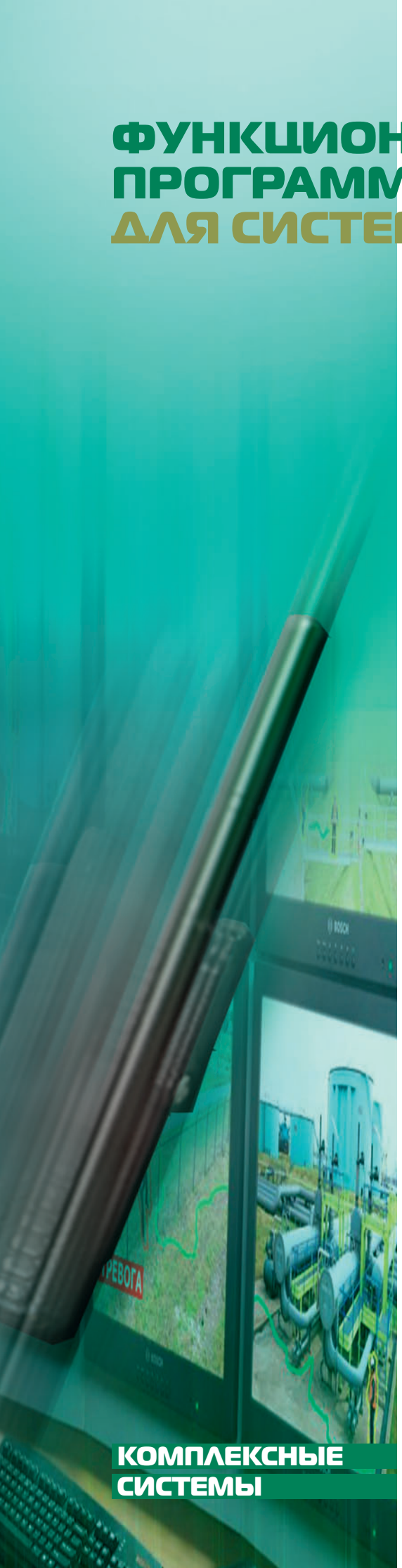
ФУНКЦИОНАЛЬНОСТЬ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ

Сергей Лёвин
главный конструктор ГК СИГМА



КОМПЛЕКСНЫЕ СИСТЕМЫ

Прикладное программное обеспечение верхнего уровня системы безопасности является своего рода венцом и лицом всего проекта. От возможностей ПО во многом зависит эффективность работы всей системы безопасности, эффективность взаимодействия персонала службы безопасности с оборудованием системы безопасности и взаимодействие различных подсистем в комплексной системе безопасности. Для оценки полноты функционала программного продукта нужен некий набор требований, на соответствие которым и можно произвести оценку. К сожалению, нормативных требований к интерфейсу пользователя, составу и функциональным возможностям ПО для объектовых систем безопасности в настоящее время в России не существует. Поэтому заказчик при выборе ПО должен опираться, прежде всего, на собственные требования. И хорошо, когда они есть. Но часто бывает, что на этапе выбора, проектирования и даже развертывания системы четких требований не существует. И тогда в процессе эксплуатации системы обнаруживаются всевозможные подводные камни и узкие места. С этим приходится либо мириться, либо путем доработок ПО «по месту» пытаться получить более-менее приемлемое решение. Для минимизации подобных рисков попробуем перечислить основной состав и функциональные характеристики программного обеспечения по различным подсистемам и рабочим местам.

Проектирование системы безопасности чаще всего начинают с определения необходимых подсистем и выбора оборудования для них. Дальше встает задача организации верхнего уровня в виде автоматизированных рабочих мест операторов службы безопасности. Если все подсистемы реализованы на оборудовании одного производителя, то с верхним уровнем, как правило, проблем не возникает. Этот же производитель предоставляет и программное обеспечение. Сложнее, если оборудование разнородное. Тогда или организуются независимые рабочие места для каждой подсистемы, правда в этом случае система не получится интегрированной, или нужно интегрирующее ПО, которое может работать с оборудованием всех подсистем. При выборе такого объединяющего ПО нужно четко сформулировать требования к нему в плане режимов работы: будет ли это только интеграция дежурного режима всех подсистем или дополнительно нужно и полноценное централизованное конфигурирование и администрирование.

