ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-X К»

ОПИСАНИЕ ПРИМЕНЕНИЯ
37222406.26.20.40.140.085 31

АННОТАЦИЯ

Настоящий документ является описанием применения специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-X K» (далее по тексту – СПО СЗИ НСД «Аккорд-X K», СПО «Аккорд-X K», «Аккорд-X K») и предназначен для лиц, планирующих и организующих защиту информации в автоматизированных системах на базе СВТ (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux.

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

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

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

СОДЕРЖАНИЕ

1 НОРМАТИВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

1.1 Необходимость и цели защиты информации

Развитие средств вычислительной техники, автоматизированных информационных систем, появление новых информационных технологий сопровождается, к сожалению, и появлением таких малоприятных явлений, как промышленный шпионаж, компьютерная преступность и, прежде всего, несанкционированный доступ (НСД) к конфиденциальной информации. Этим обуславливается актуальность и значимость проблемы защиты информации.

Острая необходимость в защите информации нашла выражение в создании Государственной системы защиты информации (ГСЗИ). Развивается правовая база информационной безопасности. Приняты и введены в действие законы «О государственной тайне», «Об информации, информатизации и защите информации», «О правовой охране программ для электронных вычислительных машин и баз данных» и др.

Целями защиты информации являются:

- предотвращение ущерба, возникновение которого возможно в результате утери (хищения, утраты, искажения, подделки) информации в любом ее проявлении;
- реализация мер защиты, адекватных угрозам безопасности информации, в соответствии с действующими Законами и нормативными документами по безопасности информации;
- реализация мер защиты, в соответствии с потребностями владельцев (пользователей) информации.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.[1]

Любое современное предприятие (учреждение, фирма и т.д.), независимо от вида деятельности и форм собственности, не может сегодня успешно развиваться и вести хозяйственную и иную деятельность без создания надежной системы защиты своей информации.

Система защиты информации должна включать в себя не только организационно-нормативные меры, но и технические средства контроля безопасности информации при ее обработке, хранении и передаче в автоматизированных системах (АС), прежде всего, программно-аппаратные.

1.2 Основные принципы организации защиты информации от НСД

Мероприятия по защите информации от НСД являются составной частью управленческой, научной, производственной (коммерческой)

[1] *Закон Российской Федерации «Об информации, информатизации и защите информации»*

деятельности предприятия (учреждения, фирмы и т.д.), независимо от их ведомственной принадлежности и формы собственности, и осуществляются в комплексе с другими мерами по обеспечению установленного режима конфиденциальности. Практика организации защиты информации от НСД при ее обработке и хранении в автоматизированных системах (АС) должна учитывать следующие принципы и правила обеспечения безопасности информации:[2]

1) соответствие уровня безопасности информации законодательным положениям и нормативным требованиям по охране сведений, подлежащих защите по действующему законодательству, в т.ч. выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;
2) выявление конфиденциальной информации и документальное оформление в виде перечня сведений, подлежащих защите, его своевременная корректировка;
3) наиболее важные решения по защите информации должны приниматься руководством предприятия (организации, фирмы), владельцем АС;
4) определение уровней полномочий субъектов доступа, а также круга лиц, которым предоставлено право присвоения уровней полномочий;
5) установление и оформление правил разграничения доступа (ПРД), т.е. совокупности правил, регламентирующих права доступа субъектов доступа к объектам доступа;
6) установление личной ответственности пользователей за поддержание уровня защищенности АС при обработке сведений, подлежащих защите по действующему законодательству путем:
   - ознакомления с перечнем защищаемых сведений, организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;
   - определения уровня полномочий в соответствии с его должностными обязанностями;
   - получения от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;
7) обеспечение физической охраны объекта, на котором расположена защищаемая АС (территория, здание, помещение, хранилище информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

---

[2] *РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. -М.: Гостехкомиссия России, 1992.*

8) организация службы безопасности информации (ответственные лица, администраторы), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

9) планомерный и оперативный контроль уровня безопасности защищаемой информации, в т.ч. проверка защитных функций средств защиты информации.

