ВОПРОСЫ КОРРЕКТНОСТИ РЕАЛИЗАЦИИ СЕССИОННОГО КОНТРОЛЯ ДОСТУПА

Введение

Существуют две модели контроля доступа, предполагающие создание режимов обработки информации средствами защиты - ролевая и сессионная. Ролевая модель контроля доступа (Role-Based Access Control - RBAC) [1] предназначена для формирования режимов обработки информации пользователями в рамках выполняемых ими ролей в информационной системе, с целью предоставления пользователю права доступа только к необходимым объектам, включая необходимую информацию, для выполнения им соответствующей роли. Разграничительная политика доступа в данном случае строится с использованием метода дискреционного контроля доступа (корректнее называть избирательным при реализации принудительного управления потоками информации [2]).

Сессионная модель контроля доступа [3] предназначена для формирования и разделения режимов обработки на одном компьютере (в общем случае – в информационной системе) одним и тем же пользователем информации различных уровней конфиденциальности, с целью защиты от утечки конфиденциальной информации в результате обработки им на том же компьютере в совершенно ином (менее защищенном) режиме открытой, либо меньшего уровня конфиденциальности, информации. Т.е. здесь также создаются различные режимы обработки информации, возможность же категорирования информации при реализации данной модели позволяет строить разграничительную политику доступа с использованием метода мандатного контроля доступа – на основе применения меток безопасности (или мандатов) [3].

Данные модели имеют принципиальное отличие – это ни в коем случае не альтернативные решения, состоящее в требовании к изолированию для сессионного контроля доступа режимов обработки информации различных уровней конфиденциальности - сессий, с целью решения наиболее актуальной современной задачи защиты информации – защиты от утечек конфиденциальной информации

при возможности обработки на том же компьютере открытой информации, уже в незащищенном (либо слабо защищенном) режиме.

Заметим, что актуальность данной задачи породила целое направление в защите информации – создание, так называемых, DLP-систем [4], основанных на контетной фильтрации исходящих из защищаемой системы потоков информации. Понятно, что эффективность подобных решений, как и иных методов контроля, даже теоретически не может быть высокой.

С целью упрощения задачи администрирования в ролевой модели контроля доступа в разграничительной политике доступа в качестве субъекта доступа используется сущность «роль» - права доступа к объектам назначаются не для учетных записей, а для ролей, что упрощает задачу включения/исключения пользователей в соответствующие роли. При этом одна и та же учетная запись может включаться в различные роль.

Рассмотрим, как ключевое отличие сессионного контроля доступа, состоящее в необходимости изолирования сессий – изолирования обработки информации различных уровней конфиденциальности на одном вычислительном средстве, сказывается на вопросах корректности его практической реализации.

Ключевая проблема использования сущности сессия в качестве субъекта доступа в разграничительной политике

Как отмечали, основу сессионной модели составляет реализация метода мандатного контроля доступа, состоящего в следующем. Иерархическими метками безопасности (мандатами) определяется уровень конфиденциальности информации и уровень допуска пользователя к конфиденциальной информации. Будем считать, что чем выше уровень допуска к информации субъекта и уровень конфиденциальности объекта, тем меньше их порядковый номер в линейно упорядоченных множествах субъектов и объектов - $C = \{C1,\ldots, Cl\}$ и $O = \{O1,\ldots, Ol\}$), и тем меньшее числовое значение метки безопасности Mi, $i = 1, \ldots, l$ им присваивается, т.е.: $M1 < M2 < M3 < \ldots < Ml$.

Замечание. В общем случае одна метка присваивается группе равноправных (имеющих одинаковый уровень допуска к информации) субъектов и группе объектов одного уровня конфиденциальности.

Используем следующие обозначения:

- Мс – метка безопасности субъекта (группы субъектов) доступа;
- Мо – метка безопасности объекта (группы объектов) доступа.

