

Интегрированная система безопасности "Цирконий – С2000" БАЖК.425621.002-03: структура, характеристики, особенности применения.

Интегрированная система безопасности (ИСБ) "Цирконий-С2000" БАЖК.425621.002-03 предназначена для использования в качестве системной основы для создания централизованных комплексов безопасности объектов различного назначения, в том числе расположенных на пространственно разнесенных территориях. Система обеспечивает разграничение и контроль доступа персонала внутри объекта, разграничение и контроль доступа к пультам управления, охрану периметров и расположенных на территории объекта зданий, сооружений, зон (помещений).

Система представляет собой многоуровневую автоматизированную систему (рис. 1) на основе сети персональных компьютеров и контроллеров, к которым подключаются технические средства обеспечения безопасности:

- а) средства обнаружения;
- б) кнопки экстренного вызова;
- в) кнопки отметки наряда;
- г) считыватели пропусков;
- д) устройства преграждающие управляемые – турникеты, двери, ворота с электромеханическими запирающими устройствами (ЭМЗУ) и т.п.;
- е) внешние устройства с релейными входами для управления исполнительными механизмами вспомогательных подсистем охранного освещения, звукового извещения и т.п.

Компьютеры системы, образующие станционную аппаратуру системы, объединяются в локальную вычислительную сеть (ЛВС) Ethernet. Функциональные возможности каждого компьютера определяются составом программного обеспечения, установленного на нем.

В общем случае система позволяет организовать:

- а) сервер базы данных (СБД), обеспечивающий централизованное хранение, защиту и использование информации системы;
- б) управляющий компьютер (УК), к которому физически подключены магистраль связи для обмена информацией с контроллерами в реальном масштабе времени;
- в) автоматизированное рабочее место (АРМ) охраны, обеспечивающее в круглосуточном режиме дежурным сотрудникам службы безопасности интерфейс по оперативному контролю и управлению периферийной аппаратурой с приоритетным отображением тревожных сообщений;
- г) АРМ административного уровня для обеспечения всех подготовительных информационных операций, необходимых для работы системы, и проведения аналитической работы по событиям в системе: изменения состояния технических средств, действия абонентов, действия операторов АРМ.

Количество компьютеров в системе не регламентируется. В минимальной конфигурации все функции стационарной аппаратуры системы совмещаются на одном компьютере. Частным случаем такой возможности является совмещение функций АРМ охраны с УК на одном компьютере, что приведено на рис. 1 для контрольно-пропускного пункта (КПП).

Каждый УК поддерживает обмен информации по 16 магистралям связи с контроллерами. В системе используются следующие интерфейсы магистралей связи:

а) ЦПКУ- 04 (специализированный интерфейс: максимальное количество контроллеров – 25 шт, максимальное расстояние – 5 км);

б) CAN (стандартный интерфейс: максимальное количество контроллеров – 31 шт, максимальное расстояние – 5 км);;

Подключение УК к магистрали осуществляется с помощью соответствующих коммуникационных комплектов.

В системе обеспечивается любое сочетание интерфейсов при построении магистралей связи данного УК.

При использовании интерфейса ЦПКУ- 04 возможно применение децентрализованного управления охраной помещений с помощью изделия "Терминал", организация постов охраны в локальных зонах пультами малой емкости на основе системы сбора и обработки информации (ССОИ) «Фокус-СМ», размещение контроллеров с рабочей температурой от -50 до $+50^{\circ}\text{C}$ (контроллеры К20) на протяженных периметрах. Кроме того, имеется возможность подключения устройства программирования допуска (УПД), представляющего собой пульт, размещаемый на рабочем месте уполномоченного лица, например, начальника цеха. УПД предназначено для оформления временного (на период до 30 суток) допуска персонала во внутренние зоны непосредственно с рабочего места уполномоченного лица, идентифицируемого по коду пропуска и паролю, набираемого на клавиатуре. Уполномоченное лицо может оформлять допуск только в зоны, разрешенные ему администратором системы.

