

**Комплекс программ
автоматизации пунктов централизованной охраны «Эгида»
исполнение 02**

Описание применения.

Р.АЦДР.000 __-01 31 01

АННОТАЦИЯ

Настоящий документ предназначен для специалистов пунктов централизованной охраны (ПЦО), связанных с эксплуатацией системы «Эгида» исполнение 02 (комплекс программ автоматизации ПЦО, далее - программа). Он содержит сведения о назначении, возможностях, составе, структуре и условиях применения программы, правилах создания и эксплуатации ресурсов системы охраны – технических средств охранно-пожарной сигнализации, рабочих мест операторов, баз данных и др.

Для инсталляции и запуска программы необходимо руководствоваться документацией на операционную систему Windows-2000, используемые типы компьютеров и программно-аппаратные средства локальной вычислительной сети.

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программа предназначена для автоматизации и информационного обеспечения действий персонала ПЦО при обработке служебных и тревожных сообщений.

Программа выполняет следующие функции:

- создание и ведение информационной базы данных по объектам, абонентам и техническим средствам охраны;
- работу с системами передачи извещений (СПИ) «Фобос», «Фобос-А», «Фобос-Тр», «Фобос-3», «Юпитер», РСПИ «Струна-3М», РСПИ LARS (пульт DT RCI 3300), прибором УО-4С и с информаторными СПИ по протоколу ID Contact;
- автоматизированный контроль состояния объектов;
- прием и выполнение команд операторов;
- SMS – управление и SMS – мониторинг объектов (управление состоянием и уведомление абонентов об изменении текущего состояния объекта при помощи SMS-сообщений);
- обработку тревожной информации с учетом контроля времени на вход абонента, графика охраны, праздничных дней, типа охраны, типа шлейфа, типа подключения оконечного устройства на объекте и “ночного времени“;
- управление любым объектом в пределах емкости ПЦО;
- переключение рабочих мест операторов;
- информационное обеспечение действий оператора при обслуживании тревожных и служебных сообщений;
- обеспечение операторов справочной и статистической информацией.

2. КОМПЛЕКТ ПОСТАВКИ

Программа поставляется в составе дистрибутивного набора программных компонентов на дистрибутивном носителе и аппаратных ключей защиты.

Установка программных компонентов на компьютер производится при помощи установочной программы (**install.exe**).

В состав программы входят два автоматизированных рабочих места:

- автоматизированное рабочее место дежурного оператора (АРМ ДПУ);
- автоматизированное рабочее место администратора базы данных (АРМ АБД).

Ключ защиты устанавливается в параллельный порт ПЭВМ, на котором установлены АРМ ПЦО, и обеспечивает выполнение условий лицензионного соглашения. Для работы ключа защиты необходим специальный драйвер, который входит в состав дистрибутивных компонент.

3. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

3.1 Требования к аппаратному обеспечению

Программа предназначена для работы на IBM совместимых ПЭВМ, удовлетворяющих следующим минимальным требованиям:

- процессор - Pentium II - 600;
- ОЗУ - 128 Мб;
- CD-ROM - для установки программы;
- видеомонитор;
- клавиатура;
- последовательный порт;
- параллельный порт (для синхронной печати протокола);
- контроллер локальной сети;
- мышь.

Дополнительно к вышеперечисленному оборудованию на ПЭВМ желательно иметь звуковую плату и колонки.

3.2 Требования к программному обеспечению

Программа предназначена для работы в среде операционной системы (ОС) Windows 2000 и СУБД IB DataBase (FireBird).

3.3 Информационная совместимость

Программа имеет конвертор базы данных (БД) формата КСА ПЦО НИЦ «Охрана» ГУВО МВД России.

4. ОПИСАНИЕ ПРОГРАММЫ

4.1. Два подхода к разработке информационной модели систем охраны.

При разработке информационной модели программного обеспечения для системы охраны возможны два подхода. Назовем их условно «от железа» и от «объекта».

