ISSN 1727-1584

УДК 004.451.23:004.056.53

***В.В. ТОРЯНИК**, канд. физ.-мат. наук,*
М.В. ЦУРАНОВ, Г.Е. ГРИГОРЬЯНЦ

Национальный университет внутренних дел

ПОЛИТИКА БЕЗОПАСНОСТИ ПРИ РАЗГРАНИЧЕНИИ РЕСУРСОВ ПК

Рассматриваются проблемы информационной безопасности при использовании персональных компьютеров несколькими пользователями. Выявлена информационная уязвимость современных операционных систем; разработаны принципы настройки компьютерной системы для минимизации вероятности ее несанкционированного использования.

Технологической основой современного информационного общества являются персональные компьютеры (ПК). Однако в силу ряда причин, среди которых главной, видимо, есть экономическая, «персональным» компьютер является для нескольких пользователей. Например, на рабочем месте - при многосменном или многозадачном режимах работы или даже дома - для членов семьи. При таком совместном использовании ПК возникают проблемы разграничения ресурсов ПК, полномочий пользователей, несанкционированного доступа к информации.

Возможность применения компьютера как персонального несколькими пользователями обеспечивается операционной системой (ОС). Традиционным методом разграничения ресурсов и полномочий является администрирование системы одним из пользователей - администратором, который управляет правами и ресурсами других пользователей. Администратор - наиболее привилегированный пользователь, имеющий неограниченный доступ к ресурсам ПК, в том числе к любым данным. Существование администратора является потенциальной угрозой безопасности хранения конфиденциальной информации.

Выбор администратора - сложная задача, и при использовании данных с ограниченным доступом еще более усложняется. Как правило, администратора выбирают либо среди пользователей данного ПК, либо среди профессиональных администраторов, занимающихся централизованным обслуживанием ПК. Для оперативного обслуживания ПК и соблюдения конфиденциальности информации целесообразно администратора выбирать среди пользователей ПК. Следует учесть также, что административные процессы используют незначительную часть времени функционирования ОС [1], поэтому административные полномочия можно предоставить пользователю системы. Однако такое решение может быть конфликтным, поскольку для одной стороны администрирование - это не только дополнительная работа, но и определенная ответственность, а для другой - это потенциальная угроза безопасности. Кроме того, произвольный выбор администратора может не удовлетворять опытных пользователей в части тонкой настройки системы.

Обычно для ограничения доступа к данным пользователи применяют средства криптозащиты. Однако эти средства не обеспечивают должного уровня безопасности, т.к. существует возможность злоумышленных действий: подмены или уничтожения зашифрованных данных, нахождения или взлома криптоключей или паролей пользователя. Для решения этих проблем, а также для устранения угрозы доступа к данным путем установки другой операционной системы была разработана специальная шифрованная файловая система - EFS (Encrypting File System). Однако, вплоть до выхода ОС Windows XP, администратор имел возможность расшифровать зашифрованные пользовательские данные. В Windows XP для расшифровки данных пользователя администратор должен получить от него специальный сертификат, в котором хранится криптоключ. Разработчики XP рекомендует использовать EFS для защиты данных от несанкционированного доступа, в том числе и с другой установленной на данном ПК ОС [2, 3].

Отметим, что корпорация Microsoft, не рассматривает возможность использования двух соответствующе настроенных однотипных ОС в качестве альтернативы администратора для многопользовательского ПК. Проблемы администрирования не рассматриваются и в других публикациях посвященных вопросам установки и эксплуатации нескольких ОС [3, 4].

Ресурсы современных ПК и ОС (начиная с Windows 2000) позволяют устанавливать несколько ОС на один ПК, а программы-мультизагрузчики - комфортно работать с ними. Учитывая это, авторы предлагают нетрадиционный метод решения проблемы администрирования. Суть его в том, что каждая копия ОС предназначена для одного пользователя, который сам будет заниматься ее администрированием. Целью исследования является построение политики безопасности, при которой, с одной стороны, максимально расширены права пользователя, а с другой - наиболее эффективно разграничены ресурсы ПК.

