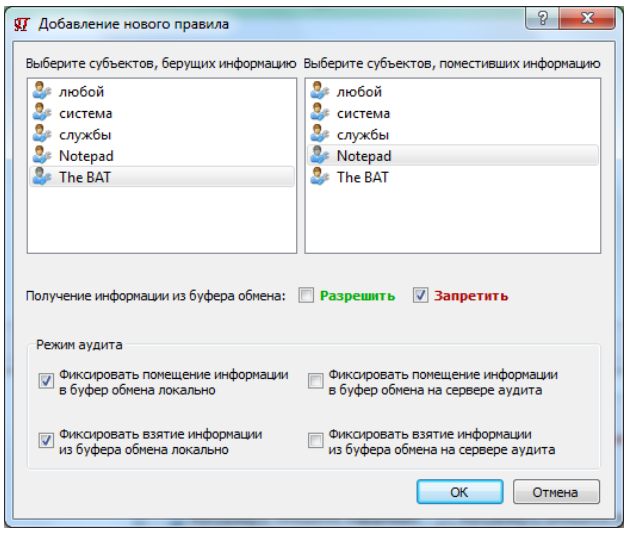

Рис.7. Задание правил доступа к буферу обмена

В правом столбце интерфейса, см. рис.7, 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 для них 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.

Данный механизм защиты, совместно с механизмом контроля доступа к создаваемым файлам, позволяют реализовать полностью изолированную обработку данных отдельными приложениями (группами приложений) в информационной системе.

4. Изменение технологии защиты данных в информационной системе.

Рассмотрим, как практическое использование методов контроля и разграничения прав доступа к создаваемым объектам в целом сказывается на технологию защиты данных в информационной системе, 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, записанные на жестком диске или на внешнем накопителе, образуют файлы. Как правило, на диске еще присутствует, 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). Эти данные невозможно прочитать, обратившись к файлу (они не образует файла), но достаточно просто получить к ним доступ с использованием сторонних программ прямого доступа к диску.

Задача предотвращения появления на накопителе обрабатываемых данных в виде остаточной информации решается отдельным механизмом гарантированного удаления файлов, состоящем в следующем. Запрос на удаление файла перехватывается средством защиты, после чего в удаляемый файл им заданное число раз записывается исходно заданная администратором информация, лишь только после чего управление передается системе для «удаления» штатными средствами ОС. В результате реализации данного решения, в качестве остаточной информации на накопителе будут скапливаться те данные, которые средством защиты принудительно записываются в файл перед его удалением.

При реализации известных методов контроля доступа к файлам, правила гарантированного удаления должны устанавливаться в отношении конкретных объектов доступа – файловых объектов, в которых предполагается сохранение пользователями конфиденциальной информации.

При использовании подобного известного 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 будут храниться 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.8, соответственно, на рис.9, в зависимости от реализованного метода контроля доступа к создаваемым файлам - дискреционный, либо мандатный, задаются правила гарантированного удаления – задаются субъекты, идентифицируемые своими именами, см. рис.4 (соответственно, уровни доступа – метки безопасности), созданные которыми файлы 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.

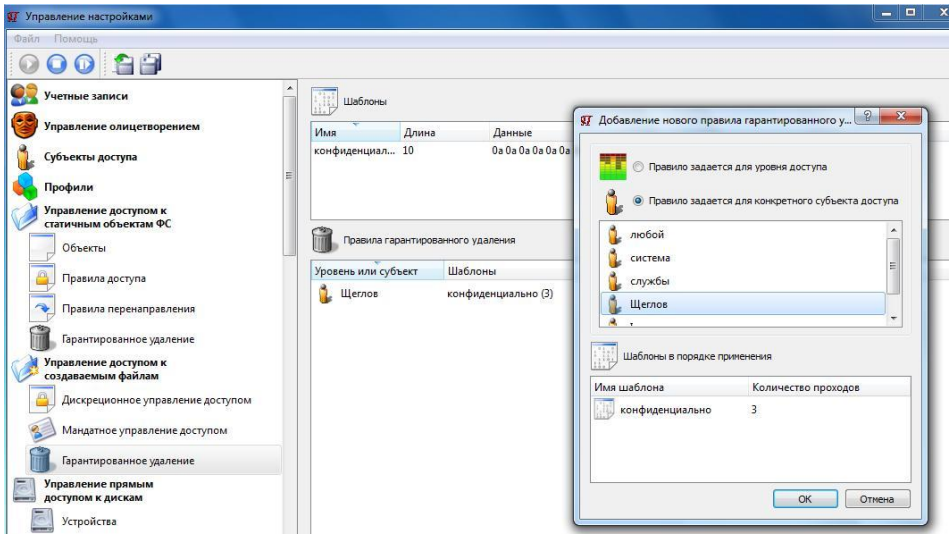

Рис.8. Интерфейс задания правил гарантированного удаления при дискреционном контроле доступа к создаваемым файлам

