ТЕХНОЛОГИЯ ИЗОЛИРОВАННОЙ ОБРАБОТКИ ДАННЫХ КРИТИЧНЫМИ ПРИЛОЖЕНИЯМИ

Введение.

Для осуществления атаки на компьютерную систему злоумышленник в любом случае должен обладать соответствующим средством реализации атаки - программой, позволяющей осуществить ему требуемые несанкционированные для этой системы действия. К подобным программам, как к средству реализации атаки, могут быть отнесены, как специально созданные с целью реализации атаки несанкционированные для системы программы, так называемые, вредоносные программы, так и используемые в системе программы (как правило, приложения), которые являются санкционированными для компьютерной системы, но по разным причинам могут быть наделены злоумышленником вредоносными свойствами. Назовем подобные приложения критичными. Если эффективная защита от запуска на компьютерной системе вредоносных программ может быть достаточно эффективно реализована предотвращением любой возможности (в том числе и системными правами, что реализует защиту от атак на повышение привилегий) исполнения создаваемых в системе файлов [1,2], то отказаться от использования критичных санкционированных приложений невозможно. В [3,4] рассмотрены и на соответствующих моделях проанализированы возможные пути наделения санкционированных программ вредоносными свойствами и на предложенной вероятностной модели контроля доступа обоснована единственная возможность защиты от атак на критичные приложения в общем случае, состоящая в изолировании обработки подобными приложениями данных в компьютерной системе. Дело в том, что, если некоторые локальные задачи защиты от наделения критичного приложения вредоносными свойствами, за счет прочтения им вредоносного кода (например, скрипта) [3] еще могут быть решены, такой пример реализации защиты приведен в [5], то предсказать какая ошибка

программирования присутствует в критичном приложении, как и с какой целью она может эксплуатироваться злоумышленником, в общем случае не представляется возможным. Используя соответствующую статистику обнаружения и исправления уязвимостей в приложениях, позволяющих реализовать ту или иную атаку, можно лишь оценить вероятность возникновения условий для осуществления подобной атаки, как следствие уровень критичности приложения [6], не более того. Исходя из этого, существует единственный обоснованный подход к решению рассматриваемой задачи защиты в общем случае, состоящий в предотвращении любого доступа критичного приложения, которое в любой момент времени следует рассматривать, как наделенного неизвестными вредоносными свойствами, к конфиденциальной информации, обрабатываемой в компьютерной системе [3,4].

Рассматриваемые в работе методы защиты, реализующие данный подход, апробированы при построении коммерческого средства защиты "Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows" (разработчик ЗАО «НПП «Информационные технологии в бизнесе»), что позволяет нам далее их иллюстрировать с использованием интерфейсов данного программного средства защиты информации.

1. Технология изолированной обработки данных.

Защита реализуется контролем и разграничением прав доступа приложений к обрабатываемым на компьютере данным, то есть реализацией разграничительной (в данном случае целесообразно говорить "разделительной") политики доступа для субъекта процесс.

Поскольку одни и те же механизмы защиты могут применяться для решения различных задач (что отличает комплексную систему защиты информации), то субъект доступа целесообразно задавать парой сущностей - пользователь, процесс, с учетом же защиты от потенциальной возможности ее обхода, за счет смены учетной записи пользователя при доступе к защищаемом ресурсу, в общем случае, субъект доступа в разграничительной

политике задается тремя сущностями - первичный (или исходный) идентификатор пользователя, полнопутевое имя процесса, эффективный идентификатор пользователя. Обоснование данного подхода к созданию субъекта доступа в современном средстве защиты представлено в [7].

Интерфейс создания и отображения созданных субъектов доступа в системе защиты проиллюстрирован на рис.1.