При использовании интерфейса CAN (контроллеры К40) обеспечивается эффективная реализация режима реального времени, благодаря следующим возможностям: автоматического доступа к шине (режим мультимастерности), приоритетного разрешения коллизий при обращении к шине, обнаружению ошибок, автоматической ретрансляции пакетов, переданных с ошибкой, подтверждению доставки пакетов, автоматическому отключению неисправных узлов.

Контроллеры К40 могут работать по двум магистралям одновременно, что используется при построении отказоустойчивых вариантов системы на основе резервирования УК и магистралей связи. Основопологающим принципом обмена интерфейса CAN является случайный доступ подключенных к магистрали устройств и поэтому инициатором обмена выступает как УК, так и контроллеры К40, что существенно улучшает динамические характеристики системы.

ПО системы поставляется в виде комплекта модулей, перечень которых и архитектура ПО приведены на рис. 2.

Программное обеспечение

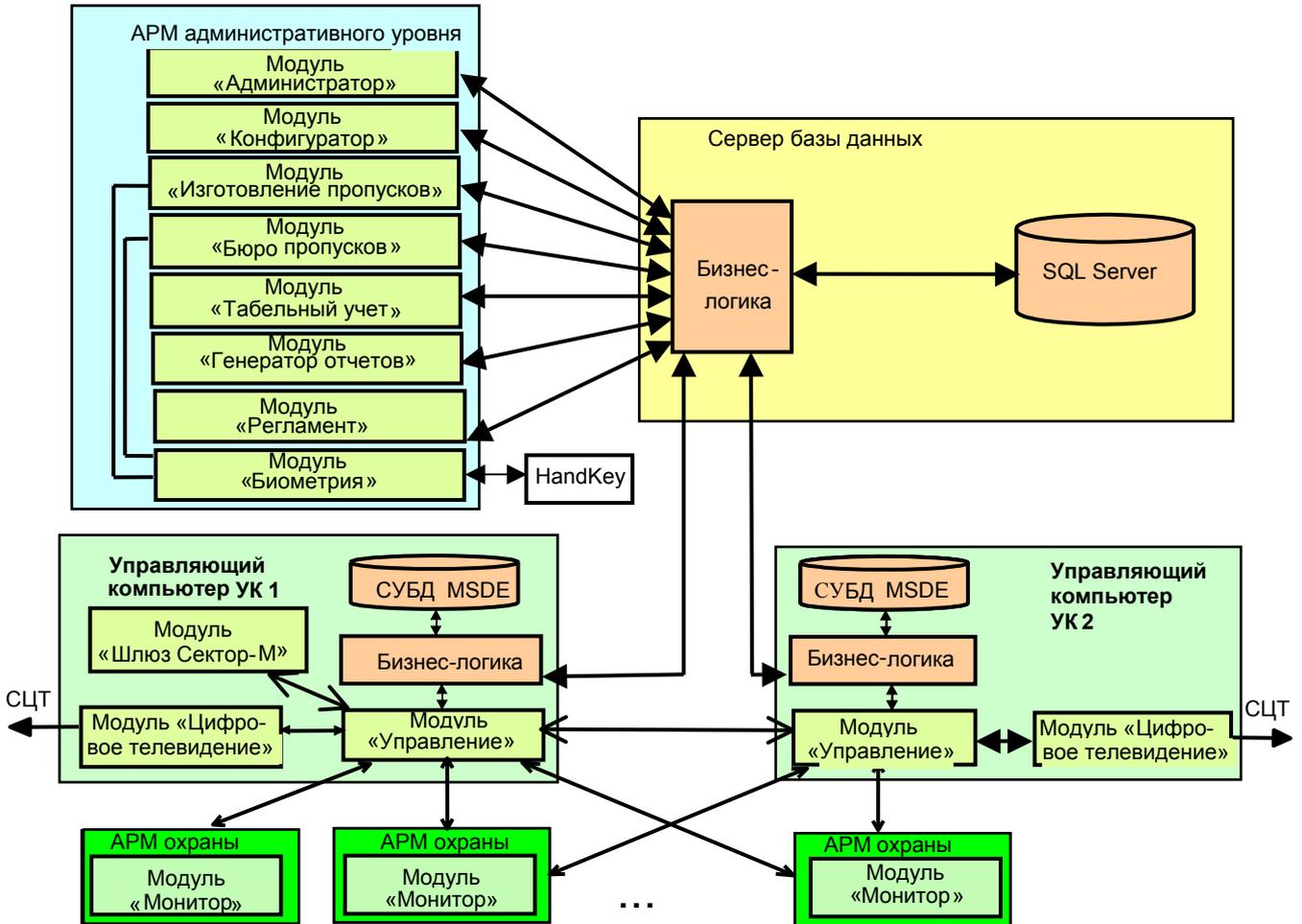


Рис. 2

Для доступа к данным используется трехуровневая модель, бизнес-логика выделена в промежуточный слой, который также отвечает и за репликацию данных между центральной базой данных и локальными базами. Приложения АРМов административного уровня являются клиентами центральной базы данных, модули «Управление» УК обмениваются оперативными сообщениями непосредственно между собой.

Функции СБД полностью реализуются программным продуктом MS SQL Server 2000 Standard (далее по тексту – SQL Server). Для СБД допускается использовать MS SQL Server 2000 Desktop Engine (далее по тексту – MSDE) при развертывании системы на одном компьютере.

Функции УК реализуются модулем «Управление». Для обеспечения возможности автономной работы (независимо от СБД) и уменьшения времени реакции системы на каждом УК создается локальная копия базы данных, управление которой выполняется с помощью MSDE. Все сообщения, связанные с подключенной к УК периферийной аппаратурой, регистрируются в первую очередь в локальной копии базы данных. При