РАБОЧЕЕ МЕСТО: ПОСТ ОХРАНЫ

ОХРАННО-ПОЖАРНАЯ СИГНАЛИЗАЦИЯ

Основная задача ПО дежурного режима ОПС – передача оператору тревожных извещений от приемно-контрольного оборудования, контроль состояния и управление объектом охраны. Приоритет, естественно, за приемом и обработкой тревожных извещений. Пользовательский интерфейс приложения должен быть спроектирован таким образом, что в каком бы «ме-

сте» программы не находился в данный момент оператор – тревогу он пропустить не должен. Также важно, как организована работа в случае множественных тревог. Оператор не должен потерять ориентацию в пространстве, если тревожных извещений несколько, и они произошли в разных частях охраняемого объекта. Возможность адекватной оценки обстановки здесь крайне важна для принятия правильных решений в сложной ситуации. В любое время оператор должен иметь возможность видеть состояние охраняемого объекта, для этого чаще всего объект охраны представляют в виде набора графических планов с размещенными на них условными значками технических средств. Такой способ представления дает возможность показывать технические средства охраны в привязке к расположению их на объекте. Если охраняемый объект достаточно большой, то отобразить на одном экране состояние всей системы достаточно проблематично, но для быстрой интегральной оценки это бывает удобно. Для этого используются текстовые сводки или общий графический план объекта, по которому можно одним взглядом определить, что в целом происходит. Необходимым элементом интерфейса является окно протокола событий, куда записываются все сообщения от системы безопасности.

СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

В интегрированной системе безопасности с единым верхним уровнем рабочее место оператора ОПС может, да и должно, включать в себя функции дежурного режима СКУД. Во многом схожа и организация работы с техническими средствами: также оборудование точек доступа отображается в виде значков на графпланах, оператор получает тревожные и информационные события, может просматривать состояние оборудования и выполнять команды управления. Кроме того, важной функцией является возможность оперативного определения местоположения людей по событиям от СКУД. Это позволит быстро найти местонахождение любого пользователя СКУД на объекте. Или определить количество и состав людей в той или иной зоне объекта. Эта информация может быть полезна для соблюдения режима доступа или оперативной эвакуации людей в случае чрезвычайной ситуации. В качестве отдельного рабочего места можно выделить КПП или проходную. Здесь организуется контроль прохода сотрудников и посетителей с предоставлением оператору информации о персональных данных пользователя, включая фотографию, паспортные данные и т. д.

СИСТЕМА ОХРАННОГО ТЕЛЕВИДЕНИЯ

С каждым годом видеонаблюдению в системах безопасности отводится все большее место. Оператор получает информацию от десятков и сотен видеокамер. Среди этого огромного потока данных система должна помочь человеку выделить действительно важные моменты. Для этого применяются интеллектуальные алгоритмы анализа видеоизображения с автоматическим выделением потенциально важных для оператора ситуаций. Кроме того, в комплексных системах очень важна интеграция видео с другими подсистемами, когда при срабатывании, например, охранной сигнализации оператору автоматически на тревожный монитор выводится изображение с камер, показывающих место срабатывания.

РАБОЧЕЕ МЕСТО: БЮРО ПРОПУСКОВ

На объектах, оснащенных СКУД с большим количеством пользователей и посетителей, появляется необходимость организации автоматизированного бюро пропусков. Для полноценной реализации этой задачи в состав ПО должен входить целый набор специализированных программных модулей. ПО для подготовки заявок на пропуск – Терминал заявок. Тип пропуска зависит от категории пользователя СКУД. Как правило, различают три основных категории: постоянные сотрудники, временные сотрудники и посетители. Если на объекте охраны к режиму доступа предъявляются серьезные требования, необходимо организовать рабочее место согласования заявок на пропуск. В случае одобрения заявки на пропуск данные по заявке становятся доступны оператору бюро пропусков. В рамках АРМ оператора бюро пропусков вводятся персональные данные пользователя. Это может делаться как вручную, так и автоматически с помощью сканера удостоверения личности. Также могут записываться биометрические данные пользователей: фотография, отпечатки пальцев. Для этого рабочее место должно быть оснащено соответствующим оборудованием: фотокамера, биометрический сканер. Далее пользователю выдается электронный идентификатор для работы в СКУД. В настоящее время чаще всего для этого используются бесконтактные электронные карты. По желанию заказчика карты могут быть персонализированы. На специальном принтере непосредственно на пластике карты печатаются необходимые реквизиты пропуска: имя, должность, фотография и т. д. Для подготовки шаблона печати и связывания шаблона с данными конкретного пользователя требуется специализированное ПО, которое может входить в состав поставки кард-принтера или в состав ПО системы безопасности.