При подходе «от железа» в качестве структурных элементов, на базе которых строится информационная модель, выбираются составные части технических средств охраны. Основной тезис подхода «от железа» можно сформулировать так: «Использование *технических средств* для охраны объектов». Т.е. сами объекты как - бы вторичны и рассматриваются через призму используемой аппаратуры. Это было бы удобно, если бы объекты проектировались и строились под конкретную систему охраны ☺. Но поскольку это, к счастью, не так, то подход «от железа» становится прокрустовым ложем, в которое пользователи вынуждены «втискивать» характеристики объектов. Исторически сложилось так, что основной информационной единицей в централизованной охране стал «пультовой номер» (П/Н), который служит для адресации приборов, объектов, используется в статистических отчетах, оперативных и неоперативных задачах и т.д.

Подход «от железа» (от П/Н) имеет следующие недостатки:

1. физически П/Н существует только в устаревших системах охраны типа «Нева-10» и для современных систем не имеет физического смысла;
2. использование П/Н затрудняет описание структуры охраняемых объектов, а для сложных объектов его использование вообще невозможно;
3. использование П/Н неудобно для адресации несколько объектов, подключенных к одному П/Н;

4. использование П/Н неудобно для управления состоянием (взятием/снятием) сложных объектов, оборудованных разными системами охраны или несколькими шлейфами сигнализации;

5. использование П/Н в качестве показателя в статистических отчетах не отражает реальную статистику по охраняемым объектам;

6. замена технических средств охраны на объекте (замена П/Н) приводит к необходимости замены (удаления и повторного ввода) информации по объекту в базе данных.

При подходе от «объекта» в качестве структурных элементов, на базе которых строится информационная модель, выбираются составные части самого объекта – зоны, разделы, их характеристики и т.д. Основной тезис подхода от «объекта» можно сформулировать так: «Охрана *объекта* при помощи технических средств». А поскольку объекты отличаются большим разнообразием, то для разработчиков программного обеспечения это означает необходимость создания соответствующих механизмов для их адекватного описания, а для пользователей – возможность конфигурировать систему охраны под свои нужды.

Подход «от объекта» имеет следующие преимущества:

1. независимость описания характеристик объекта от типа используемых технических средств охраны;

2. возможность описания объекта любой конфигурации;

3. возможность описания объекта, оборудованного приборами от разных систем охраны и наоборот, описание нескольких объектов, охраняемых при помощи одного многошлейфного прибора.

4. возможность описания объектов, оборудованных комбинированными системами охраны;

5. возможность замены технических средств на объекте без изменения в БД информации по самому охраняемому объекту;

6. возможность получения достоверной статистики по охраняемым объектам.

В системе «Эгида» при разработке информационной модели программного обеспечения использовался подход «от объекта».

4.2 Термины и определения.

В предыдущем разделе было обосновано преимущество использования при разработке информационной модели программного обеспечения подхода от «объекта». Он предполагает отказ от пультового номера, как характеристики объекта. Взамен него используются следующие понятия:

Охраняемая зона (зона) – произвольная часть имущества, здания или территории, контролируемая одним шлейфом (ШС) охранной, пожарной или охранно-пожарной сигнализации (ОПС). Зоне может быть поставлен в соответствие только *один* ШС;

Охраняемый объект (ОО или просто объект) – полная совокупность охраняемых зон, определенная в договоре на охрану с юридическим или физическим лицом;

Раздел – подмножество зон охраняемого объекта. Одна зона может входить в несколько разделов;

Абонентский номер – произвольное пятизначное число, взаимно - однозначно связанное с охраняемым объектом.

Абонент (хозорган) – пользователь услугами централизованной охраны, которому дано право изменять состояния предварительно закрепленных за ним зон.

Эти определения даны с позиции системного администратора и, возможно, не обладают академической строгостью. Поэтому, учитывая важность правильного понимания используемой терминологии, рассмотрим, как на ее основе строится информационная модель системы «Эгида».

4.3. Описание информационной модели.