изменении данных, запуске модуля или восстановлении связи репликация баз данных УК и СБД выполняется автоматически. От СБД на УК передаются данные по абонентам, операторам, техническим средствам. От УК на СБД передаются сообщения о событиях в системе: изменение состояния технических средств и каналов связи, действия абонентов, действия операторов. УК обеспечивает автоматическую инициализацию контроллеров для обеспечения их функционирования в автономном режиме при потере связи с УК и пересылку изменений в разрешительных данных по абонентам.

Функции АРМ охраны реализуются модулем "Монитор", который позволяет работать с несколькими УК, каждый из которых, в свою очередь может работать с несколькими модулями "Монитор", размещенными на разных компьютерах. Оператору, работающему с модулем "Монитор", назначаются полномочия, обеспечивающие управление и/или мониторинг соответствующих УК. Управление конкретным УК в текущий момент времени возможно только из одного модуля "Монитор", остальные модули «Монитор» позволяют осуществлять мониторинг УК. Для этого в системе реализованы функции сопоставления уровней полномочия операторов по управлению УК и уведомления операторов по передаче управления или об отказе в управлении УК при запросах на получение такой возможности.

Модуль "Монитор" предоставляет оператору возможность подачи управляющих команд для УК, периферийной аппаратуры, зон, точек доступа. Набор представляемых команд зависит от типа и текущего состояния объекта управления.

Система обеспечивает унифицированный интерфейс подключения сервисов. Интеграция периферийного оборудования обеспечивается подключением соответствующих сервисов для используемого оборудования. Каждому устройству соответствует своя DLL, содержащая параметры конфигурирования, команды управления, состояния и соответствующие им иконки. Для подключения нового устройства необходимо написать соответствующую DLL по соглашениям, принятым для системы, и включить в библиотеку с помощью модуля "Конфигуратор".

