ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.509000.056 31-ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win64 К»

ОПИСАНИЕ ПРИМЕНЕНИЯ

11443195.509000.056 31

АННОТАЦИЯ

Настоящий документ является описанием применения специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win64 K» (ТУ 509000-056-11443195-2013) (далее по тексту – СПО «Аккорд-Win64 K», «Аккорд-Win64 K», СПО «Аккорд», «Аккорд») и предназначен для лиц, планирующих и организующих защиту информации в системах и средствах информатизации на базе СВТ.

В документе приведены нормативные требования по защите информации, общие принципы и правила организации работы по обеспечению конфиденциальности информации, основные защитные функции СПО «Аккорд», его возможности, особенности установки и применения.

Перед установкой и эксплуатацией СПО «Аккорд» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые организационные меры защиты, указанные в документации.

Применение защитных механизмов СПО «Аккорд» должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

1. Назначение СПО «Аккорд»

Специальное программное обеспечение «Аккорд-Win64 K» (далее по тексту – СПО «Аккорд» или СПО «Аккорд-Win64 K») предназначено для применения на СВТ, функционирующих под управлением Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 (64-bit) или ОС Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 2008, Windows 7, Windows 8 и Windows 8.1 (32-bit) с целью обеспечения защиты от несанкционированного доступа к СВТ и АС на их основе при многопользовательском режиме эксплуатации.

В СПО «Аккорд-Win64 K» реализованы следующие основные механизмы защиты информации:

- механизм дискреционного контроля доступа;
- механизм контроля доступа на основе иерархических меток;
- механизм контроля подключения съемных машинных носителей информации;
- механизм идентификации и аутентификации пользователей;
- механизм регистрации системных событий;
- механизм контроля целостности.

СПО «Аккорд» включает в себя специальное программное обеспечение разграничения доступа в среде операционных систем Windows – СПО «Аккорд-Win64 K». Состав СПО «Аккорд» определяется при заказе в соответствии с требованиями Заказчика и указывается в формуляре.

2. Условия применения СПО «Аккорд»

2.1. Технические требования

Для установки СПО «Аккорд» требуется следующий минимальный состав технических и программных средств:

- установленная на СВТ 64-bit операционная система Windows XP, Windows Server 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 (64-bit) или Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 (32-bit);
- наличие CD ROM для установки СПО разграничения доступа;
- объем дискового пространства для установки СПО «Аккорд» – не менее 11 Мб;

При применении СПО «Аккорд» количество пользователей, регистрируемых на одном СВТ, не должно превышать 3000 человек. При использовании СПО «Аккорд» для защиты систем терминального доступа возможна регистрация до 1024 пользователей.

Количество и тип идентификаторов, используемых для идентификации пользователей, определяется Заказчиком при поставке и указывается в формуляре.

Функциональные ограничения на применение СПО «Аккорд-Win64 К» не накладываются.

2.2. Организационные меры

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности СВТ и информационных ресурсов АС необходимы:

- физическая охрана СВТ и его средств;
- наличие администратора безопасности информации (администратор БИ) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия (супервизора). Администратор БИ должен организовать установку изделия в СВТ, настройку защитных механизмов изделия в соответствии с правами доступа пользователей, осуществлять контроль за правильным использованием СВТ с установленным изделием;
- использование в СВТ технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в ГСЗИ;
- запрет на использование в СВТ любых сторонних служб и протоколов, позволяющих осуществить удаленный доступ к подконтрольным объектам (Telnet, SSH, TeamView, RemoteDesktop и т.д.).

3. Описание задачи

3.1. Особенности защитных функций СПО «Аккорд»

СПО «Аккорд» обеспечивает выполнение требований по 4 уровню контроля отсутствия недекларированных возможностей[1], по 5 классу защищенности[2], по 4 четвертому классу защиты профиля защиты средств контроля подключения съемных носителей информации (ИТ.СКН.П4.ПЗ), требованиям Задания по безопасности 11443195.509000.056 ЗБ и требованиям Технических условий ТУ 509000-056-11443195-2013.

