

Утвержден

БАЖК.425621.002-03РЭ-ЛУ

СИСТЕМА ЦИРКОНИЙ-С2000

2

**Руководство по эксплуатации
Часть 2**

Использование по назначению

БАЖК.425621.002-03 РЭ1

Содержание

1	Использование по назначению.....	3
1.1	Эксплуатационные ограничения	3
1.2	Подготовка системы к использованию.....	4
1.2.1	Меры безопасности	4
1.2.2	Установка и настройка операционных систем	5
1.2.3	Установка и настройка программного обеспечения сервера базы данных.....	6
1.2.4	Установка модулей программного обеспечения	9
1.2.5	Конфигурирование системы	18
1.2.6	Включение и опробование	21
1.2.7	Проверка работоспособности.....	22
1.2.8	Возможные неисправности	26
1.3	Использование системы	27
1.3.1	Общие сведения.....	27
1.3.2	Управление доступом	28
1.3.3	Охранная сигнализация	32
1.3.4	Управление внешними системами.....	34
1.3.5	Табельный учет	35
1.3.6	Формирование отчетов	36
1.4	Действия в экстремальных условиях.....	37
2	Техническое обслуживание	38
3	Транспортирование и хранение	40
	Перечень принятых сокращений.....	41

1 Использование по назначению

1.1 Эксплуатационные ограничения

1.1.1 Технические требования к компьютерам системы "Цирконий-С2000" БАЖК.425621.002-03 (далее по тексту – система) определяются используемой операционной системой (ОС) Microsoft Windows, редакцией системы управления базами данных (СУБД) Microsoft SQL Server и прикладным программным обеспечением (ПО) системы "Цирконий - С2000". Требования к компьютеру могут так же сильно различаться в зависимости от архитектуры системы – количества и распределения модулей по компьютерам, количества абонентов, точек доступа, контроллеров, средств контроля и управления доступом и технических средств охраны в системе.

1.1.2 Для организации автоматизированных рабочих мест (АРМ) и управляющих компьютеров (УК), а также сервера базы данных (СБД) в системах с числом абонентов до 1000 (ориентировочно), рекомендуется применение компьютеров с характеристиками системного блока не хуже указанных ниже:

- а) тип процессора PENTIUM-4
- б) тактовая частота, МГц, не менее 2000;
- в) объем ОЗУ, Мбайт, не менее 512;
- г) емкость накопителя на жестком магнитном диске, Гбайт, не менее 80;
- д) разрешение, не менее точек..... 1024 x 768 .

1.1.3 Для организации СБД в системах с числом абонентов свыше 1000 рекомендуется применение специализированных компьютеров – серверов, которые характеризуются использованием:

- а) от 2 до 4 процессоров типа PENTIUM-IV с тактовой частотой не менее 1000 МГц для повышения скорости обработки информации;
- б) RAID-массивов для повышения надежности и снижения времени доступа при хранении больших объемов информации.

1.2 Подготовка системы к использованию

1.2.1 Меры безопасности

1.2.1.1 Безопасность проведения работ, использования приборов, инструментов и оборудования должна соответствовать на всех этапах применения системы требованиям:

- а) "Правил устройства электроустановок" при работе с напряжением до 1000 В;
- б) "Правил техники безопасности при эксплуатации электроустановок потребителей";
- в) ГОСТ 12.1.019-79. ССБТ. Электробезопасность. Общие требования.

1.2.1.2 Места, где размещается аппаратура, должны соответствовать необходимому уровню безопасности работ, а приборы и оборудование должны использоваться в соответствии с инструкциями по их эксплуатации.

1.2.1.3 При эксплуатации системы должны соблюдаться общие правила электробезопасности при использовании электрических приборов:

- а) запрещается подключать составные части системы к электрической сети с напряжением и частотой, которые не соответствуют величинам, указанным в руководствах по эксплуатации на составные части;
- б) запрещается вскрывать блоки без предварительного отключения их от сети;
- в) при подключении дополнительного оборудования соответствующая часть системы должна быть отключена от сети;
- г) запрещается проведение работ по техническому обслуживанию системы и ее составных частей в грозу.

1.2.2 Установка и настройка операционных систем

1.2.2.1 Общие сведения

Версия операционной системы Microsoft Windows, устанавливаемой на СБД и УК определяется версией и редакцией используемой СУБД Microsoft SQL.

1.2.2.2 Установка и настройка ОС

Установить на компьютер необходимую ОС Microsoft Windows согласно документации на нее. Установить необходимые драйверы для работы с установленным оборудованием. Драйверы поставляются изготовителем оборудования.

Порядок настройки ОС:

- а) создать пользователя с правами администратора;
- б) перезагрузить компьютер для нового пользователя;
- в) провести настройку сетевых параметров системы для подключения к ЛВС;
- г) установить цветовую палитру экрана не хуже "High Color" (16 бит), а область экрана не менее 1024 на 768 точек;
- д) установить часовой пояс. Установить "Автоматический переход на летнее время";
- е) настроить языковые параметры системы, указав в качестве языка по умолчанию русский язык.

1.2.3 Установка и настройка программного обеспечения сервера базы данных

1.2.3.1 Функционирование СБД осуществляется под управлением следующих программных продуктов:

- ОС Microsoft Windows 2003 Server SP1, Windows XP Professional SP2;
- СУБД MS SQL Server 2000, MS SQL Server 2005;
- компонента бизнес логики СБД, обеспечивающего связь MS SQL Server с клиентскими приложениями.

1.2.3.2 Существуют несколько версий Microsoft SQL Server. В таблице 1.1 приведена совместимость с операционными системами Windows для версии Microsoft SQL Server 2000.

Таблица 1.1

Операционная система	Enterprise Edition	Developer Edition	Standard Edition	Personal Edition	Desktop Engine
Windows 2000 Professional	Нет	Да	Нет	Да	Да
Windows 2000 Server	Да	Да	Да	Да	Да
Windows 2000 Advanced Server	Да	Да	Да	Да	Да
Windows 2000 Data Center	Да	Да	Да	Да	Да

В таблице 1.2 приведена совместимость с операционными системами Windows для версии Microsoft SQL Server 2005.

Таблица 1.2

Операционная система	Enterprise Edition	Developer Edition	Standard Edition	Workgroup Edition	Express Edition
Windows 2000	Нет	Нет	Нет	Нет	Нет
Windows 2000 Professional Edition с пакетом обновления 4 (SP4)2, 4	Нет	Да	Да	Да	Да
Windows 2000 Server с пакетом обновления 4 (SP4)2	Да	Да	Да	Да	Да
Windows 2000 Advanced Server с пакетом обновления 4 (SP4)2	Да	Да	Да	Да	Да
Windows 2000 Datacenter Edition с пакетом обновления 4 (SP4)2	Да	Да	Да	Да	Да
Windows XP Home Edition с пакетом обновления 2 (SP2)	Нет	Да	Нет	Нет	Да
Windows XP Professional Edition с пакетом обновления 2 (SP2)4	Нет	Да	Да	Да	Да
Windows XP Media Edition с пакетом обновления 2 (SP2)	Нет	Да	Да	Да	Да
Windows XP Tablet PC Edition с пакетом обновления 2 (SP2)	Нет	Да	Да	Да	Да
Windows 2003 Server с пакетом обновления 1 (SP1)	Да	Да	Да	Да	Да
Windows Server 2003 Enterprise Edition с пакетом обновления 1 (SP1)	Да	Да	Да	Да	Да
Windows Server 2003 Datacenter Edition с пакетом обновления 1 (SP1)	Да	Да	Да	Да	Да
Windows Server 2003 Web Edition с пакетом обновления 1 (SP1)	Нет	Нет	Нет	Нет	Да
Windows Small Business Server 2003 Standard Edition с пакетом обновления 1 (SP1)	Да	Да	Да	Да	Да
Windows Small Business Server 2003 Premium Edition с пакетом обновления 1 (SP1)	Да	Да	Да	Да	Да

1.2.3.3 Для обеспечения совместной работы СБД, с локальными копиями базы данных, размещаемыми на УК, необходимо правильно сконфигурировать параметры установленных на них Microsoft SQL серверов, чтобы избежать проблем при их взаимодействии.

1.2.3.4 Порядок инсталляции Microsoft SQL Server описан в руководстве, поставляемым с СУБД.

1.2.3.5 Для работы в системе рекомендованы следующие редакции:

а) СБД:

- 1) Microsoft SQL Server 2000 Standard Edition или Enterprise Edition;
- 2) Microsoft SQL Server 2005 Standard Edition или Enterprise Edition;

б) УК, на которых функционирует модуль "Управление":

- 1) Microsoft SQL Server 2000 Desktop Engine (MSDE);
- 2) Microsoft SQL Server 2005 Express Edition;

в) вариант системы, когда все функции системы совмещаются на одном компьютере:

- 1) Microsoft SQL Server 2000 Desktop Engine (MSDE);
- 2) Microsoft SQL Server 2005 Standard Edition.

1.2.3.6 Не допускается использовать гетерогенные среды хранения данных, когда используются различные версии Microsoft SQL Server на СБД и УК. То есть нельзя использовать на УК Microsoft SQL Server 2005, а на СБД Microsoft SQL Server 2000 и наоборот.

1.2.3.7 Порядок настройки Microsoft SQL Server 2000 Standard:

а) в окне "Services accounts" мастера установки установить параметр Service setting – Use the Domain System Account и указать пользователя, имеющего доступ к сети и обладающего правами входа в качестве службы Microsoft Windows. Если компьютер не входит в домен Windows, то в качестве домена указать сетевое имя компьютера, на котором устанавливается Microsoft SQL Server;

б) в окне "Authentication Mode" мастера установки установить параметр Choose the Authentication Mode – Mixed Mode (SQL and Windows Authentification);

в) в окне "Choose Licensing Mode" мастера установки установить параметр Licensing Mode – количество 100.

Остальные параметры настройки принимаются по умолчанию.

Для Microsoft SQL-Server 2000 Desktop Engine настройка не требуется.

