Программно-аппаратные средства обеспечения информационной безопасности

Лекция № 6

Современные программно-аппаратные средства обеспечения информационной безопасности. Часть 1

Рахманенко И.А.

План

- ПАК “Соболь”
- Установка комплекса “Соболь”
- СЗИ НСД Аккорд АМДЗ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «СОБОЛЬ» ВЕРСИЯ 3.0

Что такое ПАК «Соболь»?

- **ПАК «Соболь»** – это программно-аппаратное средство защиты информации от несанкционированного доступа, выполняющее роль аппаратно-программного модуля доверенной загрузки (АПМДЗ).

Для чего предназначен ПАК «Соболь»?

- защиты конфиденциальной информации, персональных данных, гос. тайны (гриф «Совершенно Секретно»).
- предотвращения доступа неавторизованных пользователей к информации, обрабатываемой на компьютере.
- информирования администратора комплекса о всех важных событиях ИБ.
- предоставления случайных чисел прикладному ПО.

Применение

- Применятся для защиты автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети (ЛВС).

Применение

ПАК «Соболь»

Обеспечивает защиту:


Серверов


Рабочих станций


Моноблоков


Ноутбуков


Тонких клиентов

Поддерживает операционные системы:

Семейство ОС Windows:

- Windows 8/8.1;
- Windows 7/7 x64 Edition;
- Windows Vista/Vista x64 Edition;
- Windows XP Professional/XP Professional x64 Edition;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2;
- Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/ Server 2003 R2 x64 Edition.

Windows

Семейство ОС Linux/Unix:

- МСВС 3.0 x86;
- Альт Линукс СПТ 6.0.0 x86/x64;
- Astra Linux Special Edition "Смоленск" 1.3 x64;
- Astra Linux Common Edition "Орел" 1.9 x64;
- CentOS 6.2 x64, 6.5 x86/x64;
- Debian 6.0.3/7.6 x86/x64;
- Mandriva ROSA Desktop 2011.0 x86/x64;
- Red Hat Enterprise Linux 6.0 x86/x64, 7.0 x64;
- Ubuntu 14.04 LTS Desktop/Server x86/x64;
- VMware vSphere ESXi 5.1 Update 1/5.1 Update 2/5.5 x64.

alt linux

redhat

debian

Сертификаты ПАК «Соболь»

- Сертификат ФСТЭК №1967
- Подтверждает соответствие требованиям руководящих документов к средствам доверенной загрузки уровня платы расширения второго класса и возможность использования в автоматизированных системах до класса защищенности **1Б** включительно, **государственных** информационных системах **до 1 класса защищённости** включительно, а так же при создании **ИСПДн до 1 уровня защищённости** включительно.

Сертификаты ПАК «Соболь»

- Сертификат ФСБ №СФ/527-2623
- Подтверждает соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ **класса 1Б** и возможность использования для защиты информации содержащей сведения, составляющие **государственную тайну**.

Возможности ПАК «Соболь»

- Идентификация и аутентификация пользователей
- Блокировка загрузки ОС со съемных носителей
- Регистрация попыток доступа к ПЭВМ
- Контроль целостности системного реестра Windows
- Контроль целостности программной среды
- Контроль конфигурации

Идентификация и аутентификация пользователей

- В качестве персональных идентификаторов пользователей могут применяться: iButton
  - eToken PRO и eToken PRO (Java)
  - Rutoken
  - iKey 2032
  - Смарт-карты eToken PRO

Блокировка загрузки ОС со съемных носителей

- После успешной загрузки штатной копии ОС доступ к этим устройствам восстанавливается.
- Запрет распространяется на всех пользователей компьютера, за исключением администратора.

Сторожевой таймер

- Механизм сторожевого таймера обеспечивает блокировку доступа к компьютеру при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано комплексу «Соболь»

Регистрация попыток доступа к ПЭВМ

Электронный замок «Соболь» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти:

1. факт входа пользователя и имя пользователя;
2. предъявление незарегистрированного идентификатора;
3. ввод неправильного пароля;
4. превышение числа попыток входа в систему;
5. дата и время регистрация событий НСД.

Контроль целостности системного реестра Windows

- Данная возможность позволяет контролировать неизменность системного реестра Windows, что существенно повышает защищённость рабочих станций от несанкционированных действий внутри операционной системы

Контроль целостности программной среды

- Используемый в комплексе "Соболь" механизм контроля целостности позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки операционной системы, а также файловых систем: NTFS, FAT 32, FAT 16, UFS, UFS2, EXT3, EXT2, EXT4 в ОС семейства Linux и MS Windows

Контроль конфигурации

- Возможность контролировать неизменность конфигурации компьютера – PCI-устройств, ACPI, SMBIOS и оперативной памяти.


Сторожевой таймер
Идентификация и аутентификация пользователей
Регистрация событий безопасности системы
Блокировка загрузки ОС со съемных носителей
Контроль целостности файлов и секторов жесткого диска
Контроль целостности реестра Windows
Контроль целостности аппаратной среды
Аппаратный ДСЧ

Поддержка ОС Windows

- Windows 8/8.1;
- Windows 7/7 x64 Edition;
- Windows Vista/Vista x64 Edition;
- Windows XP Professional/XP Professional x64 Edition;
- Windows Server 2012/Server 2012 R2;
- Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2;
- Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/Server 2003 R2 x64 Edition.