Защитные функции СПО «Аккорд» реализуются применением:

1)дисциплины защиты от НСД СВТ, включая:

- идентификацию пользователя по уникальным данным для идентификации;
- аутентификацию с учетом необходимой длины пароля;
- контроль целостности программ и данных на жестком диске.

2)процедур блокирования экрана и клавиатуры по команде пользователя или по истечению установленного интервала «неактивности» пользователя;

3)дисциплины разграничения доступа к локальным и сетевым ресурсам СВТ в соответствии с установленными ПРД и определяемыми атрибутами доступа (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» пункт 6.10), которые устанавливаются администратором БИ в соответствие каждой паре «субъект доступа - объект доступа» при регистрации пользователей.

СПО «Аккорд» позволяет администратору использовать как дискреционный, так и мандатный[3] методы разграничения доступа. Администратор может предоставить пользователю выбор уровня доступа запускаемой задачи, или выбор уровня конфиденциальности всей сессии пользователя. Данный механизм позволяет обрабатывать документы разного уровня конфиденциальности одним набором прикладного ПО без ухудшения надежности защитных механизмов.

4)дисциплины управления процедурами ввода/вывода на отчуждаемые носители информации. Дополнительно для каждого пользователя контролируется список разрешённых USB-устройств в соответствии с их уникальными идентификационными номерами;

---

[1] В соответствии с требованиями руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей».

[2] В соответствии с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.).

[3] В рамках настоящего документа под мандатным принципом контроля доступа понимается принцип контроля доступа на основе иерархических меток.

5)дисциплины контроля доступа к любому устройству, или классу устройств, доступных в «Диспетчере устройств» Windows, в том числе последовательных и параллельных портов, устройств PCMCI, IEEE 1394, WiFi, Bluetooth и пр;

6)дисциплины очистки внешней памяти;

7)регистрации контролируемых событий, в том числе несанкционированных действий пользователей, в системном журнале, доступ к которому предоставляется только Администратору БИ;

8)дисциплины защиты от НСД систем терминального доступа, функционирующих на базе терминальных служб сетевых операционных систем Windows и программного обеспечения компании Citrix Systems для терминальных серверов;

9)контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций). Возможна проверка целостности программ и данных по индивидуальному списку для отдельного пользователя или группы пользователей. Подсистема контроля целостности предусматривает как статический список (проверка выполняется однократно в начале сеанса, а далее с периодичностью, заданной администратором), так и динамический список, проверка по которому выполняется при каждой загрузке контролируемого файла в оперативную память. Для статического контроля администратор может включить дополнительную функцию восстановления поврежденного файла;

10) других механизмов защиты в соответствии с требованиями нормативных документов по безопасности информации.

3.2. Построение системы защиты информации на основе СПО «Аккорд»

Построение системы защиты информации с использованием СПО «Аккорд» и ее взаимодействие с программно-аппаратным обеспечением СВТ показаны на рисунке 1.

