УДК 681.327

МОДЕЛЬ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТА И ОЦЕНКА ЕЕ КАЧЕСТВА

Докт. физ.-мат. наук, проф. ***ЗУЙКОВ И. Е., КРИВИЦКИЙ П. Г.***

Белорусский национальный технический университет

В настоящее время автоматизированные системы безопасности объектов (АСБО) активно развиваются в направлении обеспечения комплексного контроля и управления подсистемами охранной и пожарной сигнализаций, видеонаблюдения и контроля доступа [1].

Такие комплексные (интегрированные) системы, как правило, выполняют свои функции для всего объекта, на котором они установлены. Компьютеризация данных систем безопасности и использование наряду с современной «высокоинтеллектуальной» аппаратурой специально разработанного программного комплекса в качестве системного ядра являются необходимым условием их успешной работы.

Качественные показатели функционирования, определяемые из необходимости достижения некоторого приемлемого уровня безопасности, сильно варьируются в зависимости от размеров и сложности объекта, на котором система установлена и функционирует. Очевидно, обеспечение безопасности для объекта, имеющего тысячу датчиков, сотню исполнительных органов, установленных в соответствующем количестве помещений, предъявляет более высокие требования к системе, чем для объекта, на котором установлен десяток датчиков. Поэтому для интегрированных систем безопасности (ИСБ) крупных и особо важных объектов является актуальной проработка методологии алгоритмов функционирования их программного ядра.

Современный уровень развития высоких, в том числе информационных, технологий позволяет гибко реализовывать ИСБ на основе группы из нескольких компьютеров, расположенных в логически предпочтительных местах (проходная, бюро пропусков, центр контроля и управления безопасностью), соединенных между собой локальной сетью. В качестве базовой операционной системы (ОС) для ИСБ обычно используется Windows NT фирмы Microsoft (США). Такой выбор обусловлен высокими показателями надежности, развитыми средствами сетевого взаимодействия и централизованного администрирования пользователей и сетевых ресурсов всей группы компьютеров (домена).

Вышеизложенные причины для выбора базовой ОС являются достаточно важными, но следует учесть, что программный комплекс ИСБ реализует алгоритмы контроля и управления для большого количества параллельно функционирующих территориально распределенных датчиков (шлейфов сигнализации, считывателей кодов) и управляющих органов (турникетов, дверных централей, устройств подсистемы обеспечения жизнедеятельности). То есть, это – управляющая программа, функционирующая параллельно со многими приборами в режиме реального времени. Возможности эффективной реализации такого режима работы у ОС Windows достаточно скромные, поскольку она не является системой реального времени.

Кроме функциональных недостатков в ОС Windows имеются программные ошибки, обусловленные ее сложностью, универсальностью, а также наследованием в новых версиях некоторых ошибок их предшественниц. Значительное число пользователей, обладающих познаниями в программировании, осведомлено об ошибках операционных систем [2, 3], что снижает безопасность их использования.

Многочисленные производители программного обеспечения и компьютерной техники во всем мире настойчиво требуют у компании Microsoft открыть исходный программный код ОС, обвиняя ее в монополизме, сдерживании прогресса в компьютерной и программной индустрии. В случае положительного решения данного спора Windows станет совершенно открытой системой.

Учитывая вышеизложенное, выполнение разработки программного комплекса ИСБ в среде Windows допустимо на этапе проектирования, разработки и отладки макета и первой опытной версии системы безопасности. Тиражирование программного комплекса на объектах защиты увеличивает вероятность его подробного изучения с целью поиска слабых мест в его защите. Из известных недостатков в защите программного комплекса и ОС, в среде которой он функционирует, нарушитель в соответствии с положениями научной парадигмы информационной безопасности [3] будет стремиться выбрать самое слабое место (или попытается использовать комбинацию недостатков).

Поэтому качественным скачком в развитии систем безопасности является последующий перевод их программного ядра на более подходящую для выполнения данной функции ОС.

Разработка программного ядра включает, прежде всего, определение стратегии сбора информации о состоянии датчиков и выдачи управляющих команд в приборы ИСБ. Функционируя в среде, вытесняющей приоритетной многозадачности Windows при использовании стандартных средств ОС, получение каждого тревожного сообщения и выработка реакции программного ядра должны происходить либо мгновенно, либо в рамках специально созданного программного потока. В первом случае стратегия действий системы безопасности ограничена примитивными реакциями типа «сработал датчик – отобразили камеру на монитор», «сработал датчик – включили сирену», значительно уступая возможностям ее конфигурирования и централизованного управления.

