ЗАЩИТА ОТ АТАК НА УЯЗВИМОСТИ ПРИЛОЖЕНИЙ

Введение.

Одной из ключевых задач защиты информации в современных условиях становится защита от атак на уязвимости приложений. Чтобы оценить актуальность этой задачи защиты, достаточно обратиться к соответствующей статистике, которая, например, представлена в [1].

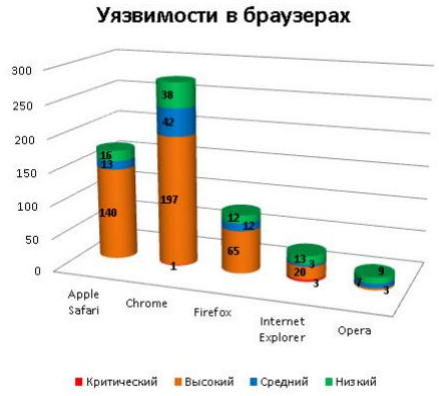

Рис.1. Статистика обнаруженных уязвимостей в браузерах за 2011 г.

При этом отметим, что в качестве критичных уязвимостей, атаки на которые необходимо предотвращать средством защиты, следует рассматривать, по крайней мере, уязвимости, характеризуемые критической, высокой и средней степенями опасности, классификация уязвимостей приведена в [1] (например, к средней степени опасности относятся уязвимости, которые позволяют удаленный отказ в обслуживании, неавторизованный доступ к данным или выполнение произвольного кода при взаимодействии пользователя, например, подключение к злонамеренному серверу уязвимым приложением).

Оценка готовности приложений к безопасной эксплуатации, с учетом статистики выявляемых в них уязвимостей, с использованием соответствующих математических моделей, была нами получена в [2]. Например, зависимость изменения данной характеристики от изменения интенсивности выявляемых уязвимостей в приложениях (при средней

продолжительности исправления уязвимости 1 месяц), представлена на рис.2.

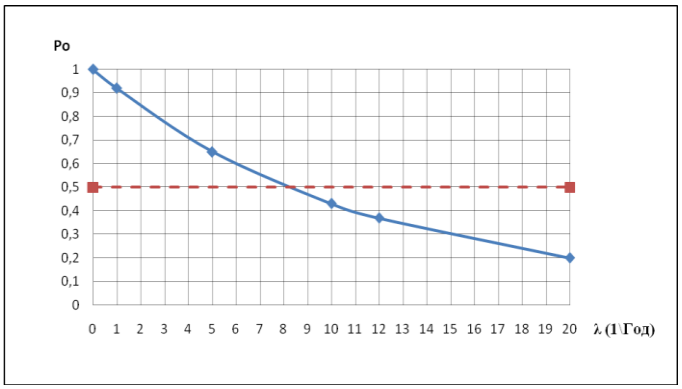

Рис.2. Влияние на эксплуатационную безопасность приложений интенсивности обнаружения в них уязвимостей

Чтобы оценить всю критичность сложившейся ситуации с безопасностью существующих приложений, достаточно вновь обратиться к рис.1, но уже с учетом исследований, проиллюстрированных на рис.2.

Теперь, что касается фундаментальности исследуемой проблемы. Достаточно очевидно, что программные средства из года в год только усложняются, при этом сроки их разработки, диктуемые конкурентным рынком, сокращаются, как следствие, ошибок в программных средствах становится больше, а исправлять их становится все сложнее. Это объективная реальность. С учетом сказанного, можно предположить, что из года в год, актуальность проблемы защиты от атак на уязвимости приложений, будет лишь возрастать, что и обусловливает фундаментальность данной проблемы.

1. Предлагаемый подход к защите.

1. Естественно, в первую очередь, при реализации защиты информации, возникает задача защиты (которую мы и будем рассматривать в работе) от, так называемых, целевых атак, атак на компьютерную систему, реализуемых с определенной конечной целью. Основными целями атак являются [2]:

- цель 1 - нарушение конфиденциальности обрабатываемой информации (хищение информации);
- цель 2 - нарушение целостности обрабатываемой информации (модификация – подмена информации, дезинформация);
- цель 3 - нарушение доступности обрабатываемой информации (уничтожение информации, либо вывод из строя информационной системы).

