ВОПРОСЫ ПОСТРОЕНИЯ МЕХАНИЗМОВ И ИНТЕРФЕЙСОВ СРЕДСТВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

А. Ю. Щеглов, *д. т. н., проф.*
(ЗАО «НПП «Информационные технологии в бизнесе»)

Современная статистика показывает, что значительная доля успешных атак на защищаемые ресурсы вычислительных средств обусловлена ошибками администрирования механизмов защиты информации. Причинами этого являются как собственно сложность современных механизмов защиты, так и невысокий уровень интуитивной понятности и информативности интерфейсов их настройки. Всё это, на наш взгляд, является следствием попытки разработчиков современных операционных систем (ОС) создавать максимально универсальные (для использования в различных приложениях) системные средства. Однако когда речь заходит о конкретных областях применений, данный подход является не то чтобы избыточным, но, что еще хуже, его реализация порой в принципе не позволяет эффективно решать конкретные задачи для конкретных приложений. Например, в части защиты конфиденциальной информации к механизмам защиты выдвигаются вполне определенные формализованные требования, задаваемые нормативными документами в данной области. Их реализация (а это является обязательным при разработке средства защиты в рассматриваемых приложениях) позволяет принципиально пересмотреть подходы к построению механизмов защиты и, как следствие, интерфейсов их настройки.

В данной статье применительно лишь к одному механизму защиты рассмотрим, в какой мере специализированные средства могут отличаться от универсальных, когда это касается вопросов защиты информации.

Наиболее практически значимыми и одновременно сложными для администрирования являются механизмы контроля доступа к ресурсам, реализующие разграничительную политику, в том числе к информационным ресурсам (конфиденциальной информации) предприятия. Реализация этой политики определяет и задание режимов обработки информации, в частности, конфиденциальной.

Рассмотрим возможности изменения существующих подходов к построению механизмов и интерфейсов средств защиты информации — СЗИ (на примере механизмов контроля доступа к ресурсам) по сравнению с решениями этой задачи для встроенных в ОС механизмов защиты и определимся, каким образом это связано с формализованными (задаваемыми нормативными документами) требованиями к защите конфиденциальной информации.

Основу построения современных ОС (в первую очередь, ОС семейств Windows и Unix) составляет их максимальная универсализация. Эти ОС могут использоваться и в домашних условиях, и на предприятии, в том числе для обработки конфиденциальной информации, поэтому на практике они создаются без ориентации на какие-либо определенные требования (в противном случае «пострадает» их универсальность).

Добавочные же средства защиты являются специализированными. Они изначально разрабатываются для защиты конфиденциальной информации и, как следствие строятся с учетом необходимости выполнения соответствующих формализованных требований. Казалось бы, каким образом это связано с построением интерфейсов настройки механизмов защиты? Однако, как покажем далее, — напрямую.

Приведем формализованные требования к механизмам защиты конфиденциальной информации (средствам вычислительной техники (СВТ) пятого класса защищенности) в части реализации контроля доступа к ресурсам.

- Комплекс средств защиты (КСЗ) должен контролировать доступ именованных субъектов (пользователей) к именованным объектам (файлам, программам, томам и т. д.).
- Для каждой пары (субъект — объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т. д.), то есть тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).
- КСЗ должен содержать механизм, обеспечивающий выполнение дискреционных правил разграничения доступа.
- Контроль доступа должен быть применим к каждому объекту и субъекту (индивиду или группе равноправных индивидов).
- Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правил разграничения доступа (ПРД), в том числе возможность санкционированного изменения списков пользователей СВТ и защищаемых объектов.
- Право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и др.).

Рассматривая данные требования, остановимся на кажущемся противоречии двух из них: «КСЗ должен содержать механизм, обеспечивающий выполнение дискреционных правил разграничения доступа» и «Право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и др.)». Поясним суть возможной противоречивой трактовки этих требований.

В общем случае принято считать, что дискреционная модель управления основывается на предоставлении доступа к объектам владельцами этих объектов. Это основная модель управления доступом к ресурсам, реализуемая современными ОС, в том числе Windows.