В системе «Эгида» используется трехуровневая информационная модель охраняемого объекта: «объект – раздел – зона». Базовым понятием в ней является понятие зоны. Оно несет на себе примерно такую же смысловую нагрузку, как пультовой номер в модели «от железа». Зона, это минимальная и неделимая с точки зрения локализации происходящих событий *часть объекта*. Размеры и конфигурация зоны не имеют принципиального значения и выбираются индивидуально для каждого конкретного случая, исходя из требований к обеспечению требуемого уровня безопасности. Для одного объекта зоной может быть форточка, а для другого – зал заседаний. Важно только то, что любое событие, происходящее на объекте, может быть локализовано только с точностью до зоны (как и за счет чего это обеспечивается, будет рассказано ниже). И если в каком-то помещении Вам надо различать источник тревоги (например окно, объем или входная дверь), то при описании структуры этого помещения в базе данных программы Вам надо создать три отдельные зоны.

В программе используются два вида зон – зоны ОПС и зоны КТЛ (контроль телефонной линии). Зоны ОПС – это зоны (части) самого объекта. Зоны этого вида могут иметь следующие типы:

- охранная;
- пожарная;
- тревожная (КТС);
- технологическая;
- аналоговая.

Первые три типа широко распространены в охране и в комментариях не нуждаются. Два последних типа введены для обеспечения работы с новыми поколениями приборов.

Состояние зоны «Технологическая» может принимать два значения «Норма» и «Нарушение». Технологические зоны могут использоваться для контроля прохода или контроля состояния разного рода переключателей и заглушек (воды, газа и т.д.).

Состояние зоны «Аналоговая» принимает не дискретные, а непрерывные значения в заданном диапазоне измерений и могут применяться для мониторинга таких параметров охраняемого объекта как температура, влажность, загазованность и т.д.

Зоны КТЛ предназначены для описания объектов, оборудованных комбинированными системами охраны. Отличия зон КТЛ от зон ОПС будут рассмотрены ниже.

Поскольку зона (по определению) является элементарным понятием (не имеет внутренней структуры), постольку из набора зон можно строить объекты любой конфигурации.

Под охраняемым объектом будем понимать полную совокупность зон, определенных в договоре на охрану. Стоит подчеркнуть, что с точки зрения этого определения объект в смысле охраны отличается от объекта в физическом смысле этого слова. Так, например, если в двухэтажном здании охраняется только второй этаж, то вот только этот этаж и будет охраняемым объектом (пусть хотя - бы и висящем в воздухе ☺). Все остальное – план подъезда.

Однако понятий зона и объект недостаточно для того, что обеспечить возможность описания объектов сложной конфигурации. Поэтому используется также понятие раздел. Раздел это произвольная часть зон из числа зон, принадлежащих объекту. Таким образом, раздел занимает промежуточное положение между зоной и объектом. Разделы удобно использовать для управления (взятия/снятия) группой зон, если это удобно пользователю. Так,

уже приводимое в пример помещение с тремя зонами (окно, объем и входная дверь) можно рассматривать как раздел, если охраняемый объект – это этаж. Тогда по команде «Взять раздел» будут автоматически взяты под охрану все входящие в него зоны. Отличие раздела от зоны и объекта в том, что его использование (в отличие от первых двух) не является необходимым при описании объекта, а используется только для удобства операторов или в силу аппаратных ограничений, связанных с тактикой работы многошлейфных приемно-контрольных приборов. Последнее обстоятельство связано со следующим. В некоторых многошлейфных приборах (например ИО «Юпитер») не предусмотрена возможность взятия/снятия отдельного ШС по команде оператора. Можно подать команду только на прибор целиком - на все ШС одновременно. С точки зрения структуры объекта это означает, что минимальной управляемой единицей является группа зон, т.е. раздел по определению. Поэтому для таких приборов со стороны объекта автоматически создается раздел, зоны которого связываются со шлейфами этого прибора. В этом случае раздел является обязательной составляющей структуры объекта.

Для адресации (идентификации) объекта используется понятие *абонентский номер* (АН) – произвольное пятизначное десятичное число. Аналогом АН в повседневной жизни может служить, например, номер личного счета в банке. Значения АН для каждого объекта должны быть уникальными, т.е. не должны совпадать, что обеспечивается процедурами программы.

Для удобства персонала ПЦО и абонентов при импорте БД из БД формата КСА ПЦО НИЦ «Охрана» абонентским номерам объектов присваиваются численные значения соответствующих им П/Н (внешне АН выглядят также, как П/Н).

