РЕАЛИЗАЦИЯ МЕТОДА МАНДАТНОГО КОНТРОЛЯ ДОСТУПА К СОЗДАВАЕМЫМ ФАЙЛОВЫМ ОБЪЕКТАМ

Введение.

В работах [1,2] авторы рассмотрели принципы и методы контроля доступа к создаваемым файловым объектам, основанные на использовании автоматической разметки создаваемых файлов. Как отмечалось [1,2], применение данных подходов позволяет реализовать корректную разграничительную политику доступа к создаваемым файлам и при этом кардинально упростить задачу администрирования, за счет исключения из разграничительной политики сущности «объект доступа».

Заметим, что мандатный контроль доступа предназначен именно для реализации разграничительной политики доступа (на основе меток безопасности) к создаваемым в процессе работы файлам, т.к. именно эти файлы и предназначены для хранения обрабатываемой на компьютере информации [2]. Статичные (или системные) файлы в общем случае не подпадают под категорирование обрабатываемой на компьютере информации, как следствие, они должны исключаться из мандатной схемы контроля доступа.

Предложенный в [2] метод мандатного контроля доступа реализован в КСЗИ «Панцирь+» для ОС Microsot Windows. Рассмотрим в данной работе практическую реализацию предложенного [2] метода и оценим его преимущества.

1. Отличия предложенного метода мандатного контроля доступа.

Под мандатным контролем доступа в общем случае понимается способ обработки запросов доступа к файловым объектам, основанный на формальном сравнении, в соответствии с заданным правилом, меток безопасности (мандатов), назначаемых субъектам и объектам доступа (в общем случае группам субъектов и объектов). Метки безопасности, как правило, являются элементами линейно упорядоченного множества M =

{M1,…, Mk} и служат для формализованного представления каких-либо свойств субъектов и объектов.

Разграничение доступа реализуется на основе задаваемого правила, определяющего отношение линейного порядка на множестве M, где для любой пары элементов из множества M, задается один из типов отношения: {>,<,=} (на практике реализуется выбор подмножества M, изоморфного конечному подмножеству натуральных чисел – такой выбор делает естественным арифметическое сравнение меток безопасности). Правило сравнения меток также назначается из каких-либо свойств субъектов и объектов, применительно к решаемой задаче защиты информации.

Наиболее широкое практическое использование мандатного метода нашло применение практики секретного делопроизводства в компьютерной обработке информации. Основу реализации обработки категорированной информации составляет классификация информации по уровням конфиденциальности. Метки безопасности объектов отражают категорию конфиденциальности информации, которая может быть сохранена в соответствующих объектах. Метки же безопасности субъектов отображают полномочия (по аналогии с формой допуска) субъектов, в части допуска к информации различных уровней конфиденциальности.

Отличительной особенностью предложенного нами метода контроля доступа к создаваемым файловым объектам [2] является исключение сущности «объект доступа» из разграничительной политики. Разграничения осуществляются исключительно между субъектами доступа, а не опосредованно, через объект.

В качестве контролируемых объектов рассматриваются создаваемые в процессе функционирования системы файлы, которые непосредственно и содержат защищаемую информацию. Задание разграничительной

политики доступа состоит исключительно в назначении меток безопасности субъектам Мс.

Контроль доступа состоит в следующем. При создании субъектом нового файла, файлом наследуется учетная информация субъекта доступа – его метка безопасности Мс (обозначим унаследованную метку Мсо, при этом Мсо= Мс). При запросе же доступа к любому файлу, анализируется наличие, а при наличии, собственно значение метки безопасности Мсо, унаследованной данным файлом. При наличии метки у файла - Мсо, эта метка сравнивается с меткой субъекта, запросившего доступ к файлу, Мс – анализируется выполнение заданных правил контроля доступа. В результате анализа данной информации, с учетом реализуемых правил контроля доступа, либо разрешается запрошенный субъектом доступ к файлу, либо отказывается в нем.

Правила, направленные на защиту от понижения категории обрабатываемой информации, имеют следующий вид:

1. Субъект С имеет доступ к объекту О в режиме “Чтения” в случае, если выполняется условие: Мс <, = Мсо.