С целью реализации данной модели в схему управления доступом к ресурсам для ОС включена такая сущность, как «владелец» объекта (например, пользователь, создавший файл). «Владелец» наделяется привилегией задавать разграничения прав доступа к файловому объекту, которым он «владеет». Благодаря этому и реализуется дискреционная модель, в данном случае предполагающая включение пользователя в схему назначения (изменения) ПРД. Однако такая схема администрирования противоречит другому требованию, которым однозначно задается, что «право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и др.)», то есть никак не обычным пользователям, в том числе и создающим файловые объекты.

Противоречия в этих требованиях нет, если дать правильное толкование сущности «владелец» применительно к рассматриваемой области использования СЗИ. С этой целью надо соотнести такие категории, как «владелец» и «собственник» информации.

Применительно к исследуемому вопросу будем говорить, что собственник — это лицо (необязательно физическое), которому принадлежит информация, владелец — лицо, получающее информацию от собственника во временное владение с целью ее обработки вычислительным средством. Очевидно, что если речь идет об использовании компьютера в домашних условиях, то пользователь, работающий на ПК, как правило, одновременно является и собственником, и владельцем информации. Как следствие, он должен иметь право назначать (изменять) ПРД к обрабатываемым им данным. Заметим, что именно такая схема исторически сложилась и широко используется встроенными механизмами защиты ОС. Однако она не годится для реализации разграничительной политики доступа к информации, обрабатываемой на предприятии, что и формализуется в требовании: «Право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и др.)». Рассмотрим, чем это обусловлено.

Здесь, как правило, «собственник» и «владелец» (в данном случае пользователь, получающий информацию во временное владение для ее обработки) — различные лица. Пользователь в рамках своих служебных обязанностей с помощью вычислительного средства осуществляет обработку информации, предоставленной собственником, и, как следствие, может осуществлять действия с этой информацией только в рамках правил, установленных собственником. Доверенным же лицом собственника выступает выделенный субъект (администрация, служба или администратор безопасности), в задачи которого входит назначать (изменять) ПРД в соответствии с политикой безопасности, формируемой собственником информации.

Таким образом, можно сделать вывод, что противоречия в рассматриваемых формализованных требованиях, регламентирующих правила создания средства для защиты обрабатываемой на предприятии конфиденциальной информации, нет. Нужно лишь корректно определить, кто есть собственник, а кто владелец информации применительно к защищаемому объекту.

В двух словах остановимся на том, к чему может привести невыполнение данных требований. Здесь можно выделить два аспекта.

Во-первых, если пользователь как временный владелец получает неограниченные права по обработке информации собственника, то, как следствие, он и несет в себе наибольшую угрозу хищения данной информации. Этим во многом объясняется тот факт, что на сегодняшний день большинство хищений информации совершают именно пользователи, что, на наш взгляд, напрямую связано с реализуемой во многих современных ОС схемой управления доступом к ресурсам.

Во-вторых, в данном случае становится «размытой» роль лица (например, администратора безопасности), отвечающего за защиту информации собственника. Дело в том, что, не назначая ПРД и не реализуя их соответствующими механизмами, администратор не может и отвечать за защиту информации собственника, а следовательно, предотвратить ее хищение.

Разобравшись с формализованными требованиями, возвратимся к вопросам построения механизмов и интерфейсов СЗИ.

Итак, в современных универсальных ОС «владелец» может назначать права доступа к созданным им объектам для других пользователей. При этом он не может изменять права доступа пользователей в общем случае, то есть не может задавать (изменять) права доступа к объектам для других пользователей.

Наверное, единственно возможное решение этой задачи и реализуется современными универсальными ОС. Суть данного подхода состоит в том, что права доступа к объекту (в частности, файловому) являются его атрибутами, то есть присваиваются непосредственно объекту. В этом случае можно задавать различные привилегии изменения атрибутов, в частности, «владельцами», которые могут регулировать права доступа остальных пользователей к отдельным файлам.

На основании сказанного можно сделать следующий важный вывод: в основе построения интерфейсов современных ОС лежит обеспечение их универсальности в части назначения прав доступа пользователей к объектам.

Однако подобная универсальность является не только излишней, но и (как следует из формализованных требований) недопустимой при защите конфиденциальной информации. Здесь требование состоит

в том, чтобы привилегированный пользователь (например, администратор безопасности) мог назначать (изменять) права доступа пользователей не к отдельным, а ко всем объектам.