Реализация мандатного контроля доступа, применяемого с целью защиты от нарушения конфиденциальности информации, состоит в проверке любого запроса доступа на непротиворечивость следующим правилам:

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

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

Иногда также разрешается запись при условии Мс > Мо.

Теперь предположим, что с целью реализации сессионного контроля доступа, отличающегося от мандатного тем, что один и тот же сотрудник предприятия может работать в различных изолированных, поскольку в различной степени защищенных, режимах с информацией различного уровня конфиденциальности - сессиях, в разграничительную политику доступа в качестве субъекта доступа включается сессия – именно сессии, а не учетной записи будет назначаться метка безопасности – метка безопасности сессии Мiсес, i = 1, …, l, которая и будет использоваться при контроле непротиворечивости запроса доступа соответствующим правилам. Пусть максимально разрешенный уровень доступа к информации сотрудника определяется неким значением метки безопасности Мi. Естественно, он может иметь доступ к информации, которой присвоена метка не ниже Мi.С учетом сказанного, данный сотрудник сможет работать с сессиями, определяемыми условием: Мiсес ≥ Мi.

Таким образом, входя в систему под одной и той же учетной записью, сотрудник может выбрать (при необходимости, сменить) сессию для обработки информации соответствующего уровня конфиденциальности, чем, к слову сказать, разрешается ключевое противоречие метода мандатного контроля доступа,

состоящее в том, что любую информацию он может сохранить только с уровнем конфиденциальности соответствующем его уровню допуска, что следует из второго правила. Ключевым моментом здесь является работа пользователем в различных сессиях под одной и той же учетной записью, именно с этой целью в разграничительную политику доступа в качестве субъекта доступа и включается сущность сессия – для упрощения задачи администрирования, и именно с этим связаны и фундаментальные противоречия подобной реализации сессионного контроля доступа. Рассмотрим их по порядку.

Чтобы говорить о потенциальном упрощении задачи администрирования необходимо рассмотреть альтернативное решение. А альтернативным решением будет реализация метода мандатного контроля доступа с созданием сотруднику различных учетных записей (можно с одним и тем же паролем на вход в систему) для его работы в различных сессиях. Выбор сессии при этом осуществляется выбором учетной записи, под которой сотрудник входит в систему, а смена сессии реализуется штатной возможностью смены пользователя. Т.е. при такой реализации сессионного контроля доступа потребуется ввести дополнительные учетные записи для каждого сотрудника, для работы ими в различных сессиях. Отметим, что, если рассматривать наиболее типовой случай – случай защиты персонального компьютера, на котором только один сотрудник может обрабатывать открытую или конфиденциальную информацию, дополнительная настройка сведется к созданию лишь одной дополнительной учетной записи, т.е. о каком-либо серьезном усложнении администрирования здесь говорить не приходится.

Совсем иное дело включение в разграничительную политику доступа сущности сессия. При рассмотрении подобной реализации сессионного доступа необходимо учитывать, что большинство приложений в процессе работы осуществляет запись/чтение конфигурационных файлов под учетной записью интерактивного пользователя, запустившего это приложение. Как следствие, приложениями будет осуществлять доступ к одним и тем же файлам в различных сессиях, поскольку доступ будет осуществляться под одной учетной записью. Если запретить подобный доступ приложениям, большинство из них не сможет корректно функционировать,

т.к. не сможет создавать конфигурационные файлы, при разрешении же подобного права доступа вообще теряется смысл в реализации сессионного контроля доступа, основным требованием к которому является изолирование обработки данных в различных сессиях.

Остается одна непротиворечивая возможность разрешения рассматриваемой проблемы - это реализация предложенного нами метода контроля доступа перенаправлением запросов доступа. Реализующее его техническое решение нами запатентовано [5]. Суть данного метода состоит в том, что для файлов или папок, доступ к которым необходимо разделить между субъектами, создаются их копии, и задаются правила переадресации запросов доступа к соответствующим копиям разделяемых объектов. Запрос доступа субъекта к объекту, поступающий от приложения к системе, перехватывается средством защиты, анализируется, и в соответствии с заданными правилами перенаправляется в требуемую копию, при этом в запросе доступа полнопутевое имя объекта заменяется на имя требуемой копии объекта, после чего уже запрос доступа передается системе.