Средства защиты информации должны иметь СЕРТИФИКАТ, удостоверяющий их соответствие требованиям по безопасности информации в соответствии с действующими Законами и нормативными документами по безопасности информации.

2 ОБЩИЕ СВЕДЕНИЯ

СПО «Аккорд-X K» представляет собой программное средство, предназначенное для применения в СВТ типа IBM PC (автономных ПК, рабочих станциях ЛВС, терминальных серверах), функционирующих под управлением ОС семейства Linux, с целью обеспечения защиты от несанкционированного доступа к информации при многопользовательском режиме эксплуатации.

СПО «Аккорд-X K» поддерживает работу под управлением следующих ОС Linux:

- CentOS 7;
- CentOS 8;
- Альт 9;
- Альт 10;
- Astra Linux Special Edition;
- Astra Linux Common Edition;
- Debian 7;
- Debian 10;
- Fedora 20;
- Fedora 24;
- OpenSUSE 12;
- OpenSUSE leap 42;
- Red Hat Enterprise Linux Server 6;
- Red Hat Enterprise Linux Server 7;
- Red Hat Enterprise Linux Server 8;
- Ubuntu 18;
- Р-Виртуализация Linux 7.5;
- РЕД ОС 7.1;
- РЕД ОС 7.2;
- РЕД ОС 7.3;
- TeNIX WS.

«Аккорд-X K» на логическом уровне состоит из следующих модулей:

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

В ядро защиты СПО «Аккорд-X K» входят:

- монитор разграничения доступа, выполняющий непосредственно функции защиты информации от НСД – МРД (модуль ядра Linux acx-core.ko);

- подключаемые программные модули аутентификации (PAM), взаимодействующие с монитором разграничения доступа для идентификации/аутентификации субъектов доступа, – подсистема идентификации и аутентификации (PAM-модуль pam_acx_local.so);
- утилиты, реализующие передачу файла конфигурации и базы данных пользователей в программный монитор разграничения доступа;
- утилита реализации статического контроля целостности объектов ОС (acx-integrity-controller).

Данные модули выполняют основные функции по защите информации от несанкционированного доступа.

Модули, не входящие в состав ядра защиты, либо являются вспомогательными и обеспечивают функционирование ядра защиты (например, предотвращают формирование БД неправильного формата), либо представляют собой утилиты для удобной настройки и администрирования СПО «Аккорд-Х К». В частности, к средствам администрирования СПО «Аккорд-Х К» относятся следующие программы:

- утилиты настройки СПО «Аккорд-Х К» acx-admin;
- утилиты установки ПРД пользователей acx-admin user, acx-admin group, acx-admin shadow, acx-admin acl;
- утилиты установки ПРД процессов acx-admin group, acx-admin acl;
- утилита работы с журналами регистрации событий acx-admin log.

Указанные средства не входят в ядро защиты СПО «Аккорд-Х К» и сами не осуществляют никаких защитных механизмов. Строго говоря, реализация всех указанных функций защиты может осуществляться и без этих средств.

3 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОРГАНИЗАЦИОННЫЕ МЕРЫ, НЕОБХОДИМЫЕ ДЛЯ ПРИМЕНЕНИЯ СПО «АККОРД-X K»

3.1 Технические требования

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

1) IBM PC AT, совместимая с процессором и объемом RAM, обеспечивающим применение операционных систем Linux;
2) объем пространства для установки СПО – не менее 128 Мб.

3.2 Организационные меры

Для эффективного применения СПО «Аккорд-X K» и поддержания необходимого уровня защищенности СВТ (РС) и информационных ресурсов АС **необходимо:**

- наличие администратора безопасности информации (супервизора; далее по тексту – Администратор БИ) – 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-X K» в СВТ, эксплуатацию и контроль правильности использования СВТ с внедренным СПО «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты СПО «Аккорд-X K». Более подробно обязанности администратора БИ по применению СПО «Аккорд-X K» изложены в «Руководстве администратора» (37222406.26.20.40.140.085 90);
- использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации.

