

# ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного  
проектирования

---

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН

11443195.4012- 006 -ЛУ

**Программно-аппаратный комплекс средств защиты  
информации от НСД для ПЭВМ (РС)**

**“Аккорд–АМДЗ”**

(Аппаратный модуль доверенной загрузки)

**РУКОВОДСТВО ПО УСТАНОВКЕ**

**11443195.4012-006 98 03**

**СОДЕРЖАНИЕ**

<b>1. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ИСПОЛЬЗУЕМОМУ ПО .....</b>	<b>3</b>
<b>2. УСТАНОВКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СЗИ НСД "АККОРД-АМДЗ" .....</b>	<b>4</b>
<b>2.1. Назначение элементов и разъемов на плате контроллера.....</b>	<b>4</b>
<b>2.2. Подсоединение контактного устройства (съемника информации).....</b>	<b>5</b>
<b>2.3. Установка контроллера в свободный слот материнской платы ПЭВМ.....</b>	<b>5</b>
<b>2.4. Назначение ТМ-идентификатора администратора безопасности информации (АБИ) .....</b>	<b>6</b>
<b>3. ТРУДНОСТИ ПРИ УСТАНОВКЕ КОМПЛЕКСА И МЕТОДЫ ИХ ПРЕОДОЛЕНИЯ. ....</b>	<b>7</b>
<b>4. СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА "АККОРД".....</b>	<b>9</b>
<b>5. УСТАНОВКА ПО РАЗГРАНИЧЕНИЯ ДОСТУПА НА ЖЕСТКИЙ ДИСК. ....</b>	<b>9</b>

Установка программно-аппаратного комплекса СЗИ НСД "Аккорд-АМДЗ" включает три основных этапа:

1. Установку платы контроллера в свободный слот ПЭВМ и регистрацию администратора БИ (супервизора), в том числе, настройку комплекса в соответствии с конфигурацией технических средств ПЭВМ.

2. Регистрацию пользователей, назначение пользователям личных ТМ-идентификаторов, паролей и времени доступа.

3. Назначения списка дисков, файлов, разделов реестра, контролируемых на целостность.

**Внимание!**

**Перед началом установки комплекса "Аккорд-АМДЗ" рекомендуется подробно ознакомиться с эксплуатационной документацией, прежде всего с "Описанием применения" (11443195.4012-006 31 03) и настоящим руководством.**

## **1. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ИСПОЛЬЗУЕМОМУ ПО**

В настоящее время технические средства комплекса защиты от НСД "Аккорд-АМДЗ" для установки в слот шины PCI выпускаются на базе контроллеров «Аккорд-5mx» и «Аккорд-5.5».

Эти модификации комплекса:

- могут использоваться на ПЭВМ с процессором 80486 и выше, объемом RAM 1 Мбайт и более;
- требуют для установки свободный слот PCI - 32, или 64 – разрядный с напряжением питания шины 3.3В или 5В;
- используют для идентификации персональные идентификаторы DS 1992 - DS 1996 с объемом памяти до 64 Кбит;
- используют для аутентификации пароль до 12 символов;
- блокируют загрузку с отчуждаемых носителей (FDD, CD ROM, ZIP, и др.);
- предусматривают регистрацию до 126 пользователей в энергонезависимой памяти;
- имеют аппаратный датчик случайных чисел (ДСЧ);
- обеспечивают контроль целостности программ и данных.

Для эффективного применения комплекса и поддержания необходимого уровня защищенности ПЭВМ и информационных ресурсов **необходимы:**

- физическая охрана ПЭВМ и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;

- наличие администратора безопасности информации (АБИ) - пользователя, имеющего особый статус и полномочия. Администратор БИ планирует мероприятия по защите информации, определяет права доступа пользователей в соответствии с утвержденным Планом защиты, организует установку комплекса в ПЭВМ, и эксплуатацию защищенной ПЭВМ, ведет учет выданных ТМ-идентификаторов, осуществляет периодическое тестирование комплекса;

- использование в ПЭВМ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ.

Контроллеры "АККОРД", входящие в состав комплекса, имеют два режима доступа к аппаратным ресурсам платы контроллера.