Поддержка ОС Linux

- FreeBSD 6.2/6.3/7.2/8.2
- МСВС 3.0 x86;
- Альт Линукс СПТ 6.0.0 x86/x64;
- Astra Linux Special Edition "Смоленск" 1.3 x64;
- Astra Linux Common Edition "Орел" 1.9 x64;
- CentOS 6.2 x64, 6.5 x86/x64;
- Debian 6.0.3/7.6 x86/x64;
- Mandriva ROSA Desktop 2011.0 x86/x64;
- Red Hat Enterprise Linux 6.0 x86/x64, 7.0 x64;
- Ubuntu 14.04 LTS Desktop/Server x86/x64;
- VMware vSphere ESXi 5.1 Update 1/5.1 Update 2/5.5 x64

Достоинства ПАК «Соболь»

- Наличие сертификатов ФСБ и ФСТЭК России.
- Защита информации, составляющей государственную тайну.
- Предоставление ресурсов в построении прикладных криптографических приложений.
- Простота в установке, настройке и эксплуатации.
- Поддержка 64-битных ОС Windows (в том числе Windows 8.1 и Windows server 2012 R2) и Linux.

Достоинства ПАК «Соболь»

- Поддержка различных типов идентификаторов.
- Гибкий выбор форматов исполнения платы (PCI, PCI-E, Mini PCI-E, Mini PCI-E Half) и вариантов комплектации.
- Возможность программной инициализации комплекса.
- Поддержка файловой системы EXT 4 в ОС семейства Linux.
- Интеграция с другими продуктами «Кода Безопасности».
- Физический датчик случайных чисел.

Модельный ряд

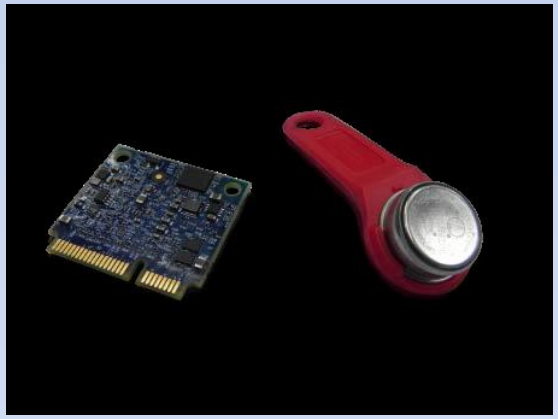
Габариты: 50 мм x 120 мм
Интерфейс: PCI (3,3 В, 5 В)

Габариты: 65 мм x 140 мм
Интерфейс: PCI Express (версия 1.0a и выше)

Модельный ряд

Габариты: 50 мм x 30 мм

Интерфейс: Mini PCI Express



Габариты: 26 мм x 30 мм

Интерфейс: Mini PCI Express

Формат платы: Mini PCI Express Half

Модельный ряд

- **Устройство блокировки питания для реализации функции сторожевого таймера.**
- **Одобрено ФСБ России**

Модельный ряд

- **Внутренний считыватель**

УСТАНОВКА КОМПЛЕКСА “СОБОЛЬ”

Установка комплекса “Соболь”

- установка программного обеспечения комплекса;
- инициализация комплекса;
- перевод комплекса в режим эксплуатации.

Установка программного обеспечения комплекса

- Программное обеспечение комплекса "Соболь" (программа управления шаблонами КЦ, утилита CreateFiles) рекомендуется устанавливать до установки в компьютер платы комплекса.