1.2.3.8 Порядок настройки Microsoft SQL Server 2005 Standard/Express:

а) в окне "Components to install" мастера установки выбрать "SQL Server Database Services". Остальные компоненты на усмотрение пользователя;

б) в окне "Instance Name" мастера установки выбрать "Default instance";

в) в окне "Services accounts" мастера установки установить параметр Use the Domain System Account и указать пользователя, имеющего доступ к сети и обладающего правами входа в качестве службы Microsoft Windows. Если компьютер не входит в домен Windows, то в качестве домена указать сетевое имя компьютера, на котором устанавливается Microsoft SQL Server. В области "Start service at the end of setup" выбрать "SQL Server", "SQL Server Agent";

г) в окне "Authentication Mode" мастера установки установить параметр Select the Authentication Mode to use for this installation – Mixed Mode (Windows Authentication and SQL Server Authentication);

д) в остальных окнах оставить настройки по умолчанию.

1.2.4 Установка модулей программного обеспечения

1.2.4.1 Модули ПО системы поставляется на компакт- диске, с которого и выполняется установка под управлением программы InnoSetup, что позволяет в случае необходимости легко деинсталлировать систему.

1.2.4.2 Перед установкой ПО системы необходимо убедиться, что на все УК и сервер БД установлено соответствующее ПО СУБД.

1.2.4.3 Состав и назначение модулей, входящих в комплект ПО системы, приведен в "Руководство по эксплуатации. Часть 1. Устройство и работа системы. БАЖК.425621.002-03РЭ".

1.2.4.4 Установка ПО системы производится в режиме автозапуска. Поэтому необходимо вставить компакт-диск в CD-ROM и следовать указаниям и сообщениям инсталлятора или самостоятельно запустить файл «Zircon-003-setup.exe» из корневого каталога компакт-диска. В результате отобразится окно (рисунок 1.1).

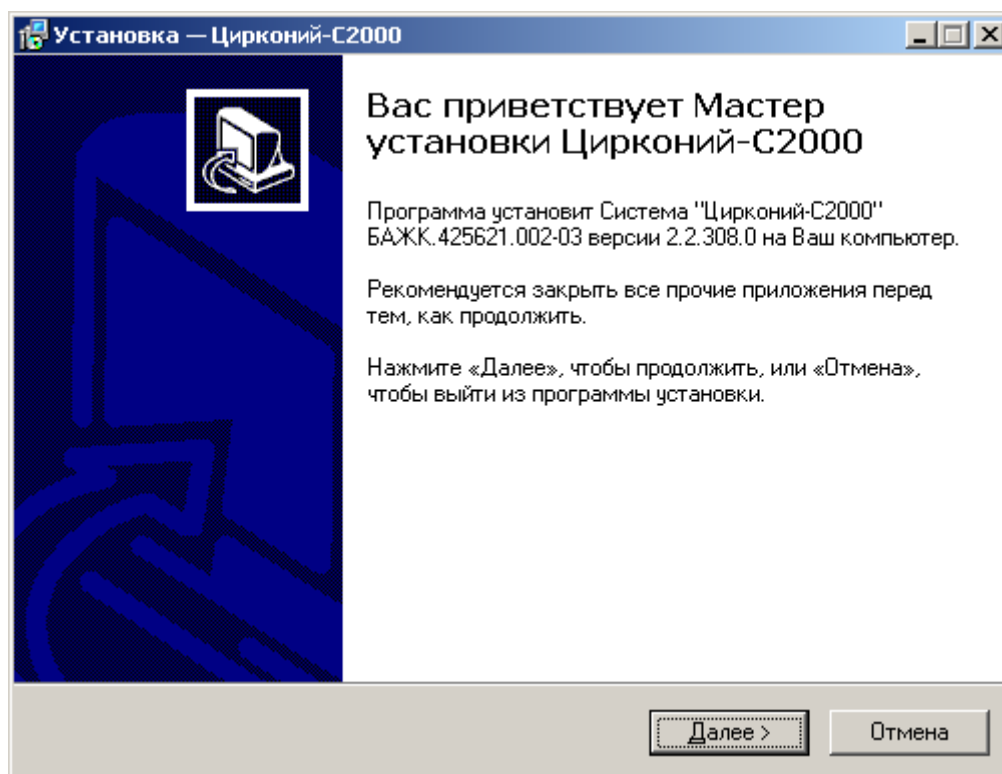


Рисунок 1.1

Нажать кнопку “Далее”. В зависимости от уже установленного программного обеспечения на компьютере будет предложено установить:

- а) MDAC 2.8 (рисунок 1.2);
- б) Windows Installer 3.1 (рисунок 1.3);
- в).NET Framework 2.0 (рисунок 1.4);
- г) Crystal Reports 10.2 (рисунок 1.5).

Необходимо согласиться с установкой и дождаться завершения установки выбранных компонентов.

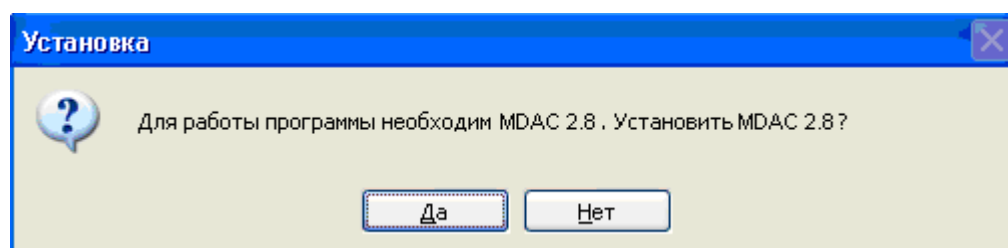


Рисунок 1.2

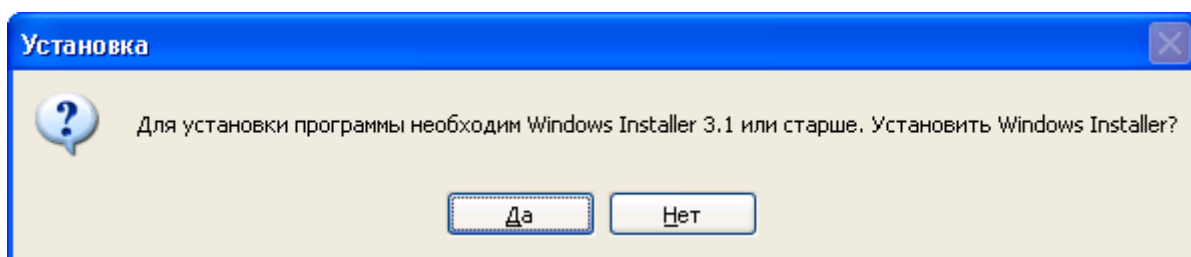


Рисунок 1.3

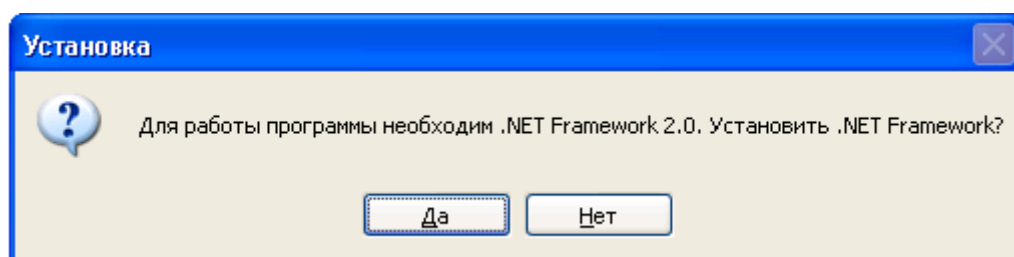


Рисунок 1.4

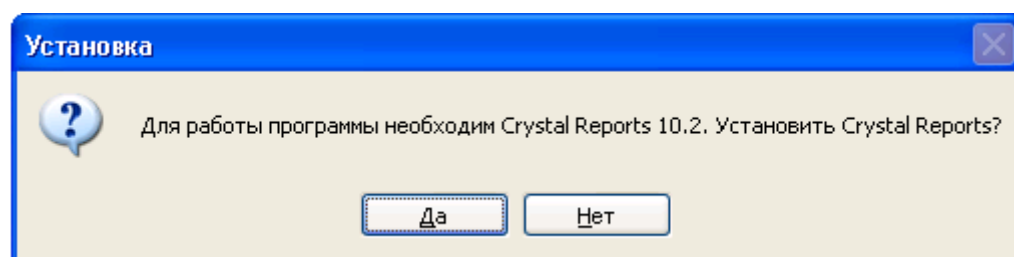


Рисунок 1.5

Далее, отобразится окно (рисунок 1.6).

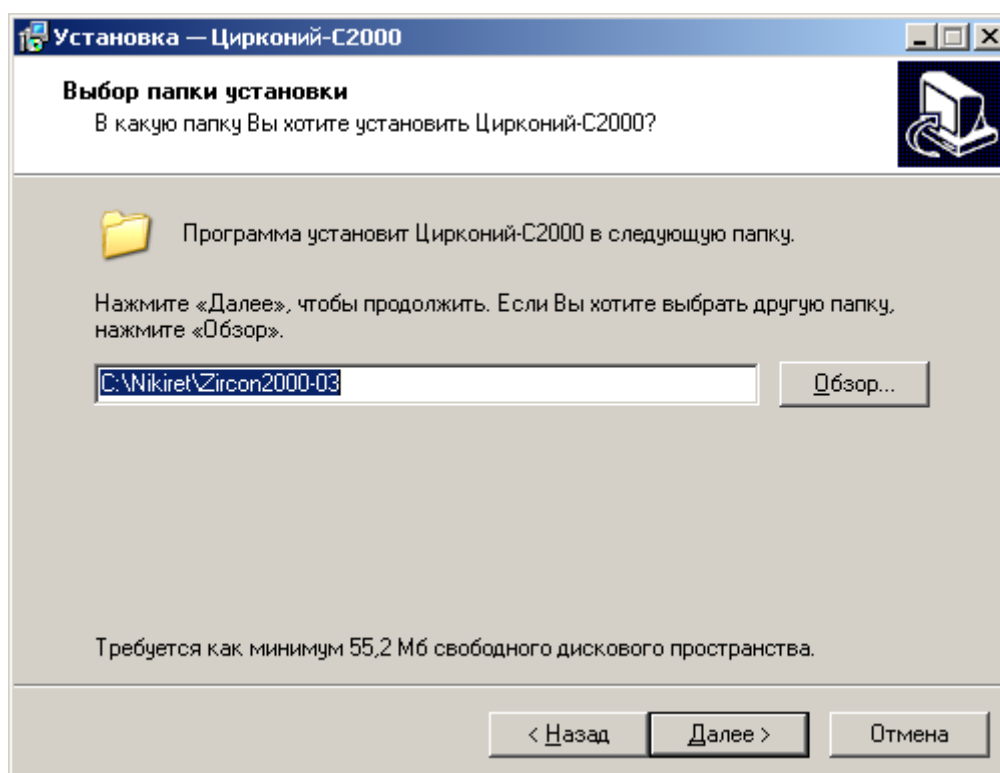


Рисунок 1.6

Для выбора пути установки нажать кнопку "Обзор...", на экране отобразится окно (рисунок 1.7).

