К. С. Седых, Универсальный драйвер охранно-пожарной сигнализации для автоматизированной информационной системы управления интегрированной системой безопасности “Бастион”,
Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки, 2001, выпуск 12, 191–194

УДК 681.5

К.С. Седых

УНИВЕРСАЛЬНЫЙ ДРАЙВЕР ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ ДЛЯ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНТЕГРИРОВАННОЙ СИСТЕМОЙ БЕЗОПАСНОСТИ «БАСТИОН»

Автоматизированные информационные системы (АИС) относятся к классу расширяемых систем, не связанных с конкретным набором оборудования. Данные системы обеспечивают наиболее гибкий подход к интеграции подсистем безопасности, дают возможность адаптации к оборудованию, удовлетворяющему всем требованиям заказчика без создания заново всего программного комплекса, а добавляя или изменяя только нужную программу управления (драйвер) соответствующего устройства. Создан новый универсальный драйвер охранно-пожарной сигнализации (ОПС), решающий широкий круг задач по обеспечению безопасности.

В настоящее время увеличиваются требования к обеспечению безопасности предприятий и организаций различных форм собственности, растет число охранных средств и операторов, занимающихся их обслуживанием и реагирующих на различного рода нештатные ситуации в процессе работы. При этом, как правило, с ростом масштабов объектов увеличение количества операторов не приводит к улучшению безопасности предприятия в целом. В связи с этим необходимо применять различные технические средства для слежения за состоянием объекта.

Развитие микроэлектроники привело к созданию высоконадежных и доступных по цене цифровых систем охранно-пожарной сигнализации (ОПС), обеспечивающих своевременную информацию о пожаре и проникновении на объект; телевизионных систем наблюдения (ТСН), позволяющих визуально контролировать ситуацию на объекте; систем контроля доступа (СКД), которые обеспечивают поддержку безопасного режима на предприятии.

Использование программных средств позволяет провести интеграцию охранного оборудования, что было невозможно сделать аппаратно.

Разработана модель построения программ, позволяющих интегрировать средства безопасности (охранно-пожарные системы, системы телевизионного наблюдения и др.) в единую охранную систему.

Система концентрирует на экране компьютера всю информацию об объекте. Информация представляется в виде планов объекта, на которых отображено расположение датчиков, телекамер, вспомогательных устройств и их текущее состояние. Система позволяет осуществлять дистанционное управление режимами отображения видеоинформации. При возникновении тревожного события система предоставляет полную картину происшествия, рекомендуемые действия, а при бездействии оператора способна выполнить некоторые акции сама в соответствии с заданной программой. АИС дает возможность разграничения доступа к ресурсам охраны. Ведение протокола событий позволяет анализировать действия оператора и уменьшает риск, связанный с недобросовестными действиями персонала охраны.

Была разработана расширяемая система, не связанная с конкретным набором оборудования, отвечающая требованию универсальности, реализующая интеграцию подсистем безопасности и типы охранного оборудования без создания заново всего программного комплекса, а добавляя или изменяя только программу управления (драйвер) нужного устройства.

АИС состоит из нескольких отдельных программных модулей: ядра системы и набора драйверов.

Ядро обеспечивает все интерфейсные функции: настройку системы, интерфейс с пользователем, ведение протокола событий, разграничение доступа к системе, различные сервисные функции, интерфейс с драйверами устройств. Здесь реализуется преобразование сообщений драйверов в текстовые сообщения пользователю; обработка сообщений и формирование реакции на них, а также обработка команд пользователя.

В функции каждого драйвера входит взаимодействие со специфическим для каждого драйвера оборудованием и обмен информацией с ядром системы. Такая архитектура программного обеспечения дает возможность несложного подключения новых драйверов, а значит, дальнейшего развития системы безопасности за счет подключения к ней новых типов оборудования.