Зона адресуется (идентифицируется) двухзначным десятичным числом в пределах одного объекта. Например, если АН объекта равен 12345, то первая зона адресуется как 12345/01.

Таким образом в программе можно описать 99999 объектов, в каждом из которых может быть 99 зон.

Раздел адресуется через АН объекта и название раздела.

В требовании уникальности АН есть одно исключение, сделанное для обеспечения совместимости системы «Эгида» с базой данных КСА ПЦО НИЦ «Охрана» (где для адресации объектов используется П/Н). В этом случае для сложных объектов, имеющих несколько П/Н, каждый из них может быть использован (и используется на практике) для его идентификации. Т.е. такие объекты имеют как бы несколько идентификаторов (смысловых аналогов АН), что противоречит требованию их уникальности.

Одним из способов разрешения этой коллизии могло бы быть требование обеспечить принудительную уникальность АН. Например, требование выбрать один ПН в качестве АН объекта, исключив при этом все остальные. Однако этот способ вряд ли можно считать удачным, так как для каждого ПЦО потребовалось бы проинформировать и переучивать сотни и тысячи абонентов без видимой для них (и для персонала ПЦО) причины. Вряд ли проблемы внутренней адресации могли бы служить для них весомым аргументом в пользу выполнения этой процедуры.

Более удобный («прозрачный») способ, реализованный в системе «Эгида», основан на использовании понятия синонимов. В этом случае, если объект имеет несколько ПН, то при импорте данных из БД формата КСА ПЦО НИЦ «Охрана» в формат системы «Эгида» каждый из них может рассматриваться как равноправный АН. При этом каждый из таких АН является синонимом по отношению к другим АН этого объекта. (Напомним, что синонимы это разные слова, имеющие одинаковое значение). Использование синонимов не лишено своих недостатков, но зато может служить некоторым логическим «мостиком» между

старым и новым механизмами адресации. Впрочем, использовать синонимы необязательно и обеспечить уникальность АН можно и вручную.

На этом разговор об информационной модели собственно охраняемого объекта можно было бы и закончить. Однако, если Вы обратили внимание, при ее описании мы нигде не упоминали о технических средствах охраны (ТСО). И это хорошо, поскольку иллюстрирует отсутствие ограничений, накладываемых структурой ТСО на структуру объекта. Это позволяет изменять структуру ТСО без какого-то ни было влияния на объект и наоборот, т.е. не затрагивать конечных пользователей – абонентов и операторов.

Однако структура структурой, но охрана объекта, в конечном итоге, обеспечивается техническими средствами. Поэтому для функционирования централизованной охраны связь между объектом и ТСО все же должна быть где – то установлена. В системе «Эгида» такая связь устанавливается между шлейфами сигнализации и зонами. Каждая зона **обязательно** должна быть связана с ШС по двум причинам:

1) для того, чтобы команды, поданные на объект, раздел или зону смогли быть преобразованы в аппаратные адреса ТСО;

2) для того, чтобы события, регистрируемые ШС, были представлены оператору в категориях объекта.

Каждая зона может быть связана только с одним ШС (обратное, в общем случае, неверно). Поскольку локализация событий в ТСО возможна с точностью до ШС (или его аналога в адресных системах – адресной метки), а каждая зона может быть связан только с одним ШС, то отсюда следует, что на уровне объекта локализация событий возможна с точностью до зоны.

