

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

| | |
|---|----------|
| 1. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ И ИСПОЛЬЗУЕМОМУ ПО | 3 |
| 2. УСТАНОВКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА СЗИ НСД "АККОРД-АМДЗ" | 4 |
| 2.1. Назначение элементов и разъемов на плате контроллера. | 4 |
| 2.2. Подсоединение контактного устройства (съемника информации) | 5 |
| 2.3. Установка контроллера в свободный слот материнской платы ПЭВМ Ошибка! Закладка не определена. | |
| 2.4. Назначение ТМ-идентификатора администратора безопасности информации (АБИ) | 5 |
| 3. ТРУДНОСТИ ПРИ УСТАНОВКЕ КОМПЛЕКСА И МЕТОДЫ ИХ ПРЕОДОЛЕНИЯ. | 6 |
| 4. СНЯТИЕ СРЕДСТВ ЗАЩИТЫ КОМПЛЕКСА "АККОРД". | 8 |
| 5. УСТАНОВКА ПО РАЗГРАНИЧЕНИЯ ДОСТУПА НА ЖЕСТКИЙ ДИСК. | 8 |

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 mini-PCI-Express выпускаются на базе контроллера «Аккорд-5.5 mini-PCIe».

Эта модификация комплекса:

- может использоваться на ПЭВМ с процессором Intel Pentium I и выше, объемом RAM 8 Мбайт и более;
- требует для установки свободный слот mini-PCI-Express;
- использует для идентификации персональные идентификаторы DS 1992 - DS 1996 с объемом памяти до 64 Кбит;
- использует для аутентификации пароль до 12 символов;
- блокирует загрузку с отчуждаемых носителей (FDD, CD ROM, ZIP, и др.);
- предусматривает регистрацию до 126 пользователей в энергонезависимой памяти;
- имеет аппаратный датчик случайных чисел (ДСЧ);
- обеспечивает 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.

Контроллер "АККОРД-5.5 mini-PCIe", входящий в состав комплекса, имеет два режима доступа к аппаратным ресурсам платы контроллера.

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

Режим 1 (специальный, или технологический), 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 (технологический) требует перевода переключателя в крайнее верхнее положение (см. Рис.1 - вид на плату со стороны установочных элементов, шинный разъем внизу). В технологическом режиме возможна перезапись внутреннего ПО контроллера без изменения аппаратной части и очистка базы данных пользователей, например, при утере ТМ-идентификатора администратора. Запись программного кода в BIOS контроллера возможна только при загрузке на компьютере однозадачной ОС. После перепрограммирования контроллера, или очистки базы данных необходимо выключить питание

компьютера, извлечь контроллер и вернуть переключатель технологического режима в исходное (крайнее нижнее) положение. Штатные операции изменения режима работы производятся под контролем службы безопасности.

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!

Для установки аппаратной части комплекса необходимо:

1. Отключить питание компьютера.
2. Открыть защитную крышку разъема mini-PCI-Express и установить в свободный слот контроллер комплекса.

2.1. Назначение элементов и разъемов на плате контроллера.

Расположение элементов на плате контроллера "Аккорд-5.5 mini-PCIe" показано на рис. 1.