2. Субъект С имеет доступ к объекту О в режиме “Записи” в случае, если выполняется условие: Мс = Мсо.

Как видим, основное отличие состоит в том, что в разграничительной политике доступа присутствуют только субъекты и их метки безопасности, размечать файловые объекты не требуется. А это не только значительное упрощение задачи администрирование, что проиллюстрируем далее, но и возможность корректного решения задачи контроля доступа к общем случае. Дело в том, что при реализации предложенного метода, вне зависимости от того, в какой объект (каталог) помещен файл, в том числе, в каталог временных файлов, в каталог, не разделяемый системой и приложениями и т.д., сохраненный файл будет однозначно автоматически размечен – им будет унаследована метка безопасности, как следствие, доступ к файлу возможен только при

выполнении заданных правил контроля. Заметим, все это касается и системных объектов (каталог), разметка которых вообще не укладывается в схему мандатного контроля доступа.

3. Практическая реализация метода мандатного контроля доступа к создаваемым файловым объектам.

Для иллюстрации обеспечиваемой простоты администрирования, полностью приведем процедуру настройки контроля доступа, реализованную в КСЗИ «Панцирь+» для ОС Microsot Windows.

Прежде всего, требуется завести пользователей в средстве защиты/в системе. Пользователи либо заводятся из интерфейса средства защиты, приведенного на рис.1, либо импортируются в средство защиты из системы, после чего для них устанавливается пароль на вход в систему, включая задание возможности входа в систему в безопасном режиме, см. рис.1, что крайне важно, с точки зрения реализации эффективной защиты. Естественно, для системных пользователей пароль установить нельзя.

В результате, заведенные в системе и в средстве защиты пользователи отображаются в окне интерфейса средства защиты, в виде, приведенном на рис.2. Системные пользователи отображаются черным цветом, пользователи с установленным паролем для входа в систему – зеленым, пользователи, пароль которым не установлен – их вход в систему невозможен, красным.

После заведения пользователей, из меню, приведенного на рис.3, задаются уровни доступа (мандатные уровни). Уровни задаются как количественным значением меток безопасности (мандатов), так и их смысловой транскрипцией.

В результате, заведенные уровни доступа отображаются в виде, представленном на рис.4.