У требования взаимно - однозначного соответствия между зонами и ШС есть одно исключение. Оно сделано для объектов, у которых необходимо обеспечить функционирование охранно-пожарной сигнализации в ночные часы и тревожной кнопки в дневные. При этом, в силу различных ограничений, объект может быть оборудован только одним ШС (а точнее одним одношлейфным прибором, т.е. фактически одним П/Н). В системе «Эгида» такую конфигурацию описать очень просто. При этом в расчет берется то обстоятельство, что эти два режима использования ШС имеют между собой мало общего и характеризуются различными реквизитами – тактикой охраны, местами расположения и типами извещателей (тревожных кнопок), описаниями, графиками охраны, хозорганами и т.д. При наличии возможности их нужно было (и это было - бы правильно) оборудовать двумя различными ШС. Однако, что невозможно для ШС, то возможно для зон! (благо, что ничего кроме описания в БД они для себя не требуют). Поэтому с точки зрения тактики охраны структуру этого объекта удобно представить в виде двух зон – охранно-пожарной и тревожной (например XXXXX/01 и XXXXX/02). Но при связывании этих зон с ТСО для них нужно указать один и тот же ШС! Вот и все. Тогда в период графика охраны зоны ОПС сработка на этом ШС будет воспринята программой как событие на зоне XXXXX/01, а в период охраны зоны КТС (скажем днем) – как событие на зоне XXXXX/02. При этом оператор получит достоверную информацию, а то, что она придет с одного и того же ШС ему знать и не обязательно.

Использование принципа независимого описания объектов и ТСО позволяет описывать системы охраны любой возможной на сегодняшний день сложности. Так, например, зоны одного объекта могут быть оборудованы ШС ТСО различного типа и наоборот, ШС одного приемно-контрольного прибора могут охранять зоны разных объектов.

В процессе работы оперативного персонала ПЦО механизмы адресации используются следующим образом. При постановке под охрану абонент сообщает оператору ПЦО абонентский номер объекта и реквизиты зоны или раздела. Система «Эгида» находит в базе данных и отображает на экране список разделов и зон по этому объекту. Затем, в соответст-

вии с типом СПИ, формируется и выполняется список команд телеуправления. При поступлении с объекта тревожной информации программа находит в сообщении аппаратный адрес ШС, а затем адрес связанной с ним зоны и АН объекта и выводит их оператору.

Рассмотрим пример.

Пусть некоторый объект был оборудован двумя шлейфами ОПС, подключенными к пультовым номерам 01/111 (входная дверь) и 02/222 (касса) СПИ «Фобос». Пусть также эти П/Н с равной вероятностью используются в заявках на взятие или снятие этого объект. При переходе на систему «Эгида» для этого объект взамен П/Н 01/111 и 02/222 будут автоматически созданы два синонима - 01111 и 02222, которые будут идентифицировать один и тот же объект, имеющий и две зоны (01 и 02). С зоной 01111/01 (синоним 02222/01) будет связан ПН 01/111, а с зоной 01111/02 (синоним 02222/02) - ПН 02/222.

Как видно из примера, численные значения АН и ПН совпадают (хотя, по сути, теперь это совершенно разные идентификаторы) и не затрагивают вопросов взаимодействия операторов и абонентов. Заявки на взятие могут выглядеть так:

- 1) возьмите под охрану весь объект номер 01111 (или 02222). Будут взяты ПН 01/111 и 02/222;
- 2) возьмите под охрану объект 01111 (или 02222) – входная дверь. Будет взят ПН 01/111;
- 3) возьмите под охрану объект 02222 (или 01111) – касса. Будет взят ПН 02/222.

Пусть, далее, в связи с истечением срока службы СПИ «Фобос» на объекте был установлен неавтоматизированный двухшлейфный прибор, и подключен к ПН 03/333 некоторой СПИ. Поскольку ПН не используется для адресации объекта, это переоборудование не приведет к необходимости изменения АН. АН может, если это удобно, остаться прежним. Один из синонимов может быть удален и использован для адресации другого объекта. Тогда с зоной 01111/01 может быть связан, например, ШС 03/333-1, тогда с зоной 01111/02 - ШС 03/333-2 соответственно. Тогда по заявке: «Возьмите объект 01111» будут взяты шлейфы 03/333-1 и 03/333-2.

Еще раз обратим внимание на ту особенность синонимов, что номера 01111/01 и 02222/01 адресуют одну и ту же зону как синонимы АН!

Все вышесказанное относительно взаимосвязи зон и ШС справедливо как в отношении зон ОПС, так и в отношении зон КТЛ. Однако зоны КТЛ имеют дополнительную особенность. Как уже упоминалось, зоны КТЛ предназначены для описания комбинированных СПИ.