4 ОСОБЕННОСТИ ЗАЩИТНЫХ ФУНКЦИЙ СПО «АККОРД-X K»

«Аккорд-X K» соответствует требованиям по 4 уровню доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий[3], 5 классу защищенности к средствам вычислительной техники[4] и технических условий (ТУ 26.20.40.140-085-37222406-2020).

Обеспечивается возможность использования «Аккорд-X K» для защиты информации в АС до класса защищенности 1Г[5] включительно.

Обеспечивается возможность использования «Аккорд-X K» для реализации мер защиты информации в государственных информационных системах до 1 класса защищенности включительно[6].

Обеспечивается возможность использования «Аккорд-X K» для реализации мер по обеспечению безопасности персональных данных до 1 уровня защищенности включительно[7].

Обеспечивается возможность использования «Аккорд-X K» для безопасности значимых объектов критической информационной инфраструктуры Российской Федерации до 1 категории значимости включительно[8].

Обеспечивается защита информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах,

---

[3] В соответствии с требованиями документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденным приказом ФСТЭК России от 2 июня 2020 г №76.

[4] В соответствии с требованиями руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

[5] В соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Классификация автоматизированных систем и требования по защите информации», утвержденного решением председателя Гостехкомиссии России от 30 марта 1992 года.

[6] В соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными Приказом № 17 ФСТЭК России от 11 февраля 2013 г.

[7] В соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденными Приказом № 21 ФСТЭК России от 18 февраля 2013 г.

[8] В соответствии с «Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденными Приказом № 239 ФСТЭК России от 25 декабря 2017 г.

представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности[9].

СПО «Аккорд-X K» обеспечивает реализацию следующих функций безопасности (ФБ):

- управление работой изделием (ФБ1);
- аудит безопасности (ФБ2);
- идентификация и аутентификация (ФБ3);
- управление доступом пользователей (ФБ4);
- контроль целостности компонентов СВТ (ФБ5);
- защита остаточной информации (ФБ6).

Защитные функции СПО «Аккорд-X K» реализуются применением:

1) Дисциплины защиты от НСД СВТ (РС), включая:
   - идентификацию пользователя по уникальному идентификатору;
   - аутентификацию с учетом необходимой длины пароля и времени его жизни;
   - ограничение времени доступа субъекта к СВТ (АС) в соответствии с установленным режимом работы пользователей;
2) Дисциплины разграничения доступа к ресурсам СВТ (АС) в соответствии с установленными ПРД и определяемыми атрибутами доступа, которые устанавливаются администратором безопасности информации (Администратором БИ) соответственно каждой паре «субъект доступа - объект доступа» при регистрации пользователей. СПО «Аккорд-X K» позволяет Администратору БИ использовать как дискреционный метод, так и метод разграничения доступа на основе иерархических меток, и обеспечивает управление потоками информации, исключая возможность ее несанкционированного переноса из объектов с меньшим уровнем конфиденциальности в объекты с большим уровнем;
3) Дисциплины управления процедурами ввода/вывода на отчуждаемые носители информации. Подсистема контроля вывода на печать осуществляет маркировку печатных документов и запрещает вывод на незарегистрированные печатающие устройства;
4) Контроля целостности критичных с точки зрения информационной безопасности программ и данных (дисциплины защиты от несанкционированных модификаций). В программной части СЗИ НСД 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

[9] В соответствии с «Требованиями к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» в редакции приказа ФСТЭК России от 14 марта 2014 г. N 31.

сеанса), так и динамический список, проверка по которому выполняется перед каждой загрузкой контролируемого файла в оперативную память;

5) Средств создания изолированной программной среды, исключающей внедрение в систему вредоносных или неразрешенных Администратором БИ программ;
6) Механизма очистки внешней памяти;
7) Механизма контроля печати, который позволяет контролировать процессы, документы, принтеры и автоматически маркировать распечатываемые листы специальными пометками, грифами и т.д.;
8) Регистрации действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

СПО «Аккорд-Х К» может применяться в произвольной и функционально замкнутой программной среде, обеспечивая при этом:

- защиту от несанкционированного доступа к СВТ (АС) и их ресурсам;
- разграничение доступа к ресурсам СВТ (АС), в т.ч. к внешним устройствам, в соответствии с уровнем полномочий пользователей;
- защиту от несанкционированных модификаций программ и данных, внедрения разрушающих программных воздействий (РПВ);
- защиту от несанкционированного изменения конфигурации программных средств СВТ (РС);
- регистрацию действий пользователей в системном журнале, доступ к которому предоставляется только Администратору БИ.