Типичная возможная ситуация – сотрудник при постановке помещения на охрану нарушил регламентированную последовательность действий, что через определенное время привело к возникновению тревоги от шлейфа сигнализации, контролирующего дверь. Требуется обнаружить комбинацию этих двух сообщений – о закрытии двери от подсистемы контроля доступа и последующей тревоге от подсистемы охранной сигнализации. Затем следует произвести элементарные действия: в сетевой базе данных по коду карточки определить личность нарушителя, информировать о нарушении дежурного оператора с предоставлением ему фотографии и других данных о сотруднике, а также блокировать выходной турникет для кода его карточки.

Если для выделения таких разделенных во времени событий создавать специальный программный поток для обработки каждого события в системе и отыскивать их характерные сочетания, то это приведет к перегрузке системы перед началом рабочего дня и сразу после его завершения. Аналогичную ситуацию может попытаться создать и нарушитель, инициировав ряд тревожных сообщений (например, многократно открывая и закрывая одну дверь).

В случае решения вопроса перегрузки системы при выполнении большого количества программных потоков обработки тревожных сообщений остается проблема зависимости программного ядра ИСБ от среды ОС. Особенности работы, показатели надежности ОС Windows явно не идеальны для функционирования программного ядра системы безопасности.

Использование возможностей локальной сети позволяет, конечно, перенести нагрузку параллельной обработки событий на обработчики шлюзовых компьютеров, предоставив им реализацию стратегии параллельного управления. Однако, это не решение проблемы, а перенос ее на другой уровень.

Разумной альтернативой многозадачности ОС может стать самостоятельная реализация механизма параллельности управления, который является отражением параллельности функционирования датчиков и приборов ИСБ. Для этого можно использовать результаты научных разработок в области сетей Петри, в частности средств описания параллельных алгоритмов логического управления [4].

В системе безопасности все датчики (шлейфы), исполнительные органы (релейные выходы) и, при необходимости, их отдельные и другие части аппаратуры системы безопасности можно

представить в виде программных объектов. Такими же объектами являются контролируемые участки здания (помещения), состояния тревог, элементы временной задержки и т. д. Для каждого объекта определяются исполняемый программный код, входные метки, состояния активности и выходные метки, т. е. указатели на объекты, которые активизируются при переходе данного объекта в неактивное состояние. Аналогично ОС Windows программно организуется цикл сообщений, в котором каждое необработанное сообщение должно быть извлечено из очереди сообщений данного объекта и обработано, т. е. передано для активизации объекту с соответствующей меткой.

Ввиду специфики управления системой безопасности (типичной задачей логического управления, не требовательной к ресурсам вычислительной среды) такая программная организация не требует слишком сложных и объемных программных текстов и тесного взаимодействия с ресурсами ОС. Поэтому ее реализация вполне осуществима в рамках сравнительно небольшого программного проекта.

В этом случае сохраняется возможность параллельного выполнения задач и обработки тревожных сообщений (выполнением программных кодов объектов). Пиковая нагрузка на программную систему при обработке порядка сотен одновременно активизируемых объектов тревоги с периодом прохода очереди объектов в одну секунду не представляет собой трудновыполнимую задачу.

Кроме устранения зависимости от базовой ОС, создание программного ядра с автономной реализацией параллелизма логического управления позволяет с минимальными затратами организовать аудит и администрирование работы системы безопасности.

В то же время реализация программного ядра в среде другой ОС не означает полного отказа от преимуществ ОС Windows и огромного количества программного обеспечения. Программное обеспечение ИСБ представляет собой комплекс программ, выполняющихся на нескольких компьютерах и обеспечивающих осуществление различных функций, часть из которых (анализ и подготовка отчетности, резервное копирование и восстановление данных системы, учет кадров и посетителей) не столь критична ко времени выполнения, надежности (живучести) и эффективно реализуется в среде Windows.

Таким образом, комплексную систему безопасности объекта следует качественно оценивать не только по наличию в ней ряда функциональных возможностей (гибкости конфигурирования, криптографической программно-аппаратной защиты, легкости подключения драйверов новых устройств). Необходимо также учитывать степень независимости реализующего стратегию управления программного ядра от среды операционной системы, а также наличие реализации системно-независимого параллельного алгоритма логического управления приборами и подсистемами безопасности объекта.

ЛИТЕРАТУРА

1. Интегрированная система технических средств охраны объекта / И. Е. Зуйков, Н. Н. Кравчук, П. Г. Кривицкий и др. // Тез. конф. ППС, сотруд., асп. и студ. БГПА. – Мн., 2000.

2. **Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.** Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 1999.

3. Компьютерная преступность и информационная безопасность / Под общ. ред. А. П. Леонова. – Мн.: АРНИЛ, 2000.

4. **Закревский А. Д.** Параллельные алгоритмы логического управления. – Мн.: ИТК НАН Беларуси, 1999.