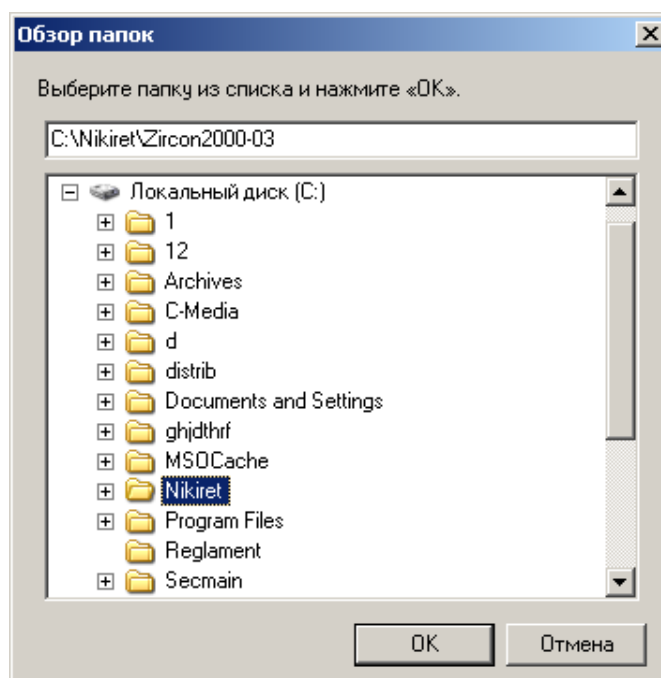


Рисунок 1.7

Выбрать соответствующий диск и каталог, куда будет установлено программное обеспечение, затем нажать кнопку "ОК".

Примечание - По умолчанию программное обеспечение устанавливается в папку C:\Nikiret\Zircon2000-03.

Нажать кнопку “Далее”, отобразится окно (рисунок 1.8).

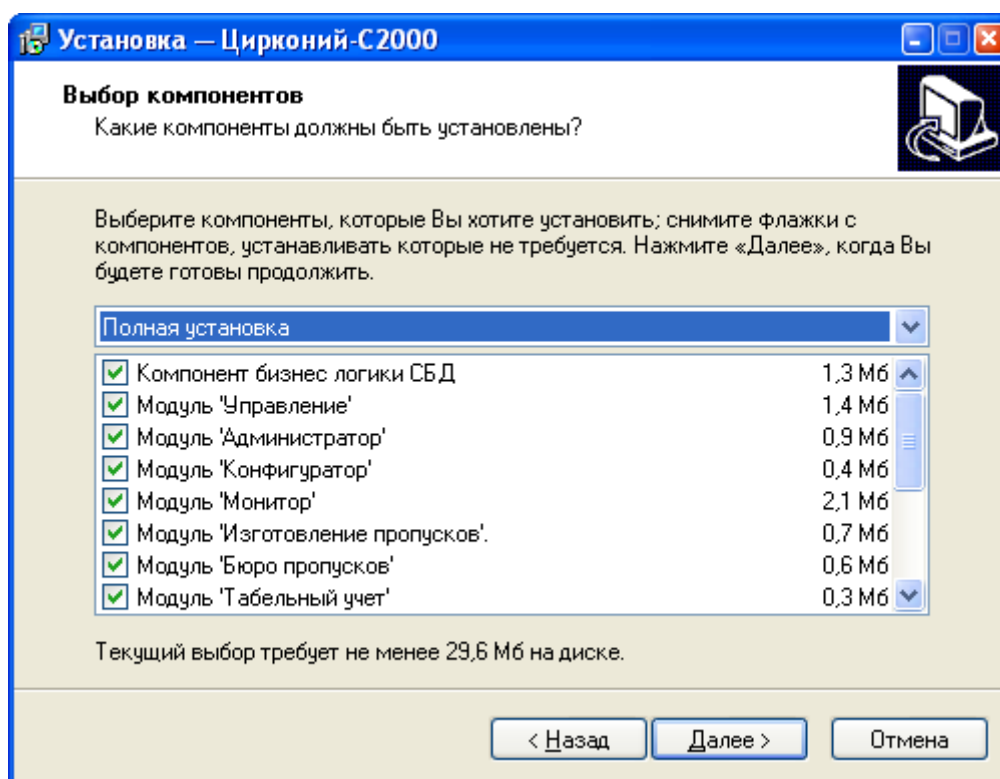


Рисунок 1.8

Выбор устанавливаемых модулей производится согласно распределению функций по компьютерам в соответствии с проектной документацией.

Нажать кнопку "Далее", на экране отобразится окно (рисунок 1.9).

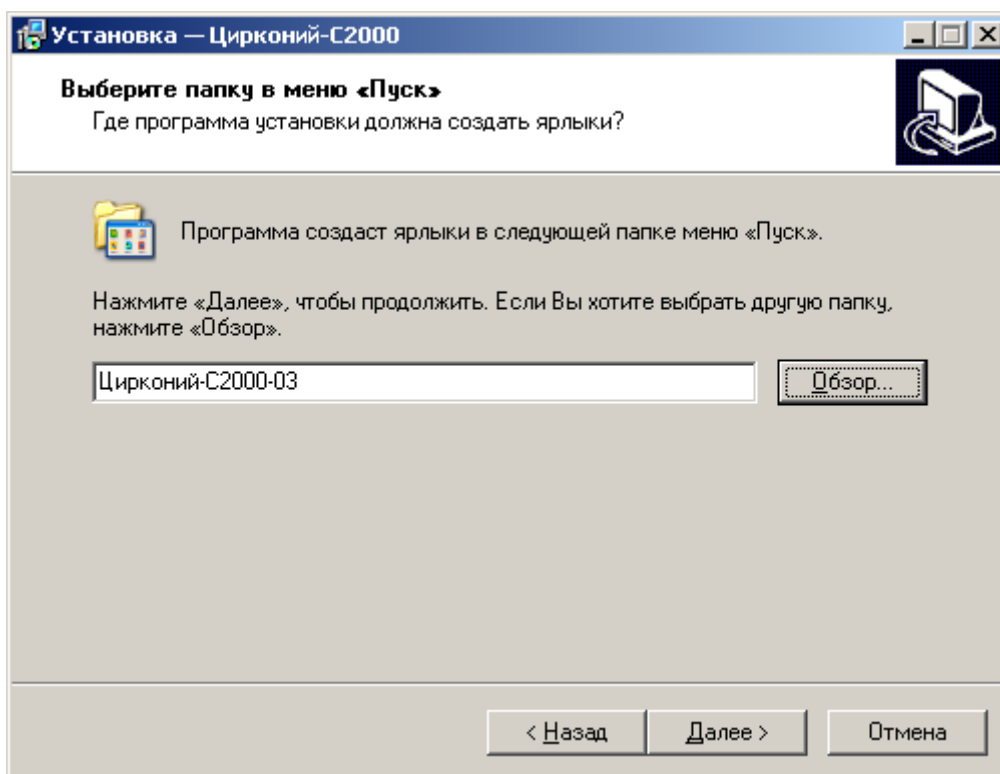


Рисунок 1.9

Выбрать папку для создания ярлыков программного обеспечения, используемых в меню «Пуск» (по умолчанию ярлыки создаются в папке Цирконий-С2000-03, в дальнейшем можно отказаться от создания ярлыков). Для выбора другой папки нажать кнопку "Обзор" и из появившегося окна выбрать необходимую папку.

Нажать кнопку "Далее", на экране отобразится окно (рисунок 1.10).

1.2.4.5 Выбрать дополнительные задачи, которые должны выполняться при установке программного обеспечения:

- а) "Создать ярлыки в меню "Пуск"
- б) "Создать ярлыки на Рабочем столе"
- в) "Создать ярлыки в папке установки"
- г) "Установить драйверы платы ПИ -1 комплекта КР-1" – если, для связи с контроллерами, в системе планируется использовать интерфейс ЦПКУ.

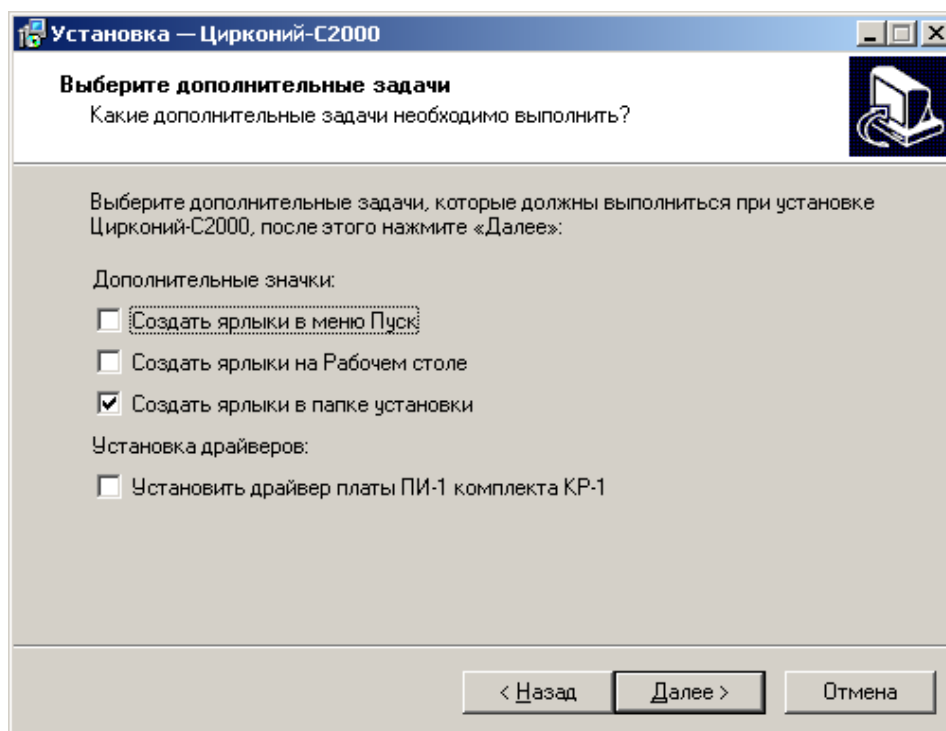


Рисунок 1.10

Нажать кнопку "Далее", на экране отобразится окно (рисунок 1.11) с готовностью установки программного обеспечения на компьютер. В этом окне приводится итоговая справка об устанавливаемых компонентах и задачах инсталлятора.

