ПРИНЦИПЫ РЕАЛИЗАЦИИ ДОПОЛНИТЕЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ КОНТРОЛЕ ДОСТУПА К СОЗДАВАЕМЫМ ФАЙЛОВЫМ ОБЪЕКТАМ НА ОСНОВЕ ИХ АВТОМАТИЧЕСКОЙ РАЗМЕТКИ

Введение.

Основой защиты обрабатываемой информации от несанкционированного доступа является реализация разграничительной политики доступа к файловым объектам, в общем случае, для субъектов доступа пользователь и процесс [1].

В дополнение к разграничительной политике, с целью защиты от хищения обрабатываемой информации, на практике широко используются методы дополнительной защиты, в первую очередь, это гарантированное удаление остаточной информации и шифрование обрабатываемой (сохраняемой на компьютере и на внешних накопителях) информации.

В работах [2,3] авторы рассмотрели принципы и методы контроля доступа к создаваемым файловым объектам, основанные на использовании автоматической разметки создаваемых файлов. Как отмечалось [2,3], применение данных подходов позволяет реализовать корректную в общем случае разграничительную политику доступа к создаваемым файлам (как дискреционным, так и мандатным методами контроля доступа [2,3]) и при этом кардинально упростить задачу администрирования, за счет исключения из разграничительной политики сущности «объект доступа».

Однако исключение сущности «объект доступа» не может не сказаться и на реализации дополнительной защиты, где также традиционно используется сущность «объект доступа».

Рассмотрим в данной работе принципы построения дополнительной защиты, предполагающей исключение сущности «объект доступа» из разграничительной политики, на примере реализации гарантированного удаления остаточной информации, понимая, что все сказанное относится и к

реализации шифрования обрабатываемой (сохраняемой на компьютере) информации.

1. Принципы контроля доступа к создаваемым файловым объектам.

Рассмотренные в [2,3] принципы контроля доступа к создаваемым файловым объектам, основанные на исключение сущности "объект доступа" из разграничительной политики, за счет автоматической разметки создаваемых файлов, состоят в следующем:

1. Сущность "объект" должна быть исключена из схемы реализации разграничительной политики доступа к создаваемым файловым объектам, по причине их отсутствия на момент задания прав доступа к файловым объектам.

2. Создаваемый субъектом доступа (в зависимости от решаемой задачи защиты, в качестве субъекта доступа следует рассматривать либо сущность "пользователь", либо сущность "процесс", либо пару сущностей "пользователь-процесс") файловый объект, в первую очередь, файл, однозначно характеризуется (уровень конфиденциальности, критичность приложения и т.д.) субъектом, создавшим этот объект.

3. При реализации разграничительной политики доступа (назначении правил доступа) должны использоваться две сущности: идентифицируемый субъект (учетная информация - идентификатор, либо метка безопасности), создавший объект, и идентифицируемый субъект, запрашивающий доступ к созданному объекту.

4. Создаваемый (модифицируемый) файловый объект (файл) должен автоматически наделяться при записи диспетчером доступа, в результате, включать в себя (в качестве атрибута, либо непосредственно в "теле" файла, в зависимости от реализации), учетную информацию субъекта, создавшего/модифицировавшего этот файл.

5. При запросе доступа к созданному файлу, диспетчер доступа, используя изначально заданные правила (матрица доступа, либо правила сравнения меток безопасности) должен анализировать учетную информацию

субъекта, создавшего этот файл (является принадлежностью созданного файла), и учетную информацию субъекта, запросившего доступ к этому файлу. На основании чего диспетчер должен разрешать, либо отказывать субъекту в запрошенном доступе.

6. В зависимости от решаемой задачи защиты и реализуемого метода контроля доступа, в качестве учетной информации могут выступать: имя пользователя (учетная запись), полнопутевое имя исполняемого файла, характеризующее субъект "процесс", метка безопасности [1].

2. Назначение гарантированного удаления остаточной информации. Требование к корректности реализации.