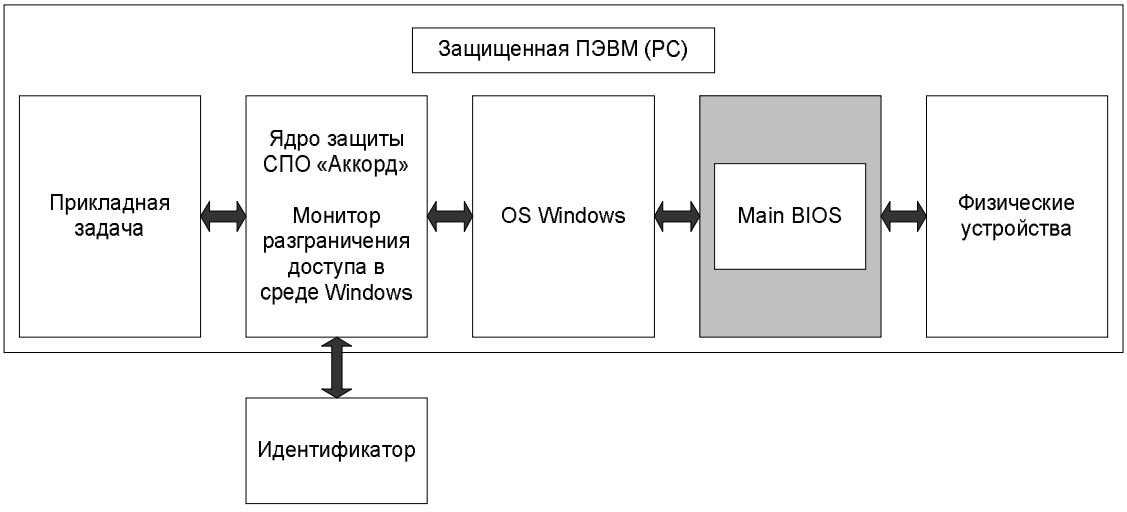

Рисунок 1 - Построение системы защиты информации с использованием СПО «Аккорд»

Защита информации с использованием СПО «Аккорд» основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам СВТ. Средства СПО «Аккорд» перехватывают соответствующие программные прерывания, анализируют запрос и в зависимости от соответствия полномочий субъекта доступа (или его прикладной задачи), либо разрешают операционной системе обработку этих событий, либо запрещают (передают операционной системе код ошибки).

СПО «Аккорд» состоит из собственно средств защиты СВТ от НСД и средств разграничения доступа к ее ресурсам, которые условно можно представить в виде взаимодействующих между собой подсистем защиты информации, описанных ниже.

3.2.1. Подсистема управления доступом

Предназначена для защиты СВТ от посторонних[1] пользователей, управления доступом к объектам доступа и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа (ПРД).

Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленных данных для идентификации с перечнем зарегистрированных на СВТ) и аутентификации (подтверждение принадлежности данных для идентификации данному пользователю) с защитой от раскрытия пароля.

В СПО «Аккорд» реализованы принципы дискреционного и мандатного управления доступом. При использовании дискреционного управления зарегистрированному пользователю устанавливаются права доступа по принципу регистрации «белого списка» разрешенных к запуску программ (задач) и данных, а также «черного списка» запрещенных ресурсов, которые прописываются в ПРД. При использовании мандатного управления пользователю (субъекту) устанавливается уровень доступа, а объекту (данным или задаче) присваивается метка доступа (гриф). При запросе пользователя на доступ к объекту, в зависимости от уровня полномочий пользователя, разрешается или запрещается запрошенный тип доступа. Возможно использование одновременно двух механизмов доступа.

Настройка подсистемы разграничения доступом СПО «Аккорд» осуществляется администратором БИ с использованием программы ACED32, см. документ «Установка правил разграничения доступом. Программа ACED32» (11443195.509000.056 97), входящий в состав эксплуатационной документации на СПО «Аккорд».

3.2.2. Подсистема регистрации и учета

Предназначена для регистрации в системном журнале событий, обрабатываемых подсистемой разграничения доступа «Аккорд-Win64 K». При регистрации событий в системном журнале указываются:

---

[1] Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретном СВТ Идентификатора).

- дата и время события;
- пользователь, осуществляющий регистрируемое действие;
- действия пользователя (сведения о входе/выходе пользователя в/из системы, запуске программ, фактах НСД и другие события.).

Перечень регистрируемых событий, их описание приводится в «Руководстве администратора» (11443195.509000.056 90).

Работа с системными журналами осуществляется с использованием программы LOGVIEW.EXE, см. документ «Подсистема регистрации. Программа работы с журналами регистрации «LogView» (11443195.509000.056 99) из комплекта эксплуатационной документации на СПО «Аккорд».

ВНИМАНИЕ! Доступ к системному журналу возможен только для администратора БИ (супервизора).