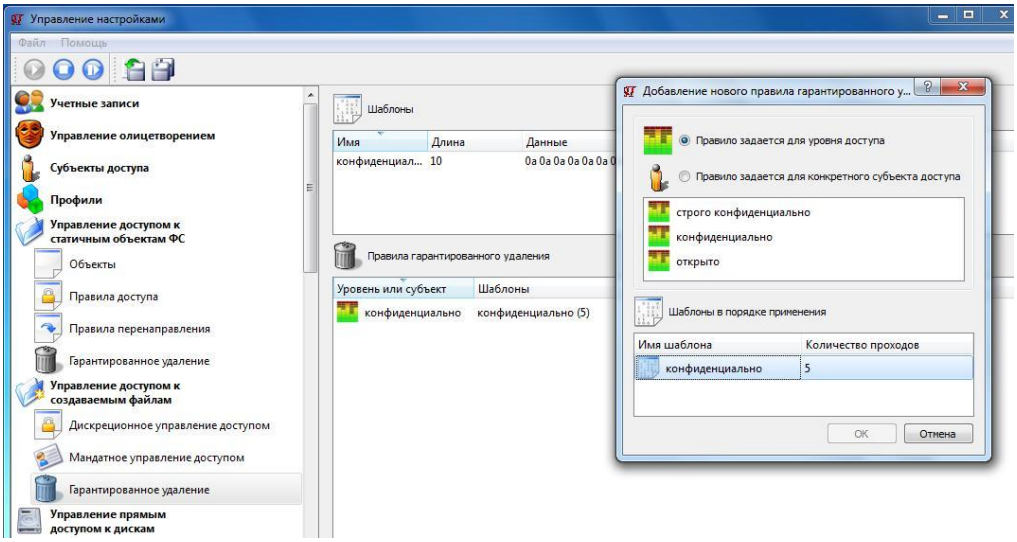

Рис.9. Интерфейс задания правил гарантированного удаления при мандатном контроле доступа к создаваемым файлам

Все сказанное относится и к вопросам реализации автоматического шифрования создаваемых файлов. Именно эти файлы, как файлы, используемые для хранения обрабатываемых данных, итребуется 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, а ошибка в администрировании здесь крайне критична, т.к. может привести к утечке конфиденциальной информации. Здесь опять следует напомнить о файлах, в которые приложения осуществляют запись с правами текущего пользователя, т.е. в которые может осуществить запись и собственно пользователь с целью сохранения даных в незашифрованном виде. Чтобы предотвратить подобные потенциальные "каналы" утечки, администратору необходимо выявить все подобные файлы и задать применительно к ним режим записи с шифрованием.

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.8, рис.9, при настройке политики шифрования файлов уже потребуется задавать не объекты доступа, данные, сохраняемые в которых, будут автоматически зашифровываться, а субъекты доступа (при мандатном контроле - уровни доступа или метки безопасности), при сохранении которыми данных, они будут автоматически зашифровываться. Учетной же информации субъекта, сохраняемой в качестве атрибута создаваемого (модифицируемого) файла в незашифрованном виде (она не является секретной информацией), достаточно, чтобы выбрать ключ шифрования для расшифрования файла, где бы (в какой папке) он не был бы создан. Данное решение также запатеновано [14].

Заключение.

Как видим, практическое применение предложенных методов контроля доступа к создаваемым объектам, позволяющее рассмотреть задачи защиты данных и системных объектов, как совершено различные задачи защиты даже в своей постановке, принципиально меняет требования к реализации многих иных механизмов защиты, решающих совсем иные задачи защиты информации. Это позволяет говорить о новой технологии защиты данных, обрабатываемых в информационной системе.

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 К.А., Щеглов А.Ю. Принцип и методы контроля доступа к создаваемым файловым объектам // Вестник компьютерных и информационных технологий. - 2012. - № 7. - С. 43-47.

9. 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.

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

11. 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.

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

13. 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.

14. 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.