УДК 004.451(075)

БЕЗОПАСНОСТЬ СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

А.Г. Олейник
Институт гражданской защиты Донбасса
Донецкий национальный технический университет

В статье анализируется выполнение технических характеристик ОС по обеспечению безопасности от несанкционированного доступа к данным пользователя. Приведены достоинства и недостатки ОС семейства Windows, а также приведены элементы безопасности ОС.

Для большинства ОС либо полностью не реализуется основной для данных приложений мандатный механизм управления доступом к ресурсам, либо не выполняется его важнейшее требование "Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителя должен быть не ниже уровня конфиденциальности, записываемой на него информации". В связи с этим далее будем говорить лишь о возможном соответствии средств защиты современных ОС классу АС 1Г (защита конфиденциальной информации).

В качестве альтернативных реализаций ОС рассмотрим семейства Unix и Windows.

Сначала остановимся на принципиальном или концептуальном противоречии между реализованными в ОС механизмами защиты и принятыми формализованными требованиями. Концептуальном в том смысле, что это противоречие характеризует не какой-либо один механизм защиты, а общий подход к построению системы защиты.

Противоречие состоит в принципиальном различии подходов к построению схемы администрирования механизмов защиты и, как следствие, это коренным образом сказывается на формировании общих принципов задания и реализации политики безопасности в организации, распределения ответственности за защиту информации, а также на определении того, кого относить к потенциальным злоумышленникам.

Для иллюстрации из совокупности формализованных требований к системе защиты конфиденциальной информации рассмотрим следующие два требования:

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

- должны быть предусмотрены средства управления, ограничивающие распространения прав на доступ.

Теперь в общих чертах рассмотрим концепцию, реализуемую в современных универсальных ОС. Пользователь файлового объекта, т.е. лицом, получающим право на задание атрибутов доступа к файловому объекту, является лицо, создающее файловый объект. Так как файловые объекты создают конечные пользователи, то именно они и назначают ПРД к создаваемым им файловым объектам. Другими словами, в ОС реализуется распределенная схема назначения ПРД, где элементами схемы администрирования являются собственно конечные пользователи.

В данной схеме пользователь должен наделяться практически таким же доверием, как и администратор безопасности, при этом нести наряду с ним ответственность за обеспечение компьютерной безопасности. Отметим, что данная концепция реализуется и большинством современных приложений, в частности СУБД (Система управления базами данных), где пользователь может распространять свои права на доступ к защищаемым ресурсам. Кроме того, не имея в полном объеме механизмов защиты компьютерной информации от конечного пользователя, в рамках данной концепции невозможно рассматривать пользователя в качестве потенциального злоумышленника

Отметим, что централизованная и распределенная схемы администрирования – это две диаметрально противоположные точки зрения на защиту, требующие совершенно различных подходов к построению моделей и механизмов защиты. При этом сколько-нибудь гарантированную защиту информации можно реализовать только при принятии концепции полностью централизованной схемы администрирования, что подтверждается известными угрозами ОС.

Возможности моделей, методов и средств защиты будем рассматривать применительно к реализации именно концепции централизованного администрирования. Одним из элементов данной концепции является рассмотрение пользователя в качестве потенциального злоумышленника, способного осуществить НСД к защищаемой информации.

Механизмы защиты семейства Windows.

Кратко остановимся на основных механизмах защиты, реализованных в ОС семейства Windows, и проведем анализ

защищенности ОС семейства Windows (NT/2000). Отметим, что здесь ряд объектов доступа (в частности, устройства, реестр ОС и т.д.) не являются объектами файловой системы. Поэтому возникает вопрос, как следует трактовать требование "Система защиты должна контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.)". Не ясно, являются ли объектами доступа, к которым, следуя формальным требованиям, необходимо разграничивать доступ пользователей, например, реестр ОС и т.д.

Основными механизмами защиты являются:

- идентификация и аутентификация пользователя при входе в систему;
- разграничение прав доступа к ресурсам, в основе которого лежит реализация дискреционной модели доступа (отдельно к объектам файловой системы, к устройствам, к реестру ОС, к принтерам и др.);
- аудит, т.е. регистрация событий.

Здесь явно выделяются возможности разграничений прав доступа к файловым объектам (для NTFS) – существенно расширены атрибуты доступа, устанавливаемые на различные иерархические объекты файловой системы (логические диски, каталоги, файлы). В частности, атрибут "исполнение" может устанавливаться и на каталог, тогда он наследуется соответствующими файлами.

При этом существенно ограничены возможности управления доступом к другим защищаемым ресурсам, в частности, к устройствам ввода. Например, здесь отсутствует атрибут "исполнение", т.е. невозможно запретить запуск несанкционированной программы с устройств ввода.