3.2.3. Подсистема контроля целостности

Предназначена для исключения несанкционированных модификаций программной среды, обрабатываемой информации, обеспечивая при этом защиту СВТ от внедрения программных закладок и вирусов.

Контроль целостности в СПО «Аккорд» реализуется:

- проверкой целостности назначенных для контроля файлов реестра, пользовательских программ и данных;
- механизмом создания изолированной программной среды, запрещающей запуск привнесенных программ.

Функционирование подсистемы обеспечения целостности в СПО семейства «Аккорд» основано на использовании следующих механизмов:

- при проверке на целостность вычисляется контрольная сумма файлов и сравнивается с эталонным (контрольным) значением, хранящимся в базе данных пользователей. Эти данные могут изменяться в процессе эксплуатации СВТ;
- для исключения фактов не обнаружения модификации файла используется сложный алгоритм расчета контрольных сумм.

4. Состав СПО «Аккорд»

СПО «Аккорд» включает в себя:

Специальное ПО разграничения доступа в среде Windows в составе:

- ядро защиты – программы, реализующие защитные функции СПО «Аккорд»;
- программы управления защитными функциями СПО «Аккорд» (настройки СПО «Аккорд» в соответствии с ПРД);

Состав СПО «Аккорд-Win64 K» представлен в табл. 3.

Таблица 1 - Состав СПО «Аккорд-Win64 K»

Функционально назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
Ядро защиты	ACRUN.SYS.	Ядро системы, выполненное как kernel mode driver. Реализует функции монитора разграничения доступа. Также он реализует функции хранителя экрана.
	ACGINAxxx.DLL	Программа, реализующая политику безопасности идентификации/аутентификации ОС Windows. Эта программа необходима для начала нового сеанса работы, отслеживания завершения сеанса работы пользователя. Также, выполняет функции вывода на экран (в режиме GUI) информации поступающей от ACRUN.SYS.
	ACED32.EXE	Программа формирования базы пользователей, а также редактор прав доступа пользователей к объектам ОС. Позволяет сформировать ПРД для конкретного пользователя (используя дискреционную или мандатную политики доступа), назначить пароль, определить параметры Screen Saver, назначить контроль целостности, сформировать список разрешённых для конкретного пользователя USB-устройств
	ACUSRMOD.DLL	Библиотека для перехвата работы с клипбордом и принтерами, также позволяет пользователю понизить гриф процесса
Программы управления (настройки)	ACBOOT.SYS	драйвер для поддержки USB клавиатуры. Используется драйвером ACRUN.SYS
	AcHookMK.DLL	Библиотека, осуществляющая блокировку компьютерной мыши и клавиатуры СВТ, оснащенного ОС Windows Server 2008/ Windows Server 2012, в режиме терминальной сессии
	ACLOCK2K.SYS	драйвер блокировки клавиатуры и мыши в ОС WINDOWS XP
	ACXALLOW.SYS	Драйвер контроля имён общих ресурсов[1]

[1)] Драйвер состоит из двух драйверов: 1. работает по принципу TDI-фильтра и применяется в ОС Windows NT, Windows Server 2000, Windows XP, Windows Server 2003. 2. использует