Инициализация комплекса

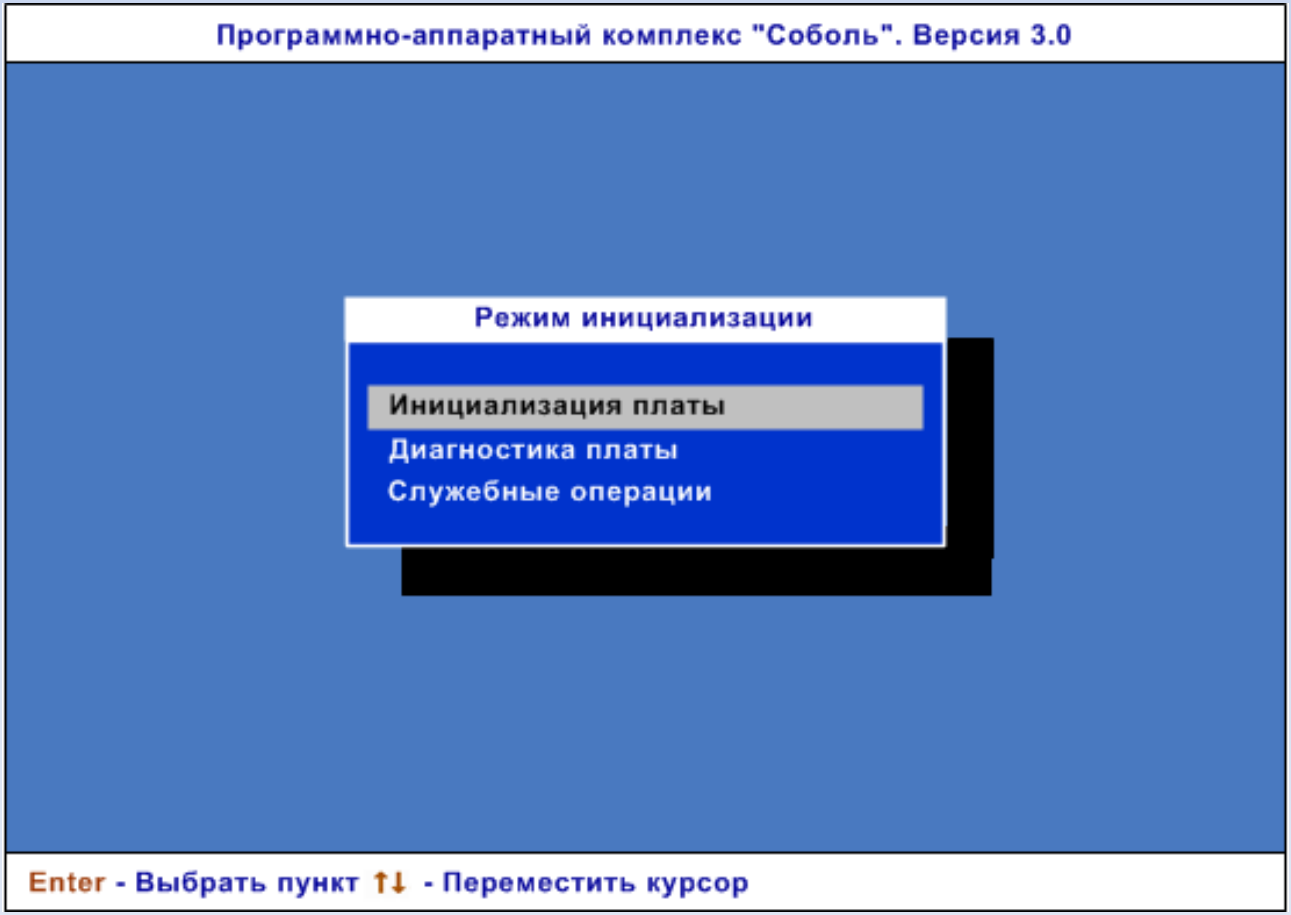
- установка платы комплекса;
- настройка общих параметров;
- настройка контроля целостности;
- настройка параметров журнала ПАК "Соболь";
- регистрация администратора комплекса;
- расчет контрольных сумм.

Установка платы комплекса

- Подключить кабели механизма сторожевого таймера
- Подключить разъемы питания
- Установить в свободный слот PCI-E/PCI
- Подключить считыватель iButton

