УДК 004.056.53

К. А. Щеглов, аспирант, **А. Ю. Щеглов,** д-р техн. наук, проф., e-mail: info@npp-itb.spb.ru,
Национальный исследовательский университет информационных технологий,
механики и оптики, Санкт-Петербург, Россия

Технология защиты данных, обрабатываемых в распределенных информационных системах

Рассмотрен новый подход к защите данных, обрабатываемых в распределенных информационных системах, основанный на реализации методов контроля доступа к создаваемым объектам — к файловым объектам и к буферу обмена, позволяющих исключить объект доступа из разграничительной политики за счет автоматической разметки создаваемых объектов. Практическая реализация данного подхода при условии сохранения разметки (создаваемых атрибутов) непосредственно в создаваемом файле позволяет сформулировать и решить задачу реализации разграничительной политики доступа к данным, обрабатываемым в распределенной информационной системе, с учетом различных возможных способов обмена данными между компонентами (компьютерами) подобной системы. При этом реализуется управление потоками данных уже в рамках системы в целом.

Ключевые слова: *распределенная информационная система, защита данных, несанкционированный доступ, контроль и разграничение прав доступа, разграничительная политика, создаваемый объект, управление потоками*

Введение

Решение задачи защиты информации от несанкционированного доступа в любой информационной системе основано на реализации контроля и разграничений прав доступа субъектов к защищаемым объектам (далее — контроля доступа), прежде всего к файловым объектам, поскольку именно они предназначены для хранения обрабатываемых данных. При этом существуют различные способы обмена данными (в рассматриваемом случае — файлами) между компонентами (компьютерами) распределенной информационной системы. Это обусловливает актуальность задачи управления потоками данных в распределенной системе, при котором при передаче файла с одного компьютера информационной системы на другой права доступа к этому файлу будут передаваться вместе с файлом. Как следствие, и на другом компьютере будут действовать исходно задаваемые разграничительной политикой права доступа к передаваемым между компьютерами файлам. Разграничительная же политика доступа при этом должна задаваться не в рамках отдельного компонента (компьютера) распределенной информационной системы, а применительно к системе в целом. Поскольку широко используемым на практике способом дополнительной защиты обрабатываемых в информационной системе данных является шифрование, то все сказанное в части проводимых в работе исследований относится и применительно к задаче криптографической защиты данных, направленной на реализацию управления потоками зашифрованных данных в распределенной информационной системе.

Принципы контроля доступа к создаваемым объектам

Реализация контроля доступа основывается на использовании одной из соответствующих абстрактных моделей [1, 2]. Наиболее широко сегодня используются модели дискреционного, мандатного и ролевого контроля доступа.

Дискреционный (иногда также называют избирательным) контроль доступа (Discretionary Access Control — DAC) основан на реализации модели "Харрисона—Руззо—Ульмана" [3]. Основу построения разграничительной политики доступа в данном случае составляет задание администратором матрицы доступа — списка правил доступа субъектов к объектам либо, наоборот, к объектам субъектов, что реализуется транспонированием матрицы доступа. Дискреционный метод контроля доступа может быть реализован с произвольным либо с принудительным для пользователей управлением потоками данных (в зависимости от того, включен ли непривилегированный пользователь, как "владелец" создаваемого объекта, в схему администрирования) [4].

Мандатный контроль доступа (Mandatory Access Control — MAC) основан на реализации абстракт-

ной модели "Белла—ЛаПадулы" [5]. Это контроль доступа с принудительным управлением потоками информации, основанный на формализации задания правил с использованием меток безопасности (мандатов) — числовых значений, отражающих соответствующие уровни безопасности субъектов (уровни доступа) и объектов (уровни конфиденциальности) в заданной иерархии. Каждому субъекту и объекту системы назначается некоторый уровень безопасности — присваивается метка безопасности. Реализация разграничительной политики доступа предполагает арифметическое сравнение этих меток на основе исходно заданного правила.