При задании идентификатора пользователя (как первичного, так и эффективного) может использоваться маска "*" - "Любой", в этом случае заданные правила будут распространяться на всех пользователей - разграничения прав доступа реализуются между процессами (приложениями), именно это нас и интересует в данной работе. 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 соответствующего каталога, маской *.exe - исполняемые файлы с соответствующим расширением и т.д., маской "*" задается то, 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. Каждому заданному субъекту доступа присваивается имя. Именно имена субъектов далее используются при задании правил доступа.

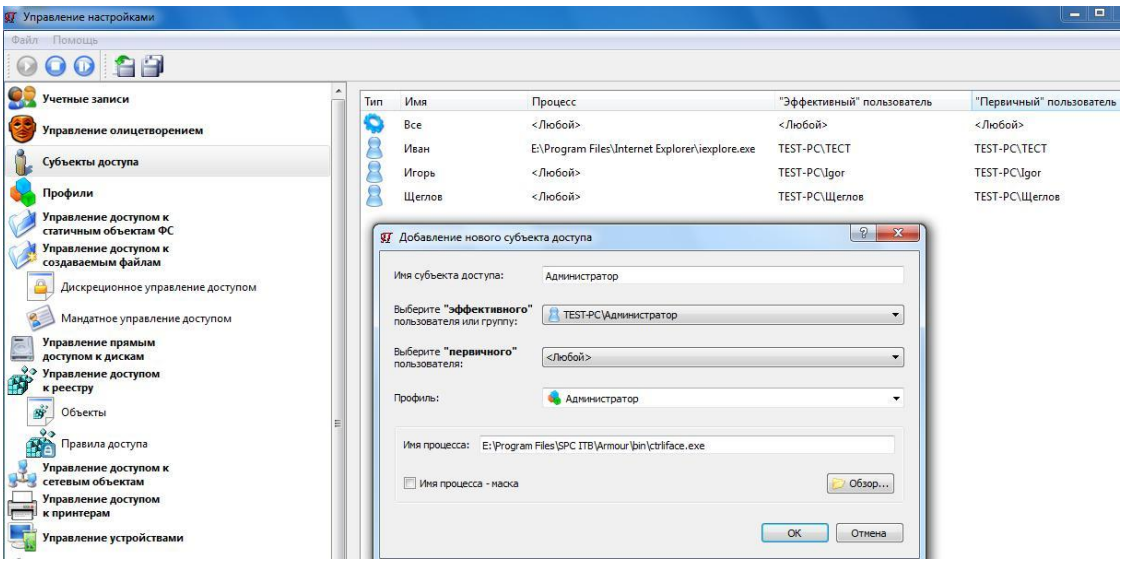

Рис.1. Создание и отображение в интерфейсе субъектов доступа

Сформулируем требования к разграничительной политике доступа, реализующей изолированную обработку данных различными приложениями.

1. Разграничения доступа должны устанавливаться между процессами (приложениями).

2. В качестве объекта доступа выступают данные, создаваемые пользователями в процессе работы на компьютерной системе, поскольку целью решаемой задачи защиты является предотвращение несанкционированного доступа критичных приложения к обрабатываемой информации.

3. Задача разграничительной политики состоит не в задании правил в отношении того, какой субъект в каком месте жесткого диска или на внешнем накопителе может создавать свои файлы, а в задании правил в отношении того, какой субъект имеет право (и какое право) доступа к данным, созданным другим субъектом. Таким образом, контроль и разграничения прав доступа должны задаваться в отношении последующего доступа к созданным субъектами данным.

4. В качестве защищаемых ресурсов, используемых для хранения обрабатываемых данных, т.е. ресурсов, к которым должна быть применима разграничительная политика доступа, следует рассматривать файловые объекты и буфер обмена.

Из представленных требований видим, что они не реализуемы известными средствами контроля и разграничения прав доступа, что требует разработки новых методов защиты и реализующих их технических решений.

2. Метод и реализация контроля доступа к файловым объектам.