Для справки. В соответствии с технической политикой вневедомственной охраны к эксплуатации в подразделениях допускаются только такие СПИ, которые обеспечивают постоянный контроль (сканирование) канала связи на всех участках от объекта до ПЦО. Информаторные СПИ такого контроля не обеспечивают, поэтому применяться могут только в комбинации со сканирующими (типа «Фобос»). Сканирующая СПИ охраняет в этом случае не сам объект, а линию связи до информаторной СПИ.

Главное назначение зон КТЛ - различать события, произошедшие на зонах объекта от событий на линии связи. Для этого зоны КТЛ имеют не одно, а два поля для связи с ТСО – одно со сканирующей и одно с информаторной СПИ.

Резюме:

- объект в физическом смысле слова может отличаться от объекта в смысле охраны;
- модель объекта охраны имеет трехуровневую структуру «объект-раздел-зона»;
- объект однозначно адресуется пятизначным десятичным числом - абонентским номером;

- при импорте из БД формата КСА ПЦО НИЦ «Охрана» абонентские номера получают значения соответствующих им П/Н и могут иметь синонимы;
- зона адресуется в пределах объекта двухзначным десятичным числом – номером зоны;
- зоны бывают двух видов – зона ОПС и зона КТЛ;
- при помощи зон можно синтезировать объекты любой конфигурации;
- для удобства пользователей группы зон можно объединять в разделы. Создание разделов не является обязательным.

4.4 Структура информационного и программного обеспечения

Информационное и программное обеспечение системы «Эгида» имеет модульную структуру (рис 1.). Каждый модуль реализован как отдельное приложение и выполняет некоторый специфический для него набор функций.

Информационное обеспечение состоит из следующих типов баз данных:

- основная информационная БД (ИБД);
- резервная ИБД;
- основная БД «Протоколы»;
- резервная БД «Протоколы».

Программное обеспечение состоит из следующих модулей:

- драйвера систем передачи извещений (СПИ);
- сервер драйверов систем передачи извещений;
- сервер событий;
- сервер состояний;
- АРМ дежурного пульта управления (ДПУ);
- АРМ дежурного ПЦО (ДПЦО);
- АРМ администратора базы данных (АБД).

В теории интерфейсов последние три модуля (АРМы) называют еще уровнем графического интерфейса пользователя или уровнем представления.

4.4.1 Описание информационного обеспечения

ИБД (основная и резервная) содержат сведения по объектам, абонентам и техническим средствам охраны. В системе может быть только одна основная ИБД, которая физически размещается на одном из компьютеров локальной сети ПЦО, но доступна для всех АРМ ДПУ. Для основной ИБД рекомендуется использовать выделенный компьютер – сервер ИБД. Резервная ИБД предназначена для обеспечения работы АРМ ДПУ в случае невозможности доступа к основной ИБД и может быть только локальной. Поэтому, для обеспечения надежной работы системы резервные ИБД должны быть проинсталлированы на каждом компьютере АРМ ДПУ. Пути к основной и резервным ИБД указываются при инсталляции системы.

В системе предусмотрены две штатные процедуры использования резервной ИБД – для горячего резервирования и замены основной ИБД.

Процедура горячего резервирования основной ИБД заключается в следующем. Каждый из серверов событий, расположенных на рабочих местах операторов постоянно проверяет («пингует») доступность основной ИБД. В случае ее недоступности он генерирует команду к АРМ ДПУ, заставляющую его перейти на резервную ИБД. В случае восстановления доступности основной ИБД сервер событий генерирует команду к АРМ ДПУ, заставляющую его вернуться к работе с основной ИБД.

Потребность в процедуре замены основной ИБД объясняется следующим. В практике охраны имеют место случаи, когда в силу территориальных или организационных причин одновременная работа в реальном времени администратора базы данных и АРМ ДПУ с одним и тем же экземпляром ИБД невозможна или нежелательна. Например, если отдел охраны территориально разнесен с ПЦО, или когда на обновление ИБД на ПЦО каждый раз требуется санкция руководителя. В этих и других случаях нужен механизм, позволяющий заменять экземпляр основной ИБД ПЦО на новый, содержащий последние изменения, произведенные администратором БД. Процедура замены основной ИБД выполняется в ручном режиме с использованием сервера событий. По команде администратора системы генерируется сетевая команда ко всем АРМ ДПУ на переход на резервную ИБД. Затем последовательно: запрашивается путь к новой ИБД, происходит ее копирование взамен старой, и, наконец, генерируется сетевая команда на подключение всех АРМ ДПУ к основной ИБД.