Идея *ролевой* модели контроля доступа (Role-Based Access Control — RBAC) [1] основана на максимальном приближении логики работы системы к реальному разделению функций персонала в организации. Применение данного метода подразумевает определение ролей в системе, где роль интерпретируется как совокупность действий и обязанностей, связанных с соответствующим видом деятельности. На самом деле, ролевая модель — это не что иное, как дискреционный контроль доступа при реализации соответствующей групповой политики доступа (разграничительной политики для групп пользователей). К достоинствам же данной модели можно отнести возможность определенной формализации ролей и, как следствие, возможность задания и последующего тиражирования неких типовых разграничительных политик доступа для соответствующих ролей. Таким образом, к базовым можно отнести абстрактные модели дискреционного и мандатного методов контроля доступа.

Важным для нас в данном случае является то, что как существующие абстрактные модели контроля доступа, так и (как следствие) реализующие их технические решения используют две равноправные сущности — субъект и объект доступа, а назначение правил предполагает задание тем или иным способом того, какие субъекты к каким объектам (или наоборот) какие права доступа имеют. При этом в качестве субъектов доступа в разграничительной политике выступают пользователи, идентифицируемые учетными записями, — именно в отношении пользователей задаваемыми правилами ограничиваются возможные действия, которые потенциально могут нанести вред.

Применительно к решению задачи защиты данных, обрабатываемых в информационной системе, следует говорить о защите создаваемых пользователями в процессе работы объектов (создаваемые файлы и буфер обмена), поскольку именно такие объекты предназначены для хранения обрабатываемых в системе данных. Подобная постановка задачи позволяет предложить совершенно новые подходы и разработать новые методы контроля доступа, устраняющие недостатки известных методов, применительно к решению этой задачи выявленные и изложенные, например, в работе [6].

Предлагаемые принципы контроля доступа к создаваемым объектам [6], основанные на их автоматической разметке при создании или модификации объекта, позволяют исключить сущность "объект доступа" из разграничительной политики доступа. Состоят они в следующем:

- сущность "объект" исключается из схемы контроля доступа, при реализации разграничительной политики используются две сущности: идентификатор (учетная информация) субъекта, создавшего объект, и идентификатор субъекта, запрашивающего доступ к созданному объекту;
- правила доступа устанавливаются между сущностями: "субъект доступа (учетная информация), запрашивающий доступ к объекту" и "субъект доступа (учетная информация), создавший этот объект";
- при создании (модификации) субъектом объекта объект наследует учетную информацию субъекта доступа, создавшего этот объект — объект размечается (учетная информация субъекта сохраняется в атрибутах созданного им объекта);
- при запросе доступа к любому объекту диспетчер доступа (решающий элемент) получает разметку этого объекта, считывая его атрибуты, и анализирует запрос на непротиворечивость заданным правилам доступа, в результате чего предоставляет запрошенный субъектом доступ к объекту либо отказывает в нем.

Таким образом, реализуется разграничительная политика (задаются правила доступа) не для субъектов к объектам, а между субъектами доступа к создаваемым ими объектам.

Контроль доступа к создаваемым объектам*

Мандатный метод контроля доступа к создаваемым файлам. Метки безопасности (уровни доступа), или мандаты, присваиваются исключительно пользователям (интерактивным пользователям) [8]. Для любого заведенного в системе пользователя может быть задан (выбран) уровень доступа. При этом метки безопасности могут назначаться не всем пользователям, а только тем, которые создают файлы, доступ к которым будет контролироваться и разграничиваться (обрабатываемые этими пользователями данные требуется защищать). Вот и все настройки разграничительной политики доступа (как и последующие иллюстрации, приводимые в работе) рассмотрены на примере интерфейса, реализованного в "Комплексной системе защиты данных "Панцирь+" для ОС Microsoft Windows" (рис. 1).

*Техническое решение, реализующее рассматриваемые далее методы контроля доступа к создаваемым объектам, запатентовано [7].

Отметим, что при настройке разграничительной политики доступа в данном случае не требуется назначения меток безопасности файловым объектам, чем обусловливаются ключевые недостатки известного метода мандатного контроля доступа (возникают проблемы включения в схему контроля системных объектов, необходимость разделения каким-либо образом неразделяемых каталогов, например временных папок, и др.).