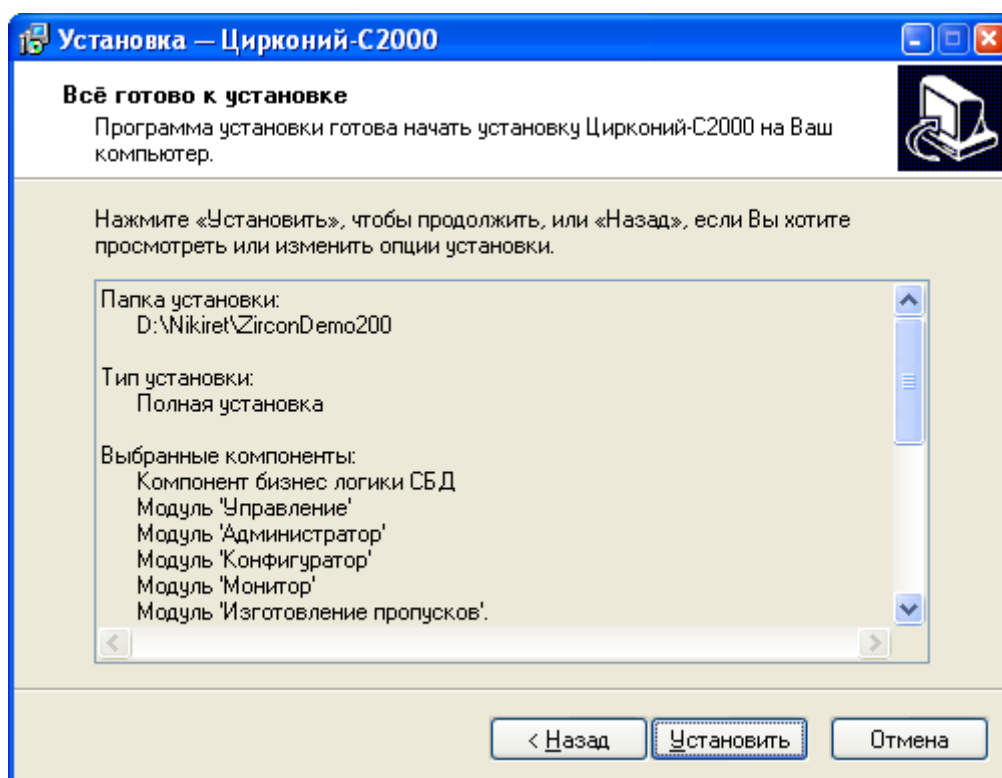


Рисунок 1.11

Нажать кнопку "Установить", на экране отобразится окно (рисунок 1.12) копирования файлов на жесткий диск.

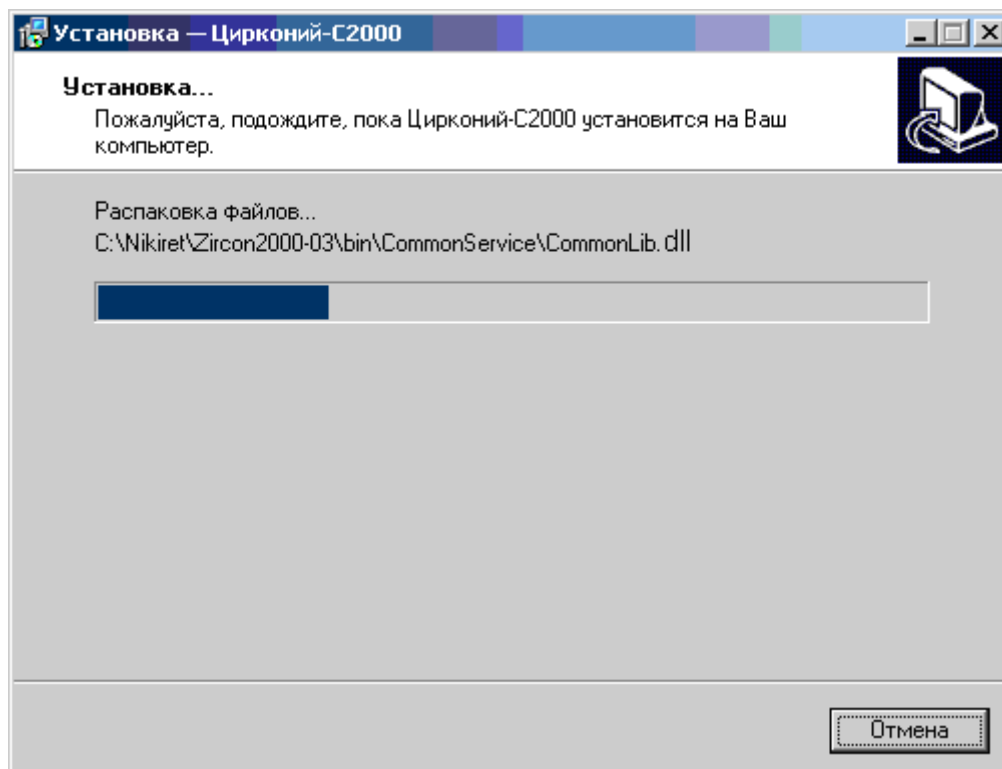


Рисунок 1.12

По завершении копирования отобразится окно (рисунок 1.13) об успешной установке программного обеспечения.

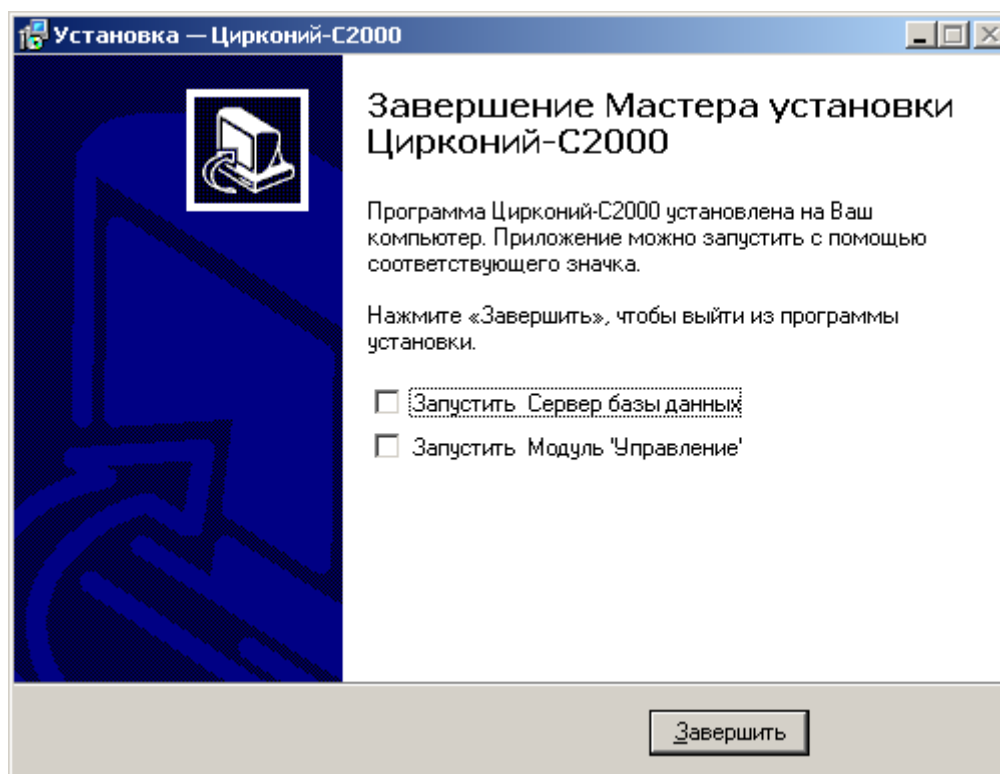


Рисунок 1.13

Для выхода из программы установки нажать кнопку "Завершить".

1.2.4.6 Если по окончании установки необходимо запустить модуль "Управление" или программное обеспечение СБД, то необходимо установить соответствующий флажок и нажать кнопку "Завершить".

1.2.4.7 Необходимые таблицы базы данных создаются автоматически при первом запуске СБД, в список абонентов автоматически заносится "условный" абонент с именем "Администратор Системы Цирконий", он же заносится в список операторов системы с именем "1", паролем "1" и правами администратора.

1.2.4.8 При установке компонентов "Компонент бизнес логики СБД" и "Модуль "Управление", для их правильной работы, необходимо убедиться, что в системе установлена служба очереди сообщений. Для этого необходимо зайти в Панель управления Microsoft Windows. Выбрать элемент "Установка и удаление программ". В открывшемся диалоговом окне выбрать "Установка компонентов Windows". В появившемся окне проверить, что установлен переключатель "Очереди сообщений". В случае если он не установлен, установить и нажать кнопку "Далее" (рисунок 1.14).