2. Основу защиты информации в компьютерной системе от несанкционированного доступа составляет реализация разграничительной политики доступа к ресурсам. Именно это решение мы и рассмотрим в работе. Однако в нашем случае, в качестве субъекта доступа уже выступает сущность "процесс" (приложение). Необходимость реализации самостоятельной разграничительной политики доступа для процессов (приложений) обусловливается тем, что в современных ОС любой запускаемый процесс наследует права доступа к ресурсам пользователя, запустившего данный процесс, т.е. все процессы (приложения), запускаемые одним и тем же пользователем, вне зависимости от статистики их уязвимости и критичности атак на уязвимости приложений, будут обладать одними и теми же правами доступа к защищаемым ресурсам.

3. Защита должна строиться в предположении о том, что нам неизвестно какая уязвимость присутствует и/или будет обнаружена в приложении в ближайшее время, к каким возможностям она приведет. Т.е. будем считать, что приложение, запущенное интерактивным пользователем, в результате эксплуатации обнаруженной в нем уязвимости, может осуществить любое несанкционированное действие под управлением этого пользователя.

Таким образом, в работе излагается подход к защите от целевых атак на уязвимости приложений, основанный на реализации разграничительной политики доступа к ресурсам для субъекта доступа процесс.

Замечание. Излагаемые в работе подходы к защите от атак на уязвимости приложений авторами апробированы и будут проиллюстрированы на примере технического решения КСЗИ "Панцирь+" для ОС Microsoft Windows.

Замечание. Реализацию разграничительной политики доступа процессов к ресурсам будем в работе иллюстрировать на примере решения одной из наиболее актуальных практических задач защиты - защиты от атак на уязвимости интернет-браузеров (на примере широко используемого браузера -IE). Понятно, что это лишь пример, все излагаемые в работе подходы могут аналогично использоваться при реализации защиты от атак на уязвимости иных приложений.

2. Определение субъекта доступа в разграничительной политике.

Субъекты доступа в общем случае должны назначаться тремя сущностями – исходное имя (SID) пользователя, эффективное имя пользователя, имя процесса – полнопутевое имя исполняемого файла процесса, из интерфейса, представленного на рис.3 (в первую очередь, как отмечали, интерес здесь для нас представляет сущность "процесс", как основной элемент разграничительной политики доступа к ресурсам). Однако не будем забывать, что одни и те же механизмы защиты должны использоваться для реализации разграничений прав доступа и для процесс (в нашем случае), и для пользователей. Обоснование необходимости задания субъекта доступа в общем случае тремя сущностями приведено в [3-5]. При задании же сущности "процесс" в субъекте доступа могут использоваться маски и переменные среды окружения, см. рис.1.

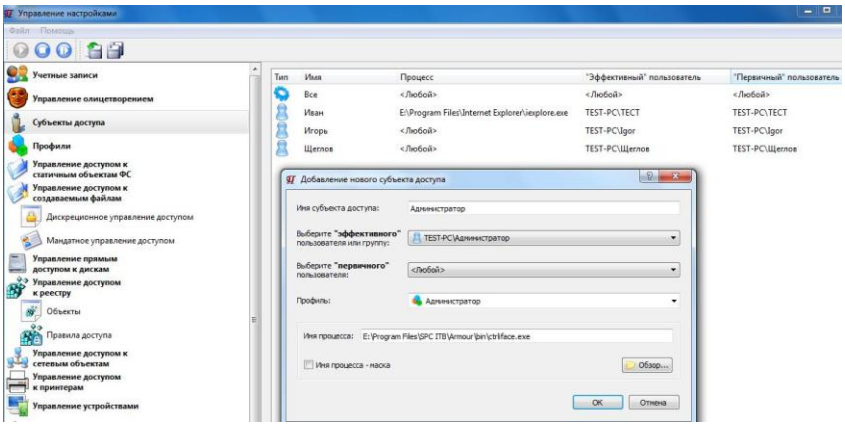

Рис.3. Задание и отображение в интерфейсе субъектов доступа

2. Защита от атак на нарушение конфиденциальности, доступности и целостности обрабатываемой информации.