Рассмотрим, как работает диспетчер доступа.

Метки безопасности назначаются контролируемым пользователям — тем пользователям, которые создают файлы, к которым требуется разграничивать права доступа. При создании файла любым подобным пользователем этот файл автоматически размечается диспетчером доступа: в атрибуты файла автоматически помещаются учетные данные субъекта (в данном случае его уровень доступа — мандат), создавшего этот файл. Подобным образом будет размечаться и неразмеченный ранее файл при его модификации контролируемым пользователем.

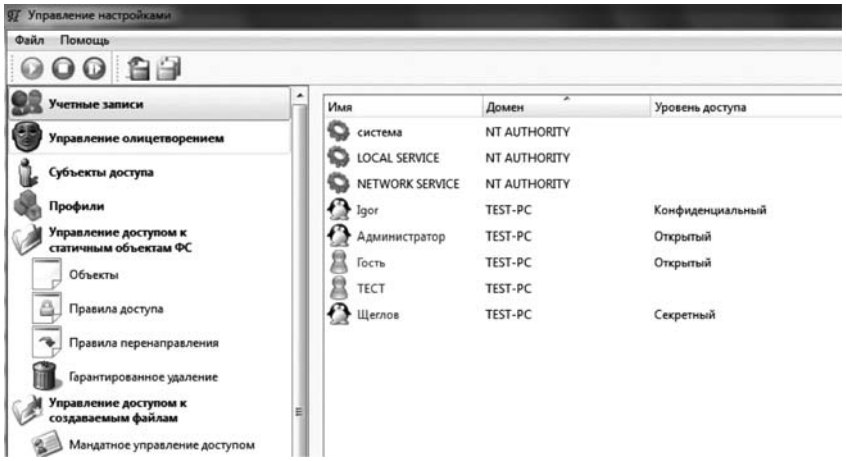

Рис. 1. Иллюстрация разграничительной политики доступа для мандатного метода контроля доступа к создаваемым файлам

При обращении к созданному в процессе работы системы файлу диспетчер доступа анализирует наличие у файла разметки и при ее наличии (в противном случае права доступа не разграничиваются) диспетчер анализирует соответствие запроса мандатным правилам доступа посредством арифметического сравнения соответствующих меток безопасности (мандатов) пользователя, запросившего доступ к файлу, и файла, унаследовавшего данную метку от пользователя, создавшего этот файл.

Отметим, что принципиальным достоинством данного метода, кроме кардинального упрощения задачи администрирования, является корректность реализации мандатной схемы контроля доступа в общем случае, так как где бы (в какой бы папке) и при каких условиях не создавался (модифицировался) бы файл контролируемым пользователем, этот файл будет однозначно размечен и в отношении него будет действовать заданная разграничительная политика доступа при последующих обращениях.

Дискреционный метод контроля доступа к создаваемым файлам. Дискреционный метод контроля доступа может быть использован для решения двух наиболее актуальных современных задач защиты информации: защиты от вредоносных программ (включая атаки на повышение привилегий, предполагающие запуск вредоносной программы с системными правами) и защиты данных от атак со стороны приложений, наделяемых вредоносными свойствами.

Субъект доступа в данном случае уже идентифицируется тремя сущностями [9]:

- исходный идентификатор пользователя (от лица которого запущен процесс);
- эффективный идентификатор пользователя (от лица которого процесс обращается к объекту);
- процесс (полнопутевое имя исполняемого файла процесса) задается из интерфейса, приведенного на рис. 2 (см. четвертую сторону обложки).

При задании идентификатора пользователя (как исходного (первичного), так и эффективного) может использоваться маска "*" — "Любой" (в этом случае заданные правила будут распространяться на всех пользователей). 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 данного каталога, маской "*" задается то, что правило будет применимо к любому процессу.

Правила доступа к создаваемым файлам задаются администратором из интерфейса и отображаются в интерфейсе, приведенном на рис. 3 (см. четвертую сторону обложки; субъекты доступа здесь отображаются присвоенными им при создании именами, см. рис. 2).

