окончании периода исследуемого сигнала иметь на выходе значения комплексных коэффициентов $G_1 — G_n$.

Анализ работы рассмотренного устройства доказывает эффективность предложенного алгоритма, что подтверждается исключением операций комплексного умножения, характерного для алгоритма БПФ. Эффективность рассмотренного алгоритма повышается, если исследуемый сигнал относится к классу низких и инфракрасных частот.

ЛИТЕРАТУРА

Исмайлов Ш. Ю., Абдуллаев И. М., Мамедов Н. Я. Преобразование и цифровая обработка непрерывных сигналов. Баку: Элм, 2004. 183 с.

Сведения об авторах

Мамедов Нураддин Ясинович — канд. техн. наук, доцент; Азербайджанская государственная нефтяная академия, кафедра высшей математики, Баку

Абдуллаев Намик Таирович — канд. техн. наук, доцент; Азербайджанский технический университет, кафедра телевидения и радиосистем, Баку; Email: a.namik46@mail.ru

Агаева Гюнель Сяйавушевна — магистр; Азербайджанская государственная нефтяная академия, кафедра информационно-измерительной и компьютерной техники, Баку; E-mail: gunel_asoa@yahoo.com

Рекомендована кафедрой телевидения и радиосистем АзТУ

Поступила в редакцию 13.02.14 г.

УДК 004.056.53

К. А. Щеглов, А. Ю. Щеглов

МЕТОД КОНТРОЛЯ ДОСТУПА К ФАЙЛАМ НА ОСНОВЕ ИХ РУЧНОЙ И АВТОМАТИЧЕСКОЙ РАЗМЕТКИ

Предложен метод контроля доступа к файлам на основе их ручной и автоматической разметки, предполагающий исключение сущности „объект доступа“ из схемы контроля доступа.

Ключевые слова: *защита информации, защита от несанкционированного доступа, контроль и разграничение доступа.*

Введение. В работе [1] предложены принципы и методы контроля доступа к создаваемым файловым объектам, а именно — к файлам, отсутствующим на момент задания администратором разграничительной политики доступа, т.е. к файлам, создаваемым пользователями после разграничения доступа, в процессе работы системы. Реализация данных принципов позволяет исключить сущность „объект доступа“ из схемы контроля доступа, а разграничительная политика позволяет разграничить доступ к обрабатываемой на компьютере информации непосредственно между субъектами доступа (что, в конечном счете, и требуется на практике), а не контролировать доступ субъектов к объектам.

В настоящей статье предложен метод контроля доступа к файлам, основанный как на автоматической, так и на ручной (реализуемой администратором) разметке файлов, исследуется универсальность и общность метода, рассматриваются варианты его практической реализации.

Контроль доступа к создаваемым файлам на основе их автоматической разметки. Рассмотрение данного метода базируется на реализованном и апробированном авторами

техническом решении компьютерной системы защиты информации (КСЗИ) „Панцирь+“ для ОС Microsoft Windows.

Субъекты доступа, определяемые тремя сущностями — исходное имя (SID) пользователя, эффективное имя пользователя, имя процесса (полнопутевое имя исполняемого файла процесса), назначаются из интерфейса, проиллюстрированного на рис. 1. Необходимость идентификации в современных средствах защиты субъекта доступа тремя сущностями обоснована в работах [2, 3]. В интерфейсе задаются субъекты, которые примут участие в разграничительной политике. При задании субъектов доступа могут использоваться маски и переменные среды окружения.

Правила доступа задаются из интерфейса (рис. 2), в котором субъекты доступа отображаются присвоенными им при создании именами (см. рис. 1).