Особенности системы:

- функция "Antipassback" – постоянный контроль последовательности прохождения точек доступа по всей территории объекта, в том числе в условиях действия дестабилизирующих факторов (открывание аварийных дверей, отключение точек доступа);

- помимо правила «2...6» лиц имеется возможность задавать по каждой зоне список вскрывающих, что ограничивает возможности доступа абонентов в зоны, находящиеся под охраной;

- возможность по каждой точке доступа задавать период действия разрешения, в том числе децентрализованно с рабочих мест уполномоченных абонентов;

- программирование реакций системы при возникновении событий, связанных с изменением состояния периферийной аппаратуры;

- унифицированный интерфейс подключения сервисов, что упрощает процесс подключения оборудования различных производителей;
- горячее резервирование управляющих компьютеров;
- дистанционный контроль средств обнаружения;
- использование любого сочетания управления охраной помещений (автоматического, централизованного, децентрализованного).

При организации магистралей с интерфейсом CAN в системе используются контроллеры K40 (рис. 3). Для расширения функциональных возможностей к контроллеру K40 могут подключаться до 7 шт. расширителей адресных (РА). РА подключаются к K40 по отдельной магистрали RS-485.

Контроллер K40, расширители адресные РА

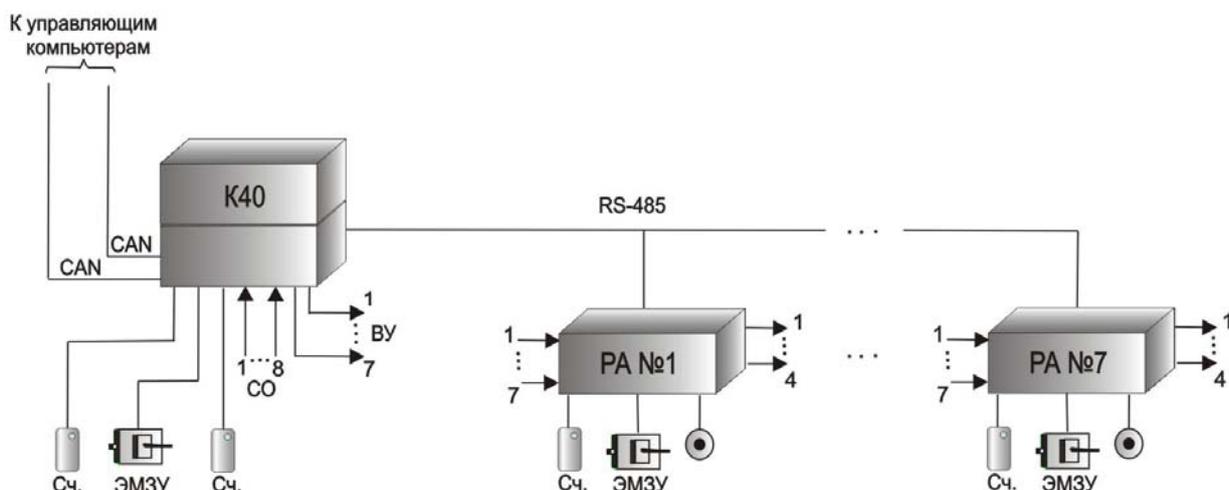


Рис. 3

Контроллер K40, реализующий функции контроля доступа и охранной сигнализации, обеспечивает:

- контроль прохода абонентов через одну точку доступа с двухсторонним контролем или две точки доступа с односторонним контролем;
- контроль состояния до 8 шлейфов СО ("обрыв", "короткое замыкание", "норма", "тревога");
- управление ЭМЗУ / турникетом;
- управление ВУ;
- коммутацию питания СО;
- подачу сигнала дистанционного контроля (ДК) на СО;
- обмен информацией по двум магистралям связи с УК;

- автоматический переход в автономный режим с накоплением информации при пропадании связи с УК и автоматическую передачу всех накопленных сообщений на УК при восстановлении связи;
- снятие с охраны и постановку на охрану зон;
- управление РА.