В [6,7] нами введена классификация файловых объектов, они подразделены на статичные и создаваемые. Статичные - это те, которые присутствуют в системе на момент реализации администратором разграничительной политики доступа к ресурсам, в первую очередь, это системные объекты. Обрабатываемая же в компьютерной системе информация (защита которой нас здесь интересует) сохраняется в создаваемых в процессе работы пользователя файлах.

Принципы контроля доступа (разграничения прав доступа) к создаваемым файловым объектам предложены нами в [6,7], реализация метода контроля доступа и сформулированные требования к корректности реализации разграничительной политики доступа рассмотрены, например, в [5].

Основная идея данного решения состоит в исключении сущности "объект доступа" из разграничительной политики, как таковой (ввиду ее отсутствия на момент задания администратором правил доступа к ресурсам). Разграничение (контроль доступа) реализуется непосредственно между субъектами доступа к создаваемым ими файлам.

Замечание. Уточним, что разграничительная политика в любом случае заключается в реализации разграничений прав доступа субъектов к объектам (в данном случае, к файлам), здесь же речь идет об исключении сущности «объект доступа» из назначаемых администратором правил доступа. В правилах указывается то, какие права доступа имеет субъект к файлам, созданным иными субъектами – в правилах отсутствует сущность «объект доступа».

Реализуется контроль доступа следующим образом. При создании субъектом нового файла, средством контроля доступа (диспетчером доступа) создаваемый файл автоматически размечается - файлом наследуется учетная информация субъекта доступа (определяемая соответствующими тремя сущностями), создавшего этот файл. Данная информация размещается в атрибутах созданного файла.

При запросе же доступа к любому файлу, средство контроля доступа анализирует наличие, а при наличии, содержимое унаследованной файлом учетной информации создавшего его субъекта доступа. Это осуществляется, по средством считывания и анализа атрибутов файла, к которому запрошен доступ.

В соответствии с заданными администратором правилами доступа, задаются исключительно между субъектами доступа из интерфейса, см. рис.4, диспетчер доступа предоставляет запрошенный субъектом доступ, либо отказывает в нем, признавая тем самым запрос доступа несанкционированным.

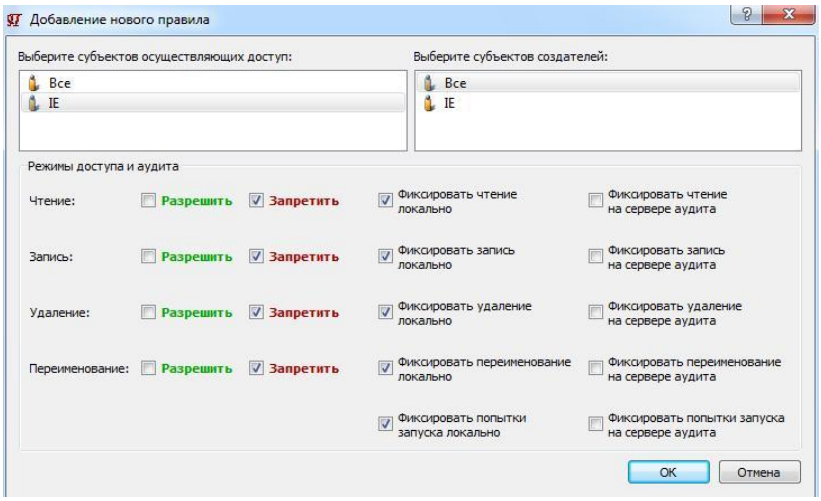

Рис.4. Задание и отображение в интерфейсе правил доступа к создаваемым файлам

В двух словах, о назначении правил доступа. В правом столбце интерфейса – «Выберите субъектов создателей», см. рис.4, задаются те субъекты (из заведенных администратором ранее из интерфейса, представленного на рис.3), последующий доступ к файлам, создаваемым которыми, будет контролироваться (разграничиваться). Для каждого заданного в правом столбце интерфейса субъекта, в левом столбце интерфейса – «Выберите субъектов, осуществляющих доступ», задаются субъекты, которым разрешается доступ к файлам, создаваемым заданным субъектом-создателем, и назначаются права доступа к этим файлам (чтение, запись, переименование, удаление), а так же режимы аудита. Право доступа "исполнение" запрещено "по умолчанию", и, как следствие, не вынесено в интерфейс, см. рис.4 (запрет исполнения создаваемых файлов является основой эффективной защиты от вредоносных программ [8].