Таким образом, ключевым элементом назначения ПРД при защите конфиденциальной информации должны являться не объекты, а субъекты доступа (пользователи). Как следствие, права доступа должны выступать не в качестве атрибутов доступа, присваиваемых объектам, а в качестве прав доступа, назначаемых субъектам, в частности пользователям. Это следует и из того, что разграничительная политика доступа к ресурсам формируется для субъектов (определяет то, что разрешено либо запрещено пользователям).

Проиллюстрируем на примерах, как могут выглядеть интерфейсы средств защиты конфиденциальной информации, а также рассмотрим работу соответствующего механизма защиты.

На рис. 1 и 2 представлены интерфейсы настройки разграничений прав доступа к объектам файловой системы на жестком диске и на внешних накопителях, локальных и разделенных в сети, для разделенных — по исходящему и входящему запросам доступа.

Рис. 1. Интерфейс настройки разграничений прав доступа к объектам файловой системы для субъекта «пользователь»

Из рисунков видим, что реализация рассмотренного подхода при построении интерфейса механизма защиты принципиально упрощает настройку: во-первых, она становится интуитивно понятной (разграничительная политика доступа априори формируется для пользователей), во-вторых, сводится лишь к занесению нескольких записей

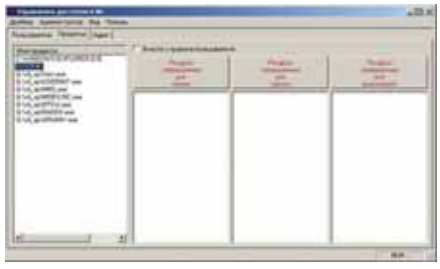

Рис.2. Интерфейс настройки разграничений прав доступа к объектам файловой системы для субъекта «процесс»

в интерфейсе. По каждому типу доступа (запись, чтение, выполнение) может быть задана разрешительная или запретительная политика. Объекты, к которым разрешается либо запрещается доступ пользователю, определяются своими полнопутевыми именами (задаются с использованием соответствующей функции обзора). Поэтому не требуется осуществлять разграничения ко всем объектам иерархии: диск, каталог, подкаталог, файл — в настройках требуется указать только соответствующий объект.

При реализации подобного подхода обеспечивается высокий уровень информативности интерфейса (надо понимать, что СЗИ настраивается в системе не единожды, в процессе эксплуатации требуется изменение настроек механизмов защиты). Для того чтобы получить информацию о правах доступа пользователя к ресурсу в системе, нет необходимости перебирать все объекты, в частности файловые, с последующим анализом установленных для них атрибутов. Достаточно выбрать пользователя, и в окне интерфейса (рис. 1) мы увидим все разрешенные и запрещенные ему права доступа, а также соответствующие политики задания разграничений.

Если же говорить о разграничениях для субъекта «процесс» (а без реализации данной возможности не может быть выполнен ряд ключевых требований к СЗИ), то здесь также целесообразно (рис. 2) назначение прав доступа субъектам (в данном случае — процессам), а не установка соответствующих атрибутов для объектов. Сложность настройки механизмов защиты в этом случае возрастает геометрически, и данный подход в рассматриваемых предположениях, на наш взгляд, вообще неприемлем.

Другой путь к упрощению администрирования связан с минимизацией числа настраиваемых типов доступа. На наш взгляд, их должно быть всего три: запись, чтение, выполнение. Права по остальным типам доступа (переименование, удаление, создание и др.) должны формироваться автоматически. Действительно, если пользователю разрешено чтение файла, то по умолчанию ему запрещены его модификация, переименование, удаление, создание нового файла (то же относится и к папке). Если пользователю разрешена запись в файл, ему разрешена его модификация, запрещены удаление, переименование, создание новых файлов. Если разрешена запись в папку, пользователю разрешаются любые действия внутри папки, запрещаются ее переименование и удаление, а также создание нового файла вне папки. Априори исключены все типы и права доступа, связанные с «владением». На наш взгляд, обоснованно минимальный набор прав доступа, выносимый для настройки в интерфейс, является его большим достоинством в части упрощения задачи администрирования механизмов защиты. Следовательно, именно к реализации такого подхода (а не к увеличению числа атрибутов с целью якобы достижения высокого уровня универсальности настроек), на наш взгляд, следует стремиться разработчикам СЗИ.

Аналогичный подход может быть реализован и при построении механизмов контроля доступа к иным ресурсам. Для демонстрации единообразия подходов к построению интерфейсов настройки механизмов защиты на рис. 3 представлен интерфейс настройки разграничений прав доступа к объектам реестра ОС.

