УДК 004.056

А. АБДУЛАЕВ, Г.И. ТОНУЕВА, Б.И. АНАРБАЕВА
E.mail. ksucta@elcat.kg

КОНФИГУРАЦИОННЫЕ ПАРАМЕТРЫ ЗАЩИТЫ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА WINDOWS

Бул макалада Windows түркүмүнүн операциялык системаларын коргоонун конфигурациялык параметрлеринин көптүгүн аныктоо боюнча изилдөөлөрдүн жыйынтыктары келтирилген.

В данной статье изложены результаты исследований по определению множества конфигурационных параметров защиты операционных систем семейства Windows, их взаимосвязи и взаимного влияния.

In this article the results of research to determine the set of configuration parameters of protection operating systems of Windows family, their interaction and mutual influence.

Совокупность всех субъектов и объектов защиты, а также значений их атрибутов безопасности, образует множество *конфигурационных параметров защиты*, устанавливаемых администратором и влияющих на функционирование средств защиты операционных систем. По своей сути процесс администрирования безопасности заключается в установке тех или иных значений конфигурационных параметров защиты [1].

При осуществлении настройки безопасности администратором безопасности вручную или с помощью существующих средств автоматизации возникают следующие проблемы:

- большое множество конфигурационных параметров защиты, из-за чего требуется много времени для настройки «вручную» [7];
- отсутствие гарантий адекватности настройки безопасности — при ручной или автоматизированной с помощью существующих средств, работающих на основе написанных скриптов, настройке безопасности не возможно, гарантировать соответствие конфигурационных параметров защиты предъявляемым требованиям по безопасности [8];
- ошибки в настройке — даже при высокой квалификации администратора безопасности сохраняется высокая вероятность возникновения ошибок, связанных с «человеческим фактором» [9].

Для решения перечисленных проблем предлагается подход к автоматизации процесса настройки безопасности на основе имитационного моделирования.

В данной статье рассматриваются субъекты, объекты защиты и их атрибуты. Поскольку базовые принципы защиты, реализованные в ОС Windows 2000/XP/Server 2003/Vista/7, являются общими для всех перечисленных систем, то проводится анализ компонентов, которые присутствуют в любой из ОС семейства Windows.

В терминах ОС Windows присутствует понятие "*участники безопасности*", которое характеризует субъекты защиты [2, 3]. Известны два основных типа участников безопасности, инициирующих запросы на доступ:

- пользователи;
- группы пользователей.

Объекты защиты (в ОС Windows) — системные сущности, содержащие или позволяющие обрабатывать информацию, доступ пользователей (групп) к которым регламентируется посредством списков DACL.

Среди субъектов и объектов защиты можно выделить наиболее критичные с точки зрения обеспечения безопасности хранящихся в ОС пользовательских данных и системной информации. К таким сущностям относятся файлы и каталоги файловой системы, элементы реестра, сервисы и разделяемые ресурсы файловой системы, а также пользователи и их группы. Среди атрибутов безопасности наиважнейшее значение имеют права доступа, поскольку именно они определяют возможность доступа, а также привилегии пользователей и групп и членство пользователей в группах, поскольку привилегии могут часто превалировать над правами, обеспечивая даже запрещенный правами доступ к объектам. Членство пользователей в группах также является критичным с точки зрения администрирования безопасности, так как косвенно — через группу — позволяет субъектам обладать правами, которые они явно не имеют [4].

Таким образом, в ОС Windows множество настроек безопасности состоит из совокупности защищаемых сущностей (таблица 1) и связанных с ними атрибутов, определяющих безопасность этих ресурсов (таблица 2).

При этом пользователи и группы составляют множество субъектов защиты, остальные сущности образуют множество объектов защиты [5].