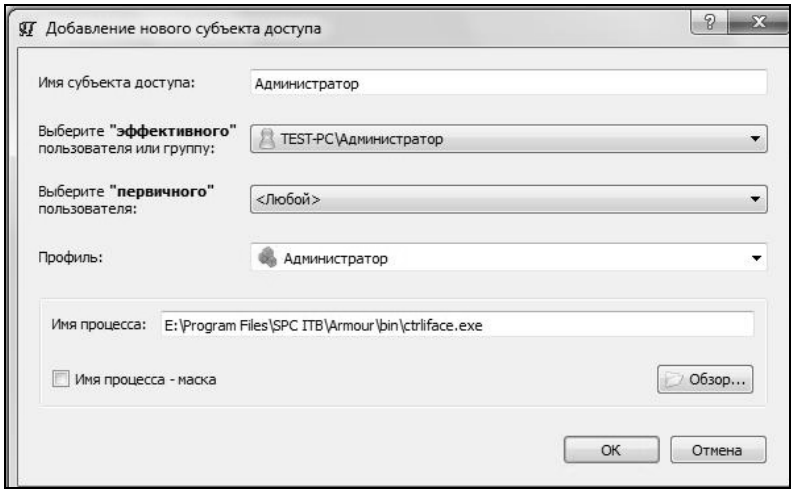

Рис. 1

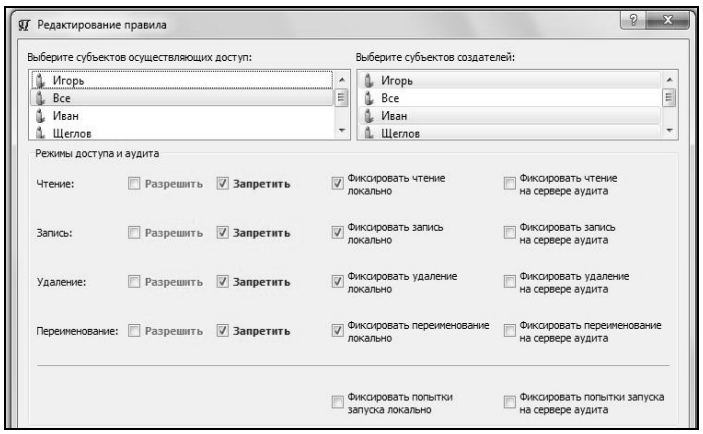

Рис. 2

Контроль доступа реализуется следующим образом. При создании субъектом нового файла он автоматически размечается средством контроля доступа, т.е. файлом наследуется учетная информация субъекта доступа (определяемая соответствующими тремя сущностями), создавшего этот файл. Данная информация размещается в атрибутах созданного файла. Аналогичным образом размечается и неразмеченный ранее файл при его модификации контролируемым субъектом.

При запросе же доступа к любому файлу средство контроля анализирует наличие унаследованной файлом учетной информации создавшего его субъекта доступа, а при наличии — ее содержимое. Это осуществляется посредством считывания и анализа атрибутов файла, к которому запрошен доступ. В соответствии с заданными из интерфейса администратором

правилами доступа (см. рис. 2) средство контроля предоставляет запрошенный субъектом доступ либо отказывает в нем, признавая тем самым запрос доступа несанкционированным.

В двух словах, о назначении правил доступа. В правом столбце интерфейса „Выберите субъектов-создателей“ (см. рис. 2) задаются субъекты, создающие файлы, последующий доступ к которым будет контролироваться. Для каждого заданного в правом столбце субъекта в левом столбце „Выберите субъектов, осуществляющих доступ“ задаются субъекты, которым разрешается доступ к файлам, созданным заданным субъектом-создателем, и назначаются права доступа к этим файлам (чтение, запись, переименование, удаление), а также режимы аудита.

З а м е ч а н и е . Запрет на исполнение создаваемого файла установлен „по умолчанию“ и не вынесен в интерфейс. Разрешать исполнение созданных пользователями файлов запрещается, в противном случае сразу возникает проблема запуска на защищаемом компьютере вредоносных программ [4].

Таким образом, рассмотренное решение позволяет реализовать эффективную разграничительную политику доступа к создаваемым файлам, т.е. непосредственно к обрабатываемой на компьютере информации.

Контроль доступа к статичным файлам на основе их ручной разметки. Рассмотрим реализацию контроля доступа к статичным (системным) файлам, т.е. файлам, которые не создаются в процессе работы компьютера, а уже присутствуют на момент настройки администратором разграничительной политики доступа. В данном случае метод контроля доступа основан на ручной разметке файлов, а не на автоматической. Разметка состоит в осуществляемой администратором записи в атрибуты файла учетной информации субъекта доступа (определяемой тремя сущностями) по аналогии с рассмотренным выше методом. Отличие заключается в том, что учетная информация субъекта доступа, используемая при ручной разметке файла, формируется не автоматически, а администратором, по его усмотрению. Это позволяет включить в схему контроля доступа, основанную на разметке файлов, статичные (системные) объекты. По отношению к ним средство контроля доступа будет обрабатывать запросы так же, как и к создаваемым файлам, используя их разметку.