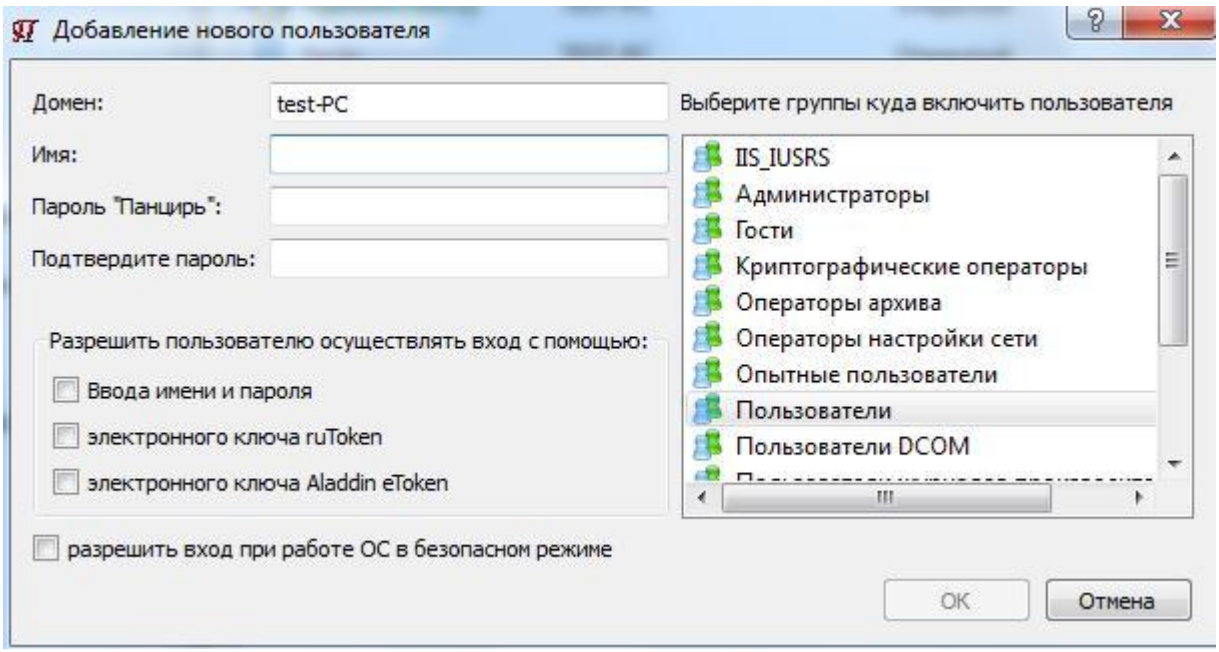


Рис.1. Интерфейс задания пользователей в средстве защиты

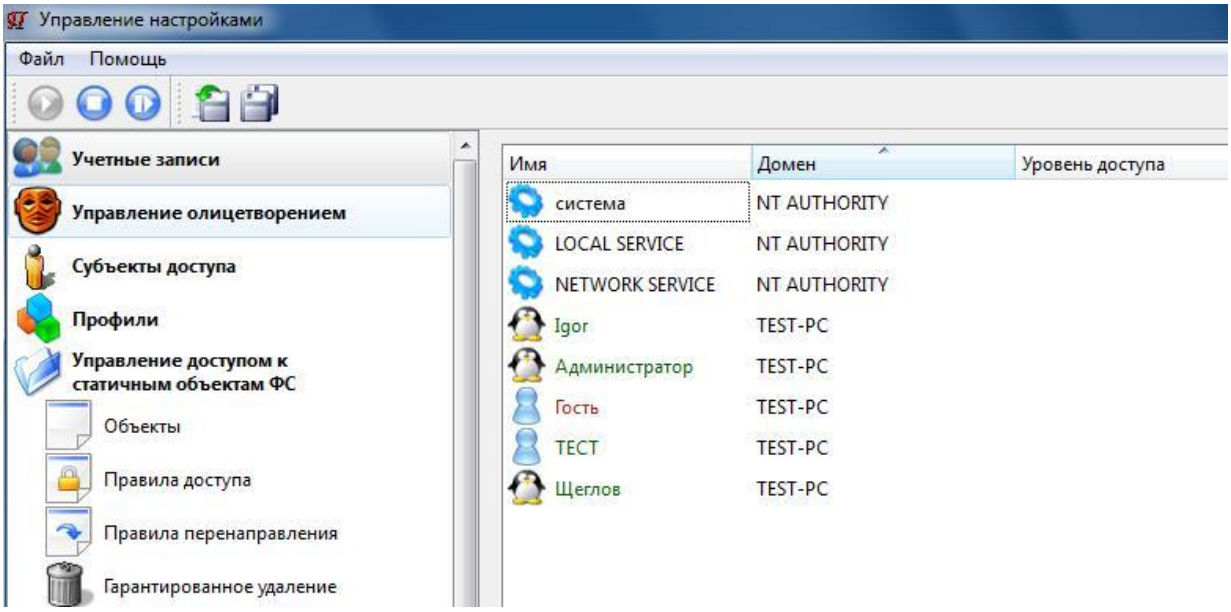


Рис.2. Отображение заведенных в системе пользователей

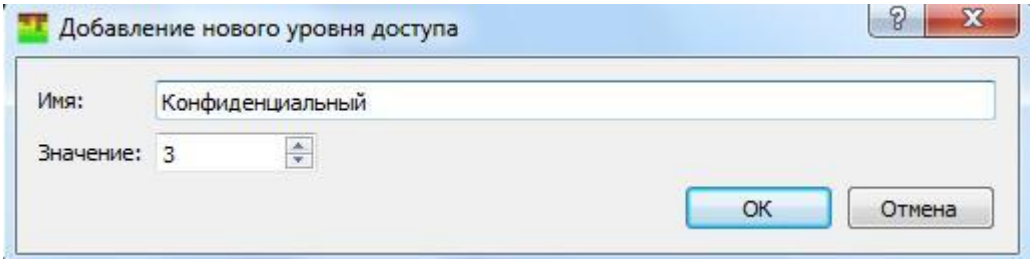


Рис.3. Меню задания уровней доступа (мандатных уровней)