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, либо модификации (с уменьшением объема) файла штатными средствами ОС, собственно данные не удаляются, осуществляется переразметка MFT-таблицы (на примере Windows). Другими словами, на жестком диске и 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 или модификации файлового объекта. Это реализуется отдельным механизмом гарантированного удаления остаточной информации, состоящем в следующем. Запрос на удаление и модификацию файла перехватывается средством защиты, после чего ею осуществляется очистка освобождаемого дискового пространства (как правило, заданное число раз записывается какая-либо информация, например, все «0», либо случайная последовательность), затем управление передается системе для «удаления» штатными средствами ОС.

При реализации данного механизма защиты, возникают специфические требования к корректности реализации. Проиллюстрируем их на примере NTFS. В NTFS все данные, хранящиеся на томе, содержатся в файлах. Главная таблица файлов (MFT) занимает центральное место в структуре NTFS-тома. MFT реализована, как массив записей о файлах, где каждая запись представляет собою совокупность пар атрибутов и их значений. Размер каждой записи фиксирован и равен 1 Кб. Если размер файла достаточно мал, чтобы поместиться в теле записи, то данные такого файла хранятся непосредственно в MFT.

В процессе работы системы, NTFS ведет запись в файл метаданных – файл журнала с именем $LogFile. NTFS использует его для регистрации всех операций, влияющих на структуру тома NTFS, как то: создание файла, удаление файла, расширение файла, урезание файла, установка файловой информации, переименование файла и изменение прав доступа к файлу. Информация, описывающая подобные транзакции, включает в себя копии записей из MFT и в дальнейшем используется для повтора или отмены изменений. Соответственно, если данные файла содержатся в записи MFT, то при каждом изменении, данные файла будут (в числе прочего) скопированы в файл журнала.

Требование к корректности реализации. Во избежание многократного дублирования данных небольших файлов, система защиты должна при создании файлов принудительно выделять пространство на томе вне таблицы MFT размером 1 Кб, что обеспечит гарантированное сохранение данных только в файле.

3. Реализация гарантированного удаления при использовании в разграничительной политике сущности «объект доступа».

Сразу оговоримся, что рассматривать здесь и далее технические решения мы будем на примере построения КСЗИ «Панцирь+» (разработчик ЗАО «НПП «Информационные технологии в бизнесе»). В этой системе защиты реализован контроль доступа, как статичным файловым объектам,

так и к создаваемым файлам, причем для каждого из этих решений реализован свой механизм гарантированного удаления, см. рис.1.

В рассматриваемой разграничительной политике ключевой является именно сущность «объект доступа». Именно через разграничения доступа субъектов к объектом определяется, в каком объекте насколько критичная информация должна сохраняться субъектами. Следовательно, правила гарантированного удаления должны устанавливаться в отношении объектов доступа – файловых объектов.

Реализуется это в два этапа. На первом этапе задаются затирающие файлы шаблоны – это та информация, которая будет записана в файл средством защиты перед его удалением ОС, см. рис.1 (это справедливо и в случае модификации – уменьшения размера, файла).

На втором этапе из интерфейса, представленного на рис.2, задаются непосредственно правила гарантированного удаления – задаются файловые объекты, применительно к которым требуется обеспечить гарантированное удаление (это могут быть файлы, каталоги, диски), для каждого из которых определяется шаблон записи и количество проходов записи (циклов перезаписи) выбранным шаблоном.