Построение разграничительной политики доступа к файловым объектам основано на реализации принципов контроля доступа к создаваемым файлам на основе их автоматической разметки, предложенным авторами в [8,9]. Поскольку техническое решение, реализующее метод контроля доступа к создаваемым файлам авторами запатентовано [10], приведем его описание в том виде, как это сделано в [10], см. рис.2.

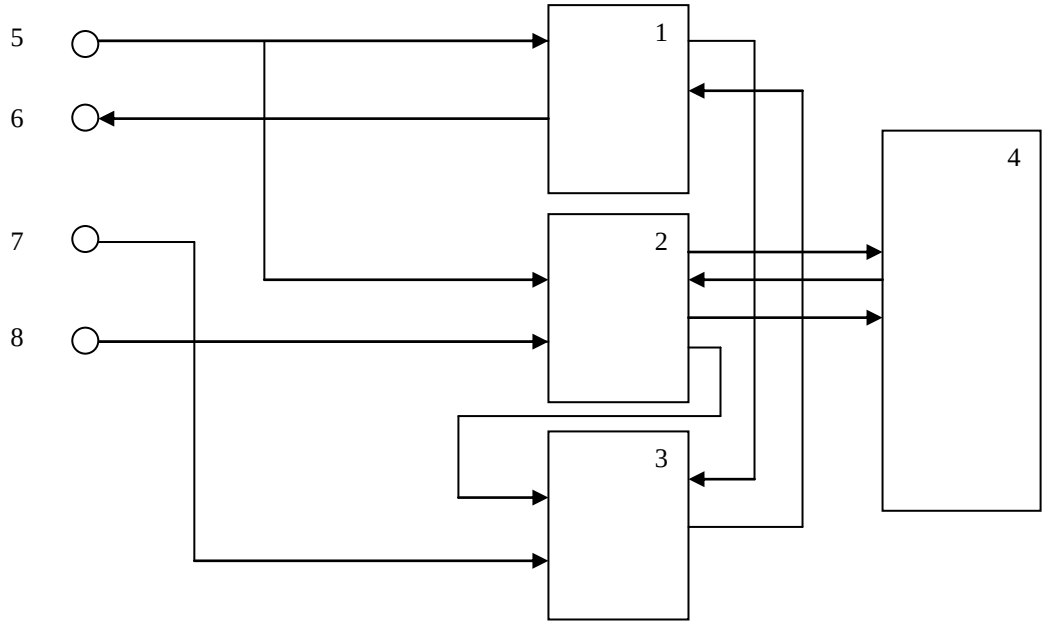

Рис.2. Система контроля доступа к создаваемым файлам на основе их автоматической разметки

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, который нас в данной работе не интересует, 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.

Отметим, что данное техническое решение позволяет не только принципиально упростить задачу администрирования, реализовать корректную разграничительную политику доступа в общем случае, за счет возможности разделения доступа ко всем файлам, в том числе, к файлам, создаваемым в каталогах, не разделяемых ОС и приложениями, например, предназначенных для хранения временных файлов (эта проблема нами исследована в [11]), но и корректно в общем случае реализовать собственно схему контроля доступа. Это обусловливается тем, что атрибуты конкретного создаваемого файла жестко привязываются к файлу, что обеспечивает защиту от обхода разграничительной политики доступа, за счет не корректной идентификации объекта доступа (существует множество способов идентификации файлового объекта, например, по длинному или короткому имени) [12].

В общем случае разграничение и контроль доступа к файлам на основе их автоматической разметки применим и для защиты статичных (системных) файлов. При этом может быть решено множество актуальнейших задач защиты информации [13]. Это решение также реализуется запатентованной нами системой [10] (в работе представлено описание работы системы [10] лишь в качестве реализации контроля и разграничения прав доступа к создаваемым файлам, что нам потребуется далее). Например, в системе защиты [2] автоматически размечаются не только создаваемые файлы с предотвращением их исполнения, но и исполняемые файлы (при их запуске), с последующим предотвращением их удаления и модификации.

