ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Утвержден
37222406.501410.071 31 - ЛУ

Модуль доверенной загрузки
«Аккорд-МКТ»

Описание применения
37222406.501410.071 31

Листов 12

Москва
2019

АННОТАЦИЯ

Настоящий документ является описанием применения на изделие «Модуль доверенной загрузки «Аккорд-МКТ» (далее по тексту – МДЗ «Аккорд-МКТ», изделие, СДЗ), и предназначен для лиц, планирующих и организующих защиту информации с его использованием.

В документе приведены основные защитные функции МДЗ «Аккорд-МКТ», его возможности, особенности настройки и применения.

Перед установкой и эксплуатацией МДЗ «Аккорд-МКТ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных средств МДЗ «Аккорд-МКТ» должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь – должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует настройку МДЗ «Аккорд-МКТ», эксплуатацию и контроль правильности его использования, осуществляет периодическое тестирование средств защиты МДЗ «Аккорд-МКТ».

Идентификатор – признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг.

Ошибки – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии МДЗ «Аккорд-МКТ».

Пояснения – в описании некоторых команд даются пояснения и рекомендации администратору БИ для использования этих команд. Пояснения выделены мелким шрифтом.

Сообщения – информация, выводимая на дисплей, которая сообщает о действиях, требуемых от пользователя, о состоянии программы и о нормально завершенных действиях.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБИ	- администратор безопасности информации
АРМ	- автоматизированное рабочее место
АС	- автоматизированная система
ЗБ	- задание по безопасности
МДЗ	- модуль доверенной загрузки
НСД	- несанкционированный доступ к информации
ОС	- операционная система
ПО	- программное обеспечение
ПС	- программные средства
РД	- руководящий документ
СДЗ	- средство доверенной загрузки
СЗИ	- средства защиты информации
СПО	- системное программное обеспечение
ТУ	- технические условия
ФПО	- функциональное программное обеспечение
ЭД	- эксплуатационная документация

1. Назначение МДЗ «Аккорд-МКТ»

Модуль доверенной загрузки «Аккорд-МКТ» является программным средством доверенной загрузки (СДЗ), предназначенным для встраивания в базовую систему ввода-вывода (БСВВ) средств вычислительной техники (СВТ), обеспечивая выполнение основных функций его защиты от НСД, в том числе настройки, контроля функционирования и управления защитными механизмами.

2. Характеристики МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» обеспечивает:

- идентификацию и аутентификацию пользователей при входе в систему по уникальному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования МДЗ «Аккорд-МКТ» по уникальному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- контроль целостности данных по спискам объектов контроля;
- администрирование, включающее:
  - регистрацию пользователей и их идентификаторов;
  - построение списков объектов для контроля целостности и указание режимов контроля;
  - работу с журналом регистрации системных событий и действий пользователей;
- возможность резервного копирования на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов;
- регистрацию и учет системных событий и действий пользователей.

3. Состав МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» является программным продуктом, предназначенным для встраивания в БСВВ СВТ и состоит из специального программного обеспечения средства доверенной загрузки «Аккорд-МКТ» (далее по тексту СПО «Аккорд-МКТ»).

4. Условия применения

СПО «Аккорд-МКТ» встраивается производителем в БСВВ СВТ на этапе изготовления и функционирует в ее составе.

МДЗ «Аккорд-МКТ» предполагает возможность эксплуатации на ЭВМ любой операционной системы, поддерживающей файловые системы: FAT16, FAT32, NTFS, Ext2, Ext3 и Ext4.

5. Описание задачи

5.1. Функции безопасности, реализованные в МДЗ «Аккорд-МКТ»

В МДЗ «Аккорд-МКТ» реализованы следующие функции безопасности:

- разграничение доступа к управлению СДЗ (ФБ1);
- управление работой СДЗ (ФБ2);
- управление параметрами СДЗ (ФБ3);
- идентификация и аутентификация (ФБ4);
- тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ (ФБ5);
- блокирование загрузки операционной системы модулем доверенной загрузки (ФБ6);
- сигнализация модуля доверенной загрузки (ФБ7);
- контроль компонентов СВТ (ФБ8);
- обеспечение безопасности после завершения работы СДЗ (ФБ9).

1.Разграничение доступа к управлению СДЗ (ФБ1).

МДЗ «Аккорд-МКТ» обеспечивает разграничения доступа к управлению СДЗ на основе ролей.

В изделии реализованы роли администратора СДЗ и пользователя.

В МДЗ «Аккорд-МКТ» администратор СДЗ это привилегированный пользователь, который определяет:

- режимы выполнения (отключения, подключения) функций безопасности;
- необходимость изменения (удаления, очищения) данных функций безопасности.

Пользователи СДЗ не обладают правами администраторов СДЗ.

2.Управление работой СДЗ (ФБ2).

МДЗ «Аккорд-МКТ» обеспечивает управление со стороны администраторов СДЗ режимами выполнения функций безопасности СДЗ.