Режим 0 (стандартный): доступ к области кода расширения BIOS только по чтению.

Режим 1 (специальный), в котором при старте компьютера код не исполняется, а области, защищенные при работе контроллера в режиме 0, становятся доступны по чтению/записи. Переход из стандартного режима в специальный требует снятия установочной металлической планки, которая крепится к плате контроллера двумя винтами. В специальном режиме возможна перезапись внутреннего ПО контроллера без изменения аппаратной части и очистка базы данных пользователей. При записи кода в BIOS контроллера следует отключить любые программные менеджеры памяти, установленные на компьютере. Штатные операции изменения режима работы

производятся под контролем службы безопасности. При этом возможна установка пломбы на крепежный винт, которая является индикатором целостности встроенного ПО.

## 2. УСТАНОВКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СЗИ НСД "АККОРД-АМДЗ"

### **Внимание!**

В SETUP компьютера параметр "Plug & Play O/S" должен быть установлен в "NO". Это обеспечивает корректную инициализацию BIOS контроллера "Аккорд", как PCI устройства.

### **Внимание!**

Установка контроллера должна производиться только при выключенном питании ПЭВМ!

Перед установкой аппаратной части комплекса необходимо:

1. Отключить питание.
2. Вскрыть корпус системного блока ПЭВМ, удалить заглушку на задней панели блока и выбрать свободный слот на материнской плате для установки контроллера комплекса.

### 2.1. Назначение элементов и разъемов на плате контроллера.

Расположение элементов и разъемов на плате контроллера "Аккорд-5.5" показано на рис. 1.