В порядке замечания отметим, что данный метод защиты, во-первых, может использоваться для решения множества задач, т.к. подобным образом могут перенаправляться и запросы доступа к исполняемым файлам, в частности, могут решаться задачи виртуализации системных средств и приложений [6]. Во-вторых, как показано в [7], данный метод вообще может позиционироваться в качестве самостоятельного метода контроля доступа – им могут быть решены все задачи, решаемые методом дискреционного контроля доступа. При этом данный метод имеет принципиальное отличие от метода дискреционного контроля, состоящее в том, что запрет доступа к объекту реализуется перенаправлением доступа к иному объекту, что, в частности может использоваться при реализации защиты системных ресурсов, при запрете доступа к которым система или приложения не могут корректно функционировать.

Техническая реализация метода сессионного контроля доступа с решением задачи перенаправления запросов доступа к разделяемым подобным образом файловым объектам нами запатентована [8].

Как видим, с учетом множества используемых в информационной системе приложений, каждое из которых должно работать со своими конфигурационными файлами, основная задача, для решения которой в разграничительную политику доступа может включаться сущность сессия – задача упрощения администрирования (поскольку никаких иных преимуществ это не дает), не то, чтобы была решена – она многократно усложнилась, что позволяет сделать вывод о том, что какого-либо практического смысла данный подход к реализации сессионного контроля доступа не имеет. Невольно при этом возникает вопрос – а что делать с иными объектами, которые могут использоваться для обмена информацией, например, с объектами реестра ОС, также аналогичным образом разделять? Ведь задача сессионного контроля доступа – это отнюдь не задача разграничения прав доступа только к файловым объектам (хоть именно в этом и состоит основная сложность ее настройки) – это, как отмечали [3], задача формирования и разделения различных режимов обработки информации различных уровней конфиденциальности, с предотвращением перевода обработки информации в менее защищенный режим, с целью защиты от ее утечки. Но гораздо хуже в данном случае иное.

Любая дополнительная защита должна усиливать, а ни в коем случае не ослаблять исходный уровень защищенности системы, что можно позиционировать в качестве основополагающего принципа построения добавочных средств защиты (в данном случае добавочных, поскольку средствами современных ОС сессионный контроль доступа реализован быть не может). При рассматриваемом же подходе к реализации метода сессионного контроля доступа отрицается основополагающий подход к построению защиты современных операционных систем, заключающийся в реализации разграничений доступа между учетными записями (между пользователями), с целью защиты от несанкционированного (не подконтрольного администратору) обмена информацией учетными записями, причем для ряда объектов, например, буфер обмена, данные разграничения не назначаются администратором – они установлены в системе разработчиком «по умолчанию». Буфер обмена лишь пример, много локальных объектов, начиная с «рабочего

стола», в системе разделяется между учетными записями по умолчанию. Таким образом, все объекты, которые разработчик ОС посчитал целесообразным разграничить между учетными записями, при реализации данного подхода становятся общими при обработке информации различных уровней конфиденциальности в различных режимах под одной и той же учетной записью. Это уже позволяет отнести данное решение к потенциально опасным, при реализации которого могут возникать дополнительные угрозы, причем угрозы именно безусловных технологических уязвимостей [9], нивелирование которых предусматривалось и реализовывалось разработчиком при создании ОС.

С учетом сказанного можем сделать вывод о недопустимости включения сессии в качестве субъекта доступа в разграничительную политику доступа, что обеспечивает обработку информации различных уровней конфиденциальности под одной и той же учетной записью.