Администратор СДЗ определяет режим выполнения (отключения, подключения, изменения) определенных функций управления:

- Разграничение доступа к управлению СДЗ;
- Управление параметрами СДЗ;
- Идентификация и аутентификация;
- Тестирование СДЗ, контроль целостности программного обеспечения и параметров;
- Блокирование загрузки операционной системы СДЗ;

– Сигнализация СДЗ.

Администратор СДЗ может управлять режимами выполнения функций безопасности СДЗ, он может отключать, подключать или изменять режим выполнения функций безопасности.

3. Управление параметрами СДЗ (ФБ3).

МДЗ «Аккорд-МКТ» обеспечивает управление параметрами СДЗ, которые влияют на выполнение функций безопасности СДЗ.

Администратор СДЗ может изменять следующие параметры: список контролируемых системных областей жесткого диска, файлов и программ пользователя, системного реестра, системный журнал СДЗ, конфигурационные и настроечные данные СДЗ.

4. Идентификация и аутентификация (ФБ4).

МДЗ «Аккорд-МКТ» обеспечивает идентификацию и аутентификацию пользователей и администраторов СДЗ.

МДЗ «Аккорд-МКТ» способен прервать процесс открытия сеанса после превышения, установленного администратором СДЗ значения (от 1 до 8), неуспешных попыток аутентификации пользователя. После прерывания процесса открытия сеанса ФБО блокируют учетные данные пользователя, с которого выполнялись попытки, на время, установленное администратором СДЗ.

Пользователи аутентифицируются прежде, чем МДЗ «Аккорд-МКТ» даст им возможность предпринимать какие-либо иные действия.

МДЗ «Аккорд-МКТ» предоставляет и применяет парольный механизм аутентификации пользователей.

Все пользователи МДЗ «Аккорд-МКТ» проходят идентификацию и аутентификацию при входе (до загрузки ОС для пользователя или до выполнения действий по управлению МДЗ «Аккорд-МКТ» для администратора) с помощью имени учетной записи и пароля. При успешной проверке идентификатора и аутентификационных данных в случае отсутствия ошибок производится загрузка ОС

5. Тестирование СДЗ, контроль целостности программного обеспечения и параметров СДЗ (ФБ5).

МДЗ «Аккорд-МКТ» обеспечивает самотестирование СДЗ, проверку целостности хранимого выполняемого кода и параметров СДЗ.

При загрузке СДЗ выполняется процедуры самотестирования:

– выполняется процедура контроля целостности, баз данных СДЗ «Аккорд-МКТ»;
– выполняется проверка целостности кода СДЗ «Аккорд-МКТ».

Если в ходе данной процедуры обнаружено нарушение целостности защищаемых файлов, то выводится соответствующее сообщение и загрузка ОС не производится.

Контроль целостности осуществляется путем мониторинга неизменности контролируемых объектов. Для этого в первую очередь определяется список контролируемых объектов. Затем для каждого из них рассчитывается эталонная

контрольная сумма. Сама проверка целостности представляет собой сравнение ранее вычисленной контрольной суммы и расчетной текущей.

Проверка целостности контролируемых объектов осуществляется автоматически после успешной авторизации в СДЗ.

6. Блокирование загрузки операционной системы модулем доверенной загрузки (ФБ6)

МДЗ «Аккорд-МКТ» обеспечивает блокирование загрузки операционной системы средством доверенной загрузки следующих случаях:

- при выявлении попыток загрузки нештатной операционной системы;
- при превышении числа неудачных попыток аутентификации пользователя;
- при нарушении целостности средства доверенной загрузки.
- при нарушении целостности загружаемой программной среды;
- при критичных типах сбоев и ошибок.

7. Сигнализация модуля доверенной загрузки (ФБ7).

МДЗ «Аккорд-МКТ» обеспечивает сигнализацию о событиях, связанных с нарушением безопасности.

Сообщения на экране возникают при задании неверных параметров пользователя, при введении неверных значений пароля, при несовпадении параметров конфигурации и несовпадении хэш-функции с эталонным значением во время проверки целостности, при превышении лимита попыток ввода пароля или идентификатора и т.п. событиях, связанных с нарушением безопасности.

8. Контроль компонентов СВТ (ФБ8).

МДЗ «Аккорд-МКТ» выполняет проверку состава компонентов аппаратного обеспечения ЭВМ при первоначальном запуске, основываясь на идентификационной информации компонентов для верификации неизменности состава аппаратного обеспечения СВТ.

МДЗ «Аккорд-МКТ» позволяет выполнять контроль целостности следующего оборудования:

- процессоры ЭВМ (подраздел CPU);
- BIOS;
- ОЗУ(подраздел MEMORY);
- жесткие диски, приводы оптических и гибких дисков, (подраздел MEDIA);
- устройства шины PCI;
- устройства USB;
- мониторы.