Отметим, что в назначаемые права доступа (см. рис. 3) не внесено право "исполнение", так как запрет исполнения создаваемых файлов должен задаваться по умолчанию, что является эффективным решением по защите от вредоносных программ [10].

Задание разграничительной политики доступа осуществляется следующим образом. Из списка заданных субъектов доступа (см. рис. 3) в поле "Выберите субъектов создателей" задаются контролируемые субъекты доступа.

Применительно к выбранному контролируемому субъекту создателю файла назначаются права доступа к создаваемым им файлам других субъектов.

С этой целью субъект, которому назначаются права доступа, выбирается в поле "Выберите субъектов, осуществляющих доступ" (рис. 3). Для выбранной пары субъектов (в левом и в правом полях интерфейса) соответствующим образом разрешаются либо запрещаются соответствующие права доступа (чтение, запись, удаление, переименование). Заданное правило отображается соответствующей строкой в интерфейсе.

Диспетчер доступа в данном случае, по сути, работает так же, как и при реализации мандатного метода, с поправкой на то, что правила доступа для анализа корректности запроса выбираются из соответствующей матрицы доступа. Принципиальным отличием здесь является то, что при создании размечаются все файлы, в том числе файлы, создаваемые и не контролируемые пользователями, так как они должны быть идентифицированы в целях предотвращения возможности их последующего исполнения, в том числе и системными правами.

Важнейшим применением данного метода контроля доступа к создаваемым файлам (соответственно, к данным) является возможность изолирования (по обрабатываемым данным) работы критичных приложений [11].

В общем случае при реализации разграничительной политики доступа к создаваемым файлам мандатный и дискреционный механизмы контроля доступа могут использоваться совместно. При этом запрос доступа будет считаться санкционированным в том случае, если он не будет противоречить ни мандатным, ни дискреционным правилам доступа. При этом диспетчером доступа анализируются сначала мандатные правила доступа, затем дискреционные.

Отметим, что применение данных методов существенно сказывается и на реализации иных методов защиты данных, например, на гарантированном удалении. В данном случае правила гарантированного удаления должны задаваться не для папок, сохраняемые файлы в которых будут автоматически удаляться, а для субъектов доступа, создаваемые файлы которыми (в какой бы папке они не создавались) должны гарантированно удаляться [12]. Отметим, что в данном случае опять же можно говорить о простоте администрирования и корректности решения соответствующей задачи защиты. Ведь если устанавливать правило гарантированного удаления для папок, необходимо его задавать и для всех папок хранения временных файлов, которые создаются большинством приложений (ведь в них также сохраняются защищаемые данные и, как следствие, остаются в виде остаточной информации на диске при их удалении).

Шифрование и метод контроля доступа к шифруемым создаваемым файлам. В случае использования метода (мандатного, дискреционного или обоих одновременно) контроля доступа к создаваемым файлам может быть решена задача принудительного хранения информации в зашифрованном виде для субъектов доступа. При этом при настройке политики шифрования файлов уже потребуется задавать не объекты доступа (папки), сохраняемые данные в которых будут автоматически зашифровываться, а субъекты доступа (при мандатном контроле — уровни доступа или метки безопасности — мандаты), при сохранении которыми данных они будут автоматически зашифровываться. Для соответствующих субъектов должны назначаться и ключи шифрования. Учетной же информации субъекта, сохраняемой в качестве атрибута создаваемого (модифицируемого) файла в открытом виде (она не является секретной информацией), достаточно, чтобы выбрать ключ шифрования для расшифрования файла, где бы (в какой бы папке) этот шифруемый файл не был бы создан. Данное техническое решение запатентовано [13].

Контроль доступа к буферу обмена. Поскольку буфер обмена предназначен для временного хранения данных, используемых для обмена данными приложениями, и на момент задания администратором разграничительной политики доступа эти данные еще не созданы, здесь также можно говорить о контроле и разграничении прав доступа к создаваемым объектам (к данным, записываемым в буфер обмена) и, как следствие, применить изложенные выше принципы контроля и разграничения прав доступа.