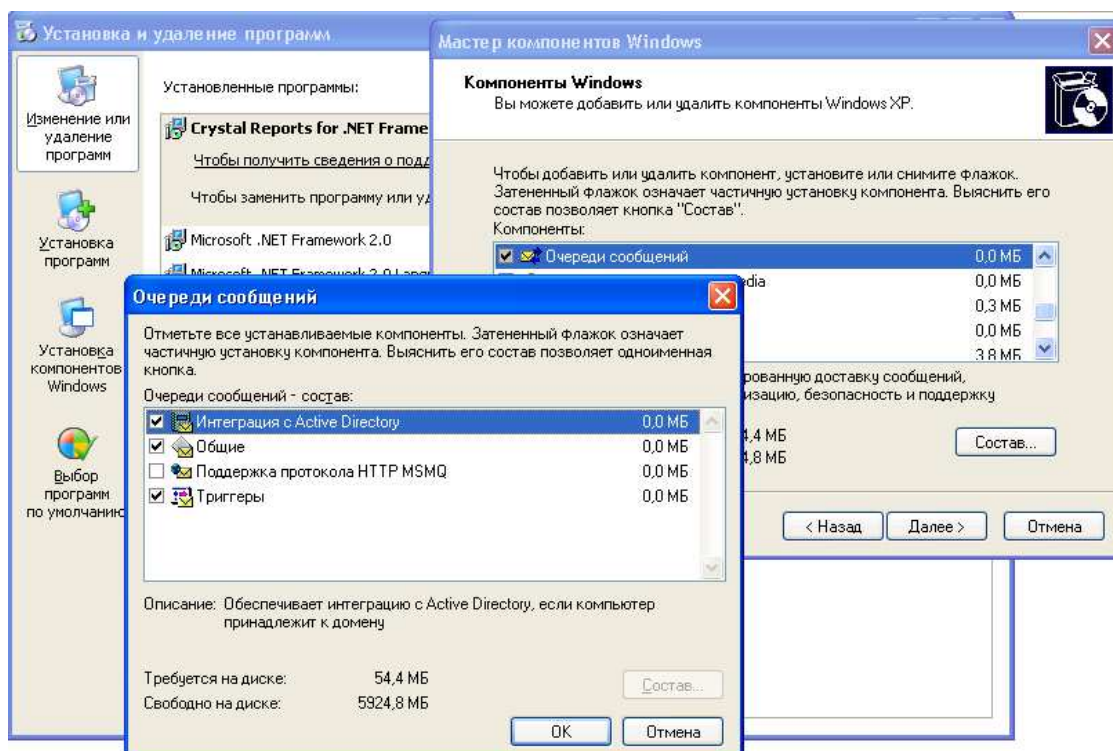


Рисунок 1.14

1.2.5 Конфигурирование системы

1.2.5.1 В данном пункте приводится общий порядок настройки системы, показано, какие модули, как, когда и для чего используются.

1.2.5.2 Для настройки системы необходимо предварительно изучить проект, схемы размещения и соединения составных частей системы. Работы по настройке можно начинать до окончания монтажных и пусконаладочных работ оборудования системы - по мере готовности отдельных точек доступа, зон (участков) охраны. Для этого необходимо иметь работоспособный СБД, на котором размещены или к которому с помощью локальной вычислительной сети (ЛВС) подключены компьютеры с модулями "Администратор", "Конфигуратор". УК на этом этапе не требуются.

1.2.5.3 Подробные описания по работе с модулями системы приведены в соответствующих руководствах по эксплуатации:

а) "Руководство по эксплуатации. Часть 1. Модули "Администратор" и "Конфигуратор" БАЖК.425969.022РЭ;

б) "Руководство по эксплуатации. Часть 2. Модули "Управление" и "Монитор". БАЖК.425969.022РЭ1;

в) "Руководство по эксплуатации. Часть 3. Модуль "Изготовление пропусков".
БАЖК.425969.022РЭ2;

г) "Руководство по эксплуатации. Часть 4. Модуль "Бюро пропусков".
БАЖК.425969.022РЭ3;

д) "Руководство по эксплуатации. Часть 5. Модуль "Табельный учет".
БАЖК.425969.022РЭ4;

е) "Руководство по эксплуатации. Часть 6. Модуль "Генератор отчетов".
БАЖК.425969.022РЭ5;

ж) "Руководство по эксплуатации. Часть 7. Модуль "Шлюз "Сектор-М".
БАЖК.425969.022РЭ6.

и) "Руководство по эксплуатации. Часть 8. Модуль "Регламент".
БАЖК.425969.022РЭ7.

1.2.5.4 Перед вводом параметров системы необходимо проверить настройки сетевых параметров компьютеров. На всех компьютерах должен быть настроен TCP/IP протокол и все они должны входить в одну ЛВС. Для проверки можно использовать программу "ping.exe", входящую в состав ОС. Программа проверяет возможность передачи IP - пакета по указанному IP - адресу и получения от него подтверждения.

1.2.5.5 Необходимо проверить связь с каждым компьютером системы, путем последовательного запуска программы на одном из компьютеров с указанием IP адресов остальных компьютеров в сети. Если сеть работает с ошибками, обратитесь к администратору ЛВС. Прежде, чем продолжить работу, необходимо добиться нормального функционирования ЛВС.

1.2.5.6 Описание конфигурации и параметров составных частей (компьютеров, коммуникационных комплектов, контроллеров, считывателей, технических средств контроля доступа и охранной сигнализации, внешних устройств и т.д.) системы создается с помощью модуля "Конфигуратор".

1.2.5.7 Для сокращения затрат на этапе ввода системы в действие рекомендуется конфигурирование проводить в соответствии с реальными проектными требованиями по размещению и подключению ее составных частей, по привязке их к зонам и точкам доступа.

1.2.5.8 Если это по каким-либо причинам затруднено, настройку системы можно проводить на тестовой конфигурации. Минимальный состав конфигурации должен содержать:

а) две зоны доступа;

б) один УК, сконфигурированный на работу с подключенной периферийной аппаратурой;

в) одну точку доступа.

Графические планы при тестовой настройке системы могут отсутствовать.

1.2.5.9 Порядок ввода информации при конфигурировании системы:

а) подготовить файлы графических планов в одном из допустимых форматов: JPEG, BMP, GIF, WMF, EMF;

б) ввести список зон;

в) ввести список УК в ЛВС;

г) ввести перечень и параметры подключенных к УК коммуникационных комплектов, контроллеров, считывателей, технических средств контроля доступа и охранной сигнализации, внешних устройств и т.д.;

д) ввести список точек доступа;

е) разместить на графических планах объекта составные части системы.

1.2.5.10 Ввод информации, используемой для администрирования системы, выполняется с помощью модуля "Администратор".

Порядок ввода информации при администрировании системы:

а) создать не меньше одной смены, указав временные интервалы разрешенного времени, рабочего времени и перерыва;

б) создать не меньше одного графика работы на текущий период (год, месяц), используя справочник смен;

в) заполнить списки подразделений и должностей;

г) ввести в список одного абонента (это может быть "условный" абонент). Заполнить на него разрешительные данные (личный код, если он используется; код "Proximity карты", которая будет использоваться в качестве пропуска на этапе настройки; тип пропуска – "Постоянный"; пропуск "Активный"; график работы; рабочую смену) и личные данные (фамилия, имя, отчество). В дальнейшем его данные будут использованы при включении, опробовании и проверке работоспособности системы;

д) назначить разрешенные точки доступа;

е) включить абонента в список операторов с правами администратора;

ж) включить в список разрешенных для управления всеми УК в системе.

После ввода всех указанных данных и параметров предварительная настройка системы завершена, и она подготовлена к первому запуску.

1.2.6 Включение и опробование

1.2.6.1 Для опробования системы необходимо завершить все монтажные и наладочные работы. Убедиться в работоспособности и правильности подключения всех составных частей системы. Проверка системы и ее составных частей осуществляется в соответствии с эксплуатационной документацией:

- а) БАЖК.425621.002-03ИМ. Система "Цирконий-С2000". Инструкция по монтажу;
- б) БАЖК.468919.006РЭ. Система "Цирконий-С2000". Комплект К20. Руководство по эксплуатации;
- в) БАЖК.468919.010РЭ. Система "Цирконий-С2000". Комплект К40. Руководство по эксплуатации.

1.2.6.2 Перед опробованием системы убедиться, что ПО установлено на компьютеры согласно проекту.

1.2.6.3 Порядок опробования системы:

- а) включить сервер СБД и убедиться, что запустился SQL сервер, о чем свидетельствует значок в панели задач. Если MS SQL Server не работает, то устранить причину и повторно запустить СБД;
- б) подать питание на периферийную аппаратуру, подключенную к УК;
- в) включить УК, автоматически должен запуститься SQL -сервер, о чем свидетельствует значок в панели задач. Если SQL -сервер не работает, то устранить причину и повторно запустить.
- г) запустить на УК модуль "Управление", должно появиться рабочее окно, что свидетельствует о запуске модуля. Если модуль не запустился, то устранить причину неисправности. Прodelать данную процедуру на каждом УК;
- д) включить АРМ охраны и запустить модуль "Монитор", должно появиться окно со строкой меню. С АРМ охраны выполнить последовательное подключение к УК, используя для регистрации данные тестового абонента, введенного при настройке системы. Проверить выполнение команд на включение / отключение нескольких контроллеров. Прodelать данную процедуру на каждом АРМ охраны;
- е) включить АРМ администратора и запустить модуль "Администратор", открыть архив сообщений. В архиве сообщений должна быть информация о командах оператора и состояниях контроллеров от всех УК.

Примечание – При обнаружении ошибок в работе ПО или периферийной аппаратуры необходимо выяснить причины их возникновения, устранить их и повторить опробование системы.

1.2.6.4 Опробование модулей административного уровня "Администратор", "Конфигуратор" и SQL -сервер было произведено при вводе параметров системы.

1.2.7 Проверка работоспособности

1.2.7.1 Общие сведения

Проверка работоспособности направлена на проверку работы основных составных частей системы в режиме взаимодействия их между собой и средств обеспечения живучести системы.

Проверку работоспособности составных частей, входящих в состав системы, проводить согласно руководствам по эксплуатации на данные составные части.

Перед проверкой убедитесь в работоспособности ЛВС и всех подключенных к ней компьютеров.

Перед проверкой все составные части системы должны быть сконфигурированы в системе в соответствии с проектом, а тестовому абоненту должны быть назначены и разрешены для прохода (доступа) все точки и зоны доступа.