Функциональное назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
	ACXLMSRV.SYS	драйвер для блокировки попыток расшарить не прописанные в правилах доступа (ПРД) ресурсы. Используется драйвером ACRUN.SYS
	ACRUNNT.EXE	сервис, необходимый для вывода на экран логотипа фирмы, блокирования с помощью мышки системы, блокирования запрещенных USB устройств, вызова внешних антивирусных модулей и вывода сообщений от ACRUN.SYS
	EDS32.DLL	библиотека ЭП, используется программой ACED32.EXE
	ACCORD.INI	файл, содержащий описание конфигурации всей системы в целом
	LOGVIEW.EXE	программа просмотра, фильтрации, вывода на печать журналов работы пользователей
	LOGBASE.EXE	программа для управления журналами пользователей (сортировка по пользователям, по датам, работа с архивами журналов)
	LOGTOPRD.EXE	программа для анализа журналов пользователей и составления ПРД по результатам анализа
	MAKEPRC.EXE	программа для назначения ПРД исключительным процессам
	ACPROC.EXE	программа для анализа журналов пользователей и составления списков используемых процессов и запускаемых программ
	ACTSKMNG.EXE	диспетчер задач. Может использоваться для создания изолированной программной среды
	ACTSKMNG.INI	файл конфигурации для ACTSKMNG.EXE
	READPRD.EXE	программа для просмотра файлов *.PRD. Т.е файлов содержащих описание правил разграничения доступа
	ACCORD.SCR	обычный хранитель экрана с информацией о продукте
	ACSETUP.EXE	программа для установки/снятия программной части системы защиты, а также изменения параметров её функционирования
	ACSETUPTC.EXE	программа для установки/снятия программной части системы защиты терминального клиента, а также изменения параметров её функционирования
	ACPRNCFG.EXE	программа настройки печати и просмотра журнала печати
	TMATTACH.DLL	библиотека, которая содержит графическое представление работы с TouchMemory. Используется программой ACED32.EXE
	TMDRV32_1.DLL	библиотека, служит для работы с TouchMemory. Используется библиотекой TMATTACH.DLL
	TMDRV32_2.DLL	– библиотека, осуществляющая связь с USB устройством «ШИПКА». Используется библиотекой TMATTACH.DLL

технологию Windows Filtering Platform и применяется в ОС Windows Vista и выше (находится в каталоге c:\accord.nt\Vista)

Функционально назначение программ	Наименование модуля	Назначение и краткая характеристика модуля
	VCTMDRV.DLL	библиотека для работы с виртуальными каналами (для передачи идентифицирующей информации), используется при работе с терминальными клиентами
	AcRunTI.exe	программа для вывода логотипа фирмы, при работе терминального клиента
	CSTMDRV.dll	библиотека, реализующая виртуальный канал по протоколу ICA, на стороне сервера
	CWSTMDRV.dll	библиотека, реализующая виртуальный канал по протоколу ICA, на стороне клиента
	RDPTMDRV.dll	библиотека, реализующая виртуальный канал по протоколу RDP, на стороне сервера
	TMDRVRDP.dll	библиотека, реализующая виртуальный канал по протоколу RDP, на стороне клиента

4.1. Принцип работы СПО «Аккорд»

После успешного выполнения процедур идентификации и аутентификации Администратора производится загрузка ОС, инсталляция специального программного обеспечения – подсистемы разграничения доступа в среде Windows на жесткий диск СВТ. Активизация монитора разграничения доступа, настройка СПО «Аккорд», регистрация пользователей и установка правил разграничения доступа (ПРД) выполняются только администратором БИ.

При регистрации пользователей администратором БИ определяются их права доступа: список исполняемых программ и модулей, разрешенных к запуску данным пользователем, и список прав доступа к объектам (ресурсам) с использованием дискреционного и/или мандатного механизма разграничения – см. «Руководство администратора» (11443195.509000.056 90).

После старта ОС управление передается «ядру защиты» СПО «Аккорд» в составе модуля ACRUN.SYS – «монитора разграничения доступа» и модуля ACGINA.DLL – библиотеки динамической компоновки параметров доступа пользователей в Windows с учетом результатов их идентификации/аутентификации.

Модуль ACRUN.SYS предназначен для разграничения доступа к ресурсам СВТ в соответствии с правилами разграничения доступа, назначенными администратором безопасности СПО «Аккорд» конкретному пользователю.

Модулем ACGINA.DLL осуществляется перехват стандартных запросов к GINA и их модификация для обеспечения работы СПО «Аккорд-Win64 K». Библиотека ACGINA.DLL использует сведения о пользователе, который выполнил идентификацию/аутентификацию. На основании этих сведений разрешается вход в систему Windows зарегистрированных пользователей, и запрещается вход в систему неавторизованных пользователей. Сведения о пользователе, которому разрешен вход в систему, передаются модулю ACRUN.SYS.