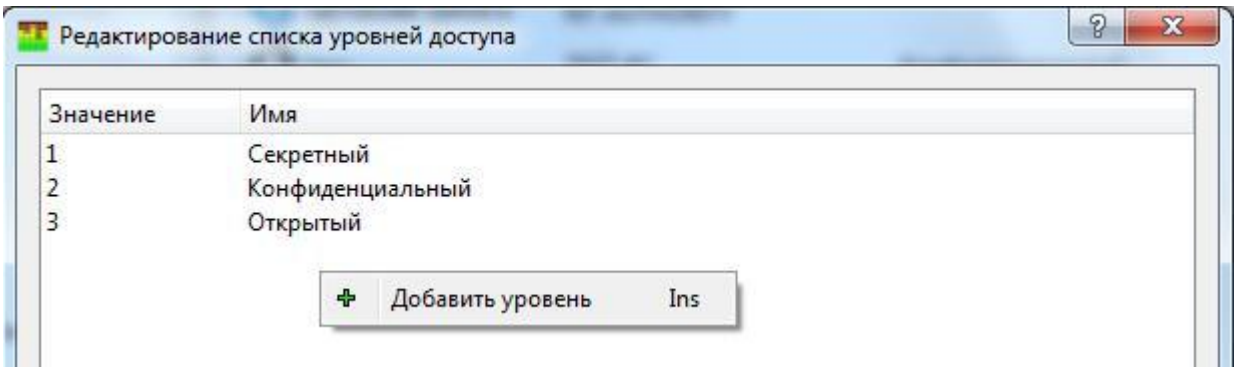
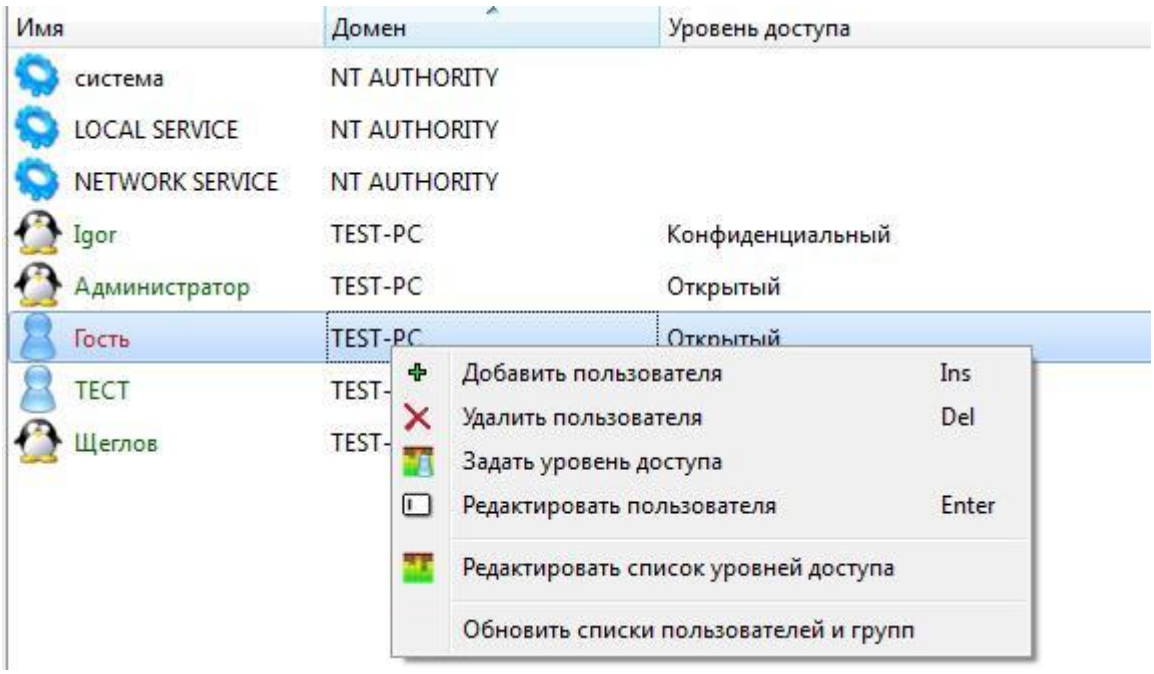
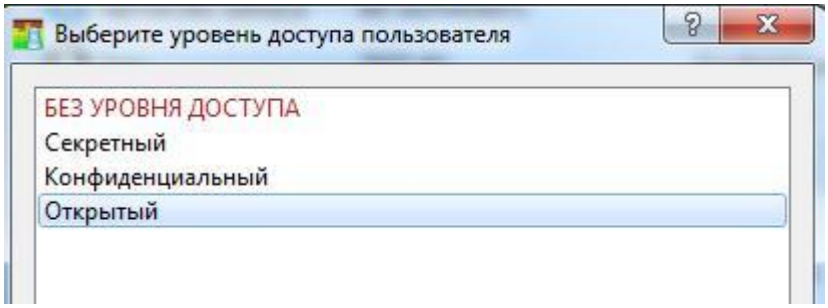