Рассмотрим решение задачи защиты, где в качестве уязвимого приложения будем рассматривать интернет-браузер IE. Заведем из интерфейса, см. рис.3, двух субъектов доступа - "Все" и "IE", см. рис.5, и зададим из интерфейса, см. рис.3, правила доступа, см. рис.6.

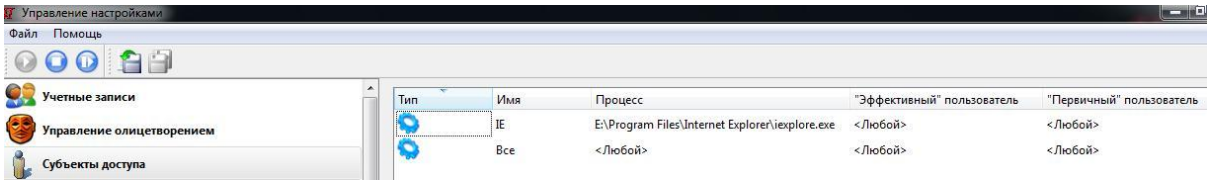

Рис.5. Заданные субъекты доступа

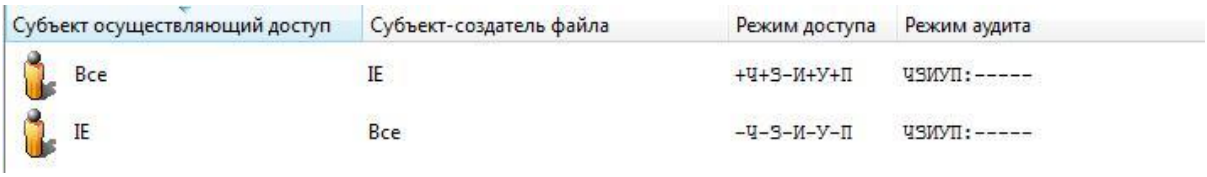

Рис.6. Заданные правила доступа

Рассмотрим, что мы получим в результате. Интернет-браузер, вне зависимости от того, какими несанкционированными свойствами он будет наделен, не получит доступ к конфиденциальной информации, обрабатываемой на компьютере - к создаваемым иными приложениями файлам (его работа в информационной системе в этой части изолирована). Предотвращается возможность нарушения конфиденциальности, целостности и доступности (в части защиты от удаления) обрабатываемой на компьютере информации, в результате реализации атаки на уязвимость интернет-браузера.

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, 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 полный доступ иных приложений к файлам, создаваемым браузером, по крайней мере тех приложений, которые при прочтении вредоносного файла могут быть наделены вредоносными свойствами. Эти вопросы исследованы в [9], где, в том числе,

представлена корректная модель контроля доступа, приведено ее обоснование.

3. Защита от атак на системные ресурсы.

Если же мы говорим о контроле (разграничении прав) доступа к системным ресурсам - к статичным объектам [4] (в общем случае, к системным файловым объектам, объектам реестра ОС, к устройствам, к сетевым ресурсам и т.д.), то при реализации разграничительной политики доступа субъектов к объектам, здесь уже необходимо задать объекты, доступ к которым будет разграничиваться, что, например, применительно к файловым объектам (включая внешние файловые накопители) реализуется из интерфейса, представленного на рис.7. Соответственно требуется задать и правила доступа субъектов, заданных для системы из интерфейса, представленного на рис.3, к объектам, что реализуется из интерфейса, представленного на рис.8.