Для поддержания резервной ИБД в актуальном состоянии предусмотрены две возможности – копирование по команде оператора и автоматическое копирование по времени один раз в сутки. Время начала автоматического копирования задается на каждом компьютере АРМ ДПУ индивидуально. В этой связи, поскольку для больших ПЦО процедура копирования основной ИБД в резервную может занимать несколько минут и приводит к значительному увеличению сетевого трафика, постольку настоятельно рекомендуется смещать время начала копирования на рабочих местах операторов относительно друг друга. Смещение зависит от объема ИБД и подбирается опытным путем. В качестве первоначального ориентира можно рекомендовать смещение в 10 мин.

БД «Протоколы» (основная и резервная) предназначены для регистрации событий, происходящих в АРМ ДПУ.

В отличие от основной ИБД, общей для всех АРМ ДПУ в сети, для каждого АРМ ДПУ ведется «своя» основная БД «Протоколы», в которой регистрируются только «свои» события. Основная БД «Протоколы» размещается в той же директории, что и АРМ ДПУ.

Резервная БД «Протоколы» по определению предназначена для хранения копий протоколов (основной БД «Протоколы») и может быть размещена на любом из компьютеров в сети. Однако такой компьютер может быть только один, т.е. копии протоколов для всех рабочих мест в сети хранятся в одном месте, хотя и каждый в своей поддиректории. Путь к резервным БД «Протоколы» хранится в основной ИБД и доступен для ввода и редактирования с любого рабочего места. Резервное копирование протоколов производится автоматически с заданным интервалом времени и при выходе из задачи.

Для восстановления основной БД «Протоколы» из резервной в программе не предусмотрено специальных средств и должно производиться средствами операционной системы.

4.4.2 Описание программного обеспечения

Структура программного обеспечения системы проектировалась исходя из анализа информационных потоков, необходимых для работы ПЦО. Такими информационными потоками являются:

- входной и выходной потоки при работе с СПИ;
- входной и выходной потоки персонала ПЦО;
- потоки сетевого взаимодействия рабочих мест.

Каждый из указанных потоков обрабатывается своим типом программного модуля.

Драйверы СПИ обеспечивают обмен информацией с аппаратной частью систем охраны в форматах протоколов СПИ конкретного типа.

Сервер драйверов обеспечивает:

- запуск необходимого количества драйверов, которое определяется исходя из конфигурации оборудования, описанной в ИБД;
- перезапуск драйверов при изменении конфигурации оборудования в ИБД или «зависании» любого из драйверов;
- реализацию сложных обменов с СПИ, включающих несколько последовательных взаимосвязанных циклов обмена типа «запрос- ответ» (сеансовую логику);
- преобразование информации из формата протокола СПИ во внутрисистемный формат и наоборот;
- обмен информацией с АРМ ДПУ посредством сервера событий.

Структурно сервер драйверов и сами драйвера скомпонованы в одно приложение.

Сервер событий обеспечивает:

- проверку доступности системных ресурсов;
- локальный и сетевой обмен данными между АРМ ДПУ и сервером драйверов;
- проверку доступности, управление переключением и заменой ИБД;
- синхронизацию сетевого времени и некоторые другие функции.

Сервер событий является распределенным ядром системы и должен быть установлен на каждом входящем в нее компьютере.

Сервер состояний предназначен для хранения текущих состояний зон охраняемых объектов, ведение основной БД «Протоколы» и обеспечивает доступ к ним сервера событий и АРМ ДПУ.

АРМ ДПУ обеспечивает работу дежурных пультов управления (отображение данных и обработку команд) и передачу тревожной информации на АРМ ДПЦО.

АРМ ДПЦО обеспечивает работу дежурного ПЦО по обслуживанию тревожных ситуаций.