Для исследования было выбрано наиболее распространенное семейство ОС Microsoft Windows. При этом не рассматривались серверные версии ОС (т.к. предполагается, что ОС будет управлять локальным ПК), Windows 98/Me (т.к. данные ОС поддерживают лишь файловую систему FAT, в которой отсутствуют средства разграничения доступа к файлам), а также Windows NT (т.к. данные ОС не поддерживают шифрованную файловую систему EFS). Таким образом, окончательный выбор Windows XP/2к обусловлен наличием в ней поддержки файловых систем NTFS и EFS. Как установлено в ходе исследования, интегрированная в ОС поддержка шифрования данных является ключевым моментом локальной безопасности ПК. Специалисты агентства национальной безопасности США считают [5] (и авторы разделяют эту точку зрения), что информационную систему невозможно надежно защитить на прикладном уровне, т.к. любые про-

ISSN 1727-1584

граммы прикладного уровня используют базовые функции безопасности, обеспечиваемые ОС. Поэтому безопасность ПК, как информационной системы, напрямую зависит от уровня безопасности ОС.

В ходе изучения эффективности интегрированных в ОС криптографических средств выявлены их основные преимущества:

- полная совместимость средств защиты с другими функциями ОС;
- возможность разграничения доступа на уровне пользователей, а не ресурсов;
- меньшая ресурсоемкость, использование средств файловой системы;
- высокая степень безопасности хранения данных;
- технология обработки файлов «на лету»;
- отсутствие стороннего программного обеспечения.

Рассмотрим более подробно два основных блока процедур обеспечения безопасности: контроля доступа и шифрования. Безопасность операционной системы Windows XP построена в соответствии с требованиями профиля «Controlled Access» (EAL4) Common Criteria [6]: пользователь определен в системе уникальным образом и аутентифицирован; назначены разрешения или запреты для пользователей или групп; память защищена от доступа других процессов; система защищена от внешнего воздействия.

Встроенная шифрующая файловая система EFS основана на шифровании с открытым ключом; в ней используется архитектура CryptoAPI. Для настройки системы EFS по умолчанию не требуется вмешательство администратора - шифрование файлов можно начинать сразу. Система EFS автоматически генерирует пары ключей шифрования и сертификат пользователя (если таковой еще не существует) [2]. Для шифрования в системе EFS применяется расширенный алгоритм DESX (Data Encryption Standard) или алгоритм 3DES (Triple-DES). Для генерации сертификатов EFS, а также для зашифровки ключей симметричного шифрования применяются программы RSA Base и RSA Enhanced, включенные в операционную систему поставщиками криптографических услуг CSP (Cryptographic Service Provider). Система EFS позволяет предотвратить компрометацию (преднамеренную или нет) конфиденциальной информации, содержащейся в компьютере, лицами, имеющими к нему доступ. Особенно необходима система EFS на переносных компьютерах или на компьютерах, где совместно работают несколько пользователей для нейтрализации атак с применением методов обхода ограничений, налагаемых таблицами управления доступом (ACL).

При получении доступа к данным через другую ОС или при краже жесткого диска, если злоумышленник не располагает ключом для расшифровки, файлы, зашифрованные в системе EFS, он увидит в виде нераспознаваемого набора знаков. Поскольку система EFS тесно интегрирована с файловой системой NTFS, шифрование и расшифровка файлов прозрачны для пользователя. При открытии файла система EFS расшифровывает его по мере считывания с диска. При сохранении файла система EFS шифрует его по мере записи на диск. Пользователь может даже не знать, что его файлы шифруются, поскольку работа с ними ничем не отличается от обычной. В используемой по умолчанию конфигурации можно начать шифрование файлов из проводника Windows без администрирования. С точки зрения пользователя шифрование файла сводится к установке для него соответствующего атрибута. Кроме того, атрибут шифрования может быть установлен для папки. Тогда любой файл, создаваемый в этой папке или добавляемый в нее, шифруется автоматически. Во избежание появления временных файлов с открытыми данными при их обработке, рекомендуется применять шифрование на уровне папок.