Таблица 1. Множество защищаемых сущностей ОС Windows

№ п/п	**Объект**	**Примечание**
1	Пользователи	Встроенные, созданные в процессе эксплуатации, локальные.
2	Группы пользователей	Встроенные, созданные в процессе эксплуатации, локальные.
3	Элементы файловой системы	Логические диски, каталоги, файлы, символические ссылки на каталоги файловой системы NTFS, точки подключения дисков, а также файлы NTFS, имеющие более одной жесткой ссылки, расположенные на разделах NTFS, локальные, открытые ОС (доступные для просмотра).
4	Элементы системного реестра	Ключи, пользовательские символические ссыпки на ключи, не предопределенные ОС; локальные, открытые ОС (доступные для просмотра).
5	Разделяемые ресурсы	Разделяемые каталоги, расположенные на разделах NTFS, локальные
6	Сервисы	Активные, локальные.
7	Объекты ядра	Процессы, потоки, каталоги диспетчера объектов, оконные станции, рабочие столы, активные, локальные.
8	Принтеры	Локальные
9	COM/DCOM- объекты	Локальные
10	WMI-объекты	Локальные
11	Параметры локальной политики безопасности	Значения параметров согласно оснастке "Локальная политика безопасности"
12	Параметры групповой	Значения параметров согласно оснастке "Групповая

	политики	политика".

Таблица 2. Множество атрибутов безопасности для сущностей ОС Windows

№ п/п	Объект	Настройки безопасности
1	Учетные записи пользователей	Идентификатор защиты пользователя, имя пользователя; тип объекта защиты; членство в группах; привилегии пользователя.
2	Учетные записи групп пользователей системы	Идентификатор защиты группы, имя группы; тип объекта защиты; привилегии групп пользователей.
3	Элементы файловой системы NTFS: логические диски, каталоги и файлы	Абсолютный путь; тип объекта защиты; атрибут наследования прав доступа; владелец; права доступа к объекту файловой системы; область действия прав доступа (если она определена).
4	Элементы файловой системы NTFS: символические ссылки и точки подключения	Имя ссылки; тип объекта защиты; путь ссылки; права доступа к ссылке.
5	Элементы файловой системы NTFS: файлы, имеющие более одной жесткой ссылки	Имя ссылки; тип объекта защиты; уникальный идентификатор объекта файловой системы; права доступа к ссылке.
6	Элементы системного реестра: разделы и ключи	Абсолютный путь; тип объекта защиты; атрибут наследования прав доступа; права доступа к объекту реестра; область действия прав доступа (если она определена)
7	Элементы системного реестра: символические ссылки	Имя ссылки; тип объекта защиты; путь ссылки; права доступа к ссылке.
8	Разделяемые ресурсы NTFS	Имя объекта; тип объекта защиты; абсолютный путь к объекту; тип разделяемого ресурса; права доступа к разделяемому ресурсу.
9	Сервисы	Название сервиса; тип объекта защиты; полное отображаемое имя сервиса; тип сервиса; текущее состояние сервиса; имена сервисов, которые должны быть запущены до запуска данного сервиса; командная строка запуска сервиса; владелец сервиса; права доступа к сервису
10	Объекты ядра: процессы	Идентификатор процесса (PID); имя процесса (имя исполняемого файла); тип объекта защиты; путь к исполняемому файлу процесса; владелец процесса; права доступа к процессу.
11	Объекты ядра: потоки	Идентификатор потока; тип объекта защиты; идентификатор процесса-родителя; владелец потока; права доступа к потоку.
12	Объекты ядра: каталоги, оконные станции, рабочие столы	Имя объекта; тип объекта защиты; владелец объекта права доступа к объекту.
13	Принтеры	Имя принтера; тип объекта защиты; владелец принтера; права доступа к принтеру.
14	COM/DCOM- объекты	Идентификатор объекта (CLSID); идентификатор библиотеки (АррШ) объекта; права доступа к объекту.
15	WMI-объекты	Имя объекта; тип объекта защиты; права доступа к

		объекту.
16	Параметры локальной политики безопасности	Название параметра защиты; тип объекта защиты; значение настройки безопасности.
17	Параметры групповой политики	Название параметра защиты; тип объекта защиты; значение настройки безопасности.