А вот альтернативный вариант, состоящий в задании различных сессий различными учетными записями корректен, его практическое использование позволяет усиливать (ни в коей мере не ослаблять) защиту, реализуемую ОС.

Упрощение задачи администрирования сессионного контроля доступа и вопросы корректности разграничительной политики доступа

Совершенно не понятно, почему при разработке ролевой модели доступа акцентировано внимание на проблеме включения/исключения пользователя в роль. Основная сложность настройки разграничительной политики доступа ведь состоит не в этом – не в создании учетных записей, а в назначении правил доступа субъектов к объектам.

В частности, самым простым при использовании метода мандатного контроля доступа является создание учетных записей и присвоение им меток безопасности. Всю сложность, порою, ограничивающую практическое применение данного метода защиты информации, составляет задача назначения меток безопасности именно объектам, в первую очередь, файловым. Ошибки администрирования в данном случае крайне критичны, они могут приводить, как нарушениям работоспособности системы и приложений, так и к созданию угроз реализации атак на защищаемую

информацию. Сложность администрирования здесь, как показали ранее, во многом связана с системными объектами, которые используются приложениями, осуществляющими доступ к ним под интерактивными пользователями, поскольку ими они и запускаются. Этим объектам, которые не используются для хранения обрабатываемой информации, но могут быть с этой целью несанкционированно использованы, требуется, исходя из каких-то соображений, назначать метки безопасности. А запрет доступа к такому системному объекту может сказаться на работоспособности приложения. Отдельную проблему составляют не разделяемые между учетными записями системой и приложениями объекты, например, это папки для временного хранения файлов. В них должны иметь возможность записи все интерактивные пользователи, но исходно файлов в этих папках нет (в них файлы хранятся временно), как следствие, метку безопасности можно установить только собственно на папку – но для одной папки можно задать только одну метку! Опять же можно использовать решение с разделением подобных папок, описанное выше, но это существенно усложнит и так крайне сложную задачу создания разграничительной политики доступа.

С целью упрощения задачи администрирования и обеспечения корректности мандатного контроля доступа в общем случае нами разработан метод контроля доступа к создаваемым файлам, реализующее его техническое решение запатентовано [10], реализовано и используется в рамках модели сессионного контроля доступа в коммерческой системе защиты информации, сертифицированной ФСТЭК России [11]. Идея данного метода защиты состоит в следующем. Метки безопасности назначаются исключительно учетным записям (соответственно сессиям). Назначения меток безопасности объектам доступа не требуется. Любой создаваемый пользователем, которому присвоена метка безопасности (в данном случае метка безопасности интерпретируется как уровень доступа учетной записи к информации) файл, автоматически размечается – им автоматически наследуется метка безопасности создавшей его учетной записи (метка безопасности сессии). При последующем доступе к размеченному подобным образом файлу, сравниваются метка безопасности учетной записи, запросившей

доступ к файлу и унаследованная файлом метка безопасности учетной записи, создавшей этот файл. Учетная запись, которой не назначена метка безопасности, не может получить доступ к размеченному файлу, к неразмеченному файлу может получить доступ любая учетная запись. Если метки безопасности есть и у учетной записи, и у файла, их значения сравниваются по заданным правилам, например, представленным выше. Может также реализовываться полная изолированность между сессиями, в этом случае будет только одно правило контроля доступа: субъект С имеет доступ к объекту О в режиме “Чтения” и «Записи» в случае, если выполняется условие: Мс = Мо.