Для практического изучения предложенного метода разграничения ресурсов ПК и доступа к данным, авторы провели эксперимент по установке трех однотипных ОС на локальный ПК. Эксперимент проводился на персональном компьютере с процессором Celeron 1,7 ГГц, ОЗУ 128 Мб и жестким диском размером 40 Гб. Для установки систем жестком на диске были созданы четыре логических диска. Три копии Windows XP инсталлировались на логические диски, отформатированные в файловой системе NTFS. Один диск был отформатирован в системе FAT 32 и предназначался для установки Windows 98, которая использовалась как гостевая ОС. Windows 98 не поддерживает NTFS и пользователи данной системы не имеют доступа к NTFS-дискам (для них логически их просто не существует). Каждая ОС комплектовалась всем необходимым программным обеспечением (ПО), большинство из которого дублировалось для каждой ОС. После установки ОС и ПО для защиты от несанкционированной установки любой другой ОС были проведены завершающие программно-аппаратные манипуляции с тестовым ПК: установка пароля для доступа к BIOS; запрет загрузки с любых устройств, кроме основного жесткого диска; закрытие и опечатывание системного блока ПК во избежание злоумышленного обнуления CMOS либо подключения другого НЖМД.

Для разграничения доступа к данным пользователей ОС авторы использовали встроенные в ОС средства разграничения доступа (СРД), которые работают лишь с файловой системой NTFS и по умолчанию отключены. Существуют два способа включения этих средств [7]: автоматический, когда ПК регистрируется в сети как член домена и ручной. Для ручной активации СРД необходимо провести манипуляцию с реестром Windows, изменив значение переменной «forceguest» (рис.1).

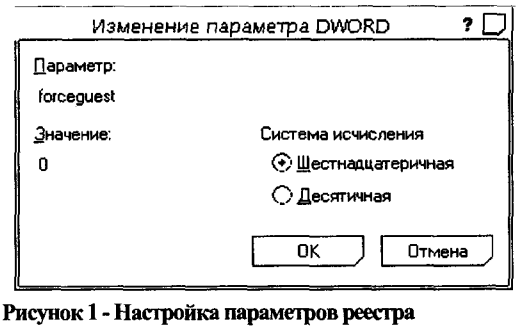

Рисунок 1 - Настройка параметров реестра

После активации СРД необходимо разграничить доступ к дискам системы (рис.2), выделив каждому пользователю свой логический диск, что позволит избежать конфликтов ПО, установленного для разных ОС, так как используемая в данный момент ОС не будет иметь доступ к остальным дискам.

ISSN 1727-1584

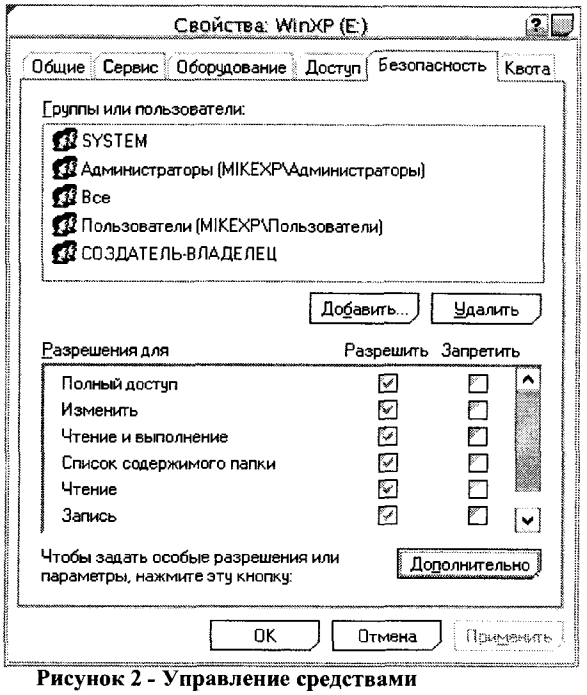

Рисунок 2 - Управление средствами разграничения доступа

Авторами также была исследована возможность деактивации СРД. Это возможно лишь при условии, что ПК не является членом домена, тогда проведя обратные манипуляции с реестром можно отключить СРД. Также исследовалась возможность получения перекрестного доступа к данным из других установленных ОС. Данные действия возможны, если пользователь другой ОС обладает правами администратора. Для получения доступа к данным необходимо стать владельцем требуемых данных (закрытые данные не имеют владельца, так как активная ОС «не знает» пользователей других пассивных ОС).