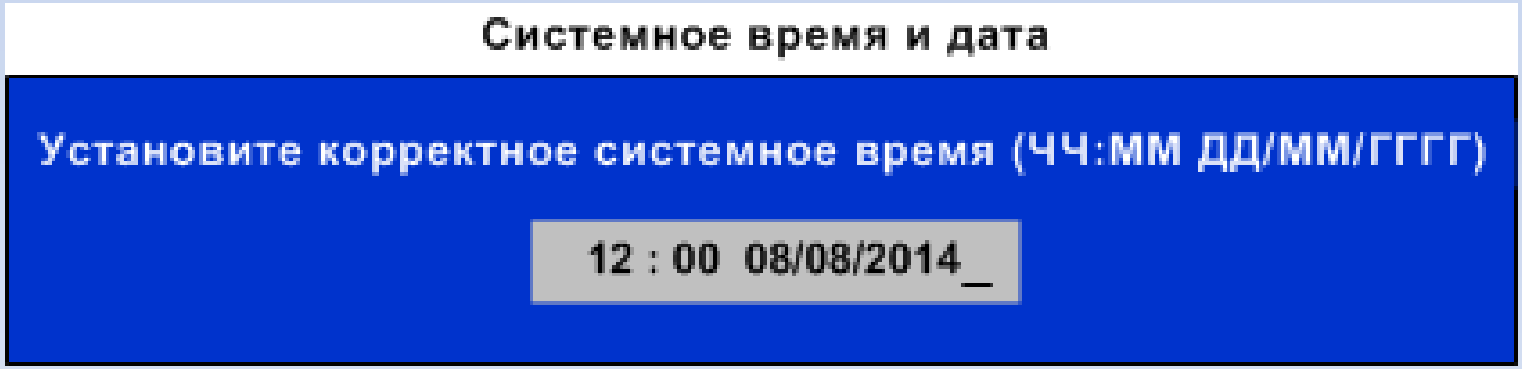
Настройка общих параметров

- После включения питания

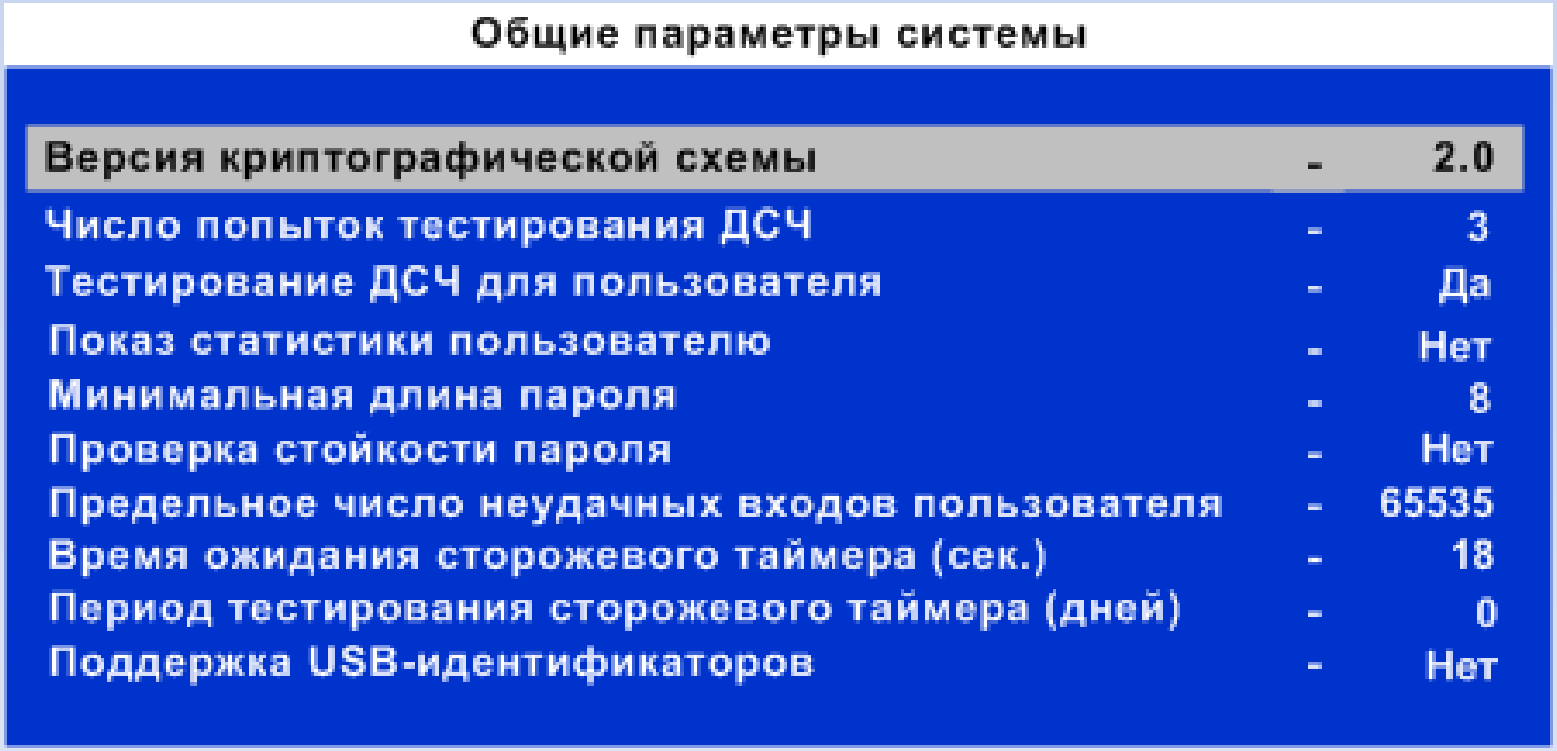


Настройка общих параметров

- Настройка системного времени



Настройка общих параметров



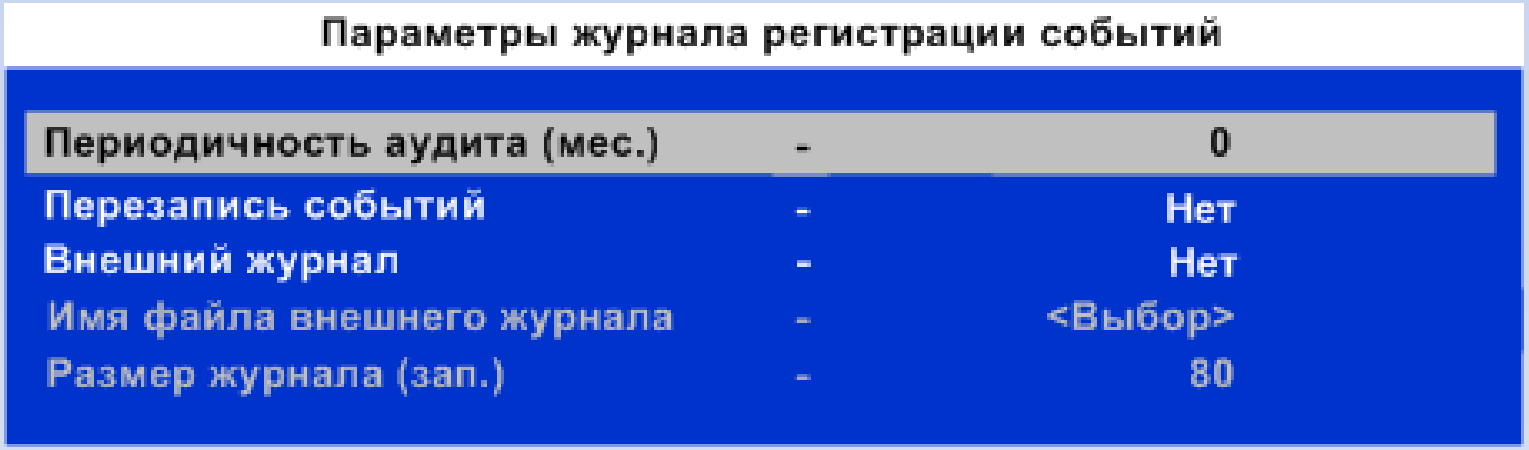
Поддержка USB-идентификаторов

- "Нет" — если вход в систему осуществляется только с помощью iButton.
- "2.0" — если вход в систему осуществляется с помощью идентификаторов iButton и USB-идентификаторов любого типа, поддерживаемых ПАК "Соболь".