Проиллюстрируем реализацию решения [10] в системе [11]. Из меню, приведенного на рис.1, создаются уровни доступа (метки безопасности), которые присваиваются пользователям и отображаются в интерфейсе, представленном на рис.2

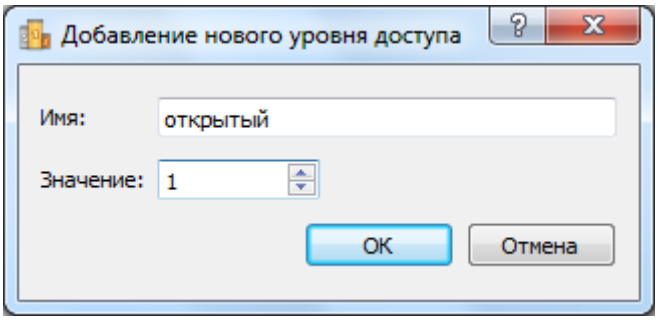

Рис.1. Меню добавления уровня доступа

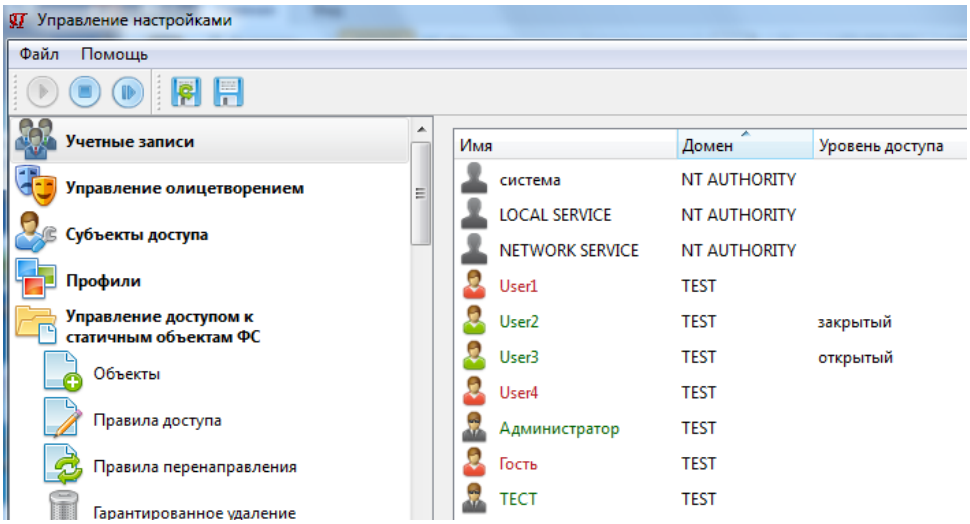

Рис.2. Интерфейс, отображающий созданных пользователей и присвоенных им уровней доступа (меток безопасности)

Из интерфейса, представленного на рис.3, задаются правила сравнения меток безопасности, используемые при анализе запросов доступа, а также правила аудита событий безопасности.