В данном случае, с определенной оговоркой, следует говорить о целесообразности реализации дискреционного метода контроля доступа, предполагающего включение в субъект доступа процесса. Дело в том, что между учетными записями в общем случае система сама по умолчанию разграничивает права доступа к буферу обмена. Оговорка состоит именно в том, что разграничение в общем случае касается сессий различных пользователей. При запуске же процесса с правами другой учетной записи в одной сессии (без перезагрузки системы или смены пользователя), например, с использованием утилиты "runas", буфер обмена между учетными записями разграничен не будет — данную возможность следует предотвратить.

В части же реализации метода дискреционного контроля доступа к буферу обмена можем отметить, что она полностью аналогична реализации метода контроля доступа к создаваемым файлам. Субъекты доступа, идентифицируемые соответствующими тремя сущностями, задаются из интерфейса, представленного на рис. 2, правила доступа (с учетом их особенностей — разрешение либо запрет получения информации из буфера обмена) — из интерфейса, представленного на рис. 4. Аналогичным же образом работает и диспетчер доступа.

Таким образом, применяя рассмотренные методы (соответствующие их реализации — механизмы за-

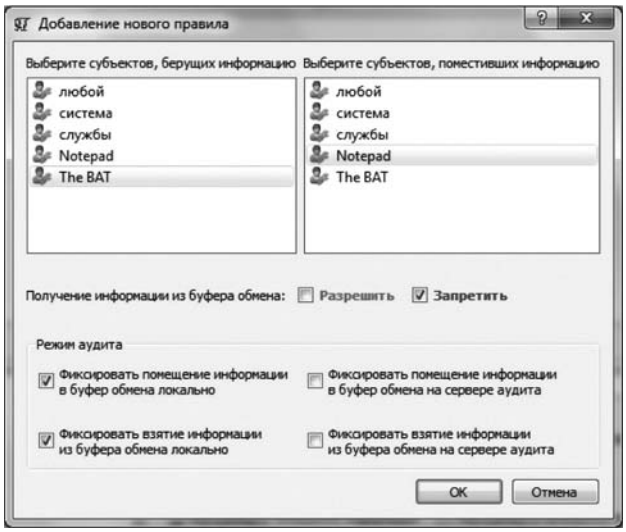

Рис. 4. Задание правил доступа к буферу обмена

щиты) можно реализовать полностью изолированную обработку данных как отдельными пользователями (группами пользователей), так и отдельными приложениями (группами приложений) в информационной системе.

Отметим, что использование предложенных методов контроля доступа к создаваемым объектам, позволяющее рассмотреть задачи защиты данных и системных объектов как совершенно различные задачи защиты даже собственно в своей постановке, принципиально меняет требования к реализации многих механизмов защиты — не только контроля доступа к файловым объектам. Это позволяет говорить о новой технологии защиты данных, обрабатываемых в информационной системе.

Технология защиты данных, обрабатываемых в распределенных информационных системах

Прежде всего рассмотрим постановку задачи защиты. Распределенная информационная система предполагает наличие нескольких компьютеров, осуществляющих обработку информации в рамках единой системы, при возможности обмена между ними данными. Данные в виде файла могут передаваться как с использованием внешних файловых накопителей, так и по сети. В обоих случаях передаваемый файл будем рассматривать как создаваемый объект, к которому должны разграничиваться права доступа субъектов, причем не на отдельном компьютере, а на всех компьютерах в составе распределенной информационной системы. При решении данной задачи разграничительная политика доступа уже может реализовываться не для отдельно взятого компьютера, а для распределенной информационной системы в целом.

Как ранее отмечено, для реализации контроля и разграничения прав доступа каждому созданному файлу должна быть сопоставлена учетная информация создавшего файл субъекта доступа (соответственно идентификатор субъекта либо метка безопасности, возможно и то и другое, в зависимости от реализуемого метода контроля и разграничения прав доступа). Именно эта учетная информация, являющаяся атрибутом файла, используется диспетчером при анализе запроса на непротиворечивость заданной разграничительной политики доступа. Естественно, что при реализации разграничительной политики доступа для распределенной информационной системы атрибуты файла должны сохраняться непосредственно в файле, что позволит передавать их тем или иным способом вместе с размеченным подобным образом файлом между компьютерами информационной системы.