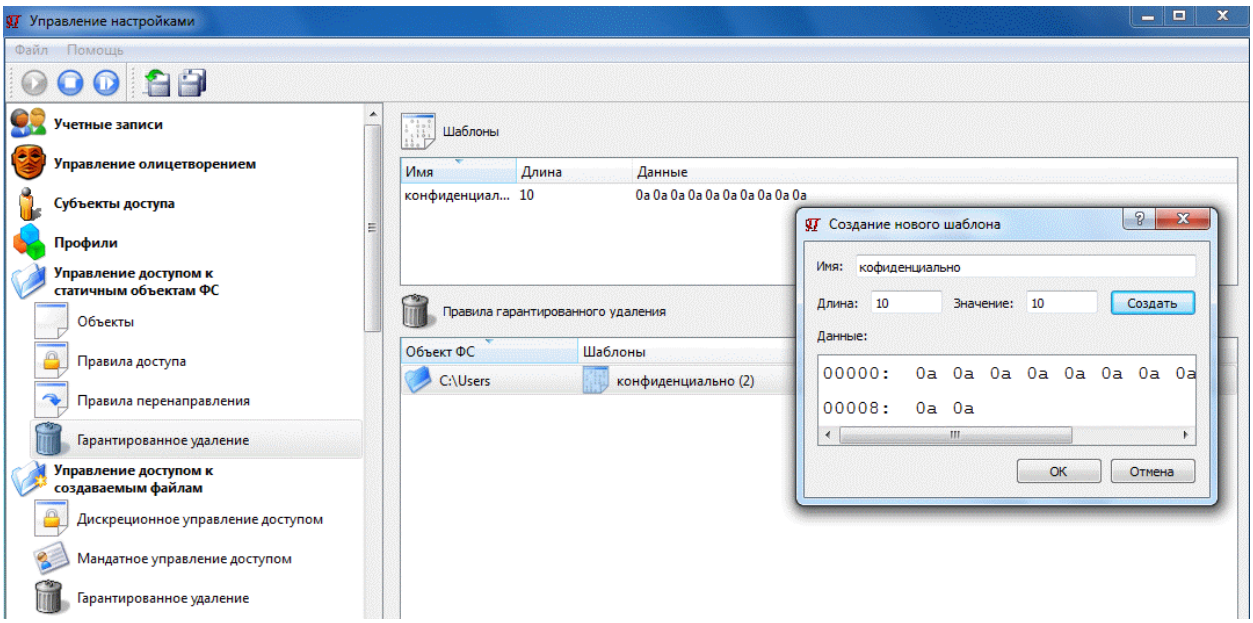

Рис.1. Интерфейс создания затирающих файлы шаблонов

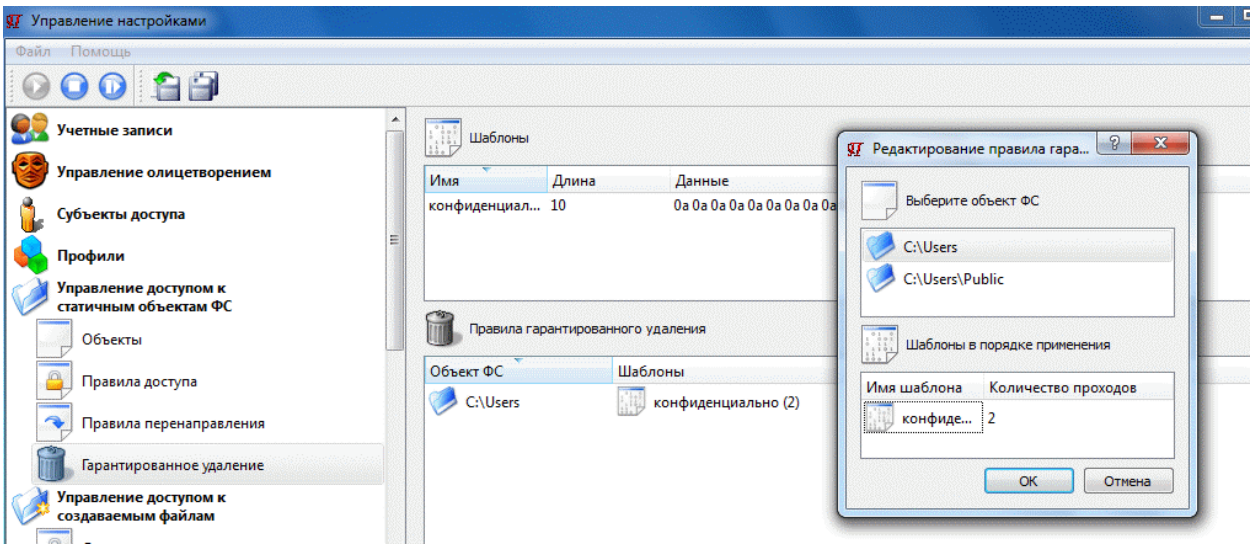

Рис.2. Интерфейс задания правил гарантированного удаления объектов

При обращении на удаление или модификацию к заданному в правилах гарантированного удаления системы защиты объекту – файлу, каталогу, диску (диспетчер доступа, перехватывающий запрос доступа, идентифицирует, какой субъект, какой доступ, к какому объекту запрашивает), системой защиты отрабатываются заданные правила гарантированного удаления.