В СПО «Аккорд-Х К» используются и некоторые дополнительные механизмы защиты от НСД к СВТ (АС). Так, в частности, для пользователя Администратор БИ может установить:

- время жизни пароля и его минимальную длину, практически исключив тем самым возможность быстрого его подбора;
- временные ограничения использования СВТ для пользователей путем определения и установки интервала времени по дням недели (с дискретностью 30 мин), в котором разрешена работа для данного пользователя;
- подачу соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к СВТ (в АС) и к их ресурсам.

5 ПОСТРОЕНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ СПО «АККОРД-X K»

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

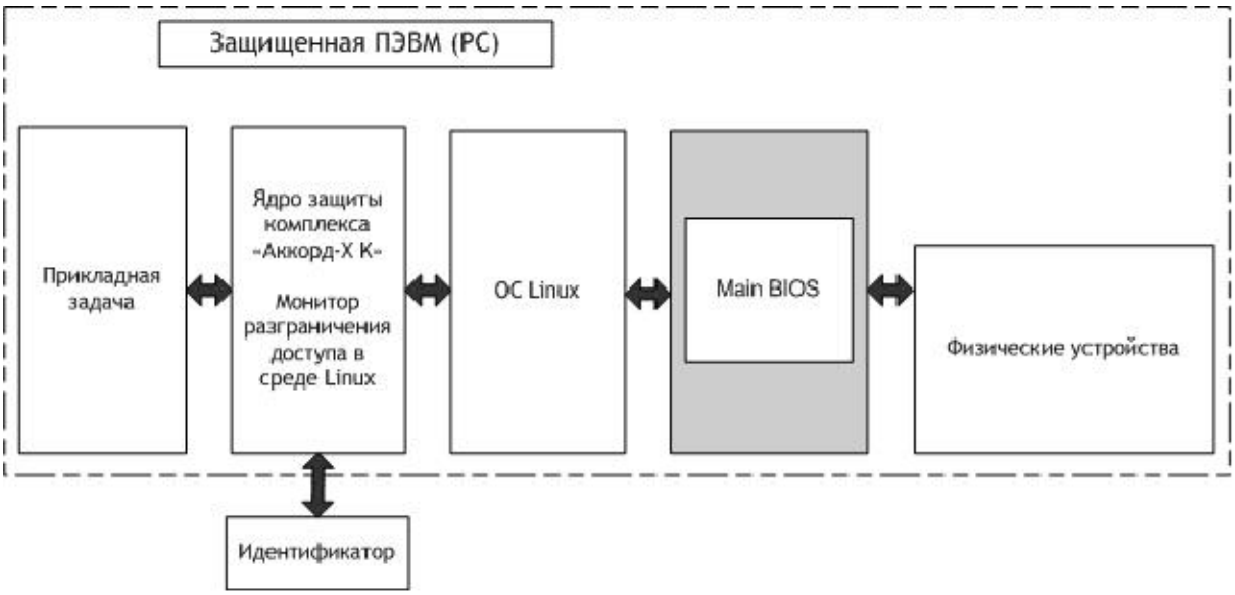

Рисунок 1. Схема построения системы защиты информации

Защита информации с использованием средств «Аккорд-X K» основана на обработке событий, возникающих при обращении прикладных программ или системного ПО к ресурсам СВТ. Средства СПО «Аккорд-X K» 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-X K» состоит из собственно средств защиты СВТ от НСД и средств разграничения доступа к ее ресурсам, которые условно можно представить в виде четырех взаимодействующих между собой подсистем защиты информации (рисунок 2).

Рисунок 2. Состав СПО «Аккорд-X K»

5.1 Подсистема управления доступом

Подсистема управления доступом включает в себя подсистему идентификации/аутентификации, предназначенную для защиты СВТ от посторонних[10] пользователей, и подсистему разграничения доступа – для управления доступом к объектам доступа и организации их совместного использования зарегистрированными пользователями в соответствии с установленными правилами разграничения доступа (ПРД).