Рис.4. Отображение заведенных в системе уровней доступа (мандатных уровней)

Далее для тех пользователей, доступ к создаваемым файлам которых должен контролироваться, сопоставляются метки безопасности - им присваивается уровень доступа, см. рис.5 а), уровень доступа назначается из созданного до этого списка, см. рис.5 б).



а) Меню задания мандатного уровня для выбранного пользователя



б) Меню выбора мандатного уровня из заданного списка

Рис.5. Задание пользователям уровней доступа (мандатных уровней)

Пользователи, с заданными для них уровнями доступа отображаются в виде, приведенном на рис.6.

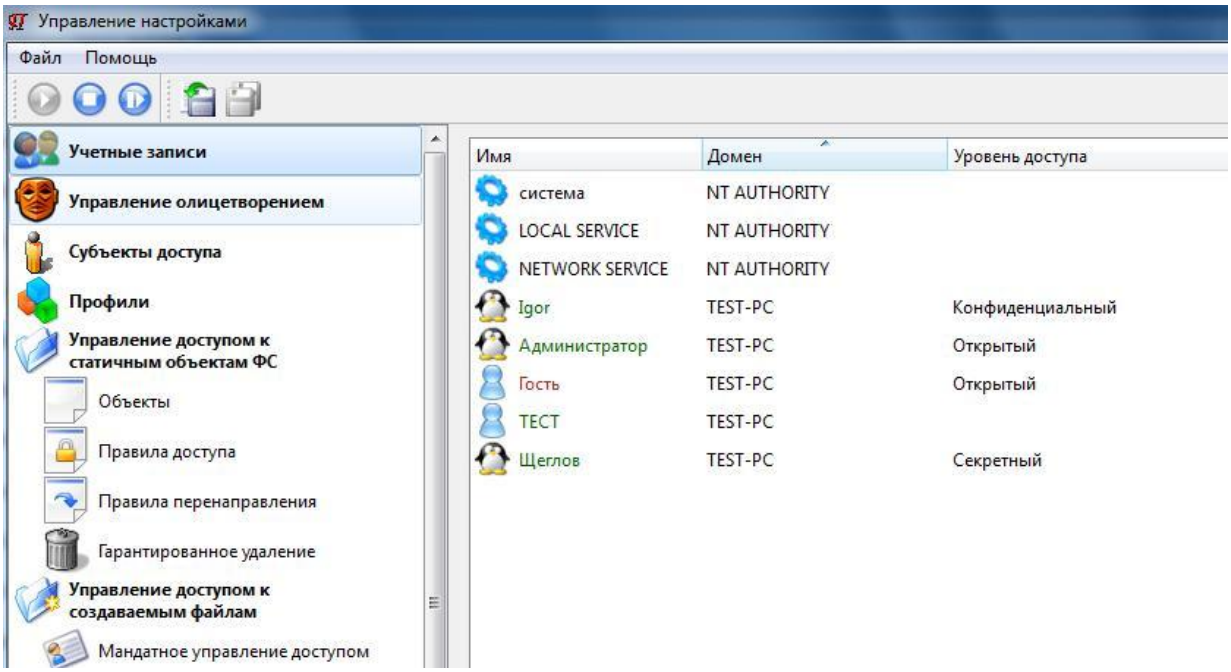


Рис.6. Отображение заведенных в системе пользователей с заданными для них мандатными уровнями