4. Реализация гарантированного удаления создаваемых файловых объектов на основе их автоматической разметки.

Контроль доступа к создаваемым файловым объектам [2,3], как отмечали, основан на автоматической разметке создаваемых файлов.

При реализации дискреционного контроля доступа, созданный файл наследует учетную информацию создавшего его субъекта - имя пользователя и полнопутевое имя процесса, при реализации мандатного контроля доступа – имя создавшего его пользователя и его уровень допуска (метка безопасности). Отображение разметки созданных файлов, которую можно просмотреть с использованием специальной утилиты, входящей в состав системы защиты, проиллюстрировано на рис.3 и рис.4.

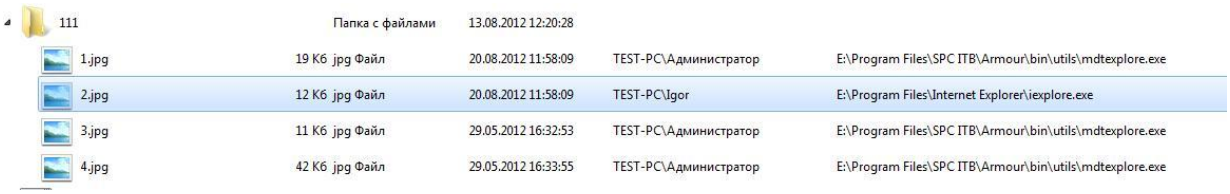

Рис.3. Отображение разметки созданных файлов при дискреционном контроле доступа

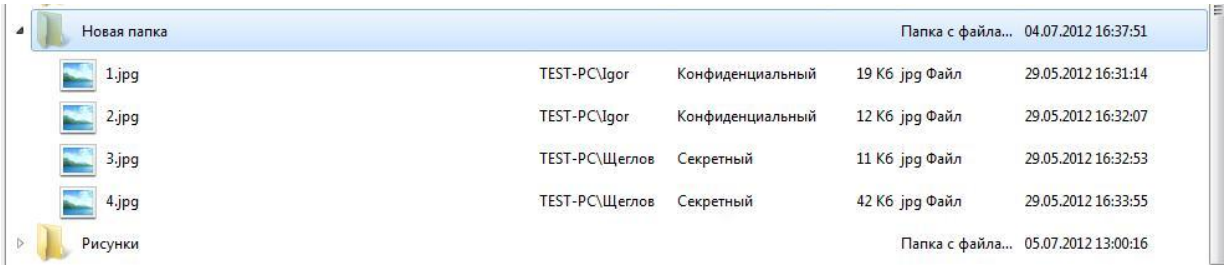

Рис.4. Отображение разметки созданных файлов при мандатном контроле доступа

При этом отсутствуют разграничения по созданию файлов, разграничивается последующий доступ субъектов к созданным (размеченным) файлам. Это обусловливает и корректность разграничительной политики в общем случае (где бы не был создан файл, в том числе, в неразделяемых системой и приложениями каталогах) он будет однозначно размечен, т.е. права доступа к нему будут однозначно определены, и простоту администрирования (доступ разграничивается между субъектами, а не субъектов к объектам [2,3].

Однако, что касается гарантированного удаления, то описанные выше принципы его реализации здесь не применимы. Любой файл любым субъектом может быть создан в любом объекте (в любой папке), что априори не позволяет исходно задать корректных правил гарантированного удаления.

Однако созданный файл однозначно описывается своей разметкой. Это позволяет реализовать принципы гарантированного удаления, основанные на автоматической разметке файлов, состоящие в следующем.