Рассмотрим реализацию ручной разметки файлов администратором на примере упомянутого апробированного решения (КСЗИ „Панцирь+“ для ОС Microsoft Windows).

Используя интерфейс программы разметки файлов (рис. 3), администратор может проанализировать текущую разметку файлов, вручную разметить выбранный файл (одновременно все файлы в выбранной папке) либо удалить существующую разметку.

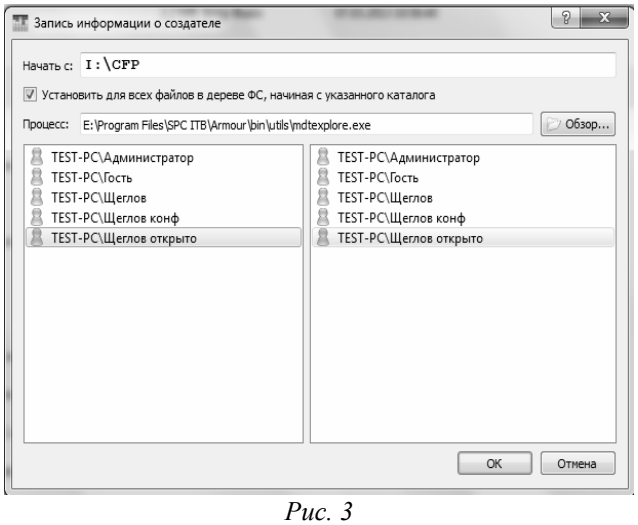

Рис. 3

В правом столбце интерфейса задается исходное имя пользователя, в левом — эффективное. Заметим, что здесь используются точные указатели имен пользователей и процессов, которые будут сохранены в атрибутах файла (файлов в выбранной папке).

З а м е ч а н и е . Применительно к рассмотренному примеру, средство защиты должно разрешать интерактивным пользователям исполнение файлов, которые размечены как созданные администратором.

Таким образом, по сути, вручную моделируются те же действия по разметке файлов, что и при их автоматической разметке.

Файлы, размеченные вручную администратором и автоматически при создании (модификации ранее не размеченных), одинаково отображаются в проводнике средства защиты (рис. 4).

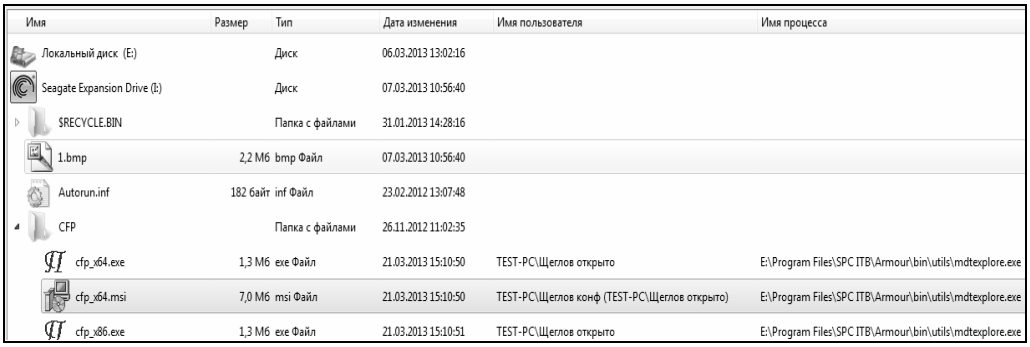

Рис. 4

Итак, используя рассмотренный метод контроля доступа к файлам на основе их разметки (и ручной, и автоматической), можно реализовать разграничительную политику доступа как к создаваемым, так и к системным файлам. Это, однако, еще не позволяет утверждать, что данный метод контроля доступа универсален, т.е. может использоваться для решения всех необходимых на практике задач контроля доступа к файловым объектам и не требует при этом дополнительного применения иных методов. Для исследования этой проблемы необходимо рассмотреть решение задачи контроля доступа к внешним файловым накопителям (все, что касается контроля доступа к файлам, хранящимся на жестком диске, рассмотрено выше).

