ОБЕСПЕЧЕНИЕ ДОСТАТОЧНОСТИ МЕХАНИЗМОВ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИМЕНИТЕЛЬНО К УСЛОВИЯМ ИСПОЛЬЗОВАНИЯ

Д.т.н., проф. А.Ю. Щеглов,
к.т.н. А.А. Оголюк
ЗАО «НПП «Информационные технологии в бизнесе»
www.npp-itb.spb.ru

При построении современных системных средств, как правило, разработчики пытаются обеспечить их максимальную универсальность, с целью расширить область практического использования (что является важнейшим потребительским свойством универсальных системных средств). Это мы видим на примере реализации современных операционных семейства Windows, например в части расширения возможностей работы с устройствами. Однако при использовании универсального системного средства при обработке конфиденциальной информации на предприятии большинство подобных свойств остаются невостребованными. Вместе с тем, подобная универсализация кардинально меняет требования и к средству защиты информации, так как при этом потенциально изменяются условия использования системного средства – появляются новые каналы утечки информации. В данной работе остановимся на исследовании проблемы обеспечения достаточности (выполнения требования к достаточности применительно к условиям использования) механизмов защиты конфиденциальной информации, обрабатываемой с использованием универсального системного средства в части решения задачи локализации его возможностей применительно к защите конфиденциальной информации, обрабатываемой в корпоративной сети предприятия.

Формализованные требования к средству защиты конфиденциальной информации.

ПОДХОД К РЕШЕНИЮ ЗАДАЧИ

Очевидно, что в общем случае причиной уязвимости (существования «канала» несанкционированного доступа (НСД) к информации) может являться либо некорректность реализации механизма защиты, либо недостаточность набора механизмов для условий использования защищаемого объекта информатизации. Вообще говоря, свойства корректности реализации и полноты (достаточности для условий использования) являются основополагающими свойствами любой технической системы, в том числе – свойствами системы защиты информации.

Рассмотрим формализованные (сформулированные в соответствующих нормативных документах в области защиты информации) требования применительно к исследуемой проблеме. Будем рассматривать механизмы защиты, реализующие разграничительную политику доступа к ресурсам.

Формализованные требования к корректности реализации разграничительной политики доступа к ресурсам определены действующим сегодня нормативным документом («Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации») в части защиты конфиденциальной информации (5 класс СВТ) следующим образом:

- КСЗ (комплекс средств защиты, в терминологии РД) должен контролировать доступ наименованных субъектов (пользователей) к наименованным 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.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту);
- КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа;
- контроль доступа должен быть применим к каждому объекту и каждому 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 списка пользователей СВТ и списка защищаемых объектов;

- право изменять ПРД должно предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

Таким образом, разграничение доступа к ресурсу (к любому ресурсу, используемому при обработке информации) реализовано корректно в том случае, если средством защиты информации реализуются представленные выше требования.

Заметим, данные формализованные требования используются при сертификации средств защиты с целью проверки корректности реализации заявляемых в средстве механизмов защиты.

Формализованные требования к достаточности (к полноте – применительно к условиям использования) реализации разграничительной политики доступа к ресурсам определены действующим сегодня нормативным документом («Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации»). В части защиты конфиденциальной информации это требования к классу АС 1Г.

Применительно к рассматриваемой проблеме нас интересует следующее требование:

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи и внешних устройств ЭВМ по их логическим адресам (номерам);
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей и полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

В порядке замечания отметим, что требования к иным группам АС (2 и 3) в современных условиях теряют свою актуальность. Это обусловлено тем, что в современных системах (например, ОС Windows и Unix) всегда должны быть заведены, по крайней мере, две учетные записи: администратора и пользователя, права доступа к ресурсам для которых принципиально различаются (работа пользователя под учетной записью администратора принципиально недопустима, если мы говорим о защите информации, так как именно на разделении их привилегий строится вся защита современных операционных систем).

Рассмотрим требования, приведенные выше. В первую очередь, следует обратить внимание на требование: «Должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа». Заметим, что данные формализованные требования используются при аттестации объектов информатизации с целью проверки достаточности в средстве защиты информации набора механизмов защиты применительно к условиям его использования.