Рассмотрим реализацию возможных разграничительных политик доступа с учетом реализуемых в системе методов контроля доступа к создаваемым файлам.

Естественно, что наиболее простой в настройке будет разграничительная политика доступа на основе меток безопасности (уровней доступа). Именно уровни доступа (их количественные значения) помещаются в качестве атрибутов в файлы. Список уровней доступа и правила арифметического сравнения меток безопасности создаются для распределенной информационной системы в целом. При создании пользователя на каждом компьютере ему назначается уровень доступа из заданного для системы в целом списка (см. рис. 1). При этом в соответствии с реализуемой технологией распределенной обработки информации на отдельно взятых компьютерах системы может обрабатываться информация не всех уровней доступа. Как следствие, пользователям на одном из компьютеров системы могут назначаться не все уровни доступа из их полного для системы списка.

Рассмотрим, как будет реализован контроль доступа в этом случае. Любой созданный в процессе работы системы файл как на компьютере, на котором он создан, так и на компьютере, на который он каким-либо способом, в том числе по сети, передан, будет иметь в своем составе метку безопасности создавшего его пользователя. Как следствие, доступ к нему на любом компьютере будет возможен только в рамках разграничительной политики, заданной для информационной системы в целом. Это относится и к шифрованию — расшифровать такой файл сможет только пользователь с соответствующим уровнем доступа — меткой безопасности, поскольку ключи шифрования в данном случае присваиваются меткам безопасности, а не конкретным пользователям.

Контроль доступа к буферу обмена как к создаваемому объекту в данном случае необходим для того, чтобы разрешить межмашинный обмен дан-

ными в информационной системе исключительно в виде файлов, что проиллюстрируем далее.

Естественно, что важнейшим требованием к корректности реализации рассмотренного метода контроля доступа будет предотвращение возможности смены атрибута переданного на другой компьютер файла, при его сохранении на этом компьютере. Проиллюстрируем необходимость выполнения данного требования примером, также рассмотрим, каким образом может быть выполнено подобное требование. Пусть данные передаются по сети с использованием электронной почты и пусть, например, для этого используется приложение "The BAT". Для решения рассматриваемой задачи требуется разрешить данному приложению чтение из буфера обмена только записанных в буфер обмена им же данных, что настраивается из интерфейса, представленного на рис. 4 (на работе приложения это не отразится, но передача данных становится возможной только посредством передачи соответствующего файла). Письмо, включая прикрепленный к нему файл, поступающее на удаленный компьютер, полностью (с вложенным в него файлом) при получении автоматически сохраняется приложением в соответствующем файле, который размечается как вновь создаваемый на этом компьютере файл — в разметке этого файла окажется метка безопасности пользователя, под которым запущено приложение (последующий доступ к письму будет возможен только пользователем, обладающим соответствующим уровнем доступа). Таким образом, имеем размеченный файл с письмом, в котором (в соответствующем формате) находится вложение — размеченный файл, полученный по почте с другого компьютера. Если попытаться далее открыть прикрепленный к письму файл, то приложением "The BAT" пользователю будет предложено либо сохранить, либо открыть этот файл. При выборе сохранения файла этот файл будет записан (создан) в выбранном пользователем месте. Как следствие, изменится исходная разметка данного файла — в новой его разметке будет указана метка безопасности пользователя, запустившего приложение "The BAT". Данную смену атрибутов необходимо предотвратить. При выборе же открытия файла приложением "The BAT" будет создан временный файл, который уже далее будет прочитан соответствующим приложением, например редактором "Word". Как видим, и в этом случае меняется разметка исходного файла, который в обоих случаях создается на удаленной машине приложением "The BAT".