Настройка системы защиты также осуществляется в два этапа. На первом этапе задаются затирающие файлы шаблоны – это та информация, которая будет записана в файл средством защиты перед его удалением ОС,

по аналогии с тем, как это показано на рис.1 (это справедливо и в случае модификации – уменьшения размера, файла).

На втором этапе из интерфейсов, представленных на рис.5, соответственно, на рис.6 (в зависимости от реализованного метода контроля доступа - дискреционный, либо мандатный), задаются непосредственно правила гарантированного удаления – задаются субъекты (соответственно, уровни доступа – метки безопасности), файлы, созданные которыми (здесь уже речь идет именно о файлах, т.к. размечаются файлы), должны гарантированно удаляться. Для каждого из субъектов (уровня доступа) определяется шаблон записи и количество проходов записи (циклов перезаписи) выбранным шаблоном, см. рис.5, рис.6.

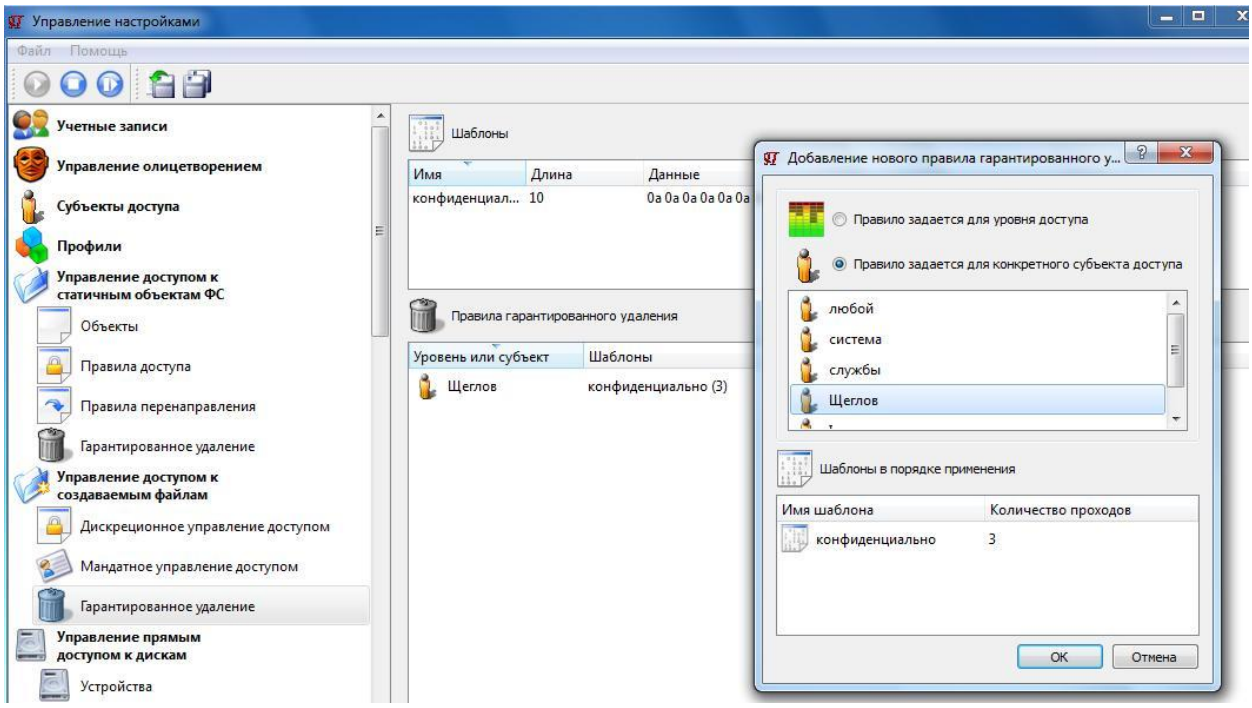

Рис.5. Интерфейс задания правил гарантированного удаления при дискреционном контроле доступа к создаваемым файлам