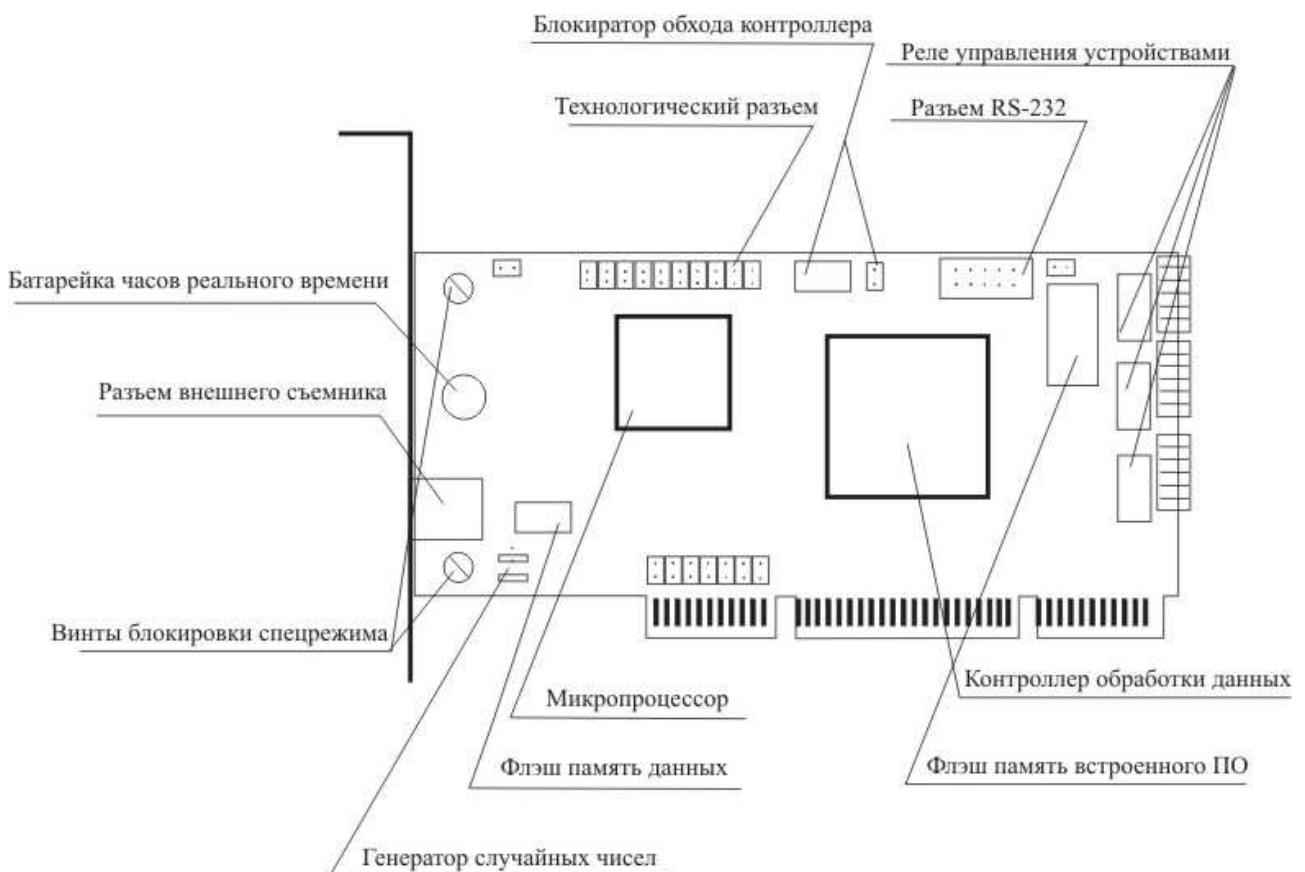


Рис. 1. Плата контроллера "Аккорд-5.5"

При установке контроллера "Аккорд" в слот PCI шины автоматически определяется свободное адресное пространство и выбирается начальный адрес для размещения BIOS контроллера в адресном пространстве, что обеспечивает стабильную работу комплекса на большинстве ПЭВМ, однако при последующей установке новых PCI устройств возможны конфликты с платами, у которых некорректно обрабатывается функция PnP.

## 2.2. Подсоединение контактного устройства (съемника информации)

### **Внимание!**

**Установка съемника информации должна производиться только при выключенной ПЭВМ!**

**Контактное устройство** (съемник информации) предназначено для обеспечения взаимодействия контроллера комплекса СЗИ НСД с персональным идентификатором пользователя (ТМ идентификатор), и может выпускаться с внутренним и внешним исполнением.

Подсоединение внешнего контактного устройства осуществляется с помощью разъема RJ-11 (подобного телефонному разъему) со стороны задней планки контроллера.

Внутренний съемник подсоединяется к плате контроллера внутри корпуса системного блока ПЭВМ. Схема подключения внутреннего съемника приведена на Рис.2.

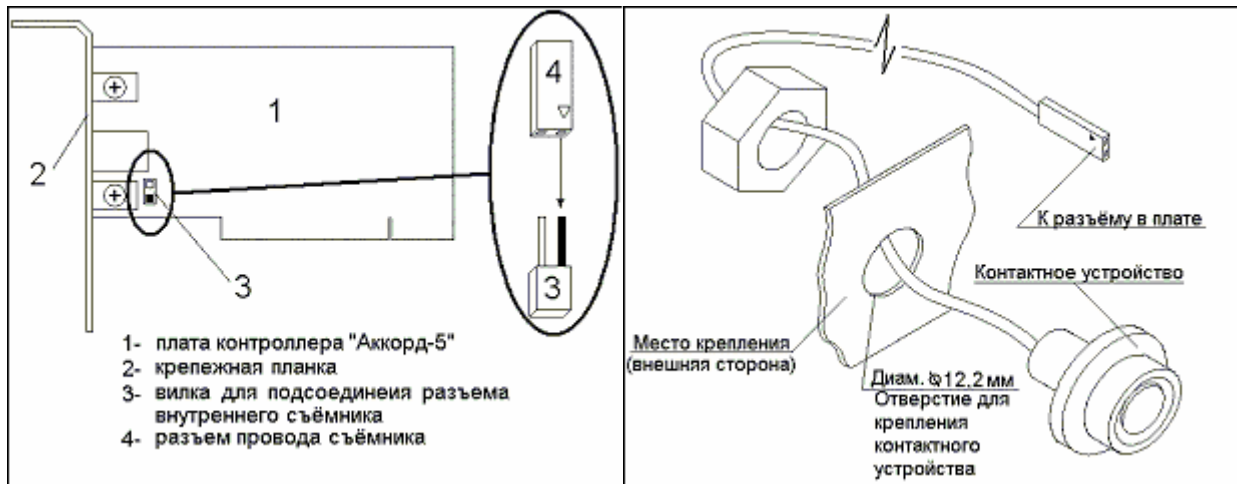


Рис. 2. Подсоединение съемника информации к плате контроллера. Рис. 3. Крепление контактного устройства.