Таким образом, рассматриваемый подход к построению интерфейсов обеспечивает высокую информативность в части отображения заданных настроек для администратора. Однако данная информативность касается одного отдельно взятого интерфейса. С учетом того, что в общем случае каждый механизм

Рис. 3. Интерфейс настройки разграничений прав доступа к объектам реестра ОС для субъекта «пользователь»

защиты имеет свой интерфейс настройки, может быть сформулирована дополнительная задача упрощения администрирования, состоящая в предоставлении администратору совокупной информации обо всех текущих настройках системы защиты. Это удобно для проведения анализа настроек после их задания, поиска противоречий в настройках, сравнения настроек для разных рабочих станций. Кроме того, данная возможность может быть использована и для уведомления пользователя о его правах доступа к ресурсам.

Например, рассмотренный подход может быть реализован следующим образом.

Всю информацию о настройках можно отобразить в одном окне интерфейса в текстовом виде с возможностью сохранения электронной или печатной копии настроек. При отображении можно выбрать (осуществить фильтрацию) только необходимые настройки, например:

- общие — в отчет помещаются настройки механизмов защиты, не требующих установки разграничений для пользователей и процессов (списки запрещенных/ разрешенных процессов, контроля целостности файловой системы и др.);
- настройки для пользователей — указываются пользователи, для которых настройки механизмов должны быть помещены в отчет (разграничение доступа к файлам и каталогам, доступ к сетевым ресурсам и т. д.);
- настройки для процессов — указываются процессы, для которых настройки механизмов должны быть помещены в отчет.

Пример окна фильтра отображаемых настроек представлен на рис. 4, окна отображения настроек в текстовом виде — на рис. 5.

Говоря о функциональных возможностях интерфейса СЗИ, следует затронуть и вопрос информирования пользователя о его правах доступа к ресурсам в процессе функционирования системы.

В качестве примера рассмотрим реализацию следующего решения. Целесообразно предоставить пользователю возможность из проводника Explorer просмотреть права его доступа к файловым объектам и устройствам ввода/вывода (накопителям), если доступ к чтению данных объектов ему не запрещен. По запросу пользователя отображаются установленные разграничения доступа к выбранному им объекту.

Для просмотра своих прав доступа к объекту пользователем может быть реализовано расширение функций проводника Explorer. При этом для просмотра прав доступа в проводнике необходимо выбрать объект, щелкнуть по нему правой кнопкой мыши и в появившемся меню (рис. 6) выбрать «Права доступа к объекту». В результате откроется окно, где будут отображены права доступа этого пользователя к выбранному ресурсу (рис. 7).

Рис. 4. Окно фильтра отображаемых настроек

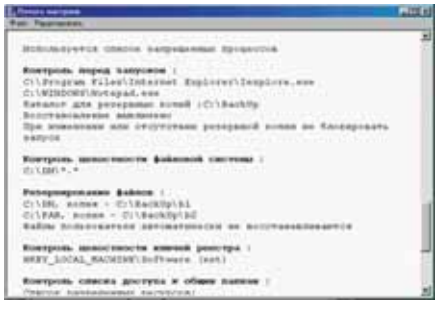

Рис. 5. Окно отображения настроек в текстовом виде

Естественно, что пользователь может просмотреть свои права доступа только к тем файловым

Рис. 6. Меню проводника Explorer с расширением функций

Рис. 7. Окно отображения прав доступа пользователей к объекту

объектам, к которым ему разрешен доступ (остальные файловые объекты не будут отображены в проводнике).

В заключение отметим, что нельзя недооценивать обоснованность принятых разработчиком решений при построении интерфейсов средства защиты. Серьезные СЗИ характеризуются сложностью администрирования. Если разработчик утверждает, что его средство просто настраивать, то либо он лукавит, либо это недостаточно надежное средство. Попытки свести задачу администрирования к «нажатию одной кнопки» также бесперспективны (если, конечно, целью использования системы является обеспечение защиты объекта). Следовательно, администрирование СЗИ — априори сложная задача. Возможность ее упрощения определяется подходами, реализованными при построении интерфейсов настройки механизмов защиты. Эффективность же решения данной задачи, в конечном счете, сказывается на защищенности системы.