Еще раз уточним, что будет происходить при назначении пользователям уровней доступа. При сохранении файла контролируемым пользователем (пользователем с присвоенным уровнем доступа), файлом автоматически будет наследоваться уровень доступа создавшего его пользователя. Наследование будет происходить и в том случае, если контролируемым пользователь модифицирует неразмеченный ранее файл.

При последующем обращении к контролируемому файлу (к размеченному файлу), доступ к нему будет контролироваться - разрешаться/запрещаться в соответствии с заданными правилами мандатного доступа.

Настройка же правил мандатного доступа осуществляется из интерфейса, приведенного на рис.7. В окне, приведенном на рис.7, настроены следующие правила контроля доступа - возможность чтения/записи пользователем файла одного с ним уровня, и возможность чтения пользователем файла более низкого уровня доступа (категории).

Замечание. Возможность записи на более высокий уровень, в большой мере в современных условиях – это теоретическая возможность, ввиду того, что современные приложения, как правило, не открывают файл только на запись, а открывают одновременно на запись/чтение. Эта возможность реализована для общности метода.

Заметим, что правила мандатного контроля доступа задаются для двух основных типов доступа – чтение и запись, запрет же исполнения для размеченных файлов (для файлов, созданных пользователями во время работы системы) установлен в правилах контроля доступа «по умолчанию», т.к. нельзя разрешать на исполнение создаваемые пользователями в процессе работы файлы (иначе сразу же столкнемся с проблемой вредоносного ПО).

Замечание. Если в интерфейсе, см. рис.7, все разрешить, будет реализована только защита от запуска вредоносных программ.