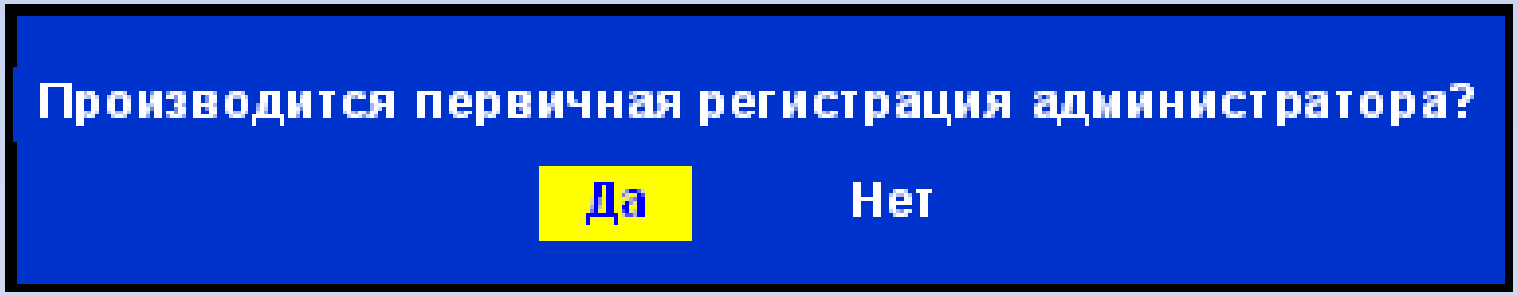
Настройка контроля целостности

- Проверка работоспособности датчика случайных чисел

Настройка журнала регистрации событий

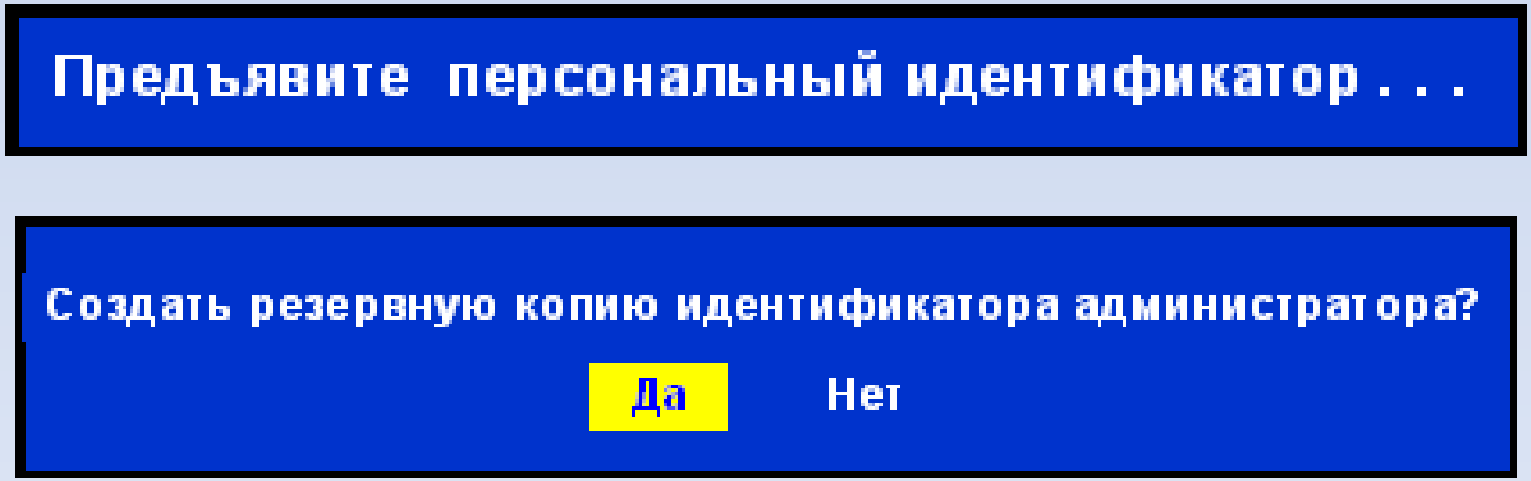


Регистрация администратора



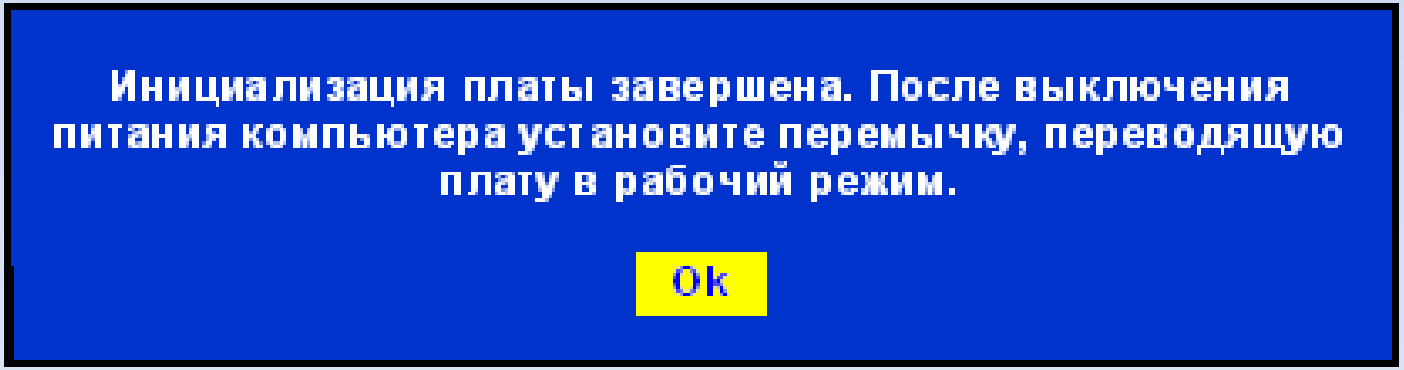
Регистрация администратора