АНАЛИЗ ДАННЫХ ОТ СИСТЕМЫ БЕЗОПАСНОСТИ

Протокол событий системы несет массу полезной информации для различных служб организации. Анализируя протоколы событий, служба безопасности может выявлять и разбирать криминальные ситуации на объекте охраны. Руководители подразделений могут получать отчеты о времени прихода и ухода с работы подчиненных для контроля трудовой дисциплины. Бухгалтерия, используя те же данные, сформирует табель учета рабочего времени. Подготовка и обработка информации для решения этих задач может выполняться как самим ПО системы безопасности, так и корпоративными информационными системами. Во втором случае нужно предусмотреть возможность передачи данных между системами.

НАДЕЖНОСТЬ ФУНКЦИОНИРОВАНИЯ ПО

В задачах построения надежных отказоустойчивых систем большую роль, наряду с оборудованием, несомненно, играет и программное обеспечение. Каким бы надежным ни была аппаратная часть системы, если ПО верхнего уровня перестанет нормально функционировать, тревожные извещения просто не дойдут до оператора. Надежность работы ПО в большей степени зависит, конечно, от качества разработки продукта. Тем не менее, источником сбоя могут служить не только непосредственные ошибки прикладного ПО, но и целый набор факторов, связанных с работой операционных систем, антивирусного ПО и т. д. Например, неполная совместимость компьютерного железа и системного ПО, выявиться это может уже в процессе эксплуатации системы. Также проблемы могут начаться после очередного обновления стороннего ПО: операционной системы, антивирусной программы или драйверов устройств. В этом случае отказоустойчивость может быть достигнута за счет резервирования ключевых программных компонентов. Немаловажную роль играет архитектура построения программной системы. Для надежной работы в ней должны быть исключены или зарезервированы узкие места, от работоспособно-

сти которых зависит функционирование всей системы в целом. Если ПО основано на клиент-серверной архитектуре, то выход из строя сервера может привести к полной неработоспособности всех клиентских программных модулей. Для исключения такой ситуации необходимо предусмотреть резервирование серверных компонентов. То же самое относится к системам, где в качестве диспетчера работы приложений используется программное ядро. Отсутствие связи с ядром приводит к невозможности обмена сообщениями между программными модулями. В таких случаях наиболее надежными являются распределенные решения, не имеющие единой точки отказа и предлагающие альтернативные варианты продолжения работы при выходе из строя какой-либо части программной системы.

ВОЗМОЖНОСТИ МАСШТАБИРОВАНИЯ

При проектировании системы безопасности нужно учитывать возможное расширение системы в будущем: добавление новых подсистем, увеличение количества технических средств или автоматизированных рабочих мест, рост числа пользователей СКУД, объединение нескольких локальных систем и т. д. Конечно, все варианты будущего развития предусмотреть сложно. Однако, можно при выборе как технических средств, так и программного обеспечения выяснить возможности их масштабирования при росте объекта охраны. В противном случае, при невозможности увеличения какой-либо характеристики системы, придется полностью заменять все решение.

ИНТЕГРАЦИЯ С ДРУГИМИ СИСТЕМАМИ ОБЪЕКТА

Работа системы безопасности часто должна быть увязана с другими инженерными системами объекта. Например, на промышленных предприятиях система противопожарной защиты передает свои сигналы в АСУТП и ПАЗ (система противоаварийной защиты). По данным, поступающим от охранной сигнализации и СКУД, могут изменяться режимы работы систем освещения, отопления и кондиционирования. Если подобная интеграция производится на программном уровне, то ПО системы безопасности должно иметь соответствующие возможности. Например, в состав ПО может входить OPC-сервер, с помощью которого организуется взаимодействие систем.

РЕШЕНИЕ УЗКО СПЕЦИФИЧЕСКИХ ЗАДАЧ

Конечно, не все возникающие задачи на объекте можно выполнить решением из коробки. Иногда у заказчика возникают такие пожелания, что ни один продукт не может это реализовать без дополнительной доработки. В этом случае нужно исходить из принципиальной возможности таких доработок. Иногда производитель ПО предоставляет документированный программный интерфейс (API) к своей системе. Тогда заказчик может выполнить разработку нового функционального модуля своими силами или привлечь сторонних программистов. Но чаще всего доработки касаются уже существующих компонентов. И тут нужно заранее оговаривать с производителем ПО возможность и условия внесения изменений. В противном случае цена доработок может многократно превысить изначальную стоимость продукта.