Проверка работоспособности системы включает:

- а) проверку взаимодействия модуля "Монитор" с модулем "Управление";
- б) проверку взаимодействия модулей "Управление" между собой;
- в) проверку взаимодействия модуля "Управление" с СБД;
- г) проверку выполнения модулем "Управление" и контроллерами функций контроля и управления доступом и охранной сигнализацией;
- д) проверку способности восстановления работы после аварийного отключения компьютеров или нарушения обмена информацией между модулями и периферийной аппаратурой.

1.2.7.2 Проверка взаимодействия модулей "Монитор" и "Управление"

Проверка взаимодействия модулей "Монитор" и "Управление" должна показать корректность работы средств идентификации и аутентификации, правильность отображения графической информации, наличие и качество обмена информацией между

модулями и достоверность занесения информации по времени и содержанию в архив сообщений.

Порядок проверки взаимодействия модулей "Монитор" и "Управление":

- а) запустить на одном из УК модуль "Управление";
- б) запустить на одном из АРМ охраны модуль "Монитор";
- в) выполнить процедуру начала дежурства с идентификационными данными тестового абонента;
- г) выполнить подключение к УК, на котором запущен модуль "Управление". Данный УК должен быть включен в список разрешенных оператору УК;
- д) выбрать на АРМ охраны управление по графическим планам;
- е) проверить соответствие введенных в модуле "Конфигуратор" графических планов с планами, отображенными модулем "Монитор", правильность размещения аппаратуры на графических планах и в дереве оборудования для данного УК;
- ж) открыть архив сообщений, в него должны быть занесены события о начале дежурства, регистрации оператора и подключения к УК. Проверить в архиве достоверность занесения информации по времени и содержанию;
- и) выполнить процедуру окончания дежурства и завершить работу с модулем "Монитор".

1.2.7.3 Проверка взаимодействия модулей "Управление" между собой

Проверка взаимодействия модулей "Управление" между собой должна показать идентичность отображаемой информации о доступе абонентов в локальных архивах сообщений для УК.

Порядок проверки взаимодействия модулей "Управление" между собой:

- а) запустить на нескольких УК модули "Управление";
- б) запустить на одном из АРМ охраны модуль "Монитор";
- в) выполнить процедуру начала дежурства с идентификационными данными тестового абонента;
- г) выполнить несколько проходов через точки доступа, управляемыми одним из работающих УК;
- д) сравнить архивы сообщений каждого УК, все они должны содержать информацию о проходах абонентов, независимо от того, на каком УК они произошли;
- е) выполнить процедуру окончания дежурства и завершить работу модуля "Монитор".

1.2.7.4 Проверка взаимодействия модуля "Управление" с СБД

Проверка взаимодействия модуля "Управление" с СБД должна показать идентичность отображаемой информации в архиве сообщений модулей "Управление" и "Администратор".

Порядок проверки (один из возможных вариантов) взаимодействия модуля "Управление" с СБД:

- а) запустить модуль "Администратор";
- б) запустить модуль "Управление" на одном из УК;
- в) запустить на одном из АРМ охраны модуль "Монитор";
- г) выполнить процедуру начала дежурства с идентификационными данными тестового абонента;
- д) в списке доступных УК должен присутствовать УК, на котором запущен модуль "Управление", выполнить подключение к нему;
- е) в модуле "Администратор" у тестового абонента удалить одну из разрешенных для прохода точек доступа, управляемых работающим УК;
- ж) сделать попытку совершить проход через эту точку доступа, система должна зарегистрировать попытку несанкционированного прохода и сформировать соответствующее сообщение в архив сообщений СБД и УК. Для просмотра архива сообщений на СБД использовать модуль "Администратор", а на УК – модуль "Монитор". Информация о попытках несанкционированного прохода в архивах должна совпадать;
- и) вновь с помощью модуля "Администратор" включить точку доступа в список разрешенных для прохода тестовому пользователю и повторить попытку прохода через неё;
- к) в архивах сообщений должны сформироваться сообщения о санкционированном проходе;
- л) выполнить процедуру окончания дежурства и завершить работу модулей "Монитор", "Администратор" и "Управление".

1.2.7.5 Проверка выполнения модулем "Управление" и контроллерами функций управления доступом и охранной сигнализацией

Проверка выполнения модулем "Управление" и контроллерами функций управления доступом и охранной сигнализацией должна показать работоспособность основного оперативного звена управления системы – модулей "Управление", сети контроллеров и периферийной аппаратуры.

Порядок проверки выполнения модулем "Управление" и контроллерами функций контроля и управления доступом и охранной сигнализацией:

- а) запустить на одном из УК модуль "Управление";
- б) запустить на одном из АРМ охраны модуль "Монитор";
- в) выполнить процедуру начала дежурства с идентификационными данными тестового абонента;
- г) выбрать УК с запущенным модулем "Управление";
- д) включить управление по графическим планам;
- е) выполнить последовательно для каждого контроллера команды отключения и включения, заметить точное время их выполнения;
- ж) с помощью зарегистрированного в системе пропуска тестового абонента выполнить проходы через все точки доступа, управляемые с данного УК, проверить запись сообщений о проходах в архив событий УК, проверить правильность отражения информации о каждом проходе абонента, направлении прохода, и времени прохода;
- и) попытаться повторить операцию с помощью незарегистрированного пропуска, в архиве сообщений должна отобразиться информация о попытке прохода неизвестным абонентом, проверить правильность отображения информации о попытке прохода и времени ее осуществления;
- к) выполнить несколько команд управления средствами охранной сигнализации и проверить запись соответствующих сообщений в архив сообщений;
- л) выполнить процедуру окончания дежурства и завершить работу модуля "Монитор".

1.2.7.6 Проверка восстановления работы после аварийного отключения

Проверка способности восстановления работы после аварийного отключения компьютеров или нарушения обмена информацией между модулями и периферийной аппаратурой должна показать, что каждый контроллер передает на УК весь накопленный архив сообщений и переходит из автономного режима в режим управления от УК.

Порядок проверки восстановления работы после аварийного отключения компьютеров или нарушения обмена информацией между модулями и периферийной аппаратурой:

- а) запустить модуль "Управление" на одном из УК;
- б) запустить на одном из АРМ охраны модуль "Монитор";

в) выполнить процедуру регистрации с идентификационными данными тестового абонента на УК;

г) с помощью зарегистрированного в системе пропуска тестового абонента выполнить проходы через какую-либо точку доступа, управляемую с данного УК, проверить запись сообщений о проходах в архив событий УК;

д) выключить УК;

е) выполнить несколько проходов через точки доступа, управляемые отключенным УК;

ж) вновь включить УК и запустить модуль "Управление";

и) в архиве сообщений УК, отображаемом в модуле "Монитор", должны появиться сообщения о проходах, совершенных в автономном режиме;

к) выполнить процедуру завершения работы модулей "Монитор" и "Управление".

1.2.8 Возможные неисправности

Возможные неисправности, связанные с ошибками при конфигурировании системы, приведены в таблице 1.2.

Предполагается, что все оборудование смонтировано правильно, на него подано питание и все составные части, в том числе и компьютеры, проверены и работоспособны. Возможные причины неисправности составных частей системы описаны в соответствующих руководствах по эксплуатации на составные части.

Таблица 1.2

Возможная неисправность	Причина неисправности	Действия оператора
Ошибка при регистрации	Ошибка при вводе имени, пароля или неправильные имя, пароль	Уточнить идентификационные данные у администратора системы и ввести правильные данные
Не работает ни один контроллер на данном УК	Введен неправильный базовый адрес интерфейса контроллера	Ввести правильный базовый адрес интерфейса контроллера
Не работает контроллер	Введен неправильный или не соответствующий сетевой адрес контроллера	Ввести правильный сетевой адрес контроллера
Отсутствует связь между модулями "Монитор" и "Управление"	Неисправна или неправильно настроена ЛВС, или не согласованы параметры сетевого подключения модулей "Монитор" и "Управление"	Выполнить проверку и настройку ЛВС, проверить параметры сетевого подключения, заданные в файлах "Communication.cfg" модулей "Монитор" и "Управление"
Нарушен обмен между УК	Неисправна или неправильно настроена ЛВС	Выполнить проверку и настройку ЛВС
Ошибка при подключении к БД	Неправильные настройки подключения к СБД. Не работает СУБД, СБД или ЛВС.	Уточнить настройки подключения к СБД у администратора. Уточнить у администратора, что СУБД, СБД и ЛВС работоспособны.

1.3 Использование системы

1.3.1 Общие сведения

1.3.1.1 Система служит основой для создания интегрированных комплексов безопасности объектов различного назначения.

1.3.1.2 В системе могут быть реализованы как отдельно, так и совмещено, функции управления доступом и функции охранной сигнализации.

1.3.1.3 Подробное описание работы с каждым из модулей из комплекта ПО (назначение, возможности, режимы работы, действия оператора и т.д.) приведено в соответствующих руководствах по эксплуатации.

Ниже приведен наиболее оптимальный порядок настройки и эксплуатации системы как при управлении доступом, так и при управлении охранной сигнализацией.

1.3.1.4 Для обеспечения первоначального допуска к работе с ПО при его установке автоматически создается один "условный" оператор с именем "Администратор" и правами администратора.

ВНИМАНИЕ! ДЛЯ ИСКЛЮЧЕНИЯ ВОЗМОЖНОСТИ ДОПУСКА ПОСТОРОННИХ ЛИЦ К РАБОТЕ С МОДУЛЯМИ ПО ИДЕНТИФИКАЦИОННЫМ ДАННЫМ "УСЛОВНОГО" ОПЕРАТОРА НЕОБХОДИМО, В СООТВЕТСТВИИ С РУКОВОДСТВОМ ПО ЭКСПЛУАТАЦИИ МОДУЛЯ "АДМИНИСТРАТОР":

- ВВЕСТИ ДАННЫЕ НОВЫХ АБОНЕНТОВ В СПИСОК АБОНЕНТОВ;
- ВКЛЮЧИТЬ ЗАНЕСЕННЫХ АБОНЕНТОВ В СПИСОК ОПЕРАТОРОВ С УКАЗАНИЕМ ИХ ПОЛНОМОЧИЙ ПО ДОСТУПУ К ИНФОРМАЦИИ И УПРАВЛЕНИЮ;
- УДАЛИТЬ В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ ИЗ СПИСКОВ АБОНЕНТОВ И ОПЕРАТОРОВ ВСЕ ДАННЫЕ НА "УСЛОВНОГО" ОПЕРАТОРА.