Множество перечисленных конфигурационных параметров защиты (субъектов, объектов ОС семейства Windows и их атрибутов безопасности) составляют основу для построения имитационной модели подсистемы контроля доступа КС на базе ОС семейства Windows. Такая модель, позволяет описывать состояние и поведение механизмов ОС,

обеспечивающих ее защиту, путем моделирования поведения составляющих ее субъектов и объектов защиты, и собственно анализ безопасности проводить над полученной моделью, не затрагивая фактическое распределение параметров защиты и их значений.

Механизмы, влияющие на контроль доступа в ОС семейства Windows, и алгоритмы их влияния документированы лишь частично [6].

Разработанная имитационная модель КС на базе ОС семейства Windows позволила связать конфигурационные параметры защиты ОС и критерии безопасности и, предложить подход к оценке эффективности настройки безопасности КС.

Факторами, влияющими на доступ субъектов к объектам, во всей линейке ОС семейства Windows (начиная с Windows 2000) являются [2]:

- права доступа субъектов;
- членство пользователей в группах;
- общие права доступа;
- взаимное влияние разрешений и запретов;
- владелец объекта;
- привилегии субъектов;
- права доступа к родительскому объекту;
- замещение прав доступа;
- предопределенные права субъектов;
- действующая политика безопасности;
- параметры ключей реестра.

В проведенных исследованиях определено, что все такие факторы образуют иерархию.

Таким образом, при попытке осуществления субъектом доступа к объекту, механизмы защиты, использующие перечисленные факторы, работают в строгой последовательности. Множество видов доступа к каждому объекту ограничено множеством прав доступа, специфичным для объектов этого типа. Действие всех других механизмов защиты можно

спроецировать на множество прав доступа. Проекцию факторов на права доступа, включая сами права доступа, будем называть множеством доступных прав (МДП).

В заключении можно отметить, что результаты исследования и анализа механизмов контроля доступа на базе ОС семейства Windows позволит выделить конфигурационные параметры, влияющие на безопасность ОС, определить степень их влияния, разработать форму представления критериев безопасности и задать их область определения.

Список литературы

1. Schneider, F. B. Enforceable Security Policies [Текст] / F. B. Schneider // ACM Transactions on Information and System Security (TISSEC).-2000 - vol. 3, No. 1. - P. 30-50.

2. Соломон Д. Внутреннее устройство Microsoft Windows 2000. Мастер-класс [Текст] / Д. Соломон; М. Руссинович. - М.: Изд. дом "Русская редакция"; Спб.: Питер, 2001. - 752 с.

3.Москвин Д. А. Метод - оптимизации настройки безопасности ОС Windows [Текст] / Д. А. Москвин // Материалы всероссийской конференции "Методы и технические средства обеспечения безопасности« информации". - 2007. - с.27-28.

4. Owre, S. PVS: A Prototype Verification System. Proc. of 11-th International Conference on Automated Deduction [Электронный ресурс] / S. Owre, N. Shankar, J. Rushby. — LNCS 607:748-752. - Springer. - 1992. - URL http://pvs.csl.sri.com/, режим доступа: свободный.

5. Брагг, Р. Система безопасности Windows 2000 [Текст] / Р. Брагг. - М.: Изд. дом "Вильяме", 2001. - 592 с.

6. Gollmann, D. Computer Security [Текст] / D. Gollmann. - John Wiley and Sons, 1999. - 320 p. - ISBN 0471978442.

7. Sloman, M. Engineering Policy-Based Ubiquitous Systems [Текст] / M. Sloman, E. C. Lupu // Computer Journal. - 53(7) - 2010. -P. 1113-1127.

8. Москвин Д. А. Методология оценки эффективности управления информационной безопасностью и оптимизации рабочей безопасной конфигурации для операционных сред [Текст] / Д. А. Москвин, М. О. Калинин // Проблемы информационной безопасности. Компьютерные системы. - 2010. - № 1. - с. 27-31.

9. Москвин, Д. А. Автоматизация настроек безопасности информационных систем [Текст] / Д. А. Москвин, М. О. Калинин // Сборник материалов XII Санкт-Петербургской международной конференции "Региональная информатика (РИ-2010)". -2010. - с.42-43.