- Ввод пароля администратора
- Регистрация идентификатора администратора
- Создание резервной копии идентификатора



Расчет контрольных сумм

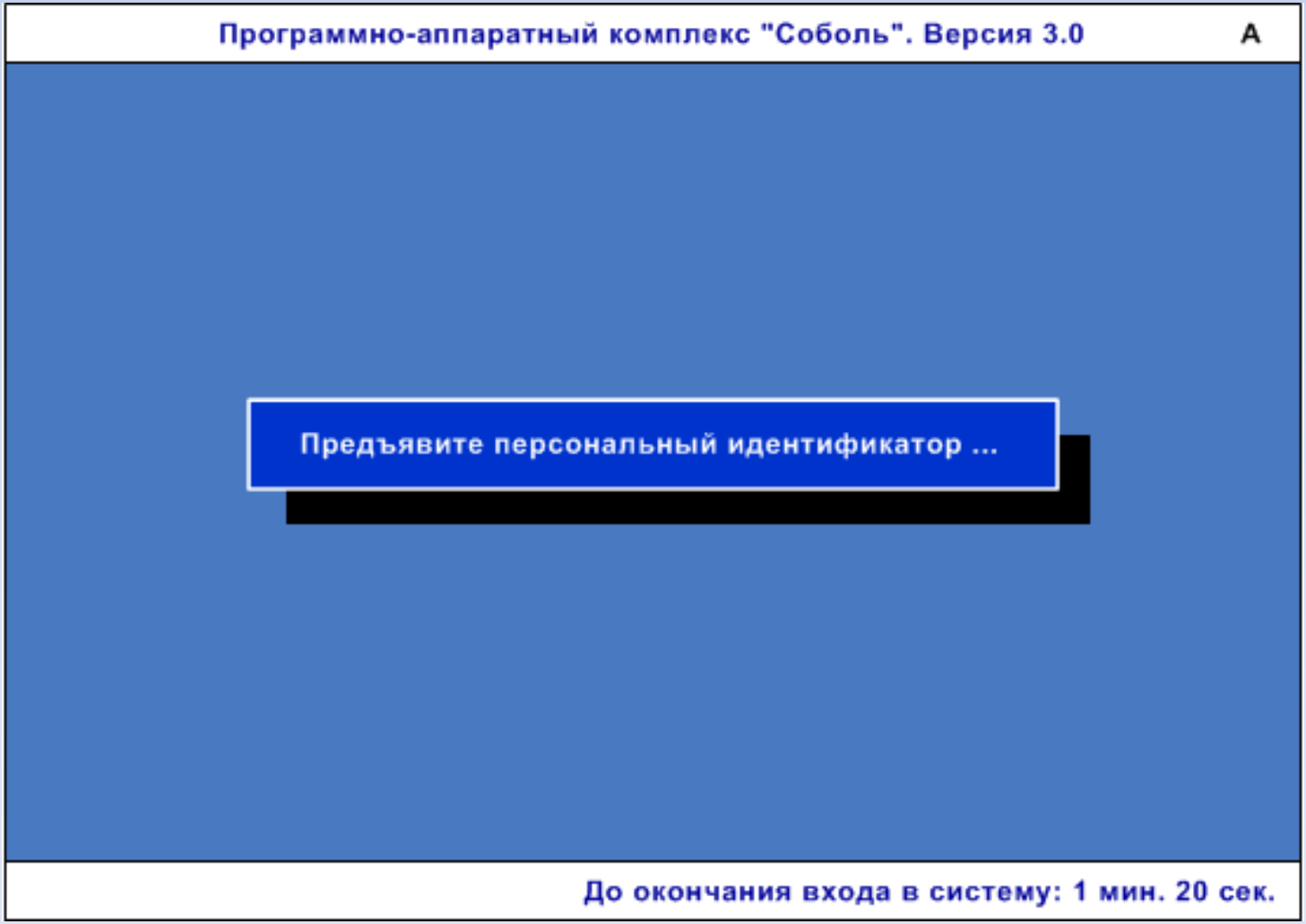
- Расчет эталонов объектов, заданных исходными шаблонами КЦ. На экране будет отображаться процесс расчета.
- Компьютер выключится автоматически.