Кроме того, «монитор разграничения доступом» ограничивает доступ пользователя к ресурсам, расположенным как локальных, так и на сетевых дисках, в соответствии с едиными правилами разграничения доступа (ПРД).

5. Входные данные

Входными данными СПО «Аккорд-Win64 К» являются:

1) Идентификационные и аутентификационные данные пользователей. В зависимости от выбранного метода идентификации, идентификационными данными пользователя являются логин пользователя, введенный с клавиатуры (основной метод идентификации/аутентификации) или данные аппаратного персонального идентификатора (дополнительный метод идентификации/аутентификации). Аутентификационными данными пользователя является пароль, введенный пользователем с клавиатуры.

2) Параметры (атрибуты) доступа пользователей к объектам доступа СВТ, используемые драйвером ACRUN.SYS в рамках функционирования. Параметры сохраняются в файле с расширением «amz» путем сериализации соответствующих структур данных в бинарный формат.

3) список контроля целостности программ и данных СВТ, используемый драйвером ACRUN.SYS в рамках функционирования. Список вместе с параметрами доступа пользователей сохраняется в файле с расширением «amz» путем сериализации соответствующих структур данных в бинарный формат.

6. Выходные данные

Выходными данными СПО «Аккорд-Win64 К» являются:

1)Журнал регистрации событий пользователя, сохраняемый в файле с расширением «low». Формируется путем сериализации событий в бинарный формат.

2)Журнал ошибок. Различаются следующие виды журналов:

- журнал работы утилиты acsetup, сохраняемый в файле acsetup.log;
- журнал работы утилиты Aced32, сохраняемый в файле aced32.log;
- журнал попыток логина пользователей, сохраняемый в файле acevents.log.

Все файлы имеют текстовый вид, формат которого определяется регистрируемым событием.

7. Поставка СПО «Аккорд»

СПО «Аккорд-Win64 К» (ТУ 509000-056-11443195-2013) поставляется в составе (базовая комплектация):

1) специальное ПО «Аккорд» (разграничения доступа в среде Windows) – на CD;

2) эксплуатационная документация - на CD;

3) формуляр на СПО «Аккорд» (11443195.509000.056 ФО) – 1 брошюра;

4) комплект упаковки.

8. Установка и настройка СПО «Аккорд»

Установка СПО «Аккорд» и его настройка с учетом особенностей политики информационной безопасности, принятой на объекте информатизации (ОИ), осуществляется, как правило, специалистами по защите информации организации (предприятия, фирмы и т.д.) в соответствии с требованиями эксплуатационной документации на СПО «Аккорд».

Установка СПО «Аккорд» включает:

1) установку на жесткий диск СВТ специального программного обеспечения разграничения доступа с дистрибутивных носителей и активизацию подсистемы разграничения доступа с помощью программы ACSETUP.EXE – осуществляется администратором БИ в соответствии с «Руководством по установке СПО «Аккорд-Win64 K» (11443195.509000.056 98);

2) настройку защитных механизмов СПО «Аккорд» в соответствии с правилами разграничения доступа (ПРД) к информации, принятыми в организации (на предприятии, фирме и т.д.) – осуществляется администратором БИ в соответствии «Руководством администратора» (11443195.509000.056 90);

3) реализацию организационных мер защиты, рекомендованных в эксплуатационной документации на СПО «Аккорд».

9. Техническая поддержка

В случае необходимости консультации ЗАО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 235-89-17

+7 (926) 762-17-72

или по адресам электронной почты:

help@okbsapr.ru

support@okbsapr.ru

Вопросы по эксплуатации комплекса можно также задать на форуме на нашем сайте www.accord.ru.

Наш адрес в Интернете http://www.okbsapr.ru/.