При использовании внутреннего контактного устройства (съемника информации) его установка производится, как правило, на заглушке зарезервированного места для дисководов.

Порядок подсоединения съемника информации:

- 1) Отключить питание ПЭВМ.
- 2) Вскрыть корпус системного блока ПЭВМ.
- 3) Вынуть резервную заглушку (для FDD,CD,ZIP) на передней панели системного блока.
- 4) В резервной заглушке просверлить отверстие  $\varnothing 12,2$  мм для крепления контактного устройства.
- 5) Вставить контактное устройство в отверстие и закрепить его с помощью гайки на резервной заглушке в соответствии с Рис. 3.
- 6) Ввести провод контактного устройства внутрь ПЭВМ и произвести подключение съемника информации к плате контроллера в соответствии с Рис 2.
- 7) Установить заглушку на место и закрыть корпус ПЭВМ.

### **Внимание!**

**Провод центрального контакта съемника (обозначен на соединительном разъеме знаком <треугольник>) должен соответствовать правому контакту разъема X3. Неправильное подсоединение съемника информации к плате контроллера к фатальным последствиям не приведет, однако контроллер не сможет работать с ТМ-идентификатором, и не будет выполнять свои функции.**

## 2.3. Установка контроллера в свободный слот материнской платы ПЭВМ

Контроллер устанавливается в любой свободный PCI слот материнской платы и фиксируется стопорным винтом к задней панели корпуса.

## **2.4. Назначение ТМ-идентификатора администратора безопасности информации (АБИ)**

После установки контроллера включить питание компьютера. В процессе загрузки управление передается контроллеру «Аккорд» и выполняется начальная инициализация. Определяется состав аппаратных средств ПЭВМ и данные заносятся в энергонезависимую память контроллера. Далее производится форматирование базы данных пользователей и внутреннего журнала. После завершения инициализации на экран выводится стартовое меню, в котором доступны для выбора только пункты – «Администрирование».

### **ВНИМАНИЕ!**

При помощи программы администратора, записанной в энергонезависимой памяти контроллера, **обязательно** зарегистрировать главного администратора БИ и назначить ему ТМ-идентификатор (особо обратите внимание на процесс генерации секретного ключа пользователя – если ТМ-идентификатор регистрируется впервые, то следует сгенерировать новый секретный ключ, если ТМ-идентификатор уже зарегистрирован на другом комплексе «Аккорд», то следует выбрать опцию «уже записан в ТМ»). Если все действия произведены правильно, то после выхода из программы администрирования по клавише <Esc> выполняется процедура идентификации/аутентификации и становятся доступными для выбора остальные пункты стартового меню администратора. Если этого не происходит, то вернитесь в режим администрирования и проведите регистрацию администратора (супервизора) более внимательно в соответствии с «Руководством администратора». **Будьте внимательны и тщательно изучите документацию на комплекс (в частности «Руководство администратора»).**

Перезагрузите компьютер и убедитесь в том, что в процессе загрузки появляется сообщение на синем фоне: "Прислоните ТМ-идентификатор..." и после прикосновения ТМ-идентификатором Гл. администратора к съемнику информации происходит загрузка ПЭВМ и выводится стартовое меню администратора.

Зарегистрируйте пользователей и назначьте им права доступа (ПРД) к ресурсам ПЭВМ с помощью программы администратора (в стартовом меню выбрать пункт "Администрирование"). Комплекс "Аккорд-АМДЗ" установлен!

### **3. ТРУДНОСТИ ПРИ УСТАНОВКЕ КОМПЛЕКСА И МЕТОДЫ ИХ ПРЕОДОЛЕНИЯ.**

**Нет реакции на прикосновение ТМ-идентификатором к контактному устройству (съемнику).**

Причина: Кабель внутреннего контактного устройства подключен к плате контроллера неверно.