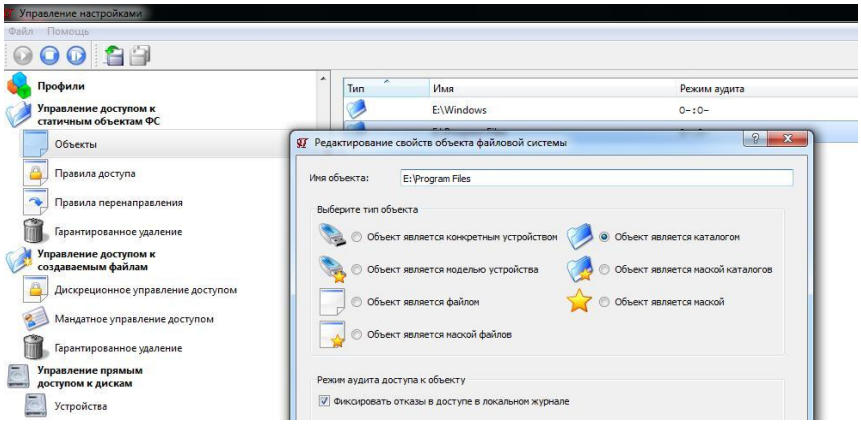

Рис.7. Интерфейс задания файлового объекта доступа

Замечание. Объект доступа может задаваться, как своим полнопутевым именем, так и маской, а также переменными среды окружения.

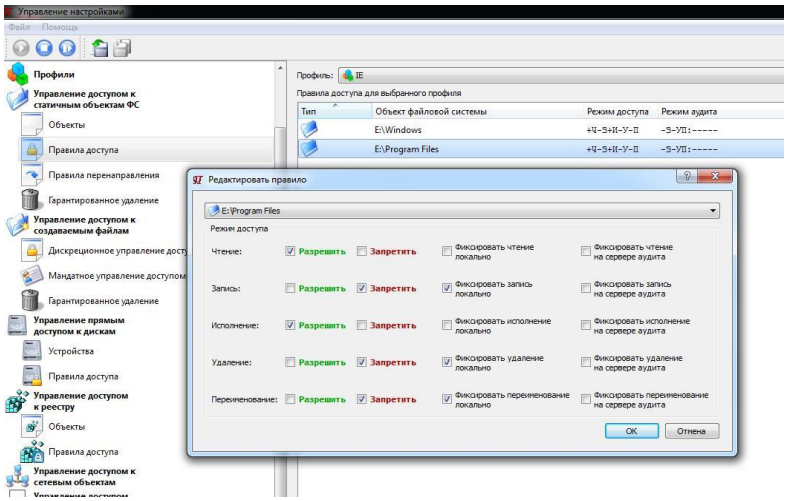

Рис.8. Интерфейс задания прав доступа субъекта к объекту

Рассмотрим реализацию защиты системных ресурсов, на примере системных файловых объектов и объектов реестра ОС, от целевых атак на уязвимости интернет-браузера (приложения). Соответствующие разграничительные политики для субъекта IE приведены на рис.9 и на рис.10.

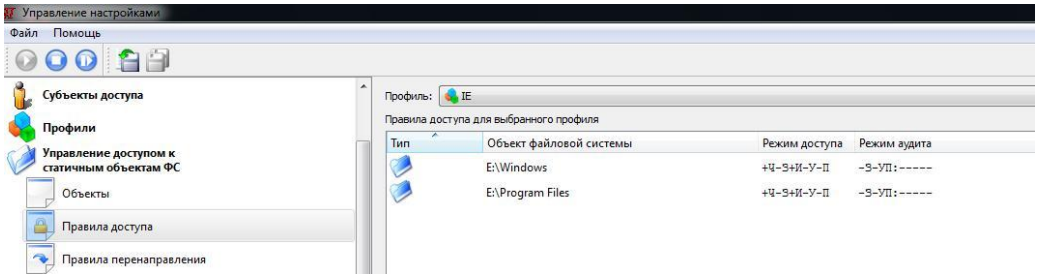

Рис.9. Заданные правила доступа к системным файловым объектам

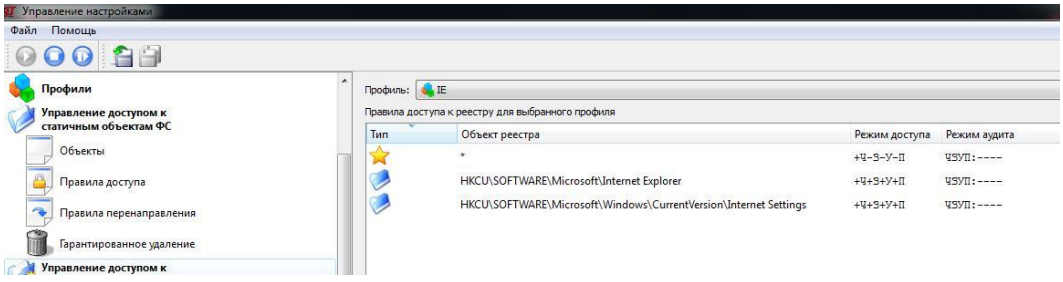

Рис.10. Заданные правила доступа к объектам реестра ОС

Оценим получаемый результат. Разграничительной политикой доступа к статичным (системным) файловым объектам, см. рис.9, предотвращается возможность несанкционированной модификации