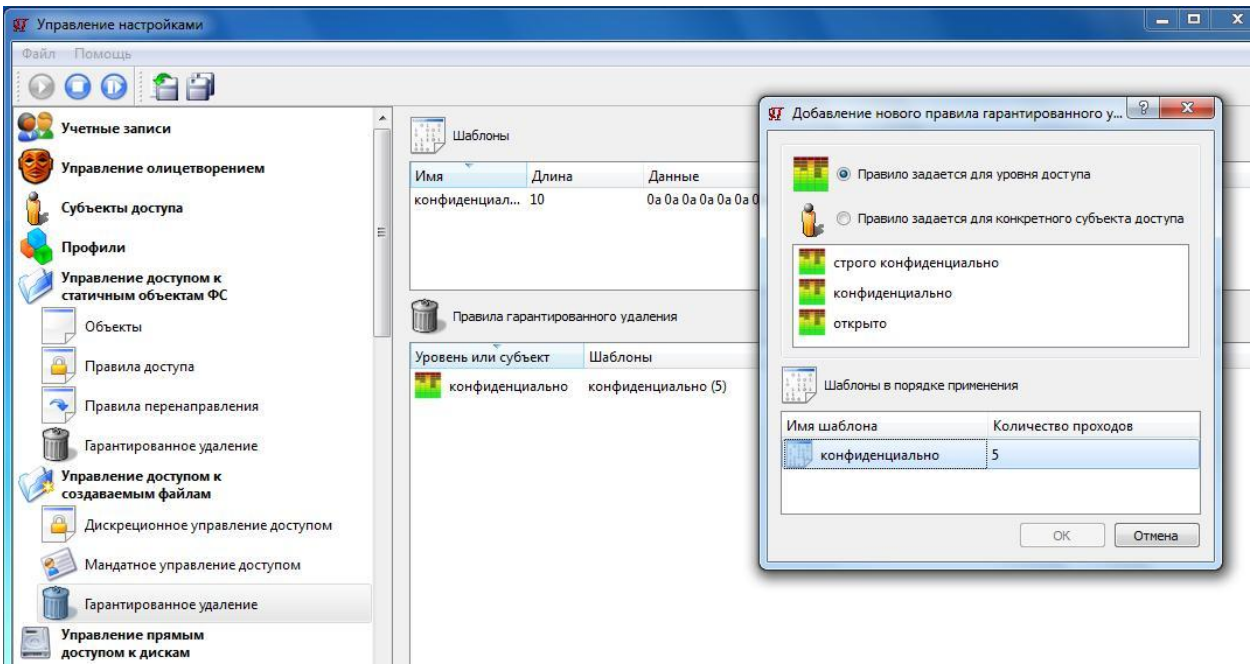

Рис.6. Интерфейс задания правил гарантированного удаления при мандатном контроле доступа к создаваемым файлам

При обращении на удаление или модификацию к любому файлу (диспетчер доступа, перехватывающий запрос доступа, идентифицирует, какой субъект, какой доступ, к какому объекту запрашивает), системой защиты считывается разметка файла, анализируются и отрабатываются заданные правила гарантированного удаления для данного созданного файла.

Заключение. Как видим, и задача гарантированного удаления, при реализации контроля доступа к создаваемым файлам, решается корректно в общем случае (корректность решения задачи гарантированного удаления обусловливается однозначной разметкой всех создаваемых в процессе функционирования системы файлов и анализом разметки при доступе к любому файлу), причем сложность администрирования системы защиты и в этом случае минимальна! Однако, куда важнее иное. Реализация системой защиты контроля доступа к создаваемым файловым объектам, основанного на их автоматической разметке, предполагает возможность (если не необходимость, в частности, как в рассматриваемом случае) отказа от сущности «объект доступа» во всех механизмах защиты обрабатываемой на

компьютере информации, что во многом требует пересмотра собственно существующих принципов защиты компьютерной информации.

Литература.

1. 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.

2. Щеглов К.А., Щеглов А.Ю. Принцип и метод дискреционного контроля доступа к создаваемым файловым объектам // Вопросы защиты информации, 2012. - Вып. 96. - № 1. - С. 30-38.

3. 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.