ЗАЩИТА ПРОГРАММ ОТ АВТОРИЗОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

М.П.РЕВОТЮК, Е.П. БАЦЕКИНА

Статистика компьютерных преступлений показывают доминирование угроз безопасности от сотрудников организации. Авторизованные пользователи имеют легитимную возможность физического доступа к рабочим станциям и разделяемым файлам локальных вычислительных сетей.

Операционные системы семейства Windows 2000/XP/2003, предоставляя необходимые средства контроля последовательности событий раскрутки вычислительного процесса, начиная от загрузки операционной системы, автоматически не создают достаточные условия безопасности. Объект рассмотрения –специализированные системы динамической защиты программ, обеспечивающие, в частности, организацию фоновой аутентификации, удаленный контроль условий целостности, проверку наличия аппаратного ключа, автоматическое восстановление .

Обрамлением интервала активности пользователя на рабочей станции являются события, контролируемые процессом Winlogon. Обработка событий реализуется динамически подключаемой библиотекой GINA, которая может быть заменена прикладной версией. Для обеспечения стандартной функциональности или поддержки клиентов других операционных систем удобно применить каскадный фильтр операций вызова функций библиотеки. В результате имеется возможность связи стандартных событий с наличием аппаратного идентификатора или ключа.

При этом речь не идет о подмене стандартного интерфейса управления сеансами посредством смарт-карт, а об усилении набора условий запуска прикладной программы.

Взаимосвязь агентов контроля и восстановления, размещаемых на сети, обеспечивается построением взаимно аутентифицированной связи “клиент-сервер” на основе SSPI, где обе стороны представлены стандартными учетными записями LSA. Ввиду доступности процессу Winlogon сети до и после обмена контекстами безопасности, возможно использование сертифицированных протоколов криптозащиты. Включение в пакет дополнительной аутентификации условия отказа в открытии сеанса вне регламента эксплуатации рабочей станции или сервера используется как прием скрытия активизируемых элементов системы или защиты критических ресурсов системы.