приложением IE исполняемых файлов и файлов настройки ОС и приложений. Разграничительной же политикой доступа к объектам реестра ОС, см. рис.10, IE разрешается доступ только к необходимым ему для корректного функционирования объектам реестра.

Отметим, что в данном случае решается задача защиты от атак на уязвимости приложения, реализуемых с цель нарушения доступности обрабатываемой информации, за счет вывод из строя информационной системы, в результате уничтожения/модификации системных ресурсов.

4. Дополнительные меры защиты.

Напомним, что исходным посылом при реализации защиты от атак на уязвимости приложений исходно являлась реализация разграничительной политики доступа к ресурсам, в предположении о том, что приложение, запущенное интерактивным пользователем, в результате эксплуатации обнаруженной в нем уязвимости, может осуществить любое несанкционированное действие под управлением этого пользователя. это обусловливает целесообразность реализации ряда дополнительных мер, направленных на противодействие обходу злоумышленником реализованной разграничительной политики доступа к создаваемым и статичным файловым объектам. Основными способами обхода разграничительной политики доступа к ресурсам на практике сегодня являются повышение привилегий пользователя (в том числе, получение прав администратора, либо системного пользователя), за счет олицетворения (штатная возможность современных ОС [3]) уязвимого процесса (точнее потока, порождаемого процессом) с правами другого пользователя, и прямой доступ к диску (не к файловому объекту, к которому разграничиваются права доступа).

Соответствующие разграничительные политики доступа для субъекта IE в части предотвращения прямого доступа приложением к диску, представлена на рис.11, в части предотвращения возможности

олицетворения приложения, запускаемого из под одного пользователя, с иным пользователем (в том числе, привилегированным), представлена на рис.12.