Принципиальные недостатки защитных механизмов ОС семейства Windows (NT/2000/XP). Прежде всего рассмотрим принципиальные недостатки защиты ОС семейства Windows. В ОС Windows невозможна в общем случае реализация централизованной схемы администрирования механизмов защиты или соответствующих формализованных требований. Связано это с тем, что в ОС Windows принята концепция реализации разграничительной политики доступа к ресурсам (для NTFS).

В рамках этой концепции разграничения для файла приоритетнее, чем для каталога, а в общем случае – разграничения для включаемого файлового объекта приоритетнее, чем для включающего. Это приводит к тому, что пользователь, создавая файл и являясь его "владельцем", может назначить любые атрибуты доступа к такому

файлу (т.е. разрешить к нему доступ любому иному пользователю). Обратиться к этому файлу может пользователь (которому назначил права доступа "владелец") вне зависимости от установленных администратором атрибутов доступа на каталог, в котором пользователь создает файл. Данная проблема непосредственно связана с реализуемой в ОС Windows концепцией защиты информации.

Далее, в ОС семейства Windows (NT/2000/XP) не в полном объеме реализуется дискреционная модель доступа, в частности, не могут разграничиваться права доступа для пользователя "Система". В ОС присутствуют не только пользовательские, но и системные процессы, которые запускаются непосредственно системой. При этом доступ системных процессов не может быть разграничен. Соответственно, все запускаемые системные процессы имеют неограниченный доступ к защищаемым ресурсам. С этим недостатком системы защиты связано множество атак, в частности, несанкционированный запуск собственного процесса с правами системного. Кстати, это возможно и вследствие некорректной реализации механизма обеспечения замкнутости программной среды.

В ОС семейства Windows (NT/2000/XP) невозможно в общем случае обеспечить замкнутость (или целостность) программной среды.

Стоит отметить, что с точки зрения обеспечения замкнутости программной среды [т.е. реализации механизма, обеспечивающего возможность пользователям запускать только санкционированные процессы (программы)] действия пользователя по запуску процесса могут быть как явными, так и скрытыми.

Возвращаясь к обсуждению недостатков, отметим, что в ОС семейства Windows (NT/2000/XP) невозможно встроенными средствами гарантированно удалять остаточную информацию. В системе просто отсутствуют соответствующие механизмы.

Кроме того, ОС семейства Windows (NT/2000/XP) не обладают в полном объеме возможностью контроля целостности файловой системы. Встроенные механизмы системы позволяют контролировать только собственные системные файлы, не обеспечивая контроль целостности файлов пользователя. Кроме того, они не решают важнейшую задачу данных механизмов контроль целостности программ (приложений) перед их запуском, контроль файлов данных пользователя и др.

Что касается разделяемых сетевых ресурсов, то фильтрации подвергается только входящий доступ к разделяемому ресурсу, а запрос доступа на компьютере, с которого он осуществляется,

фильтрации не подлежит. Это принципиально, так как не могут подлежать фильтрации приложения, которыми пользователь осуществляет доступ к разделяемым ресурсам. Благодаря этому, очень распространенными являются атаки на протокол NETBIOS.

Кроме того, в полном объеме управлять доступом к разделяемым ресурсам возможно только при установленной на всех компьютерах ЛВС файловой системы NTFS. В противном случае невозможно запретить запуск несанкционированной программы с удаленного компьютера, т.е. обеспечить замкнутость программной среды в этой части.

Из приведенного анализа можно видеть, что многие механизмы, необходимые с точки зрения выполнения формализованных требований, ОС семейства Windows не реализуют в принципе, либо реализуют лишь частично.

Вывод

С учетом сказанного можем сделать важный вывод относительно того, что большинством современных универсальных ОС не выполняются в полном объеме требования к защите АС по классу 1Г. Это значит, что, учитывая требования нормативных документов, они не могут без использования добавочных средств защиты применяться для защиты даже конфиденциальной информации. При этом следует отметить, что основные проблемы защиты здесь вызваны не невыполнимостью ОС требований к отдельным механизмам защиты, а принципиальными причинами, обусловленными реализуемой в ОС концепцией защиты.

Список литературы

1. Безбогов А.А, Яковлев А.В., Мартемьянов Ю.Ф. «Безопасность операционных систем : учебное пособие » – М. : "Издательство Машиностроение-1", 2007. – 220 с.

2. Воропаева В.Я., Щербов И.Л. «Адаптация информационно-телекоммуникационных систем к внешним воздействиям» // Научные труды Донецкого национального технического университета. Серия: «Вычислительная техника и автоматизация».- Выпуск 23(201).- Донецк, ДонНТУ, 2012.- С.83-88.

3. Воропаева В.Я., Щербов И.Л., Хаустова Е.Д. «Управление информационной безопасностью информационно-телекоммуникационных систем на основе модели «PLAN-DO-CHECK-ACT»» // Научные труды Донецкого национального технического университета. Серия: «Вычислительная техника и автоматизация».- Выпуск 2(25).- Донецк, ДонНТУ, 2013.