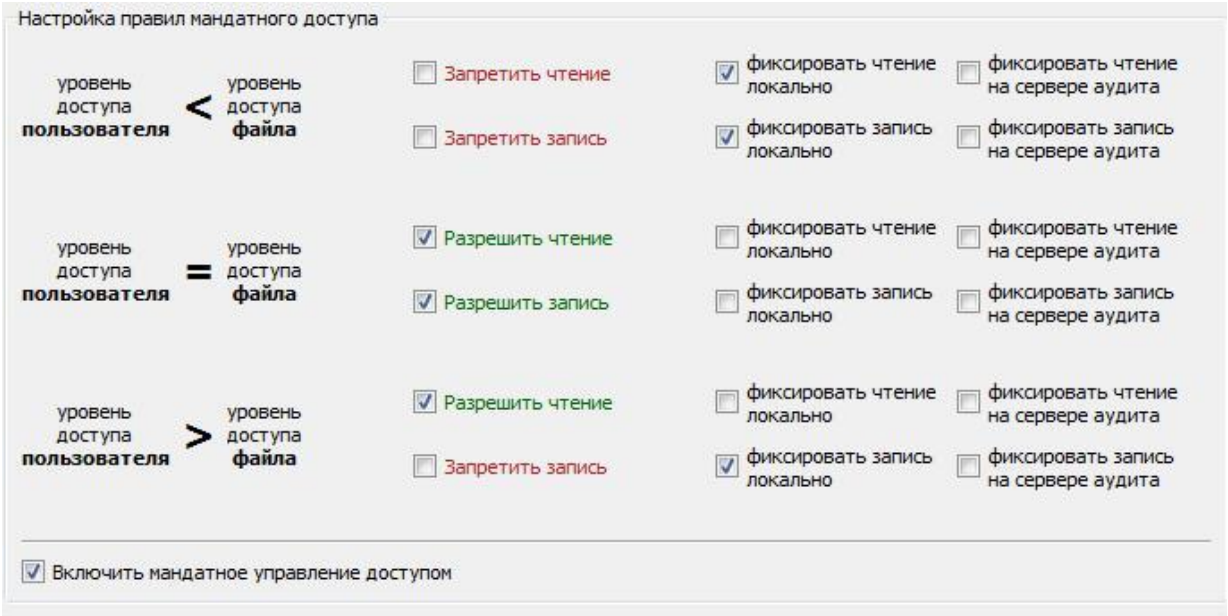


Рис.7. Интерфейс настройки правил мандатного контроля доступа

Вот и все настройки. Больше ничего не требуется, а главное, не требуется каким-либо образом размечать файловые объекты (назначать им метки безопасности). Вся разметка создаваемых в процессе работы файлов (т.е. тех файловых объектов, к которым имеет смысл контролировать доступ с использованием меток безопасности - мандатов) производится автоматически средством защиты.

Для возможности обзора произведенной в процессе работы системой разметки файлов, создаваемых контролируемыми субъектами (пользователями), в состав средства защиты включена специальная утилита обзора разметки созданных файлов. С ее использованием, выбрав соответствующий файловый объект в проводнике, администратор может посмотреть, какие права унаследованы файлом при его создании (отображается имя пользователя, создавшего файл, и его уровень доступа), рис.8.

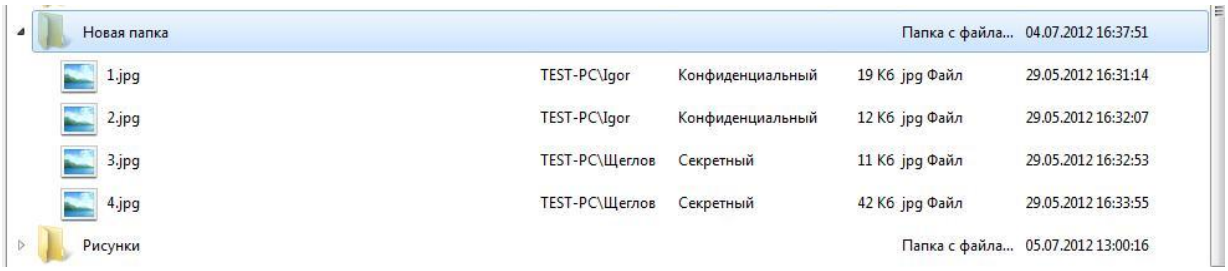


Рис.8. Отображение разметки созданных контролируемыми пользователями файлов

Соответственно, в журнале аудита отображается выполнение, либо нет (в зависимости от настроек аудита) заданных правил мандатного контроля при доступе пользователей к контролируемым файловым объектам, см. рис.9.

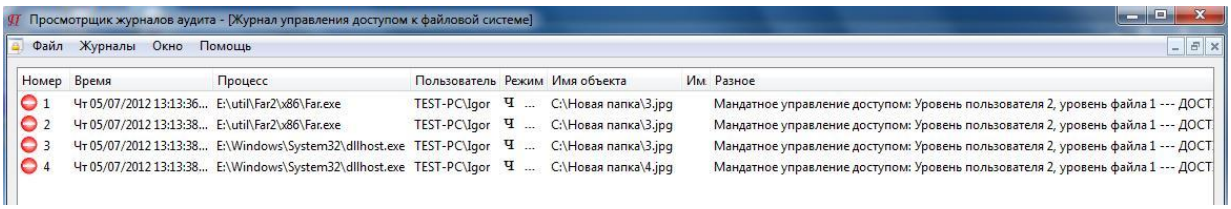


Рис.9. Регистрация попыток несанкционированного доступа к контролируемым файлам в журнале аудита

Заключение.

Как видим, упрощение администрирования, при реализации мандатного контроля доступа к создаваемым файловым объектам, не то, чтобы значительно, оно кардинально. Требуется лишь назначить метки безопасности пользователям и правило контроля доступа, вот и все! Ошибиться при этом невозможно, а это также вопросы безопасности. И что важно, при этом можно быть уверенным в корректной реализации мандатной схемы контроля доступа.

Литература.

1. 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.
2. 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.