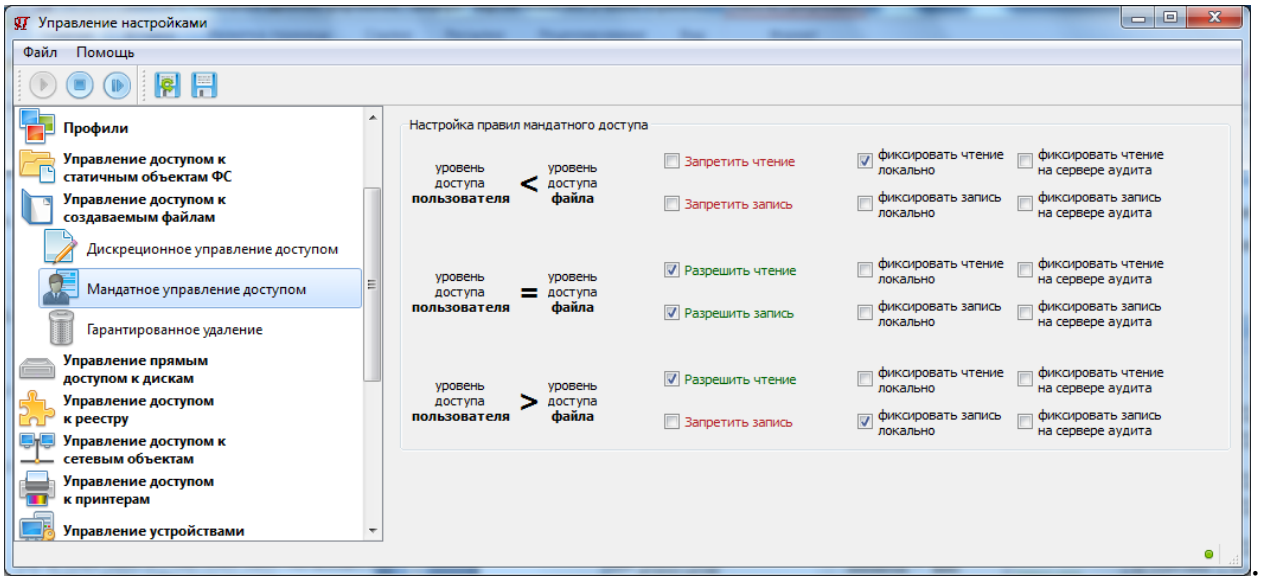

Рис.3. Интерфейс настройки правил мандатного доступа (правил сравнения меток безопасности)

Вот и все настройки, ничего больше не требуется – мандатная (в нашем случае сессионная) разграничительная политика доступа создана, трудоемкость по ее настройке минимальна!

С использованием соответствующей утилиты, см. рис.4, администратор может просмотреть разметку созданных файлов, отображаемую в виде, представленном на рис.5, а также осуществить ее вручную (включая удаление разметки), что важно при внедрении системы защиты в эксплуатируемую информационную систему, чем реализуется запатентованное техническое решение - система с ручной и с автоматической разметкой файлов [12].