Защита от посторонних пользователей обеспечивается процедурами идентификации (сравнение предъявленного идентификатора с перечнем зарегистрированных на СВТ) и аутентификации (подтверждение подлинности) с защитой от раскрытия пароля. Для идентификации пользователей используются персональные идентификаторы.

В СПО «Аккорд-X K» реализованы принципы дискреционного управления доступом и управления на основе иерархических меток.

При использовании дискреционного управления доступом 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 управления доступом на основе иерархических меток пользователю (субъекту) устанавливается уровень доступа, а объекту (файлу, папке, сетевому ресурсу, съемному диску) присваивается метка

[10] *Под посторонними пользователями понимаются все лица, не зарегистрированные в системе (не имеющие зарегистрированного в конкретном СВТ (РС) идентификатора).*

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-X K» осуществляется Администратором БИ с использованием утилиты acx-admin (см. документ «Руководство администратора» (37222406.26.20.40.140.085 90), входящий в состав эксплуатационной документации на СПО «Аккорд-X K»).

5.2 Подсистема регистрации и учета

Подсистема регистрации и учета предназначена для регистрации в системном журнале событий, обрабатываемых подсистемой разграничения доступа «Аккорд-X 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 документе «Руководство администратора» (37222406.26.20.40.140.085 90).

Работа с системными журналами осуществляется с использованием утилиты acx-admin log (см. документ «Руководство администратора» (37222406.26.20.40.140.085 90), входящий в состав эксплуатационной документации на СПО «Аккорд-X K»).

В Н И М А Н И Е !
Доступ к системному журналу возможен только Администратору БИ

5.3 Подсистема обеспечения целостности

Подсистема обеспечения целостности предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) конфигурации технических средств СВТ, программной среды, обрабатываемой информации, обеспечивая при этом защиту СВТ от внедрения программных закладок и вирусов.

Контроль целостности в СПО «Аккорд-X K» реализуется путем:

- проверки целостности конфигурации технических средств СВТ перед каждым сеансом работы пользователя;
- проверки целостности назначенных для контроля системных файлов, пользовательских программ и данных;
- создания замкнутой программной среды, запрещающей запуск измененных программ.

Функционирование подсистемы обеспечения целостности 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 необнаружения модификации файла используется алгоритм расчета контрольных сумм - вычисление значения их хэш-функций;
- при контроле целостности индивидуального списка файлов пользователя результирующая хэш-функция хранится на жестком диске, но в алгоритме расчета используется секретный ключ пользователя, записанный в идентификаторе;
- секретный ключ пользователя формируется из последовательности случайных чисел и записывается в идентификатор пользователя при регистрации. Этот секретный ключ используется при выработке КС и исключает возможность несанкционированной модификации файлов из индивидуального списка контролируемых файлов.

6 ПРИНЦИП РАБОТЫ СПО «АККОРД-Х К»

Специальный загрузочный носитель «МАРШ!» с СПО «Аккорд-Х К» в первоначально сконфигурированном виде (для варианта поставки на СЗН «МАРШ!-2.0») устанавливается в свободный USB-порт на СВТ (РС) (для вариантов поставки на CD-диске и/или USB-флеш установка носителя «МАРШ!» не производится). После установки носителя «МАРШ!» Администратор БИ должен корректным образом настроить программную часть СПО Аккорд-Х К (см. «Руководство администратора» на СПО Аккорд-Х К 37222406.26.20.40.140.085 90). Активизация монитора разграничения доступа, регистрация пользователей и установка правил разграничения доступа 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 механизма разграничения на основе иерархических меток (см. документ «Руководство администратора» 37222406.26.20.40.140.085 90).

С помощью утилиты acx-admin в специальный файл данных вносятся списки файлов, целостность которых будет проверяться при запуске СВТ (РС) данным пользователем. После регистрации пользователю выдается персональный идентификатор, о чем делается запись в журнале учета носителей информации.