Перевод комплекса в режим эксплуатации

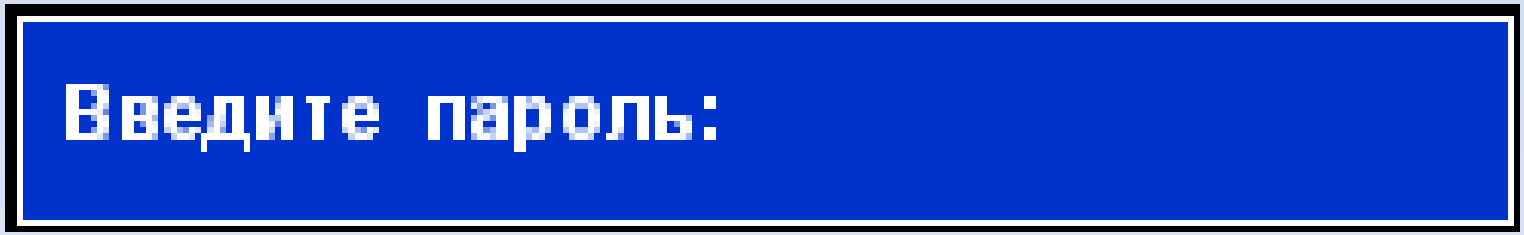
- При наличии подключенного к плате комплекса "Соболь" считывателя iButton отсоедините считыватель от платы
- Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI
- Установите перемычку на разъеме J0 платы
- Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI.
- При необходимости подключите к плате считыватель iButton