В общем случае разметка файлов, с записью в их атрибуты учетной информации субъекта доступа, может осуществляться, как автоматически, так и вручную [14], что существенно расширяет возможности механизмом контроля и разграничения прав доступа к файловым объектам. Все это позволяет нам говорить в общем случае о технологии контроля и разграничения прав доступа к файловым объектам на основе их разметки.

Далее в работе нас будет интересовать реализация контроля и разграничения прав доступа к создаваемым файлам на основе их автоматической разметки.

Проиллюстрируем настройку механизма защиты, реализующего описанное выше техническое решение. Правила доступа задаются из интерфейса и отображаются в интерфейсе, приведенном на рис.3. (субъекты доступа здесь отображаются присвоенными им при создании именами, см. рис.1).

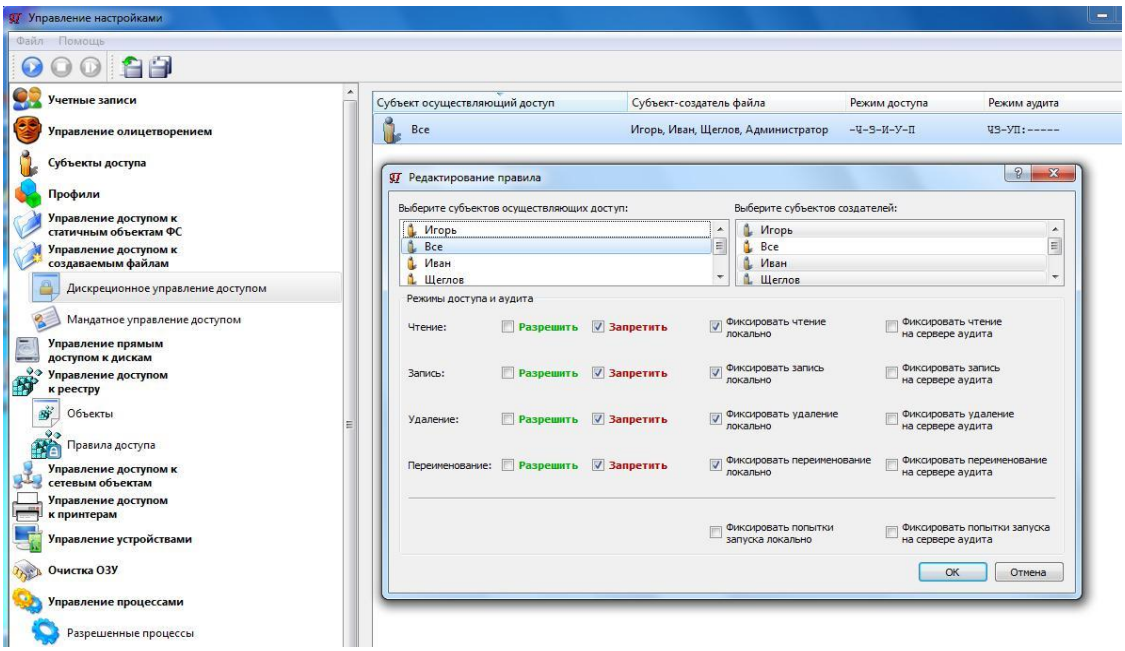

Рис.3. Задание и отображение в интерфейсе правил доступа к создаваемым файлам

В назначаемые права доступа, см. рис.3, не внесено право "исполнение" (вынесена лишь возможность аудита попыток запуска создаваемых файлов, см. рис.3) , так как запрет исполнения создаваемых файлов является, по мнению авторов, единственной обоснованной возможностью эффективной защиты от вредоносных программ [1,2]. К слову сказать, запуск создаваемых файлов предотвращается и для системных процессов, что является основой защиты от атак на повышение привилегий, состоящих в запуске внедренной вредоносной программы системным процессом (или драйвером), что становится возможным, за счет эксплуатации выявляемых уязвимостей в подобных системных субъектах.