Особенностью и, несомненно, преимуществом СПО «Аккорд-Х К» является проведение процедур идентификации, аутентификации и контроля целостности (программных компонентов, файлов).

После предъявления идентификатора выполняется процедура аутентификации (ввод пароля) пользователя. Для проведения процедуры аутентификации пароль вводится в виде символов <*>. Этим предотвращается возможность раскрытия индивидуального пароля и использования утраченного (похищенного) идентификатора.

С данными, полученными в результате идентификации/аутентификации пользователей, выполняется процедура хэширования. Таким образом, пароль пользователя не хранится в открытом виде.

Далее выполняется поиск свертки идентификационных параметров пользователя в базе данных СПО «Аккорд-Х К». Если предъявлен зарегистрированный идентификатор, и пароль введен правильно, то выполняется контроль целостности защищаемых объектов.

При положительном результате контрольных процедур пользователю становится доступной процедура входа в ОС. Если предъявленный пользователем идентификатор не зарегистрирован в списке (сообщения «Недопустимый идентификатор», «Ошибка чтения идентификатора»), или нарушена целостность защищаемых объектов (сообщение «Нарушение целостности»), пользователь не сможет выполнить вход в ОС. Для продолжения работы потребуется вмешательство Администратора БИ.

Монитор разграничения доступа предназначен для разграничения доступа к ресурсам СВТ (АС) в соответствии с правилами разграничения доступа, назначенными Администратором БИ.

Каждому пользователю или группе пользователей Администратор БИ может назначить индивидуальный список файлов, которые будут контролироваться на целостность при входе данного пользователя в систему.

Механизм контроля целостности реализуется процедурой сравнения двух векторов для одного массива данных: эталонного (контрольного), выработанного заранее на этапе регистрации пользователей, и текущего, выработанного непосредственно перед проверкой.

Эталонный (контрольный) вектор вырабатывается на основе хэш-функций (контрольной суммы) защищаемых файлов и секретного ключа пользователя, который хранится в идентификаторе.

Важной составляющей безопасности при работе операционной системы является динамический контроль целостности процессов (задач) в оперативной памяти СВТ (РС). Администратор БИ может задать список процессов для динамического контроля, и в процессе функционирования СПО «Аккорд-Х К» резидентная часть монитора разграничения доступа проверяет загружаемый процесс и обеспечивает оперативный контроль целостности исполняемых файлов перед передачей им управления. Тем самым обеспечивается защита от программных вирусов и закладок. В случае положительного исхода проверки управление передается операционной системе, и процесс запускается на исполнение. При отрицательном исходе проверки загрузка и запуск задачи не происходит.

Монитор разграничения доступа ограничивает доступ пользователя к ресурсам, расположенным как на локальных, так и на сетевых и сменных дисках, в соответствии с едиными правилами разграничения доступа.

7 ПОСТАВКА СПО «АККОРД-Х К»

СПО «Аккорд-Х К» поставляется в составе:

1) специальное программное обеспечение «Аккорд-Х К» – на одном из следующих видов носителей по выбору Заказчика:
   - CD-диск;
   - USB-флеш;
   - специальный загрузочный носитель «МАРШ!-2.0»;
2) эксплуатационная документация – на оптическом носителе;
3) формуляр на СПО «Аккорд-Х К» (37222406.26.20.40.140.085 ФО) – 1 брошюра;
4) комплект упаковки.

8 УСТАНОВКА И НАСТРОЙКА СПО «АККОРД-X K»

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

Установка и настройка СПО «Аккорд-X K» осуществляется Администратором БИ в соответствии с документом «Руководство администратора» (37222406.26.20.40.140.085 90) и включает в себя несколько этапов (подробнее см. таблицу 1).