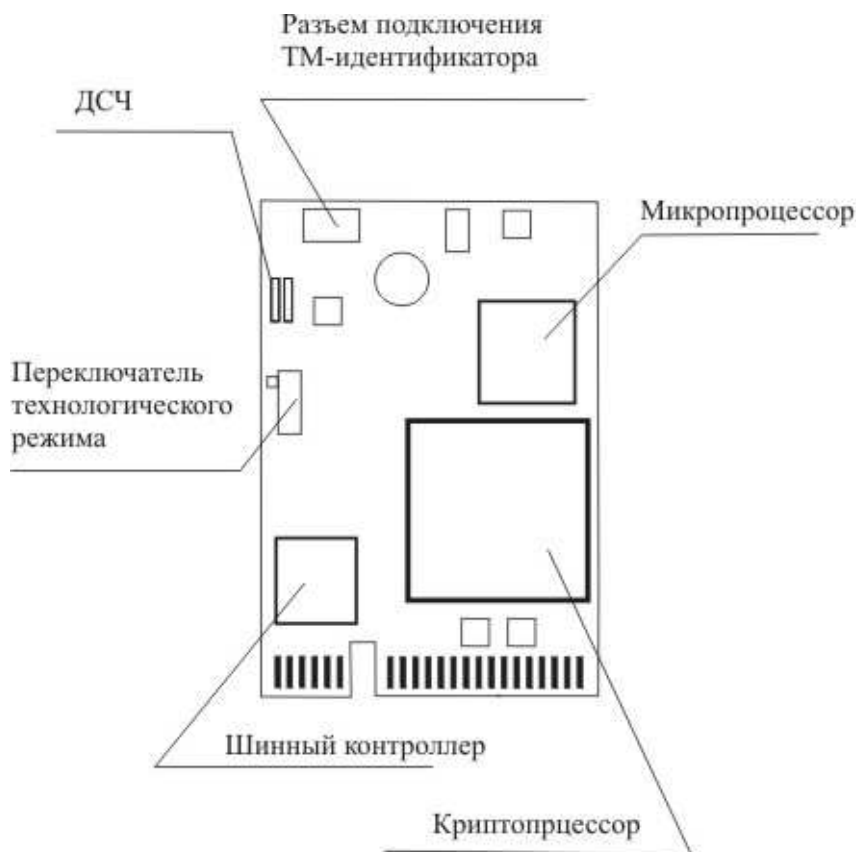


Рис. 1. Плата контроллера "Аккорд-5MX mini-PCI"

После установки в компьютер контроллер "Аккорд-5.5 mini-PCIe" при старте автоматически определяет свободное адресное пространство и выбирает начальный адрес для размещения расширения BIOS в адресном пространстве. Это обеспечивает стабильную работу комплекса на большинстве ПЭВМ, однако возможны конфликты с устройствами, 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).

Контроллер Аккорд-5МХ mini-PCie имеет двухконтактный разъем (на схеме обозначен как «Разъем подключения ТМ-идентификатора»), через который можно вывести провода на внешнее контактное устройство. Возможен вариант, когда эти провода коммутируются на разъем RJ11, например, разъем подключения модема. В этом случае к разъему RJ11 подключается штатный внешний съёмник из состава комплекса. Варианты подключения определяются конструктивными особенностями конкретного компьютера.

2.3. 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.

В дальнейшем с помощью программы администратора (в стартовом меню выбрать пункт "Администрирование") можно регистрировать новых пользователей, менять состав контролируемых объектов и работать с журналом регистрации событий. Комплекс "Аккорд-АМДЗ" установлен!

3. ТРУДНОСТИ ПРИ УСТАНОВКЕ КОМПЛЕКСА И МЕТОДЫ ИХ ПРЕОДОЛЕНИЯ.

При старте компьютера управление не передается контроллеру «Аккорд»

Жесткий диск не размечен и не отформатирован, т.е. не имеет ни одного логического раздела.

Причина: Если на жестком диске нет загрузочной записи (MBR) и не установлен ни один сменный загрузочный диск, то нет и возможности перехватить загрузку при старте контроллера «Аккорда».

Действия:

Разметить диск и отформатировать его в одной из файловых систем, которые поддерживает СЗИ «Аккорд», вставить любой загрузочный диск.

Контроллер находится в технологическом режиме.

В этом случае не выполняется старт программы микропроцессора на плате контроллера и загрузка не перехватывается.

Действия:

Перевести контроллер в рабочий режим.

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

Причина: Кабель контактного устройства подключен неверно.

Действия:

1. Выключить компьютер.
2. Поменять полярность подключения проводов к контактному устройству, которое связано с разъемом на плате контроллера.

При попытке стереть в контроллере «Аккорд-5.5 mini-PCIe» базу данных пользователей (контроллер в технологическом режиме) выдается сообщение: «Контроллер неисправен либо не установлен.»