Списки контроля целостности аппаратуры настраивает администратор СДЗ.

Если обнаруживается несовпадение параметров конфигурации, записанных в памяти контроллера, и текущих параметров системы, выдается сообщение «Контроль не пройден» и загрузка компьютера блокируется– для

обычного пользователя; или выводится запрос на администрирование, если идентифицирован администратор.

9. Обеспечение безопасности после завершения работы СДЗ (ФБ9).

СДЗ обеспечивает недоступность информационного содержания ресурсов СВТ, использовавшихся в процессе работы СДЗ программным обеспечением и данными СДЗ, после завершения работы СДЗ путем его очистки.

Конструктивные особенности СДЗ обеспечивают недоступность ресурсов средства доверенной загрузки из программной среды СВТ после завершения работы средства доверенной загрузки.

5.2. Настройка и использование МДЗ «Аккорд-МКТ»

Настройка и использование МДЗ «Аккорд-МКТ» осуществляется, как правило, специалистами Заказчика (Потребителя) в соответствии с требованиями эксплуатационной документации.

Настройка МДЗ «Аккорд-МКТ» включает в себя:

1) Регистрацию администратора БИ (супервизора) (подробнее см. «Руководство администратора», входящее в комплект поставки МДЗ «Аккорд-МКТ» (37222406.501410.071 90)).

2) Регистрацию пользователей и настройку защитных средств МДЗ «Аккорд-МКТ»– см. «Руководство администратора» (37222406.501410.071 90).

6. Входные и выходные данные

Входными данными для МДЗ «Аккорд-МКТ» являются:

- идентификатор пользователя;
- пароль для входа в МДЗ «Аккорд-МКТ»;
- параметры подсистемы контроля целостности МДЗ «Аккорд-МКТ», реализующие защитные функции контроля целостности данных по спискам объектов контроля;
- параметры настройки системного журнала регистрации событий «Аккорд-МКТ»;
- параметры подсистемы администрирования.

Выходными данными для МДЗ «Аккорд-МКТ» являются:

- готовые списки файлов и программ пользователя, по результатам анализа которых выносится решение о прохождении процедуры контроля целостности;
- результат, выносимый подсистемой идентификации и аутентификации пользователей;
- файлы логов, формирующиеся по результатам работы системного журнала регистрации событий «Аккорд-МКТ»;
- списки пользователей МДЗ «Аккорд-МКТ» с определенными для них параметрами учетных записей, сформированные в результате работы подсистемы администрирования.

7. Поставка МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» поставляется в комплектности, соответствующей техническим условиям (ТУ 501410-071-37222406-2016).

8. Правовые аспекты применения МДЗ «Аккорд-МКТ»

МДЗ «Аккорд-МКТ» и сопутствующая документация защищены Законом России об авторских правах, а также положениями Международного Договора.

Любое использование МДЗ «Аккорд-МКТ» в нарушение Закона об авторских правах или в нарушение положений ЭД на МДЗ «Аккорд-МКТ» будет преследоваться в установленном порядке.

Авторские права на МДЗ «Аккорд-МКТ» принадлежат ОКБ САПР.

Разрешается делать архивные копии специального программного обеспечения МДЗ «Аккорд-МКТ» для использования Потребителем, который приобрел МДЗ «Аккорд-МКТ» в установленном порядке.

Ни при каких обстоятельствах поставляемое специальное программное обеспечение не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции ОКБ САПР уведомление об авторских правах не допускается ни при каких обстоятельствах.

При необходимости применения средств МДЗ «Аккорд-МКТ» для других целей решение этого вопроса возможно только при наличии письменного согласия разработчиков.

Отметим, что предыдущие ограничения не запрещают легальным пользователям распространять собственные исходные коды или модули, связанные с применением специального ПО для МДЗ «Аккорд-МКТ». Однако тот, кто получает такие исходные коды или модули, должен приобрести собственную копию нашего специального ПО, чтобы на законном основании использовать его и иметь сертификат соответствия.

Относительно СПО и документации, поставляемых в составе МДЗ «Аккорд-МКТ», ОКБ САПР гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в Формуляре.

При обнаружении ошибок или дефектов пользователь направляет подробную рекламацию в ОКБ САПР в установленном порядке. При этом обязательным является наличие корректно заполненного формуляра на МДЗ «Аккорд-МКТ».

МДЗ «Аккорд-МКТ» поставляется по принципу «as is», т.е. владельцы авторских прав ни при каких обстоятельствах не предусматривают никакой компенсации за дополнительные убытки пользователя, включая любые потери прибыли, потери сохранности или другие убытки, вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования нашей продукции.

При покупке и применении МДЗ «Аккорд-МКТ» предполагается, что покупатель знаком с данными требованиями и согласен с положениями настоящего раздела.

9. Техническая поддержка

В случае необходимости консультации АО «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) 762-17-72

или по адресу электронной почты help@okbsapr.ru.

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