МИНИМАЛЬНОЕ КОЛИЧЕСТВО АБОНЕНТОВ – ОДИН АБОНЕНТ, ОН ЖЕ ОПЕРАТОР С ПРАВАМИ АДМИНИСТРАТОРА, ДОПУЩЕННЫЙ К СПИСКУ ОПЕРАТОРОВ.

1.3.2 Управление доступом

1.3.2.1 Управление доступом включает в себя:

- а) конфигурирование системы;
- б) ввод разрешительных данных на абонентов;
- в) оперативное управление доступом в автоматическом режиме и по командам оператора АРМ охраны;
- г) анализ действий абонентов по архиву сообщений.

1.3.2.2 Конфигурирование системы осуществляется с помощью модуля "Конфигуратор".

Конфигурирование системы для управления доступом включает в себя:

- а) состав, связи, режимы работы, системные адреса технических средств контроля и управления доступом;
- б) списки контролируемых точек и зон доступа;
- в) алгоритмы доступа;
- г) подготовку графических планов с размещением технических средств;

д) разрядность кода пропуска.

Все данные при конфигурировании системы заносятся и хранятся на сервере БД.

1.3.2.3 Ввод разрешительных данных абонентов является административным средством управления функциями доступа.

1.3.2.4 Ввод данных осуществляется операторами с соответствующими правами при помощи модулей "Администратор", "Изготовление пропусков" и "Бюро пропусков":

- а) подготовить списки подразделений, должностей;
- б) составить графики работы и рабочие смены;
- в) подготовить списки абонентов системы.

1.3.2.5 С помощью модуля "Изготовление пропусков":

- а) разработать шаблоны всех типов пропусков;
- б) для хранения файлов фотографий абонентов создать специальный каталог на компьютере, где установлен модуль "Изготовление пропусков";
- в) разработать правила наименования файлов с фотографиями, обеспечивающие однозначное их соответствие с абонентами системы. В качестве имени файла можно использовать табельный номер абонента.

1.3.2.6 Пропуска абонентов системы разделяются на три типа:

- а) постоянные личные. Срок действия – неограничен;
- б) временные личные. Срок действия ограничен датой начала и окончания действия пропуска;
- в) разовые обезличенные, предназначены для посетителей. Срок действия ограничен датой начала и окончания действия пропуска.

1.3.2.7 Для абонентов, которым будет назначен постоянный или временный тип пропуска, рекомендуется следующий порядок ввода данных:

- а) сформировать в соответствии с процедурой, принятой на данном объекте, заявку на оформление абоненту постоянного (временного) пропуска. Заявка должна содержать личные данные на него, номера графиков работы и рабочих смен, список разрешенных точек и зон доступа;
- б) утвердить и передать заявку в бюро пропусков для изготовления пропуска;
- в) сфотографировать абонента, присвоить имя файлу с фотографией и занести в предназначенный для этого каталог;
- г) занести личные данные на абонента, график работы, вес;

- д) изготовить и утвердить пропуск, распечатать учетную карточку абонента;
- е) передать заявку с отметкой бюро пропусков на АРМ администратора. Оператору с соответствующими правами занести с помощью модуля "Администратор" разрешительные данные абонента (в соответствии с имеющейся заявкой): номер рабочей смены, зоны доступа и точки доступа и активизировать пропуск. Для абонентов с временным пропуском дополнительно указать период действия пропуска. Постоянный пропуск действует с момента электронного утверждения его оператором. Временный пропуск действует только в указанный период;
- ж) вернуть заявку с отметкой оператора АРМ администратора в бюро пропусков;
- и) выдать пропуск абоненту.

1.3.2.8 Для оформления разовых пропусков должно быть предварительно изготовлено с помощью модуля "Изготовление пропусков" требуемое количество обезличенных пропусков.

1.3.2.9 Для данных абонентов рекомендуется следующий порядок:

- а) сформировать, в соответствии с процедурой, принятой на данном объекте, заявку на оформление абоненту разового пропуска. Заявка должна содержать личные данные на него, а также график нахождения на работе, период действия пропуска (дата начала и окончания действия), список разрешенных точек и зоны доступа;
- б) утвердить и передать заявку в бюро пропусков для оформления пропуска;
- в) оператор с помощью модуля "Бюро пропусков" выбирает один из свободных обезличенных пропусков, имеющих в системе. Возможен выбор обезличенного пропуска также с помощью модуля "Изготовление пропусков";
- г) произвести фотографирование абонента или сканирование его документов (фотография, фамилия, имя, отчество и, при необходимости, другие сведения);
- д) ввести согласно заявке личные данные на абонента, а также график нахождения на работе, период действия пропуска (дата начала и окончания действия), список разрешенных точек и зон доступа;
- е) работник бюро пропусков активизирует пропуск и выдает его абоненту;
- ж) после сдачи пропуска все данные на абонента сохраняются, а пропуск возвращается в список свободных обезличенных пропусков.

1.3.2.10 Оператор АРМ администратора с соответствующими правами может оперативно изменять следующие разрешительные данные абонента:

- а) период действия временных и обезличенных пропусков;

б) активность пропуска (блокировать его, убрав флаг активности, или включить в список утерянных пропусков)

в) разрешенные точки и зоны доступа;

г) личные данные и файл фотографии или документа абонента;

д) рабочую смену;

е) график работы, в том числе временный дополнительный график работы на определенный период.

1.3.2.11 Управление доступом может осуществляться как в автоматическом режиме, так и по командам оператора АРМ охраны.

1.3.2.12 Оперативное управление доступом в автоматическом режиме осуществляется модулем "Управление".

1.3.2.13 При управлении в автоматическом режиме система обеспечивает управление и контроль доступа абонентов по алгоритму "В", правилу "2...6 лиц", а также автоматическую постановку зоны, оснащенной средствами обнаружения (СО), на охрану и снятие ее с охраны, если данные условия доступа заданы при конфигурировании.

1.3.2.14 Если для зоны задано правило "2...6 лиц", то вход в нее и снятие ее с охраны возможны только после регистрации необходимого числа абонентов из списков допущенных (имеют право на доступ в данную зону) и ответственных (имеют право на снятие зоны с охраны). После снятия зоны с охраны системой постоянно осуществляется контроль находящихся в ней абонентов, то есть число абонентов в зоне не должно быть меньше, чем необходимо для ее снятия с охраны. Если число абонентов оказывается меньше, то система формирует тревожное сообщение. При выходе последнего абонента зона автоматически ставится на охрану.

1.3.2.15 Оперативное управление доступом по командам оператора АРМ охраны осуществляется с помощью модуля "Монитор", который взаимодействует с модулем "Управление".

1.3.2.16 Модуль "Монитор" предоставляет оператору интерфейс для взаимодействия с любым УК системы. Управление могут осуществлять только операторы АРМ охраны. Список операторов АРМ охраны формируется с помощью модуля "Администратор" из списка абонентов операторов системы. Каждому оператору могут быть назначены индивидуальные полномочия по управлению системой по доступу и допуску к информации.

Оператор может управлять средствами контроля доступа (контроллерами, УПУ), а также проходами абонентов через точки доступа, если при конфигурировании для точки доступа задан алгоритм "А".

Более подробные сведения о работе оператора по управлению средствами контроля и управления доступом приведены в руководстве по эксплуатации модулей "Монитор" и "Управление".

Все события (проходы абонентов, действия операторов, режимы работы и состояния средств контроля доступа) отображаются в окне сообщений, заносятся и хранятся в архиве системы.

1.3.3 Охранная сигнализация

1.3.3.1 Система имеет возможность управления любыми СО, имеющими выход в виде нормально-замкнутой или нормально-разомкнутой контактной группы реле.

1.3.3.2 Система обеспечивает следующие тактики снятия с охраны и постановки на охрану:

- а) автоматическая (вход первого абонента в зону и выход последнего абонента из зоны только через точку доступа, оснащенную считывателями на вход и выход);
- б) централизованная (по командам оператора АРМ охраны);
- в) децентрализованная (по командам абонента с соответствующими полномочиями с терминала).

1.3.3.3 Управление охранной сигнализацией включает в себя:

- а) конфигурирование;
- б) автоматический режим;
- в) управление по командам оператора АРМ охраны и (или) абонентом с терминала;
- г) анализ тревог по архиву сообщений.

Конфигурирование системы в целом аналогично конфигурированию при управлении доступом.

1.3.3.4 Конфигурирование системы в части управления охранной сигнализацией включает в себя:

- а) состав, связи, режимы работы и параметры контроллеров, СО;
- б) точки доступа и зоны охраны;
- в) графические планы с размещенными контроллерами и СО.

1.3.3.5 При конфигурировании можно указать:

- а) зону размещения СО;
- б) нормальное состояние контактной группы (замкнутое, разомкнутое);
- в) состояние контактной группы при отключении питания;
- г) наличие или отсутствие питания (активное, пассивное);
- д) отключение (включение) питания при снятии зоны с охраны (постановки зоны на охрану);
- е) временной интервал задержки постановки зоны под охрану;
- ж) наличие дистанционного контроля;
- и) включение внешних устройств при срабатывании технических средств охраны;
- к) рекомендации по действиям оператора при возникновении тревожных ситуаций.

1.3.3.6 Автоматический режим управления СО возможен только при оснащении всех входов и выходов зоны средствами контроля и управления доступом (считыватели пропусков устанавливаются с обеих сторон точки доступа).

1.3.3.7 Система автоматически распознает события, влияющие на снятие и установку зоны под охрану:

- а) вход в зону первого абонента через точку доступа;
- б) выход из зоны последнего абонента и выполняет необходимые процедуры постановке зоны на охрану и снятию зоны с охраны.

1.3.3.8 При входе в зону первого абонента снимаются с контроля СО, которые были указаны для этой цели в процессе конфигурирования системы.

При выходе последнего абонента из зоны СО ставятся на контроль.

При отсутствии средств контроля доступа система обеспечивает только централизованную и (или) децентрализованную тактику управления.