Для решения рассматриваемой проблемы достаточно запретить приложению "The BAT" размечать создаваемые им файлы вложений (не файлы писем), т. е. файлы, создаваемые в соответствующей служебной папке. У администратора должна быть возможность задавать приложения и папки, при создании которыми в этих папках файлы размечаться не будут (либо, наоборот, в зависимости от разграничительной политики, будут).

Что касается реализации дискреционного метода контроля доступа применительно к решению рассматриваемой задачи, то он реализуется по полной аналогии, отличие составляет лишь содержимое атрибутов создаваемых файлов, в том числе передаваемых в составе файлов между компьютерами, и, естественно, способ анализа диспетчером заданных правил доступа. Кроме того, существенно расширяются возможности разграничительной политики доступа в распределенной информационной системе в случае включения в субъект доступа сущности "идентификатор компьютера" (например, имя). При этом решается задача однозначной идентификации в разграничительной политике доступа пользователей, заведенных на различных компьютерах системы с одинаковыми именами (учетными записями). Настройка подобной разграничительной политики доступа в составе распределенной информационной системы в целом существенно сложнее, чем при реализации мандатного контроля доступа, но при этом имеет существенно более широкие практические возможности за счет реализаций разграничения права доступа между приложениями, используемыми в распределенной информационной системе.

Заключение

Рассмотренная технология защиты данных в информационной системе, основанная на применении методов контроля доступа, реализующих автоматическую разметку создаваемых объектов, позволяет получить принципиально новое свойство разграничительной политики доступа в распределенной информационной системе, причем с использованием различных способов обмена данными между компонентами (компьютерами) системы, а также кардинально повысить эффективность системы защиты информации за счет реализации возможности управления потоками данных в системе в целом.

Рассмотренная в работе технология защиты данных с учетом соответствующих особенностей может быть реализована для различных типов операционной системы. Иллюстрация же в работе приводится на примере реализованного и апробированного технического решения [14], в котором технология защиты данных реализована применительно к операционной системе семейства Microsoft Windows.

Список литературы

1. **Девянин П. Н.** Модели безопасности компьютерных систем. М.: Издательский центр "Академия"', 2005.

2. **Цирлов В. Л.** Основы информационной безопасности автоматизированных систем. Р.: Феникс, 2008.

3. **Harrison M., Ruzzo W., Ullman J.** Protection in operating systems // Communication of the ACM. 1976. V. 19, N. 8. P. 461—471.

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

5. **Bell D. E., LaPadula L. J.** Security Computer Systems: Unified Exposition abd MULTICS Interpretation. Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

6. **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.

7. **Щеглов А. Ю., Щеглов К. А.** Система контроля доступа к файлам на основе их автоматической разметки. Патент на изобретение № 2524566. Приоритет изобретения 18.03.2013.

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

9. **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.

10. **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.

11. **Щеглов К. А., Щеглов А. Ю.** Защита от атак на уязвимости приложений // Информационные технологии. 2014. № 9. С. 34—39.

12. **Щеглов К. А., Щеглов А. Ю.** Принципы реализации дополнительной защиты информации при контроле доступа к создаваемым файловым объектам на основе их автоматической разметки // Вопросы защиты информации. 2014. Вып. 104, № 1. С. 29—34.

13. **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.

14. **Щеглов А. Ю., Щеглов К. А., Павличенко И. П., Корнетов С. В.** Комплексная система защиты информации "Панцирь+" для ОС Microsoft Windows. Свидетельство о регистрации программы для ЭВМ № 2014660889 от 17.10.2014. Правообладатель ЗАО "НПП "Информационные технологии в бизнесе".

K. A. Shcheglov, Graduate Student, **A. Yu. Shcheglov,** Professor,
Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, Russia
e-mail: info@npp-itb.spb.ru

Network Informational System Data Securing Technology

We review the new network informational system data securing approach based on newly created objects (file system objects and clipboard) access control methods implementation, which allows to exclude object from access policy (with help of created objects automatic labeling). Practical implementation of such approach (while saving labeling directly in created file) allows to formulate and solve the task of implementing data (processed in network informational system) access policy in a view of different possible ways of data exchange between computers in such system. Herewith we implement data streams managing already within whole system. Reviewed protection method is based on practical realization which was patented by authors of "File objects access control system based on auto-labeling" solution. This solution allows to rethink known realization of both access control methods including discretionary and mandate ones. This not only dramatically simplifies setting file objects access policy (by eliminating the "access object" essence from access control scheme), but also settings correct implementation in the general case is provided in the same time.