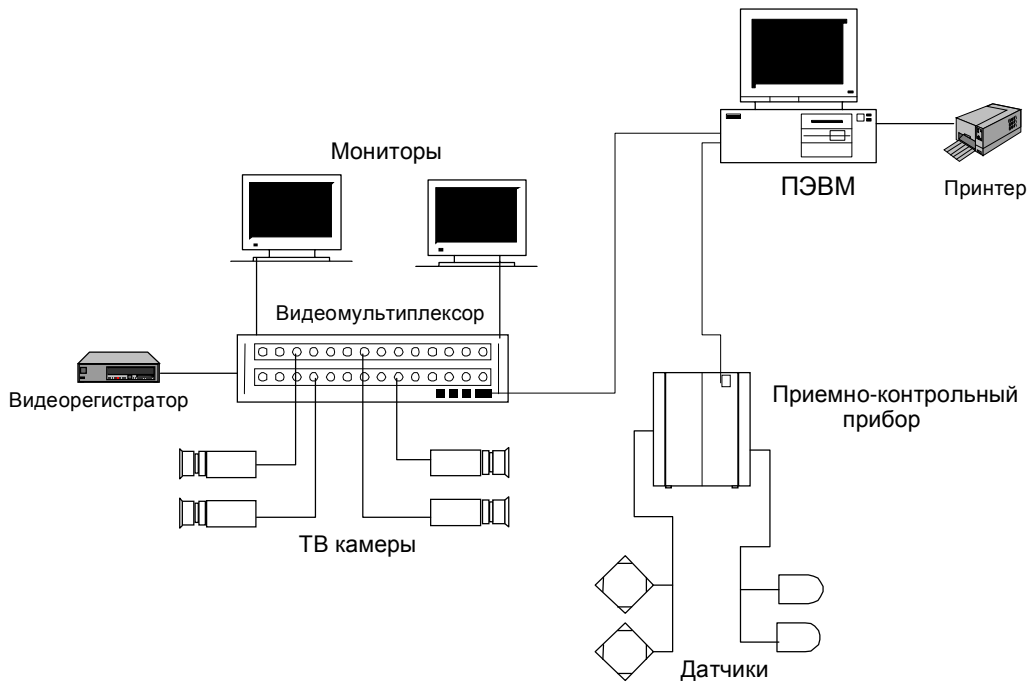
Важной проблемой при работе с системами безопасности является надежность. Поэтому в программном продукте минимизирована возможность потери информации, регламентированы действия пользователей системы.

Другой проблемой, возникающей при проектировании программ управления системами безопасности, является наглядное представление событий, происходящих в системе. Это необходимо для обеспечения наиболее быстрой и адекватной реакции оператора системы на происходящие события, представленные графически, текстовым или звуковым сообщениями. Наиболее целесообразно подавать информацию сразу в нескольких вариантах.

Система должна обеспечивать отображение всех поступающих событий в графическом режиме на мониторе компьютера и обрабатывать их в соответствии с параметрами, заданными при настройке. Кроме того, для обеспечения наглядности происходящих событий необходимо использовать графические планы охраняемой территории для показа места возникновения какого-либо события при помощи пиктограмм устройств определенного типа. Реализация лишь одного из предложенных вариантов дает меньше уверенности в том, что пользователь сможет быстро оценить обстановку. Дополнительно, для привлечения внимания пользователя, могут использоваться звуковые сообщения, выдаваемые по событиям и настраиваемые при установке системы.

В соответствии с действующими за рубежом, а с 1998 года и в России, стандартами безопасности, определяющими требования к техническим средствам обеспечения безопасности важнейших объектов, каждая подсистема безопасности должна в качестве центрального устройства содержать специализированную ЭВМ, снабженную своими собственными средствами программирования, хранения программ, отображения информации, протоколирования событий и т. д.

В интегрированной системе безопасности компьютер выполняет роль общего средства управления и объединенного устройства отображения, а также существенно расширяет набор предоставленных оператору сервисных функций, не являясь, однако, определяющим режим охраны объекта. Структурная схема проектируемой системы изображена на рисунке (1).



Р и с. 1. Структурная схема интегрированной системы безопасности

При проектировании АИС управления интегрированной системой безопасности «Бастион» были разработаны драйверы устройств ОПС для контроля состояния этих устройств. Этими устройствами являются: устройство охранно-пожарной сигнализации Vista-501, пожарная станция Esa8 фирмы ESMI и пожарная станция UniPos FS5008 болгарской фирмы UniPos. На основе накопленного опыта и анализа сообщений и драйверов данных устройств разработан универсальный драйвер ОПС. Он позволяет описывать формат сообщений от устройств безопасности, типы сообщений, количество сообщений и т.д.