Таким образом, совокупность рассмотренных выше формализованных требований определяет, что средство защиты информации (в части реализации разграничительной политики доступа к ресурсам) реализовано корректно (средство защиты может быть сертифицировано), а набор механизмов защиты в данном средстве достаточен применительно к условиям его использования (объект информатизации может быть аттестован) в том случае, если средствами защиты осуществляется контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа, причем выполняются все требования к корректности реализации контроля доступа.

Теперь вернемся к вопросу универсализации современных системных средств. На практике необходимость контроля доступа ко всем ресурсам вычислительного средства – это весьма избыточная постановка задачи (для рассматриваемых приложений – защита конфиденциальной информации на предприятии, во многом просто бессмысленная). Это обусловливается универсализацией операционных систем (априори предполагающих своей целью максимальное расширение функционала для конечного потребителя), многие возможности которых, в том числе в части подключения внешних устройств, на предприятии избыточны (не востребованы, например подобными устройствами становятся мобильные телефоны).

На наш взгляд, единственно разумным здесь является подход к решению задачи, состоящий в следующем:

- в качестве защищаемых ресурсов должны выступать только ресурсы, в частности устройства, используемые пользователями в рамках выполнения своих служебных обязанностей (что и реализует выполнение требования к полноте и достаточности применительно к условиям использования);
- к этим ресурсам (устройствам) должен осуществляться контроль доступа пользователей в соответствии с матрицей доступа (при выполнении соответствующих требований к корректности реализации).

Вывод. Важнейшим механизмом защиты в части выполнения требований к полноте реализации разграничительной политики доступа к защищаемым ресурсам – к достаточности применительно к условиям использования является механизм управления подключением и отключением ресурсов (устройств). Реализация данного механизма позволяет реализовать в системе защиты контроль доступа только к тем устройствам, которые необходимы пользователям для выполнения своих служебных обязанностей – это и есть защищаемые устройства в соответствии с формализованными требованиями (подключение иных устройств должно предотвращаться рассматриваемым механизмом защиты).

Заметим, что подмена технического решения задачи управления подключением и отключением устройств всевозможными организационными мерами, на наш взгляд, недопустима (такой подход, к сожалению, сегодня часто реализуемый на практике, в принципе, не может обеспечить эффективного противодействия хищению информации, создавая лишь видимость защиты). Кстати говоря, подобный подход (организационные меры) не предусматривается и соответствующими формализованными требованиями, к которым в нормативном документе (для АС класса 1 Г) может быть отнесено следующее:

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещение АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещение АС и хранилище носителей информации, особенно в нерабочее время.

РЕАЛИЗАЦИЯ МЕХАНИЗМА УПРАВЛЕНИЯ ПОДКЛЮЧЕНИЕМ И ОТКЛЮЧЕНИЕМ УСТРОЙСТВ

Прежде чем начать рассмотрение реализации механизма, сформулируем два важнейших требования к реализации разграничительной политики доступа к ресурсам, которые напрямую следуют из представленных выше требований к корректности реализации механизмов защиты: все задачи администрирования должны решаться только администратором (в нашем случае, администратором безопасности), основу настройки механизма должна составлять разрешительная политика (все, что не разрешено и явно не указано, то запрещено).

Кроме того, напомним, что иерархия задания устройств, принятая в ОС Windows, следующая: класс устройств, модель устройств, устройство (устройство может сопровождаться серийным номером). Представление иерархии устройств в ОС Windows проиллюстрировано на *рис. 1*.

В основе архитектуры защиты современных универсальных операционных систем (в частности, ОС семейств Windows и Unix) лежит принцип «полного доверия к пользователю». По-видимому, это обусловливается самой историей со-