Задание разграничительной политики доступа осуществляется следующим образом. Из списка заданных субъектов доступа, отображаемого в интерфейсе настройки правил доступа именами, см. рис.3, в поле "Выберите субъектов создателей" задаются контролируемые субъекты доступа - те субъекты, к файлам, созданным которыми, будут разграничиваться права доступа других субъектов.

Применительно к выбранному (в поле "Выберите субъектов создателей") субъекту создателю файлов назначаются права доступа к созданным 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.3. Для выбранной пары субъектов (в левом и в правом полях интерфейса), см. рис.3, назначаются правила доступа - соответствующим образом разрешаются, либо запрещаются соответствующие права доступа (чтение, запись, удаление, переименование). Заданное правило отображается соответствующей строкой в интерфейсе, см. рис.3.

Отметим, что для одноименных субъектов доступа все права доступа (естественно, кроме исполнения) разрешены по умолчанию - при их выборе откроется интерфейс, позволяющий настраивать только правила аудита. Требования же к корректности назначаемых правил доступа, реализация которых позволят построить безопасную систему (без возможности утечки прав доступа) сформулированы и обоснованы в [15].

Рассмотрим, как работает диспетчер доступа, реализующий изложенный метод контроля и разграничения прав 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 к любому файлу, диспетчером доступа анализируется наличие у него разметки. Если файл не размечен (не отнесен к создаваемым), к нему будет разрешен запрашиваемый доступ, в случае модификации этого файла, он будет автоматически размечаться. Если файл размечен, и к нему запрашивается доступ на исполнение любым субъектом (в том числе и субъектом, не заданным в разграничительной политике доступа),

данный запрос доступа будет отклонен. Иначе - запрос не на исполнение и файл был создан контролируемым субъектом доступа (который был задан в поле интерфейса "Выберите субъектов создателей", см. рис.3), то диспетчером анализируется соответствие запроса заданным правилам доступа. В результате проведенного сравнения, запрошенный доступ диспетчером либо разрешается, либо отклоняется. При модификации такого созданного файла он будет наследовать учетную запись модифицирующего его субъекта, в случае, если создание файлов эти субъектом контролируется. Если же файл был создан (размечен, как создаваемый) не контролируемым субъектом доступа, его будет запрещено исполнять, но в отношении него не будут разграничиваться права доступа.

В состав средства защиты включена утилита, позволяющая администратору просмотреть разметку созданных файлов (для каждого созданного файла отображаются учетные данные субъекта доступа, создавших файлы - учетная запись пользователя и полнопутевое имя процесса) из окна интерфейса, представленного на рис.4.

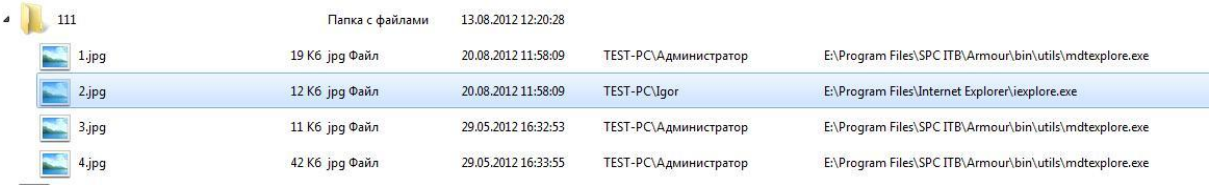

Рис.4. Отображение разметки созданных файлов

На примере проиллюстрируем простоту администрирования представленного средства защиты при решении рассматриваемых в работе задач изолирования обработки данных критичными приложениями. В качестве примера критичного приложения, работу которого будем изолировать в системе, рассмотрим интернет-браузер. Разграничительную политику доступа проиллюстрируем на примере решения задачи защиты от атак на интернет-браузер Internet Explorer (далее IE).