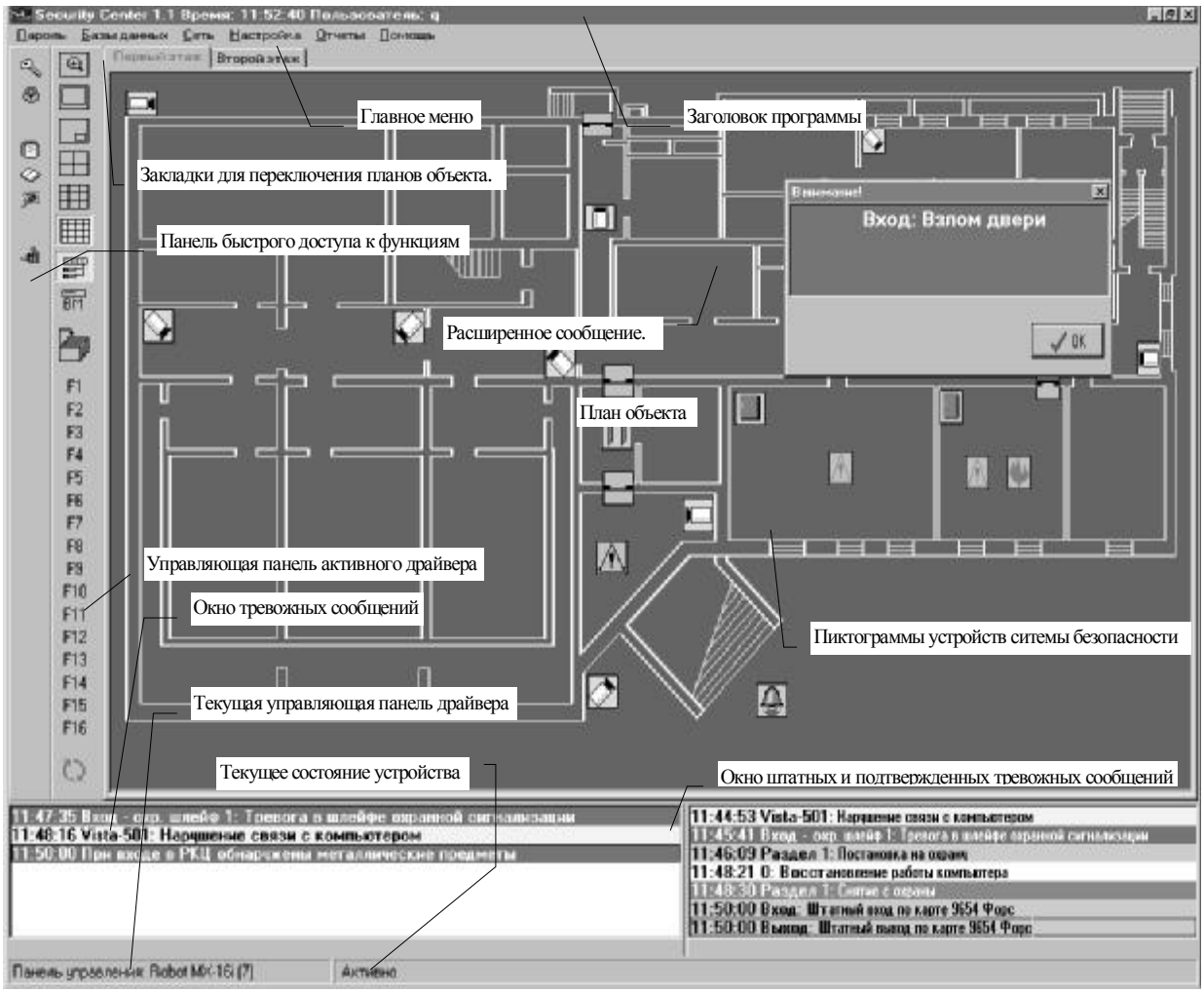
При применении универсального драйвера ОПС возможно дальнейшее развитие системы безопасности. Для добавления нового устройства необходимо (например, при расширении предприятия, когда возникает потребность оснастить ОПС еще одно здание; при добавлении

новой системы безопасности, для того, чтобы вписать ее в существующую систему или поднять уровень безопасности предприятия) проанализировать формат сообщений от устройства и описать их в универсальном драйвере.

В дальнейшем кроме протоколирования возможно управление устройствами посредством универсального драйвера ОПС (если для устройства стандартно предусмотрено наличие управляющих команд).

Таким образом, данная АИС дает возможность несложного подключения новых драйверов и дальнейшего развития системы безопасности за счет подключения к ней новых типов оборудования.

Интерфейс программы обеспечивает отображение информации в графическом режиме изображенном на рис.2.



Р и с. 2. Пример экрана программы

Как видно из данной схемы, интерфейс АИС содержит следующие элементы, присутствующие на экране постоянно:

- название программы;
- текущую дату и время;
- фамилию оператора;
- основное меню управления и настройки параметров;
- клавиши быстрого доступа к часто используемым функциям системы;
- зоны штатных и тревожных сообщений;
- планы объекта с закладками, на которых указаны их названия;
- пиктограммы основных узлов системы.

Также обеспечен оперативный вывод окон с описанием события и рекомендуемой реакцией оператора.

Визуальный контроль за состоянием элементов системы осуществляется путем назначения каждому состоянию устройства определенной цветовой палитры пиктограммы. Для обеспечения большей информативности системы предусмотрена возможность использовать звуковые (голосовые) сообщения о событиях и предпринимаемых действиях.

Автоматизированная информационная система управления интегрированной системой безопасности разработана под операционные системы Windows9x, Windows NT в среде программирования Delphi 3.0 фирмы Borland.

Для защиты АИС управления интегрированной системой безопасности был применен электронный ключ HASP фирмы Aladdin.

В результате проведенных исследований был разработан подход к программной реализации интегрированной системы безопасности. Система отвечает таким важным требованиям, как разграничение доступа к охранным ресурсам и ведение полного протокола событий в системе, включая и действия операторов, что обеспечивает защиту от такого явления, как “внутренний саботаж”.

Применение программы управления интегрированной системой безопасности дает возможность ограниченному числу операторов системы оперативно обрабатывать значительный объем информации за счет наглядности представления данных и автоматизации ряда функций подсистем. Единообразное протоколирование данных в системе позволяет осуществлять, при необходимости последующий просмотр и анализ работы системы безопасности.