Единственным способом противодействия угрозам перекрестного доступа является применение системы EFS. Расшифровать данные из другой ОС практически невозможно, так как для шифрования применяется уникальный ключ, который зависит не только от имени пользователя, но и от даты установки и других параметров ПК, которые сложно воссоздать в другой ОС.

Проанализируем результаты с точки зрения безопасности. Недостатком встроенной в ОС системы шифрования, как, впрочем, и любой системы шифрования, является возможность удаления зашифрованных данных, что является реализацией угроз целостности и доступности хранимых данных [7]. Следует указать, что, как правило, системные папки («рабочий стол», «корзина») где могут быть документы, обрабатываемые в текущий момент, не шифруются. Удаленные в корзину файлы находятся в дешифрованном виде и их содержимое доступно. Очевидно, что данная брешь не критична и устраняется шифрованием указанных папок.

Предложенная методика имеет ряд преимуществ по сравнению с классическим методом: повышение стабильности работы компьютерной системы; отсутствие административного доступа к информации; удобство системного шифрования.

Недостатками системы являются: возможность доступа к незашифрованным данным; невозможность скрытия логической структуры данных; возможность удаления данных; необходимость тонкой настройки системы.

Таким образом, в ходе исследования проблемы конфигурирования многопользовательской компьютерной системы были выработаны принципы политики безопасности, основные на мультиоперационном режиме работы ПК. При этом общий уровень безопасности определяется тонкой настройкой каждой ОС и применением интегрированного шифрования данных.

ЛИТЕРАТУРА

1. Девянин П.Н. Метод разделения административных и пользовательских полномочий // Защита информации. Конфидент. –2004. -№ 2. -С.56-58.

2. Windows XP Networking Features and Enhancements (Сетевые средства и усовершенствования в системе Windows XP). –URL: http://www.microsoft.com/windowsxp /pro/techinfo/howitworks/networking/default.asp.

3. Ботт Э., Зихерт К. Эффективная работа: Безопасность Windows. –СПб.: Питер, 2003. -628 с.

4. Дополнительные сведения о средствах обеспечения безопасности в системе Windows. –URL: http://www. microsoft.com/windows2000/technologies/security/default.asp.

5. Лоскокко П., Смэлли С., Макелбауер П., Тейлор Р., ТернерД., Фарелл Д. Неизбежность провала: ошибочные предположения о безопасности современных компьютерных систем // Защита информации. Конфидент. -2004. -№ 2. -С.38-48.

6. Вишняков Д. Б. Защита информации: операционная система Windows 2000 фирмы Microsoft // Вопросы защиты информации. -2002. -№ 3. -С.42-53.

7. ВеберК., Бадур Г. Безопасность Windows XP: Готовые решения сложных задач защиты ПК. –СПб.: «ДиасофтЮП», 2003. -464 с.

Поступила в редколлегию 03.02.2005

ТОРЯНИК В.В., ЦУРАНОВ М.В., ГРИГОР'ЯНЦ Г.Є. ПОЛІТИКА БЕЗПЕКИ ПРИ РОЗМЕЖУВАННІ РЕСУРСІВ ПК

Розглядаються проблеми інформаційної безпеки при використанні персональних комп'ютерів декількома користувачами. Виявлена інформаційна уразливість сучасних операційних систем. Розроблені принципи налаштування комп'ютерної системи для мінімізації вірогідності її несанкціонованого використання.

***

TORYANIK V.V., ZURANOV M.V., GRIGORIANZ G.E. POLICY OF SAFETY AT DIFFERENTIATION RESOURCES OF THE PERSONAL COMPUTER

The problems of informative safety at the use of the personal computers by a few users are considered. The information vulnerability of the modern operating systems was detected. The principles of adjusting of the computer system for minimization of probability of its unauthorized use are developed.