Для решения данной задачи защиты создадим двух субъектов доступа - "Все" и "IE", см. рис.5, и зададим для них правила доступа, представленные на рис.6.

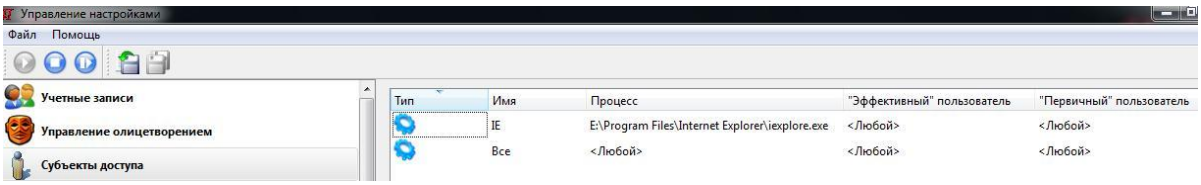

Рис.5. Отображение заданных субъектов доступа

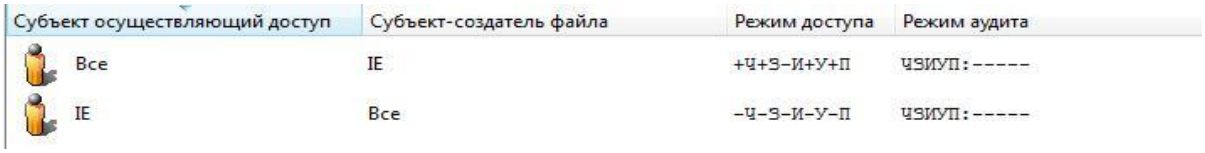

Рис.6. Отображение заданных правил доступа

Рассмотрим, что мы получим в результате реализации данной простейшей в настройке 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), включая запуск приложения и системными правами, 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. В общем случае можно 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, который может быть внедрен в систему критичным приложением, могут быть наделены вредоносными свойствами.

В порядке замечания отметим, что рассмотренные принципы контроля доступа к создаваемым файлам, основанного на их автоматической разметки, могут быть применены и для реализации принудительного шифрования создаваемых файлов контролируемыми субъектами доступа. Принципиальным в данном случае является то, что любой файл, создаваемый от лица соответствующего субъекта (при задании контролируемого субъекта доступа также может учитываться и учетная запись пользователя, и процесс), где бы он не создавался, будет зашифровываться, что гарантирует хранение критичной информации в компьютерной системе и на внешних накопителях только в зашифрованном виде. Для выбора же ключа шифрования для последующего расшифрования файла используется автоматическая разметка файла, определяющая, каким субъектом доступа создан этот зашифрованный файл. Это техническое решение, позволяющее получить принципиально новые свойства защиты, авторами также запатентовано [16].

3. Метод и реализация контроля доступа к буферу обмена.

Поскольку контроль и разграничение прав доступа к данным, сохраняемым в буфере обмена, можно рассматривать, как контроль доступа к создаваемым данным, здесь применимы принципы реализации разграничительной политики доступа, изложенные ранее. Аналогичным образом, создаваемые данные автоматически размечаются - диспетчером доступа запоминается, каким субъектом записаны данные в буфер обмена. Последующий же доступ к сохраненным в буфере обмена данным разграничивается между субъектами по заданным администратором правилам доступа. Опять же объект доступа исключен из разграничительной политики, разграничения прав доступа задаются исключительно между субъектами, не разграничиваются права доступа по записи (созданию) данных в буфер обмена - разграничивается последующий доступ к созданным подобным образом данным.

Рассмотрим практическую реализацию механизма защиты. 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.1, 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 они реализованы в отношении создаваемых файлов.