Keywords: *network informational system, data securing, unauthorized access, data access control and policy, access policy, newly created object, data streams, management*

References

1. **Devjanin P. N.** *Modeli bezopasnosti komp'juternyh sistem*. M.: Izdatel'skij centr "Akademja", 2005.

2. **Cirlov V. L.** *Osnovy informacionnoj bezopasnosti avtomatizirovannyh sistem*. R.: Feniks, 2008.

3. **Harrison M. A., Ruzzo W. L. and Ullman J. D.** Protection in operating systems. *Communication of the ACM*. 1976. V. 19, N. 8. P. 461—471.

4. **Shcheglov A. Yu.** *Zashhita komp'juternoj informacii ot nesankcionirovannogo dostupa*. SPb.: Nauka i tehnika, 2004.

5. **Bell D. E., LaPadula L. J.** *Security Computer Systems: Unified Exposition abd MULTICS Interpretation*. Revision 1, US Air Force ESD-TR-306, MITRE Corporation MTR-2997, Bedford MA, March 1976.

6. **Shcheglov K. A., Shcheglov A. Yu.** Princip i metody kontrolja dostupa k sozdavaemym failovym ob'ektam. *Vestnik komp'juternyh i informacionnyh tehnologij*. 2012. N. 7. P. 43—47.

7. **Shcheglov A. Yu., Shcheglov K. A.** *Sistema kontrolja dostupa k fajlam na osnove ih avtomaticheskoj razmetki*. Patent na izobretenie N 2524566. Prioritet izobretenja 18.03.2013.

8. **Shcheglov K. A., Shcheglov A. Yu.** Realizacja metoda mandatnogo dostupa k sozdavaemym fajlovym ob'ektam. *Voprosy zashhity informacii*. 2013. Vyp. 103. N. 4. P. 16—20.

9. **Shcheglov K. A., Shcheglov A. Yu.** Prakticheskaja realizacija diskrecionnogo metoda kontrolja dostupa k sozdavaemym fajlovym ob'ektam. *Vestlik komp'juternyh i informacionnyh tehnologij*. 2013. N. 4. P. 43—49.

10. **Shcheglov K. A., Shcheglov A. Yu.** Zashhita ot vredonosnyh programm metodom kontrolja dostupa k sozdavaemym fajlovym ob'ektam. *Vestnik komp'juternyh i informacionnyh tehnologij*. 2012. N. 8. P. 46—51.

11. **Shcheglov K. A., Shcheglov A. Yu.** Zashhita ot atak na ujazvimosti prilozhenij. *Informacionnye tehnologii*. 2014. N. 9. P. 34—39.

12. **Shcheglov K. A., Shcheglov A. Yu.** Principy realizacii dopolnitel'noj zashhity informacii pri kontrole dostupa k sozdavaemym failovym ob'ektam na osnove ih avtomaticheskoi razmetki. *Voprosy zashhity informacii*. 2014. Vyp. 104. N. 1. P. 29—34.

13. **Shcheglov A. Yu., Shcheglov K. A.** *Sistema kontrolja dostupa k shifruemym sozdavaemym fajlam*. Polozhitel'noe reshenie na vydachu patenta na izobretenie po zajavke N 2013129406/08(043781) ot 26.06.2013.

14. **Shcheglov A. Yu., Shcheglov K. A., Pavlichenko I. P., Kornetov S. V.** *Kompleksnaja sistema zashhity informacii "Pancir+" dlja OS Microsoft Windows*. Svidetel'stvo o registracii programmy dlja JeVM N 2014660889 ot 17.10.2014. Pravoobladatel' ZAO "NPP "Informacionnye tehnologii v biznese".