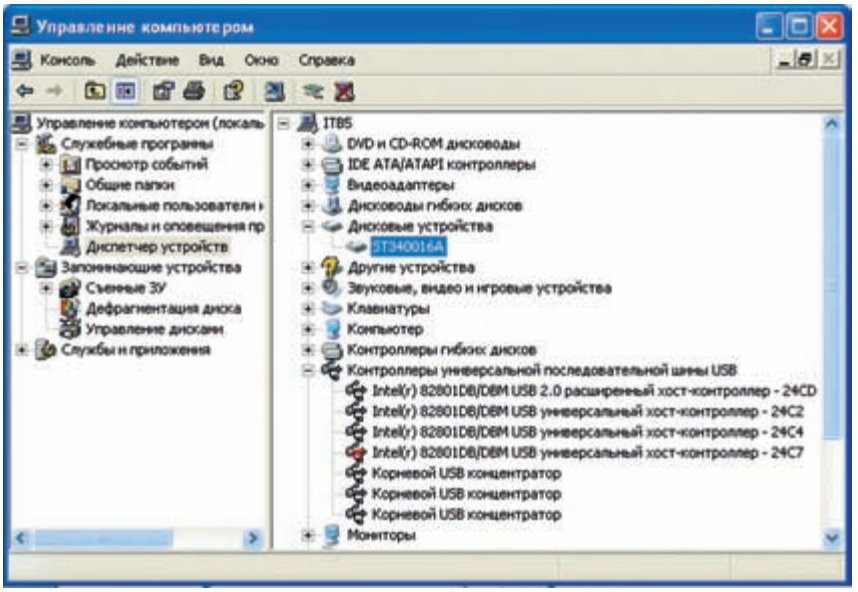


Рис. 1.

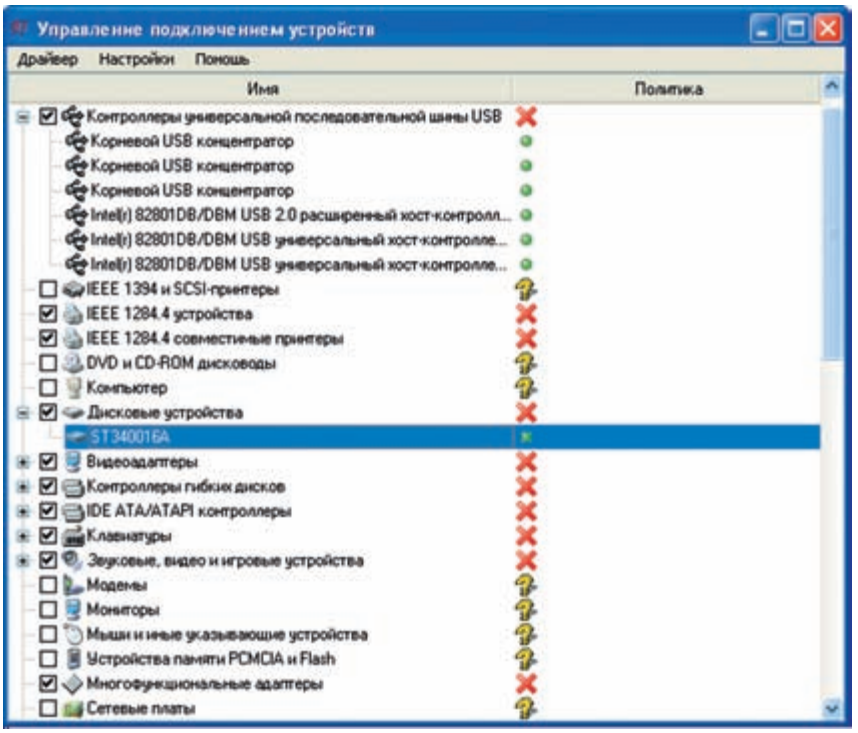


Рис. 2.

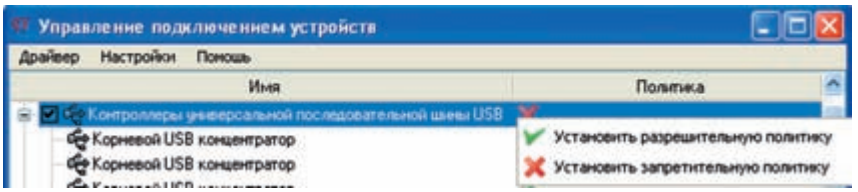
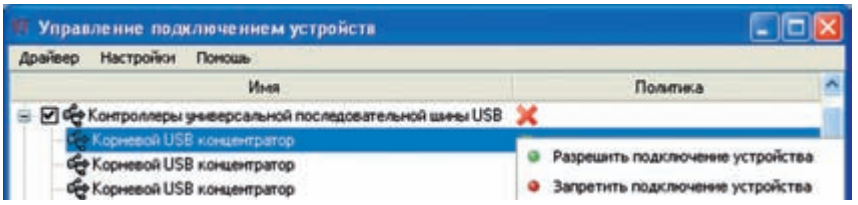


Рис. 3.