Реализация контроля доступа к внешним файловым накопителям. Исследование общности предлагаемого метода контроля доступа к файлам необходимо вследствие того, что рассмотренный метод не разграничивает пользователей по созданию файлов в файловых объектах — разграничиваются права доступа между субъектами к уже созданным файлам. При этом закономерно возникает вопрос, связанный с требованием запретить запись пользователю на внешний файловый накопитель. Разграничений по созданию нового файла в соответствии с рассматриваемым техническим решением администратор установить не может.

В рамках проводимого исследования требуется выяснить, является ли задача контроля доступа к файловому накопителю (в том числе, внешнему) задачей контроля доступа к файловым объектам. Для корректного анализа файловое устройство в разграничительной политике доступа должно определяться не буквой диска, которая присваивается системой (при определенных условиях эту букву можно заменить, что несет в себе серьезную угрозу обхода злоумышленником разграничительной политики доступа к файловому устройству), а непосредственно своим идентификатором в системе.

Проиллюстрируем реализацию контроля доступа к файловым накопителям (устройствам) в КСЗИ „Панцирь+“ для ОС Microsoft Windows. Вид интерфейса задания объекта доступа — файлового устройства по его идентификатору в системе — показан на рис. 5. Как видно, файловые устройства задаются в разграничительной политике доступа непосредственно своими идентификаторами с учетом, в том числе, их серийных номеров.

В соответствии с вышеизложенным можно сделать важный вывод о том, что контроль доступа к файловым накопителям должен быть реализован не как контроль доступа к файло-

вым объектам, а как контроль доступа к устройствам, что представляет собой совсем иную задачу защиты информации. Как следствие, можно заключить, что предложенный метод контроля доступа к файлам, основанный на их ручной и автоматической разметке, обладает соответствующей общностью и может рассматриваться как универсальный (самодостаточный) метод контроля доступа к файловым объектам, не требующий одновременного с ним применения иных методов контроля доступа к файловым объектам.

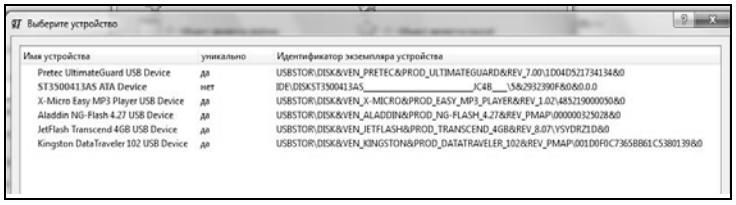

Рис. 5

Заключение. Важность обеспечения и обоснования общности предложенного метода контроля доступа к файлам, основанного на их ручной и автоматической разметке, обусловливается тем, что данный метод позволяет реализовать совсем иные принципы контроля доступа — объект, как таковой, исключается из схемы контроля доступа, в ней присутствуют только субъекты. Как следствие, меняется сама технология (и многие методы) защиты. В частности, гарантированному удалению, шифрованию, контролю на целостность и т.д. подвергается не хранящаяся в определенных файлах информация, а информация, создаваемая определенными субъектами, так как она может создаваться ими в любых файлах — разграничений доступа к созданию файловых объектов не задается.

СПИСОК ЛИТЕРАТУРЫ

1. *Щеглов К. А., Щеглов А. Ю.* Модель контроля доступа к создаваемым файловым объектам // Изв. вузов. Приборостроение. 2012. Т. 55, № 10. С. 37—40.
2. *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.
3. *Щеглов А. Ю.* Защита компьютерной информации от несанкционированного доступа. СПб: Наука и техника, 2004. 384 с.
4. *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.

Сведения об авторах

Константин Андреевич Щеглов — студент; Университет ИТМО, кафедра вычислительной техники, Санкт-Петербург; E-mail: schegl_70@mail.ru

Андрей Юрьевич Щеглов — д-р техн. наук, профессор; Университет ИТМО, кафедра вычислительной техники, Санкт-Петербург; E-mail: info@npp-itb.spb.ru

Рекомендована кафедрой вычислительной техники

Поступила в редакцию 15.04.13 г.