РА обеспечивает:

- контроль прохода абонентов через одну точку доступа с односторонним контролем;
- контроль состояния до 8 шлейфов СО ("обрыв", "короткое замыкание", "норма", "тревога");
- управление ЭМЗУ;
- управление ВУ;
- коммутацию питания СО;
- подачу сигнала дистанционного контроля (ДК) на СО;
- обмен информацией с К40 по магистрали RS-485;
- снятие с охраны и постановку на охрану зон.

Характеристики контроллера К40 и РА приведены в таблице 1.

Таблица 1

Характеристики К40, РА

Наименование	Вариант исполнения	
	К40	РА
Тип интерфейса	CAN (2 порта), RS-485	RS-485
Расстояние по магистрали от верхнего уровня, м, не более	5000	1200
Возможность работы с резервной магистралью	есть	нет
Количество подключаемых СО, кнопок, датчиков	8	8
Количество подключаемых Proximity считывателей Wiegand 26, шт.	2	1
Количество выходов для подключения внешних устройств, шт.	8	5
Количество цепей управления ВУ при напряжении ± 60 В и токе: - не более 2 А, - не более 200 мА.	2 6	1 4
Емкость базы данных карточек, шт.	16000	-
Емкость буфера передаваемых сообщений, шт.	16000	-
Рабочая температура, °С	от минус 40 до плюс 50	от минус 40 до плюс 50
Напряжение питания, В	от 20 до 30	от 20 до 30
Ток потребления, мА, не более	30	20
Габаритные размеры, мм	218 x 292 x 56,5	218 x 147 x 56,5

Особенности К40:

- возможность загрузки программного обеспечения по магистрали CAN;

- наличие самодиагностики:

а) при включении питания проходит тест внутренних узлов и в случае успешного завершения включается индикатор, сигнализирующий о нормальной работоспособности;

б) возможность проверки работоспособности всех входных и выходных цепей (в тестовом режиме);

в) индикатор на корпусе показывает наличие обмена с верхним уровнем;

- микропроцессорный анализ сигнала в шлейфах сигнализации для предотвращения саботажа;

- встроенная грозозащита входных и выходных цепей;

- наличие в цепях управления ВУ и питания самовосстанавливающихся предохранителей.

Для обеспечения надежности и живучести все АРМ охраны, УК и контроллеры имеют возможности работы в автономном режиме и автоматического перехода в централизованный режим. Нарушение функционирования отдельных составных частей не приводит к нарушению функционирования системы в целом.

В тех случаях, когда комплексы безопасности объектов должны сохранять централизованное управление при отказе отдельных составных частей, применяют резервирование. Система обеспечивает различные схемы резервирования составных частей административного и оперативного уровней управления (УК, коммуникационных комплектов, магистралей). Резервирование любого АРМ осуществляется путем установки соответствующего модуля на любой компьютер, подключенной к ЛВС системы.

В частности, при выходе из строя одного АРМ охраны модуль "Монитор", установленный на любом другом АРМ, в том числе и на УК, может быть запущен, что обеспечивает полное резервирование АРМ охраны. Все данные, необходимые для работы модуля "Монитор" (данные о конфигурации и состоянии УК), хранятся на УК и становятся доступны модулю "Монитор" после подключения к УК.

Система построена по модульному принципу и формируется из отдельных поставочных комплектов аппаратуры, программного обеспечения и монтажных частей, допускает подключение дополнительного оборудования и программирование управления по возникающим событиям. Это позволяет на основе системы без избыточных затрат создавать высоконадежные комплексы физической защиты ЯОО и проводить их поэтапное совершенствование.

**Для использования системы «Цирконий-С2000»
необходимо выполнять следующие условия:**

1. Рабочий проект должен быть выполнен или согласован с НИКИРЭТ.
2. Монтаж и инсталляция должны выполняться силами или с участием НИКИРЭТ, либо сторонними организациями прошедшими обучение в НИКИРЭТ.
3. Должен быть заключен договор на гарантийное и постгарантийное обслуживание системы.