Действия:

1. Выключить компьютер.
2. Подключить разъем кабеля контактного устройства к разъему X3 контроллера, повернув его на 180 градусов. Если опять нет реакции на прикосновение ТМ-идентификатором к контактному устройству (съемнику) - обратитесь к поставщику комплекса.

**Контроллер работает нормально, но при установке подсистемы разграничения доступа драйвер не обнаруживает контроллер (Сообщение: 'ТМ-контроллер не установлен или неисправен.').**

***Включен режим "Shadow RAM".***

Причина: В Setup ПЭВМ включен режим "Shadow RAM" областей памяти, в которых находится BIOS контроллера "Аккорд".

Действия:

1. При включении ПЭВМ войти в программу Setup (у компьютеров разных фирм комбинация клавиш для входа в Setup различна, поэтому пользуйтесь описанием материнской платы).
2. Отключить режим "Shadow RAM" для тех областей памяти, в которых расположен BIOS контроллера "Аккорд".
3. Выйти из программы Setup с сохранением изменений.

***Драйвер не соответствует версии контроллера.***

Действия:

Повторить процедуру установки драйвера контроллера "Аккорд".

Соответствие драйвера типу контроллера (для справок) приведено в таблице.

Тип контроллера	Имя драйвера
"Аккорд-5"	TMAC5.EXE, TMAC5.SYS
"Аккорд-5mx"	TMAC5X.EXE, TMAC5XWDM.SYS
"Аккорд-5.5"	TMAC55.EXE, TMAC55WDM.SYS

**При попытке стереть в контроллере "Аккорд-5" базу данных пользователей (контроллер в технологическом режиме со снятой установочной планкой) выдается сообщение: "Контроллер неисправен либо не установлен."**

***Программа очистки базы данных пользователей запускается из многозадачной ОС (Windows 95/98, Windows NT)***

В многозадачной ОС каждой программе или процессу выделяется виртуальная память, а программа очистки БД пользователей работает с платой контроллера по физическому адресу.

Действия: установить плату контроллера в компьютер с MS DOS или загрузить Windows 95/98 в режиме "Command prompt only". Очистить базу данных пользователей.

***Версия программы очистки БД не соответствует версии контроллера.***

Причина: Для каждой версии контроллера используется своя программа очистки БД пользователей. Контроллеру "Аккорд-5.5" соответствует программа IP55.EXE.

Действия: используйте программу, соответствующую типу контроллера.

**Контроллер работает нормально, но после выполнения процедур идентификации/аутентификации и контроля целостности загрузка ОС не выполняется (в левом верхнем углу темного экрана мигает курсор).**

***Компьютер заражен загрузочным вирусом.***

Комплекс «Аккорд АМДЗ» аппаратно берет на себя процесс загрузки ПЭВМ. Если все процедуры контроля и идентификации пользователя выполнены правильно, то загрузка передается стандартному загрузчику ОС по определенному адресу. Компьютерные вирусы, которые располагаются в загрузочной области жесткого диска, обычно помещают себя в область стандартного загрузчика. Сам загрузчик при этом помещается в другое место служебной области диска и управление ему передается после работы программы-вируса. Пользователь может долгое время работать на зараженной ПЭВМ, не замечая наличия вируса. Комплекс «Аккорд АМДЗ» при установке на ПЭВМ вступает в конфликт с программой-вирусом, что проявляется в зависании при попытке загрузить ОС.

Действия:

Извлечь плату контроллера из ПЭВМ, загрузиться со сменного носителя, проверить диск на наличие вирусов. При обнаружении программ-вирусов попытаться очистить от них жесткий диск. Если попытка неудачная, отформатировать диск, установить заново ОС и, убедившись в отсутствии вирусов продолжить установку СЗИ «Аккорд».

***Жесткий диск отформатирован нестандартной программой, или его параметры (размер логических разделов, файловая система и т.д.) были изменены после форматирования какой-либо программой-утилитой, например Partition Magic.***

Действия:

Отформатировать диск стандартной программой из состава ОС.