Программа очистки базы данных пользователей запускается из многозадачной ОС (Windows 95/98, Windows NT/2000/XP)

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

Действия: загрузить на компьютере со сменного носителя MS DOS или 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 mini-PCIe» 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 недокументированные функции в системном BIOS, или процедуре загрузки. Например, на некоторых компьютерах фирмы COMPAQ устанавливалась процедура SETUP в виде «скрытого» первого раздела жесткого диска; на компьютерах других фирм обнаруживались недокументированные функции обработчика INT13; в третьем случае процедура удаленной сетевой загрузки BootRom занимала область памяти большую, чем было прописано в системном BIOS. Выполнение загрузки стандартным способом по стандартному адресу на таком компьютере приводит к конфликту и зависанию.

Действия:

Извлечь контроллер «Аккорд» из ПЭВМ, с помощью утилиты asgetmbr.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.

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.

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 дисковод для гибких дисков дистрибутивную дискету 1, или компакт-диск из комплекта поставки.

2. Запустите находящуюся на дискете (диске) программу SETUP.EXE. Следуйте рекомендациям программы-инсталлятора. Программа 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

Рекомендуется распечатать эти файлы и ознакомиться с изменениями, которые необходимо внести в файлы AUTOEXEC.BAT и CONFIG.SYS для правильного функционирования системы "Аккорд". Эти изменения должны быть рассмотрены на предмет корректности их установки с учетом загружаемого ими окружения (особенно при использовании меню в файле CONFIG.SYS). Это необходимо сделать, так как бывают случаи, когда вызовы программ комплекса включаются дважды или некорректно, хотя программа INSTALL в большинстве случаев правильно создает файлы AUTOEXEC.ACC и CONFIG.ACC.

Если при установке выбран вариант с внесением изменений в файлы AUTOEXEC.BAT и CONFIG.SYS, то по завершению установки компьютер необходимо перезагрузить. Также необходима перезагрузка после установки комплекта ПО «Аккорд NT/2000»/

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.

Эти изменения сводятся к следующему:

1. В файл AUTOEXEC.BAT должен быть включен вызов драйвера TMC5X.EXE с необходимыми параметрами.

2. Вместо какой-либо программной оболочки (обычно NC.EXE) в файле AUTOEXEC.BAT должен быть установлен вызов C:\ACCORD\ACRUN.EXE. Следует заметить, что программа ACRUN.EXE может быть запущена с ключом /R, т.е. C:\ACCORD\ACRUN.EXE /R. В этом случае при завершении работы программы ACRUN.EXE будет произведена перезагрузка ПЭВМ. Именно

этот режим работы следует считать основным, однако на время тестирования ключ /R можно не включать. Программа ACRUN.EXE является монитором прав доступа и запускает стартовую задачу, назначенную тому пользователю, который вошел в систему.

3. В файл CONFIG.SYS должна быть включена загрузка драйвера AMDZ5X.SYS:

DEVICE= C:\ACCORD\AMDZ5X.SYS

Данный драйвер запрещает применять клавиши <Ctrl>, <Alt> и любые их комбинации в процессе исполнения файлов CONFIG.SYS и AUTOEXEC.BAT. Нажатие любой комбинации данных клавиш вызывает перезагрузку компьютера. Тем самым исключается возможность прерывания исполнения файлов CONFIG.SYS и AUTOEXEC.BAT пользователем. Данная строка должна быть помещена в файле CONFIG.SYS первой. В случае применения QEMM-386 данная строка должна быть первой после вызова DOSDATA.SYS, QEMM386.SYS, DOS-UP.SYS. Загрузка QEMM386.SYS должна выполняться с ключами BE:N BF:N. Также для любого менеджера памяти следует запретить использование области памяти, в которой находится BIOS контроллера.

После включения вызовов компонентов защиты необходимо выполнить перезагрузку компьютера.

Обратите внимание, что при установке правил разграничения доступа к сетевым ресурсам следует явно указать имя сервера, имя тома и только потом каталог или файл на сервере (см. примеры в "Руководстве администратора").

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.