ОКБ ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.509000.055 31-ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win32 К»

ОПИСАНИЕ ПРИМЕНЕНИЯ

11443195.509000.055 31

Литера $О_1$

АННОТАЦИЯ

Настоящий документ является описанием применения специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win32 K» (ТУ 509000-055-11443195-2013) (далее по тексту – СПО «Аккорд-Win32 K», «Аккорд-Win32 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 на СПО «Аккорд», 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. Общие сведения 4
2. Технические требования и организационные меры, необходимые для применения СПО «Аккорд» 5
2.1. Технические требования 5
2.2. Организационные меры 5
3. Особенности защитных функций СПО «Аккорд» 6
4. Построение системы защиты информации на основе СПО «Аккорд» 8
4.1. Подсистема управления доступом 8
4.2. Подсистема регистрации и учета 9
4.3. Подсистема контроля целостности 9
5. Принцип работы СПО «Аккорд» 11
6. Поставка СПО «Аккорд» 12
7. Установка и настройка СПО «Аккорд» 13

1. Общие сведения

Специальное программное обеспечение «Аккорд-Win32 K» (далее по тексту – СПО «Аккорд») предназначено для применения на СВТ, функционирующих под управлением ОС Microsoft Windows 8.1 Professional и ОС Microsoft Windows Server 2008 Enterprise с целью обеспечения защиты от несанкционированного доступа к СВТ и АС на их основе при многопользовательском режиме эксплуатации.

СПО «Аккорд» включает в себя специальное программное обеспечение разграничения доступа в среде операционных систем Windows – СПО «Аккорд-Win32 K».

Состав СПО «Аккорд» определяется при заказе в соответствии с требованиями Заказчика и указывается в формуляре.

2. Технические требования и организационные меры, необходимые для применения СПО «Аккорд»

2.1. Технические требования

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

- установленная на СВТ 32-битная операционная система Windows 8.1 Professional, Windows Server 2008 Enterprise;
- наличие на СВТ HDD и CD ROM для установки СПО разграничения доступа;
- объем дискового пространства для установки СПО разграничения доступа – 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.

2.2. Организационные меры[1]

Для эффективного применения СПО «Аккорд» и поддержания необходимого уровня защищенности СВТ и информационных ресурсов АС **необходимы:**

- физическая охрана СВТ и его средств;
- наличие администратора безопасности информации (супервизора) - привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку СПО «Аккорд» в СВТ, эксплуатацию и контроль за правильным использованием СВТ с внедренным СПО «Аккорд», осуществляет периодическое тестирование средств защиты СПО «Аккорд». Более подробно обязанности администратора БИ по применению СПО «Аккорд» изложены в «Руководстве администратора» (11443195.509000.055 90).

1 Более подробно приведены в «Руководстве администратора» (11443195.509000.055 90) и «Руководстве оператора» (пользователя), 11443195.509000.055 34 и других документах ЭД на СПО «Аккорд».

3. 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 11443195.509000.055 ЗБ и требованиям Технических условий ТУ 509000-055-11443195-2013.

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 файлов реестра, а также 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, 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.

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.

---

[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.

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 файлов реестра и 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.

4. 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.

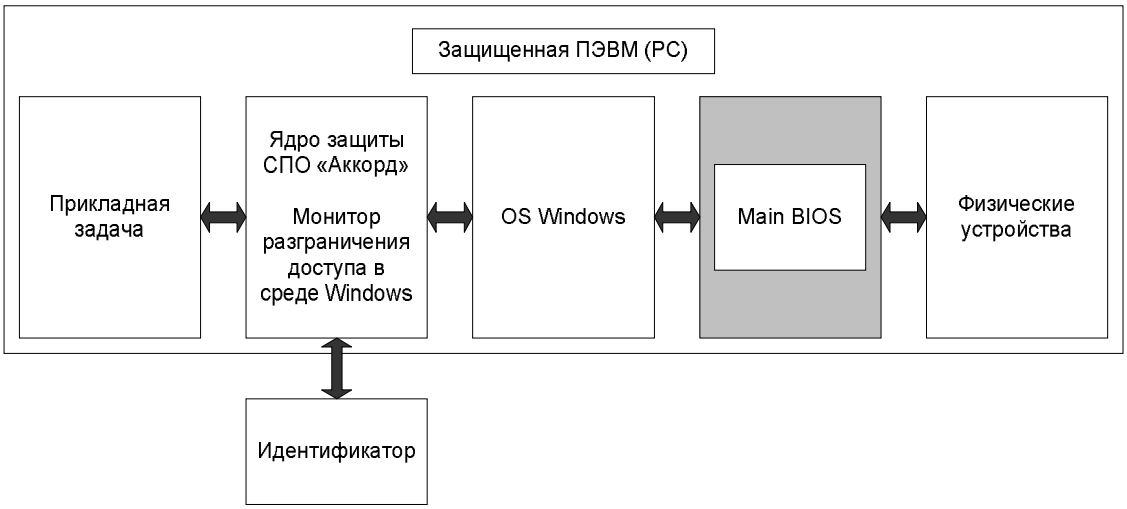

Рисунок 1 - Построение системы защиты информации с помощью СПО «Аккорд»

Защита информации с использованием средств СПО «Аккорд» основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам СВТ. Средства СПО «Аккорд» перехватывают соответствующие программные и/или аппаратные 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 его ресурсам, которые условно можно представить в виде взаимодействующих между собой подсистем защиты информации, описанных ниже.

4.1. 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 принадлежно-

[1] Под посторонними пользователями понимаются все лица, не зарегистрированные в системе.

сти 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 так же «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» (11443195.509000.055 97), входящий в состав эксплуатационной документации на СПО «Аккорд».

4.2. Подсистема регистрации и учета

Предназначена для регистрации в системном журнале событий, обрабатываемых подсистемой разграничения доступа «Аккорд-Win32 K». При регистрации событий в системном журнале указываются:

- 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» (11443195.509000.055 90).

Работа с системными журналами осуществляется с использованием программы LOGVIEW.EXE, см. документ «Подсистема регистрации. Программа работы с журналами регистрации «LogView» (11443195.509000.055 99) из комплекта эксплуатационной документации на СПО «Аккорд».

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

4.3. Подсистема контроля целостности

Предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) 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 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.

5. 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» (11443195.509000.055 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-Win32 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).

6. Поставка СПО «Аккорд»

СПО «Аккорд-Win32 К» (ТУ 509000-055-11443195-2013) 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» (11443195.509000.055 ФО) – 1 брошюра.

4) комплект упаковки.

7. 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 в себя:

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» (11443195.509000.055 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» (11443195.509000.055 90);

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

ЗАКЛЮЧЕНИЕ

ОКБ САПР предлагает «горячую линию» для консультаций по телефонам (495) 994-49-97, 8-926-762-17-72 без дополнительной оплаты. Звоните нам по телефону поддержки с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) по существу вопросов о применении СПО семейства «Аккорд»™. Вопросы по эксплуатации СПО «Аккорд» можно также прислать по электронной почте по адресу support@okbsapr.ru и 03@accord.ru или задать на форуме на нашем сайте www.accord.ru.