***На компьютере вирусы не обнаружены, жесткий диск отформатирован стандартным образом, но загрузка ОС не выполняется.***

Причина:

Некоторые фирмы-производители компьютеров используют нестандартные недокументированные функции в системном BIOS, или процедуре загрузки (например, на некоторых компьютерах фирмы COMPAQ устанавливалась процедура SETUP в виде «скрытого» первого раздела жесткого диска). Выполнение загрузки стандартным способом по стандартному адресу на таком компьютере приводит к конфликту и зависанию.

Действия:

Извлечь контроллер «Аккорд» из ПЭВМ, с помощью утилиты acgetmbr.exe, которая поставляется на гибком диске с документацией на комплекс, скопировать образ MBR (главной загрузочной записи) в файл. С помощью какой-либо утилиты, например Norton Disk Editor, скопировать содержимое системного BIOS в файл. Выслать эти два файла с подробным описанием модели и конфигурации компьютера в ОКБ САПР по адресу support@okbsapr.ru.

**Контроллер работает нормально, но после выполнения процедур идентификации/аутентификации и контроля целостности загрузка ОС Windows 95/98 не выполняется (выводится графический экран загрузки Windows, и компьютер «зависает»). Для пользователя с правами администратора загрузка выполняется нормально.**

Причина: В параметрах доступа пользователя включен режим управления режимами загрузки ОС Windows, но в файле MSDOS.SYS не установлен параметр BootMenu=1.

Действия:

Отключить для пользователя режим управления загрузкой ОС, сняв все флаги в соответствующем разделе, или прописать строку «BootMenu=1» в разделе [Options] в файле MSDOS.SYS.

## **4. СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА "АККОРД".**

### **Внимание!**

Снятие защиты разрешено только администратору БИ (супервизору).

Для снятия защиты необходимо выполнить следующие действия:

1. Отключить питание.
2. Вскрыть корпус системного блока ПЭВМ.
3. Снять аппаратную часть комплекса.
4. Если установлено ПО разграничения доступа «Аккорд-1.95», то следует удалить вызовы соответствующих модулей из файлов AUTOEXEC.BAT и CONFIG.SYS.

## **5. УСТАНОВКА ПО РАЗГРАНИЧЕНИЯ ДОСТУПА НА ЖЕСТКИЙ ДИСК.**

ПО поставляется по **отдельному заказу** на дискетах, или компакт-диске.

Установка ПО комплекса на жесткий диск ПЭВМ осуществляется в следующей последовательности:

1. Вставьте в CD привод дистрибутивный компакт-диск из комплекта поставки СПО.
2. Запустите находящуюся на диске программу SETUP.EXE. Программа инсталляции создаст на диске C:\ каталог C:\ACCORD (C:\ACCORD.NT для комплекса «Аккорд NT/2000») и скопирует туда программное обеспечение. На данном этапе не производится никаких изменений жесткого диска, кроме создания каталогов или файлов.

Для комплекса «Аккорд-1.95» будут созданы файлы AUTOEXEC.ACC и CONFIG.ACC, которые представляют собой копии файлов AUTOEXEC.BAT и CONFIG.SYS с внесенными изменениями, необходимыми для работы комплекса, или эти изменения вносятся в файлы AUTOEXEC.BAT и CONFIG.SYS, если при установке выбрать соответствующую опцию

При помощи программы C:\ACCORD\ACED32.EXE (см. "Установка правил разграничения доступа. Программа ACED32") зарегистрировать пользователей и назначить им правила доступа к ресурсам компьютера.

Активизация подсистемы разграничения доступа к ресурсам ПЭВМ (АС) для комплекса «Аккорд 1.95» заключается в изменении установок в файлах AUTOEXEC.BAT и CONFIG.SYS в соответствии с дополнениями, указанными в созданных при инсталляции файлах AUTOEXEC.ACC и CONFIG.ACC. Внимательно ознакомьтесь с «Руководством по установке комплекса Аккорд 1.95» и следуйте рекомендациям и требованиям этого документа.

После включения вызовов компонентов защиты необходимо выполнить перезагрузку компьютера.

В комплексе «Аккорд NT/2000» для активизации и снятия подсистемы разграничения доступа и задания дополнительных параметров служит программа AcSetup.EXE. Внимательно ознакомьтесь с «Руководством по установке комплекса Аккорд NT/2000» и следуйте рекомендациям и требованиям этого документа.