Рис. 4.



здания данных системных средств, изначально операционные системы создавались как персональные операционные системы. Применительно к рассматриваемой задаче (защита конфиденциальной информации в корпоративной сети предприятия) уточним, что настройками механизма контроля подключения устройств в ОС Windows обеспечивается лишь возможность запрещать подключать известные устройства (которые подключены к системе), т.е. реализуется не разрешительная, а запретительная разграничительная политика. Это не позволяет противодействовать данным механизмом подключению нового (не известного ранее системе) устройства, как следствие, в рассматриваемых приложениях данный механизм защиты становится во многом бесполезен. Теперь рассмотрим реализованные нами подходы.

Из *рис. 1* видим, что далеко не все классы устройств следует контролировать (в принципе, являются защищаемыми ресурсам), например клавиатуру или мониторы. С учетом этого при реализации механизма предусмотрена возможность задания классов контролируемых устройств (для выбранных классов реализуется разрешительная разграничительная политика). В порядке замечания отметим, что новый класс устройств может быть создан только администратором. Рассмотрим пример реализации данного механизма защиты, выполненного в виде системного драйвера. Интерфейс механизма защиты представлен на *рис. 2*.

Таким образом, сначала администратору следует выбрать контролируемые классы устройств. В результате этого механизмом защиты будет контролироваться только подключение устройств, входящих в выбранные классы. Затем для каждого контролируемого класса устройств следует задать политику *(рис. 3)*, а для каждого устройства задать разрешение и запрет его подключения (рис. 4). Заданные настройки отобразятся в окне интерфейса.

Для того чтобы устройства, подключение которых следует разрешить, отобразились в интерфейсе механизма защиты, при первоначальной настройке механизма они должны быть подключены к компьютеру. Заметим, что в общем случае рекомендуется использовать разрешительную политику. При этом подключение иного устройства, кроме заданных администратором, становится невозможным. Запретительная политика реализована опционально, с целью обеспечения необходимой универсальности реализации разграничительной политики доступа к ресурсам. Некоторые устройства могут иметь родительские и/или дочерние устройства (при подключении устройства, «записи» о нем могут попадать в различные классы устройств). Для разрешения подклю-

чения устройства (при реализации разрешительной политики) необходимо установить соответствующие разрешения для всех соответствующих устройств в иерархии. Для этого в интерфейсе настройки механизма предусмотрено автоматическое отображение и переход от устройства к его родительским и/или дочерним устройства (если такие есть) *(рис. 5)*.

В случае если устройство имеет серийный номер изготовителя, при реализации разрешительной политики и задании данного устройства разрешенным для подключения разрешается подключать устройство только с данным серийным номером (аналогичные устройства с иным номером, либо не имеющим номера, подключить становится невозможным).

Наличие серийного номера устройства и собственно номер можно посмотреть из интерфейса, выбрав соответствующее устройства, справочная информация, предоставляемая по устройству, и вид ее представления проиллюстрированы на *рис. 6*.

Данная опция предоставляет весьма широкие возможности по реализации политики безопасности. Например, можно разрешить подключать только одно (либо несколько фиксированных) Flash-устройств (а это возможность ограничения объема разрешенного к подключению устройства, возможность реализации организационных мер по хранению устройств и т.д.). Если мы говорим об устройствах, на которых может храниться идентифицирующая пользователя либо ключевая информация (это те же Flash-устройства, электронные ключи и др.), возможность идентифицировать устройство при подключении по его серийному номеру предотвращает сам факт создания ключа-двойника. По своей сути, при этом реализуется двухфакторная аутентификация, одним из параметров которой является серийный номер устройства (уже нет необходимости хранить пароль на устройстве в зашифрованном виде).

Таким образом, как следует из представленного описания механизма защиты, рассматриваемого в работе, он гарантирует возможность подключения пользователем только заданных администратором безопасности устройств, причем не только типов устройств, но и в идеале конкретных устройств – по их серийным номерам. Это позволяет администратору гарантированно исключить возможность несанкционированного подключения злоумышленником мобильных накопителей или иных устройств с целью хищения конфиденциальной информации.