В этом случае абонентами являются операторы системы и пользователи, работающие с терминалом, которые подразделяются на три категории в соответствии с полномочиями по доступу к информации и управлению.

Ввод данных на абонентов операторов системы выполняется согласно пункту 1.3.2, за исключением данных для пропусков, которые не заполняют.

1.3.3.9 Ввод данных на пользователей терминалами осуществляется с помощью модуля "Администратор" в следующей последовательности:

а) ввести личные данные пользователей терминалов (абонентов) на основании утвержденных документов;

б) назначить абонентам полномочия (старший смены, пользователь, сотрудник СБ, техперсонал);

в) ввести для абонентов с полномочиями "пользователь" список точек и зон, разрешенных для постановки и снятия с охраны с помощью терминала;

г) указать для каждой зоны порядок работы с терминалом (требуется или нет набор кода на терминале, комиссионное снятие с охраны). При комиссионном снятии с охраны ввести количество абонентов, выполняющих снятие;

д) откорректировать, при необходимости, список пользователей терминала для данной зоны.

1.3.3.10 На АРМ охраны поступают все сообщения об изменении состояния технических средств охраны. Все поступающие сообщения сохраняются в архиве сообщений и доступны к дальнейшему просмотру и анализу.

1.3.4 Управление внешними системами

1.3.4.1 Системы цифрового телевидения

Для возможности управления системами цифрового телевидения (СЦТ) необходимо:

а) установить СЦТ на УК или на отдельном компьютере;

б) на УК, который будет управлять СЦТ, создать устройство "Видеосервер";

в) настроить требуемые параметры устройства "Видеосервер";

г) добавит к устройству "Видеосервер" требуемое количество видеокамер и настроить их.

Управления ведеокамерами может выполняться с АРМ охраны либо средствами управления, предоставляемыми СЦТ.

1.3.4.2 Система контроля управления доступом "Сектор- М"

Для взаимодействия с системой контроля управления доступом (СКУД) "Сектор- М" необходимо:

а) при конфигурировании сети добавить в список компьютеров системы компьютер системы "Сектор-М", присвоить ему тип "Сектор-М" и указать каталог обмена;

б) сконфигурировать точки доступа, обслуживаемые "Сектор-М".

1.3.5 Табельный учет

1.3.5.1 Возможность работы с модулем "Табельный учет" определяется в модуле "Администратор" путем установки соответствующей опции, разрешающей или запрещающей работу с данным модулем при назначении доступных действий оператора.

1.3.5.2 Для работы модуля необходимо наличие:

а) заполненных списков абонентов, операторов, графиков, смен, подразделений, создаваемых с помощью модуля "Администратор";

б) заполненного списка зон, создаваемого с помощью модуля "Конфигуратор";

в) информации о проходах абонентов через зоны табельного учета.

1.3.5.3 В качестве зоны табельного учета назначается вся территория объекта, и учет ведется по фактам пересечения внешних контрольно-пропускных пунктов (КПП).

Зоны табельного учета назначаются оператором с правами администратора в модуле "Администратор".

1.3.5.4 Модуль имеет возможность формирования и печати за любой предшествующий или текущий месяц следующих отчетов, включающих информацию по сотрудникам:

а) табель в соответствии с типовой межотраслевой формой № 13, утвержденной постановлением Госкомстата России;

б) опоздания на работу и уход с работы ранее установленного времени.

1.3.5.5 Табель учета использования рабочего времени заполняется с занесением информации по каждому сотруднику.

Учет отработанного времени и нарушений трудового распорядка ведется на основании рабочих графиков. При этом, если график работы не заполнен, то учет отработанного времени не ведется.

Отклонения от рабочего графика (опоздания, уход раньше с работы) фиксируются в соответствии с назначенной сменой по времени начала и окончания работы соответственно. При этом, если задано допустимое время опоздания или ухода раньше с работы, то фиксация отклонений (опозданий и уходов раньше) производится только при превышении указанного параметра.

1.3.5.6 Подробное описание работы с модулем "Табельный учет" приведено в "Система "Цирконий-С2000". Комплект программного обеспечения. Руководство по эксплуатации. Часть 5. Модуль "Табельный учет". БАЖК.425969.022РЭ4".

1.3.6 Формирование отчетов

1.3.6.1 Модуль "Генератор отчетов", устанавливаемый, как правило, на АРМ администратора, позволяет оператору формировать, просматривать, выводить на печать и сохранять типовые отчеты, используя базу данных системы на СБД. Модуль может быть установлен на любом компьютере системы.

1.3.6.2 Модуль обеспечивает формирование следующих отчетов:

- а) список тревожных сообщений;
- б) список попыток несанкционированного доступа (НСД);
- г) список перемещений и времени нахождения абонентов в заданных зонах;

1.3.6.3 Модуль обеспечивает вывод следующей информации из архива:

- а) всей информации;
- б) тревожной информации;
- в) нарушение абонентами режимов доступа;
- г) информации о проходах абонентов;
- д) общее число тревог по всем УК и количество тревог по каждому УК;

1.3.6.4 Подробное описание работы с модулем "Генератор отчетов" приведено в "Система "Цирконий-С2000". Комплект программного обеспечения. Руководство по эксплуатации. Часть 6. Модуль "Генератор отчетов". БАЖК.425969.022РЭ5".

1.4 Действия в экстремальных условиях

1.4.1 Архитектура системы позволяет строить комплексы безопасности, обладающие высокой живучестью.

Для использования всех возможностей системы и действий эксплуатирующего и обслуживающего персонала в экстремальных условиях рекомендуется создание руководства по эксплуатации системы применительно к конкретному объекту.

В составе руководства по эксплуатации рекомендуется разработать инструкции персоналу, которые должны регламентировать поведение и действия персонала в различных условиях эксплуатации системы, в том числе экстремальных, а также взаимодействие с личным составом службы безопасности и сил охраны.

Для отключения системы при возникновении экстремальных условий необходимо:

- а) завершить на каждом компьютере работу с модулем (модулями):
 - 1) выбрать пункт главного меню "Выход";
 - 2) на запрос о выходе из программы нажать кнопку "Да". Работа с модулем (модулями) будет завершена;
- б) завершить работу на компьютере. Отключить питание компьютера;
- в) отключить контроллеры;
- г) отключить питание источника бесперебойного питания;
- д) отключить блоки питания периферийной аппаратуры.

2 Техническое обслуживание

2.1 Техническое обслуживание системы проводится с целью обеспечения надежности работы и предупреждения отказов. Техническое обслуживание включает:

а) ежесменное – профилактический осмотр и проверка станционной аппаратуры при приеме (сдаче) дежурства;

б) годовое – проверка технического состояния периферийной аппаратуры, кабелей и магистралей.

2.2 Объем ежесменного технического обслуживания приведен в таблице 2.1.

Таблица 2.1

Технические требования	Трудоемкость	Методика проведения работ
Комплектность станционной аппаратуры, внешний вид составных частей	1 человек, 5 мин на один компьютер	Проверить внешним осмотром наличие, в соответствии с проектом, всех частей системы на рабочем месте, целостность пломб на блоках. Составные части системы, органы управления и индикации не должны иметь видимых повреждений. Изоляция кабелей, жгутов не должна иметь заметных повреждений. Надписи и обозначения на лицевых панелях должны быть четкими.
При подаче оператором АРМ охраны команды "Выполнить ДК" на группы СО не должен формироваться сигнал "Неисправность"	1 человек, 2 мин на группу СО	Подать команду "Выполнить ДК" с АРМ охраны. На экране монитора на время до 7 с ("быстрые" СО) и на время до 30 с ("медленные" СО) в окне состояния проверяемого СО должно отображаться состояние "Выполнение ДК". При неисправности какого-либо СО на экране отображается сигнал "Неисправность" с указанием номера отказавшего СО.

2.3 Объем годового технического обслуживания приведен в таблице 2.2.

Таблица 2.2

Технические требования	Трудоемкость	Методика проведения работ
На поверхностях блоков и жгутов не должно быть трещин, сколов, нарушения лакокрасочных покрытий и изоляции, надписи и обозначения на лицевых панелях должны быть четкими.	1 человек, 2 мин на один блок, кабель	Проверить внешним осмотром надежность подключения заземляющих проводников к клеммам "┐" на всех составных частях системы, магистралях, состояние лакокрасочных покрытий, четкость надписей и обозначение на лицевых панелях блоков на рабочем месте и соответствие проектной документации. Очистить поверхность корпусов от пыли и грязи увлажненной ветошью. Лицевые панели и органы управления очистить от пыли кистью-флейц.
Целостность мест ввода кабелей и соответствие требованиям инструкции по монтажу БАЖК.425621.002ИМ.	1 человек, 1,0 ч на 10 кабельных вводов.	Проверить внешним осмотром надежность подключения проводников кабелей к клеммам колодок блоков коммутации и подставок контроллеров, распределительных коробок, отсутствие заметных повреждений изоляции кабелей, жгутов соединительных проводников, а также мест ввода кабелей.
Проверка сопротивления заземляющих устройств и соответствие требованиям проекта и инструкции по монтажу БАЖК.425621.002ИМ	2 человека, 25 мин на один контур заземления	Провести измерение сопротивления заземляющих устройств прибором типа М416.

2.4 Техническое обслуживание составных частей системы проводится в соответствии с требованиями эксплуатационных документов на них.

Рекомендуется один раз в два месяца проводить проверку системных установок операционной системы. Работа выполняется инженером по эксплуатации вычислительной техники в соответствии с руководством по эксплуатации операционной системы.

3 Транспортирование и хранение

3.1 Транспортирование и хранение системы должно осуществляться по составным частям в соответствии с требованиями эксплуатационной документации или других технических документов на них.

Перечень принятых сокращений

АРМ	–	автоматизированное рабочее место
БД	–	база данных
ДК	–	дистанционный контроль
ЛВС	–	локальная вычислительная сеть
ОС	–	операционная система
ПО	–	программное обеспечение
СО	–	средство обнаружения
СБД	–	сервер базы данных
СУБД	–	система управления базами данных
УК	–	управляющий компьютер
ЭМЗУ	–	электромеханическое запирающее устройство
MSDE	–	Microsoft SQL Server 2000 Desktop Engine

Лист регистрации изменений

[illegible]