Таблица 1 - Установка и настройка СПО «Аккорд-X K»

№	Описание процедуры	СПО «Аккорд-X K» в варианте поставки на СЗН «МАРШ!-2.0»	СПО «Аккорд-X K» в вариантах поставки на CD-диске и/или USB-флеш
1.	Установка в СВТ (РС), в том числе настройка загрузки ОС с USB-носителя «МАРШ!»	+	-
2.	Настройка СПО «Аккорд-X K» с учетом конфигурации технических и программных средств СВТ (РС), в том числе:	-	+
2.1.	- регистрация Администратора БИ (или нескольких администраторов) и пользователей	-	+
2.2.	- редактирование параметров учетных записей Администратора БИ и пользователей	+	-
3.	Установка на жесткий диск СВТ (РС) СПО «Аккорд-X K» и активизация подсистемы разграничения доступа	-	+
4.	Настройка защитных механизмов СПО «Аккорд-X K» в соответствии с правилами разграничения доступа к информации.	+	+
5.	Реализация организационных мер защиты, рекомендованных в эксплуатационной документации на СПО «Аккорд-X K»	+	+

Обозначения в таблице:

«+» – процедура выполняется для данного варианта поставки СПО «Аккорд-X K»;

«-» – процедура не выполняется для данного варианта поставки СПО «Аккорд-X K».

9 УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ

Созданная структура защиты информации при применении СПО «Аккорд-X K» должна поддерживаться механизмом установления полномочий пользователей СВТ (АС) и управлением их доступом к информационным ресурсам защищаемой АС.

Для этого на предприятии (учреждении, фирме и т.д.) должна создаваться служба безопасности информации или назначаться ответственное лицо (Администратор БИ), на которых возлагается разработка и ввод в действие организационно-нормативных документов по применению СВТ (АС) с внедренными средствами защиты СПО «Аккорд-X K». Этими документами должно предусматриваться ведение ряда учетных и объектовых документов.

Перечень организационных мер, необходимых для обеспечения СПО «Аккорд-X K» требуемого уровня защиты информации, а также функции и обязанности Администратора БИ и пользователей приведены в документах «Руководство администратора» (37222406.26.20.40.140.085 90) и «Руководство оператора (пользователя)» (37222406.26.20.40.140.085 34).

10 ПРАВОВЫЕ АСПЕКТЫ ПРИМЕНЕНИЯ СПО «АККОРД-Х К»

Специальное программное обеспечение «Аккорд-Х К» и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование СПО «Аккорд-Х К» в нарушение закона об авторских правах или в нарушение положений эксплуатационной документации на СПО «Аккорд-Х К» будет преследоваться предприятием-изготовителем в силу его возможностей.

Предприятие-изготовитель разрешает делать архивные копии программного обеспечения «Аккорд-Х К» для использования потребителем, который приобрел СПО «Аккорд-Х К» в установленном порядке.

Ни при каких обстоятельствах программное обеспечение «Аккорд-Х К» не должно распространяться между другими предприятиями (фирмами) и лицами. Удалять в СПО «Аккорд-Х К» уведомление об авторских правах ни при каких обстоятельствах не допускается.

При необходимости применения СПО «Аккорд-Х К» для других целей, решение этого вопроса возможно только при наличии письменного согласия ОКБ САПР.

Отметим, что ограничения не запрещают Вам распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения «Аккорд-Х К». Однако, тот, кто получает от Вас такие исходные коды или модули, должен приобрести собственную копию нашего программного обеспечения, чтобы на законном основании использовать его и иметь сертификат соответствия.

Относительно физических экземпляров аппаратуры и документации, поставляемых в составе СПО «Аккорд-Х К», предприятие-изготовитель гарантирует их исправность в соответствии с гарантийными обязательствами, указанными в документе «Формуляр» (37222406.26.20.40.140.085 ФО).

При обнаружении ошибок или дефектов пользователь СПО «Аккорд-Х К» должен направить в адрес предприятия-изготовителя подробный отчет о возникших проблемах, который позволит найти и зафиксировать проблему.

СПО «Аккорд-Х К» поставляется по принципу «as is», т.е. предприятие-изготовитель ни при каких обстоятельствах не предусматривает никакой компенсации за Ваши дополнительные убытки, 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 СПО «Аккорд-Х К».

При покупке и применении СПО «Аккорд-Х К» предполагается, что Вы знакомы с данными требованиями и согласны с положениями настоящего раздела.

При покупке и применении Комплекса предполагается, что Вы знакомы с данными требованиями и согласны с положениями настоящего раздела.

11 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/.