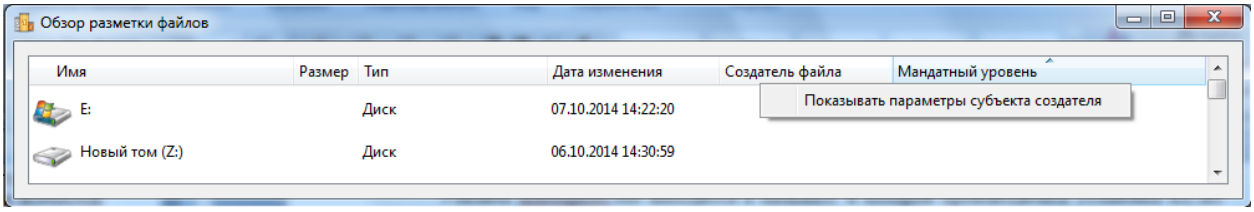

Рис.4. Меню утилиты обзора разметки файлов и их ручной разметки

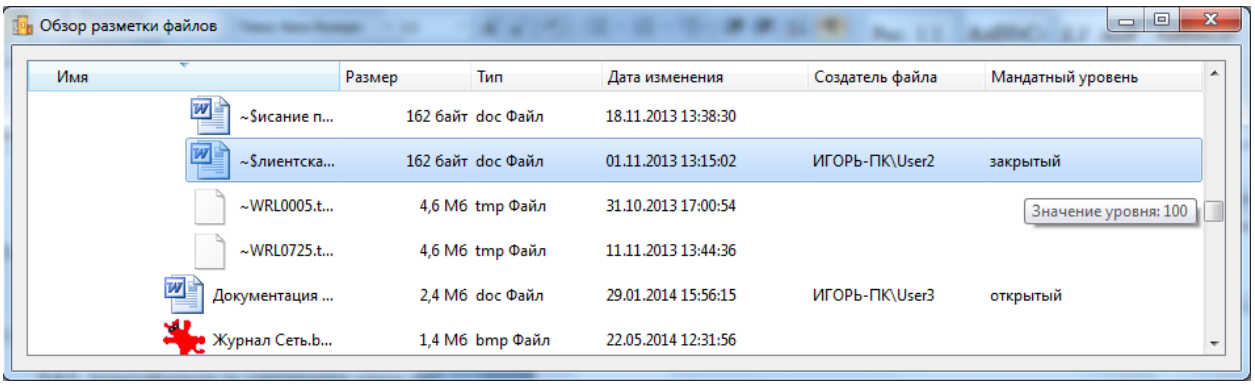

Рис.5. Отображение разметки файлов

Теперь о корректности реализуемой с использованием рассмотренного метода контроля доступа разграничительной политики. Она корректна в общем случае. Какой файл не будет вновь создан, какой файл, включая системный, не будет модифицирован учетной записью, для которой назначена метка безопасности, к нему будет возможен доступ исключительно в рамках реализуемых правил мандатного (сессионного) контроля доступа. Снимает это решение и проблему реализации контроля доступа к временным файлам – любой создаваемый временный файл будет автоматически размечаться, к нему будут разграничиваться права доступа, что проиллюстрировано на рис.5.

Как видим, данное решение отличается не только предельной простотой администрирования, но и реализацией корректной разграничительной политики доступа в общем случае. При подобной простоте настройки разграничительной политики доступа трудно представить себе возможные ошибки администрирования, которые могут приводить к угрозам утечки конфиденциальной информации.

Заключение

В заключение отметим, что именно описанное в работе решение позволяет реально многократно упростить задачу администрирования при реализации сессионного контроля доступа, не противоречит основополагающему принципу построения добавочных средств защиты и обеспечивает корректность реализации разграничительных политик доступа.

Литература

1. Sandhu R., Coyne E. J., Feinstein H. L., Youman C. E. (August 1996). «Role-Based Access Control Models». IEEE Computer (IEEE Press) 29 (2): 38–47.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004.

3. Щеглов А.Ю. Принцип сессионного контроля доступа к ресурсам – основа основ реализации разграничительной политики в корпоративных приложениях, 09.03.2007 [Электронный ресурс]// URL:/ http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/princip_sessionnogo_kontrolya_dostupa_k_resursam_osnova_osnov_realizacii_razgranichitelnoj_politiki_v_korporativnyh_prilozheny a/ (дата обращения 24.02.2016).

4. Васильев В. Рынок DLP переживает кризис доверия [Электронный ресурс]// URL:/ http://www.pcweek.ru/security/article/detail.php?ID=135206 (дата обращения 24.02.2016).

5. Щеглов А.Ю., Щеглов К.А. Система переформирования объекта в запросе доступа // Патент на изобретение №2538918.

6. Ковешников М.Г., Щеглов К.А., Щеглов А.Ю. Технология виртуализации систем // Вестник компьютерных и информационных технологий - 2015. - № 10. - С. 50-54.

7. Ковешников М.Г., Щеглов К.А., Щеглов А.Ю. Метод и абстрактная модель контроля и разграничения прав доступа перенаправлением (переадресацией) запросов доступа // Научно-технический вестник информационных технологий, механики и оптики - 2015. - Т. 15. - № 6(100). - С. 1122–1129.

8. Щеглов А.Ю., Щеглов К.А. Система сессионного контроля доступа к файловым объектам // Патент на изобретение №2562410.

9. Щеглов К.А. Постановка и подходы к решению задачи защиты информации от несанкционированного доступа в общем виде // Вестник компьютерных и информационных технологий. - 2016. - № 1. - С. 32-44.

10. Щеглов А.Ю., Щеглов К.А. Система контроля доступа к файлам на основе их автоматической разметки // Патент на изобретение №2524566.

11. Щеглов А.Ю., Паличенко И.П., Корнетов С.В., Щеглов К.А.. Комплексная система защиты информации "Панцирь+" для ОС Microsoft Windows. Свидетельство о регистрации программы для ЭВМ №2014660889 от 17.10.2014.

12. Щеглов А.Ю., Щеглов К.А. система контроля доступа к файлам на основе их ручной и автоматической разметки // Патент на изобретение №2543556.