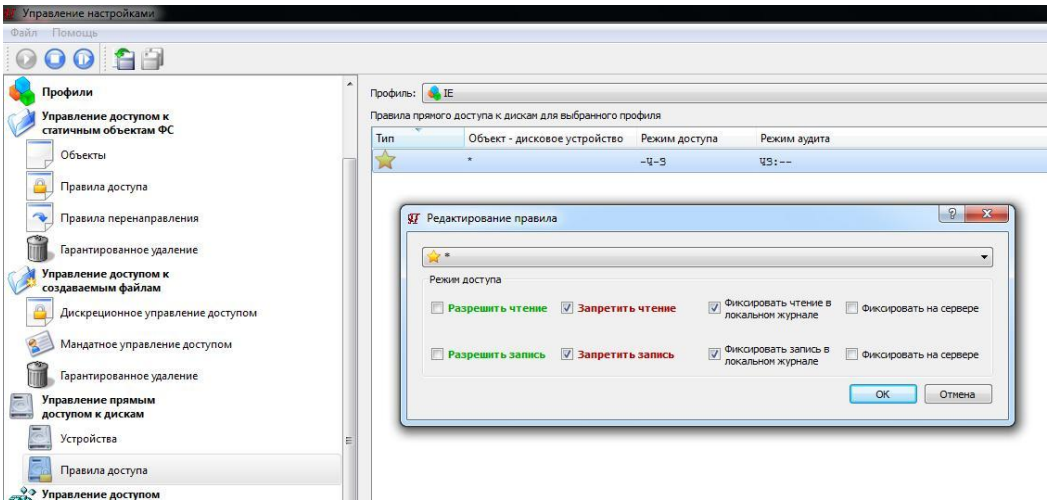

Рис.11. Задание правил прямого доступа приложения к дискам

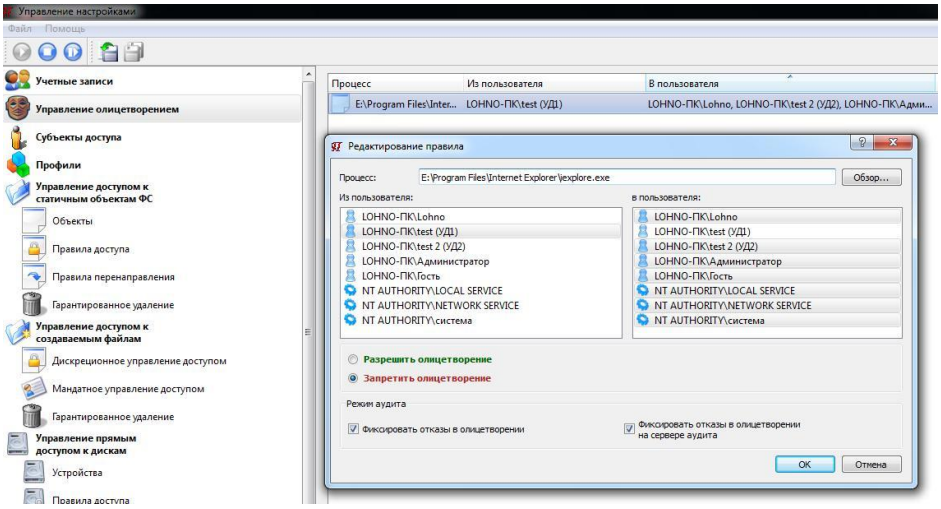

Рис.12. Задание правил олицетворения приложения с иными пользователями

Отметим, что из интерфейса, приведенного на рис.11, целесообразно настроить правила контроля доступа, противодействующие прямому доступу IE к любому диску (целесообразно запретить прямой доступ не только к жесткому диску, но и к любому внешнему накопителю, при этом объект доступа в разграничительной политике задается маской "Все" - обозначение "*", см. рис.11), а из интерфейса, приведенного на рис.12, целесообразно настроить правила контроля, противодействующие

смене имени пользователя, от "лица" которого запущен IE, на любое иное имя пользователя, от "лица" которого далее IE будет функционировать (целесообразно запретить любую смену имени (SID) пользователя для приложения IE).

Заметим, что существуют и иные меры дополнительной защиты, правда, уже не столь актуальные, как изложенные, которые, ввиду ограничения на объем рукописи, не рассмотрены в данной работе.

Заключение.

В заключении к работе акцентируем внимание читателя на следующих важных моментах:

1. Как видим, одна из актуальнейших современных задач защиты информации может быть решена, причем решена эффективно. Однако решение этой задачи требует пересмотра основных устоявшихся принципов реализации разграничительной политики доступа к ресурсам, требует реализации новых подходов к защите информации от несанкционированного доступа.
2. Изложенный подход к защите, это не некая теоретическая возможность, все технические решения реализованы и апробированы.
3. Изложенный подход к защите универсален в том смысле, что его эффективное применение возможно не только с целью защиты от атак, направленных на эксплуатацию уязвимости приложений (что рассмотрено нами в данной работе), но и целью защиты от любого рода атак, связанных с наделением приложений несанкционированными возможностями (за счет макро-вирусов, вредоносных скриптов и т.п. [9]) и последующей эксплуатацией этих возможностей.

Литература.

1. Статистика уязвимостей за 2011 год от Лаборатории Касперского [Электронный ресурс]//URL:/ http://it-sektor.ru/statistika-uyazvimosteyi-za-2011-god-ot-laboratorii-kasperskogo.html.

2. ГОСТ Р 53114-2008. Защита информации. обеспечение информационной безопасности в организации, 2009.

2. К.А. Щеглов, А.Ю. Щеглов. Защита от атак на уязвимости приложений. Модели контроля доступа // Вопросы защиты информации. - 2013. - Вып. 101. - № 2. - С. 36-43.

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

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

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

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

7. К.А. Щеглов, А.Ю. Щеглов. Модель контроля доступа к создаваемым файловым объектам // Изв. ВУЗов. Приборостроение. - 2012. - Т. 55. - № 10. - С. 37-40.

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

9. К.А. Щеглов, А.Ю. Щеглов. Защита от атак со стороны приложений, наделяемых вредоносными функциями. Модели контроля доступа // Вопросы защиты информации. - 2012. - Вып. 99. - № 4. - С. 31-36.