Данный механизм является ключевым при решении задачи обеспечения достаточности механизмов защиты конфиденциальной информации применительно к условиям использования. Он позволяет локализовать возможности системы. Основной принцип этого состоит в следующем – должна предоставляться возможность подключения к системе только тех устройств, доступ к которым может разграничиваться между пользователями (при выполнении соответствующих требований к корректности реализации).

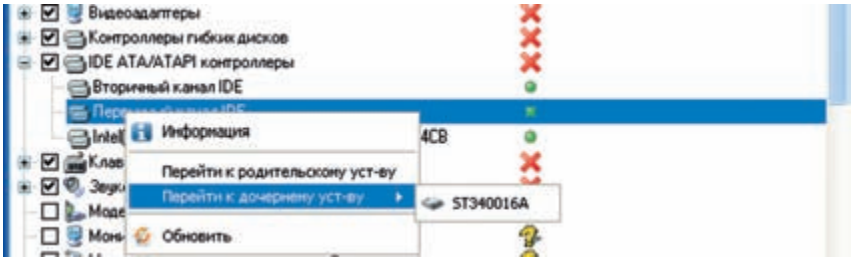
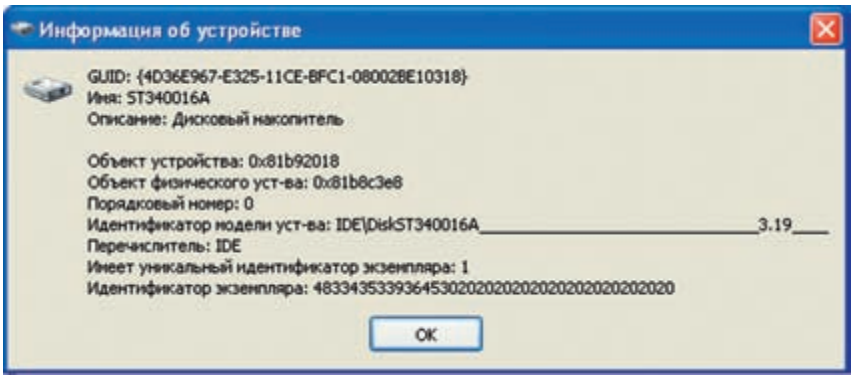


Рис. 5.

Рис. 6.



Вернемся к вопросам аттестации объектов информатизации. Видим, что при использовании рассмотренного в работе (либо подобного ему) механизма защиты становится прозрачной и легко формализуемой собственно процедура аттестации. Действительно, аттестуется некий объект, характеризуемый некими условиями использования. Данные условия использования должны быть локализованы рассмотренным механизмом. Следует проверить, обеспечивает ли средство защиты разграничения (соответственно, корректно реализованные, что уже должно подтверждаться сертификацией этого средства) ко всем ресурсам (в частности, устройствам), которые входят в состав системы (например, реестр операционной системы), либо могут быть подключены к системе в соответствии с условиями ее использования. Если да, все в порядке. Если нет, необходимо либо изменять условия применения (опять же рассмотренным механизмом – изменять список ресурсов, в частности устройств, которые могут подключаться к системе), либо добавлять соответствующие механизмы защиты, обеспечивающие достаточность их набора применительно к заданным условиям использования системы. Естественно, что никакие организационные меры в части решения данных вопросов неприемлемы, если, конечно, конечной целью является защита информации.

Например, если защищаемый компьютер по условиям использования должен функционировать не в сети, рассмотренным в работе механизмом защиты должна быть предотвращена возможность подключения к системе устройств, обеспечивающих доступ в сеть (см. рис. 2). Если же защищаемый компьютер по условиям использования должен функционировать в сети, то рассмотренным в работе механизмом защиты должна быть предусмотрена возможность подключения к системе требуемых устройств, обеспечивающих доступ в сеть, а средство защиты должно содержать в своем составе механизмы контроля (разграничения между пользователями) доступа к сетевым ресурсам.

В заключение еще раз отметим, что рассмотренный в работе механизм защиты является ключевым при обеспечении защиты конфиденциальной информации, так как без его применения, в принципе, невозможно локализовать условия использования защищаемого вычислительного средства и, как следствие, гарантировать достаточность механизмов защиты.