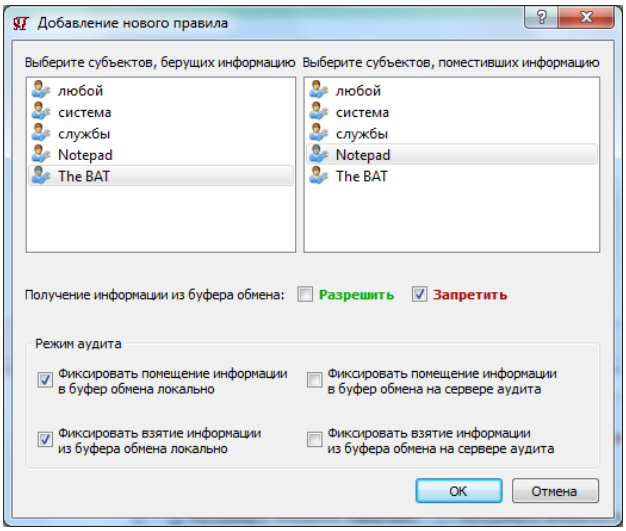

Рис.7. Задание правил доступа к буферу обмена

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 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.5, рис.6, 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.5, следует запретить доступа к данным, записываемым в буфер обмена субъектом доступа "Все", см. рис.5.

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.

Как видим, предложенные авторами принципы контроля и разграничения прав доступа к создаваемым файлам могут быть использованы не только применительно к защите файловых объектов - они могут быть реализованы при построении защиты любых создаваемых в системе объектов, что позволяет в общем случае говорить о технологии контроля и разграничения прав доступа к создаваемым объектам.

Заключение.

В заключении отметим, что в работе рассмотрено решение задачи изолирования обработки данных критичными приложениями, где под критичными мы понимали, как вредоносные программы, так и программы (приложения), которые по разным причинам могут наделяться вредоносными свойствами, позволяющими злоумышленнику осуществить несанкционированный доступ с использованием этих приложений к обрабатываемым в компьютерной системе конфиденциальным данным. Однако постановка задачи защиты, для решения которой может использоваться рассмотренная технология и методы защиты, может быть принципиально иной. Если рассматривать в качестве критичных приложений те приложения, которые могут быть использованы злоумышленником для хищения данных, в рассматриваемом случае - санкционированным пользователем - инсайдером, например, приложения, позволяющие передавать обрабатываемые в компьютерной системе конфиденциальные данные во внешнюю сеть, то может ставиться и, по средством изолирования обработки данных приложениями, решаться задача защиты от хищения конфиденциальных данных инсайдерами. Однако детальное рассмотрение этой задачи защиты информации и ее решения выходит за рамки настоящей работы.

Литература.

1. 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.

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

3. 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.

4. 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.

5. Маркина Т.А., Щеглов А.Ю. Метод защиты от атак типа drive-by загрузка. - Известия ВУЗзов. Приборостроение. - 2014. - Т. 57. - № 4. - С. 15-20.

6. Щеглов К.А., Щеглов А.Ю. Эксплуатационные характеристики риска нарушений безопасности информационной системы // Научно-технический вестник информационных технологий, механики и оптики. - 2014. - Т. 89. - № 1. - С. 129-139.

7. 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.

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 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.

10. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к файлам на основе их автоматической разметки. Положительное решение на выдачу патента на изобретение по заявке №2013112048/08(017910) от 18.03.2013.

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

12. Щеглов К.А., Щеглов А.Ю. Способ задания и хранения прав доступа субъектов к файловым объектам // Вестник компьютерных и информационных технологий. - 2013. - № 12. - С. 45-49.

13. Щеглов К.А., Щеглов А.Ю. Принципы и методы контроля доступа к статичным файловым объектам с исключением из разграничительной политики доступа сущности "объект доступа" // Вестник компьютерных и информационных технологий. - Москва, 2013. - № 8. - С. 53-59.

14. Щеглов К.А., Щеглов А.Ю. Метод контроля доступа к файлам на основе их ручной и автоматической разметки // Известия ВУЗов. Приборостроение. - 2014. - Т. 57. - № 7. - С. 41-45.

15. 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.

16. 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.