Вход в систему

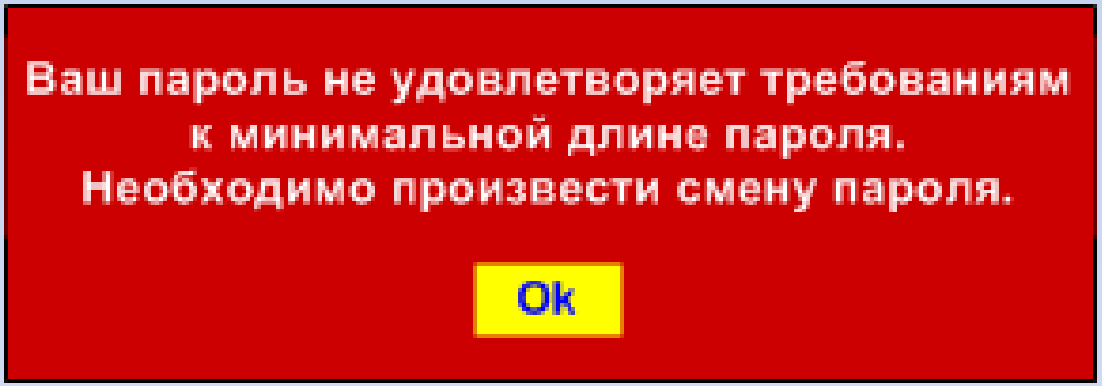


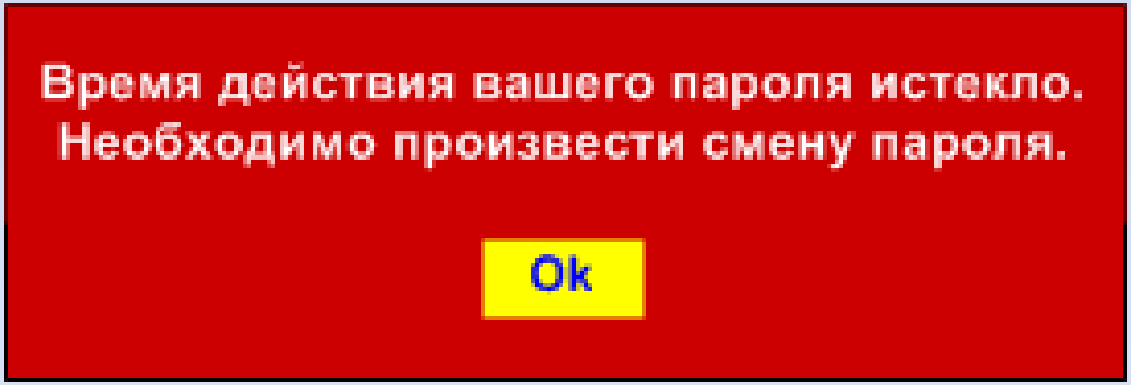
Вход в систему

- Предъявите выданный вам персональный идентификатор
- Введите ваш пароль

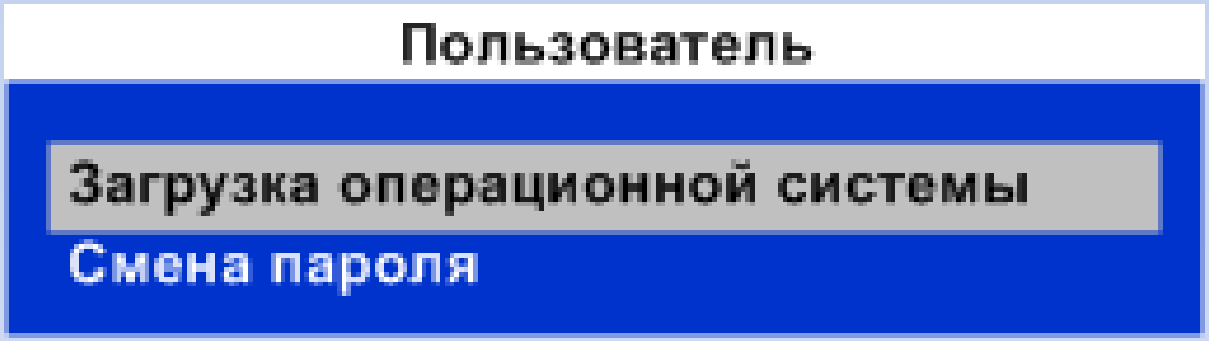


Требования смены пароля





Загрузка операционной системы

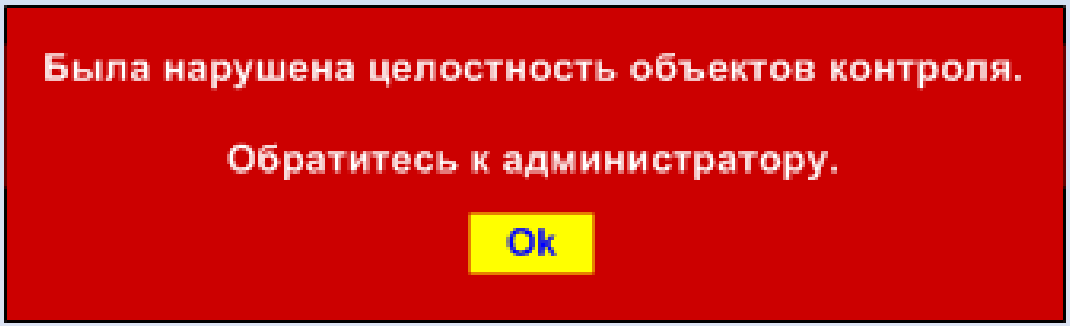


Дальнейшие действия системы могут быть следующими:

- Начнется загрузка операционной системы компьютера.
- Если включен режим контроля целостности, то перед загрузкой операционной системы начнется проверка целостности заданных объектов.

Контроль целостности

- Если администратор задал вам жесткий режим контроля целостности, то компьютер будет заблокирован и в строке сообщений появится сообщение "Компьютер заблокирован



СЗИ НСД АККОРД АМДЗ

Аккорд-АМДЗ

- Аппаратный модуль доверенной загрузки - обеспечивает доверенную загрузку ОС вне зависимости от ее типа для аутентифицированного пользователя

Компоненты

Аппаратные компоненты:

- Контроллер;
- Контактное устройство;
- Идентификатор;

Программные компоненты:

- BIOS контроллера комплекса Аккорд-АМДЗ;
- Firmware, в котором реализованы функции АМДЗ

Средства идентификации

ТМ-идентификатор

ПСКЗИ ШИПКА

Возможность выбора средств идентификации

ТМ-идентификатор

ПСКЗИ ШИПКА

Смарт-карта

Отпечаток пальца

Сетчатка глаза

Любые средства идентификации

Аппаратные интерфейсы

- PCI (Аккорд-5.5)
- PCI-Express (Аккорд-GX , Аккорд-LE)
- miniPCI-Express (Аккорд-GXM)
- miniPCI-Express half size (Аккорд-GXMH)

Разграничение прав доступа к данным

- «Аккорд-Win32», «Аккорд-Win64» – для операционных систем семейства Windows;
- «Аккорд-X» – для операционных систем Linux.

Сервер централизованного управления (СЦУ)

- Удаленный сбор журналов работы пользователей
- Централизованная смена паролей
- Оперативное оповещение о НСД
- Обновление списка контроля целостности
- Создание учетных записей пользователей

Защитные функции комплекса

1)Защита от НСД СВТ, включая:

- идентификацию пользователя по уникальному Идентификатору;
- аутентификацию с учетом необходимой длины пароля и времени его жизни;
- аппаратный (до загрузки ОС) контроль целостности технических средств СВТ, программ и данных на жестком диске (в том числе системных областей диска и модулей программной части комплекса);
- ограничение времени доступа субъекта к СВТ в соответствии с установленным режимом работы пользователей;
- блокировку несанкционированной загрузки СВТ с отчуждаемых носителей (FDD, CD-ROM, ZIP-drive, USB-disk и др.);

Защитные функции комплекса

2)процедур блокирования экрана и клавиатуры по команде пользователя

или по истечению установленного интервала «неактивности» пользователя;

3) Разграничение доступа к локальным и сетевым ресурсам

Контроль доступа

Дискреционный и мандатный методы разграничения доступа.

- При использовании мандатного доступа с контролем процессов (исполняемых модулей) выполняется процедура управления потоками информации.
- Возможен выбор уровня доступа запускаемой задачи или выбор уровня конфиденциальности всей сессии пользователя.

Защитные функции комплекса

4)Управление процедурами ввода/вывода на отчуждаемые носители информации.

Для каждого пользователя контролируется список разрешённых USB-устройств и SD карт в соответствии с их уникальными идентификационными номерами;

Защитные функции комплекса

5)Контроль 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;

Защитные функции комплекса

6)Гарантированная очистка оперативной памяти и остаточной информации на жестких дисках и внешних носителях;

7)Контроль вывода на печать документов из любых программ, автоматическая маркировка печатных листов специальными пометками, грифами и т.д.

Процесс печати протоколируется в отдельном журнале (создаётся учетная карточка документа);

Защитные функции комплекса

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

9)Защиты от НСД систем терминального доступа;

Защитные функции комплекса

10) Контроль целостности критичных с точки зрения информационной безопасности программ и данных.

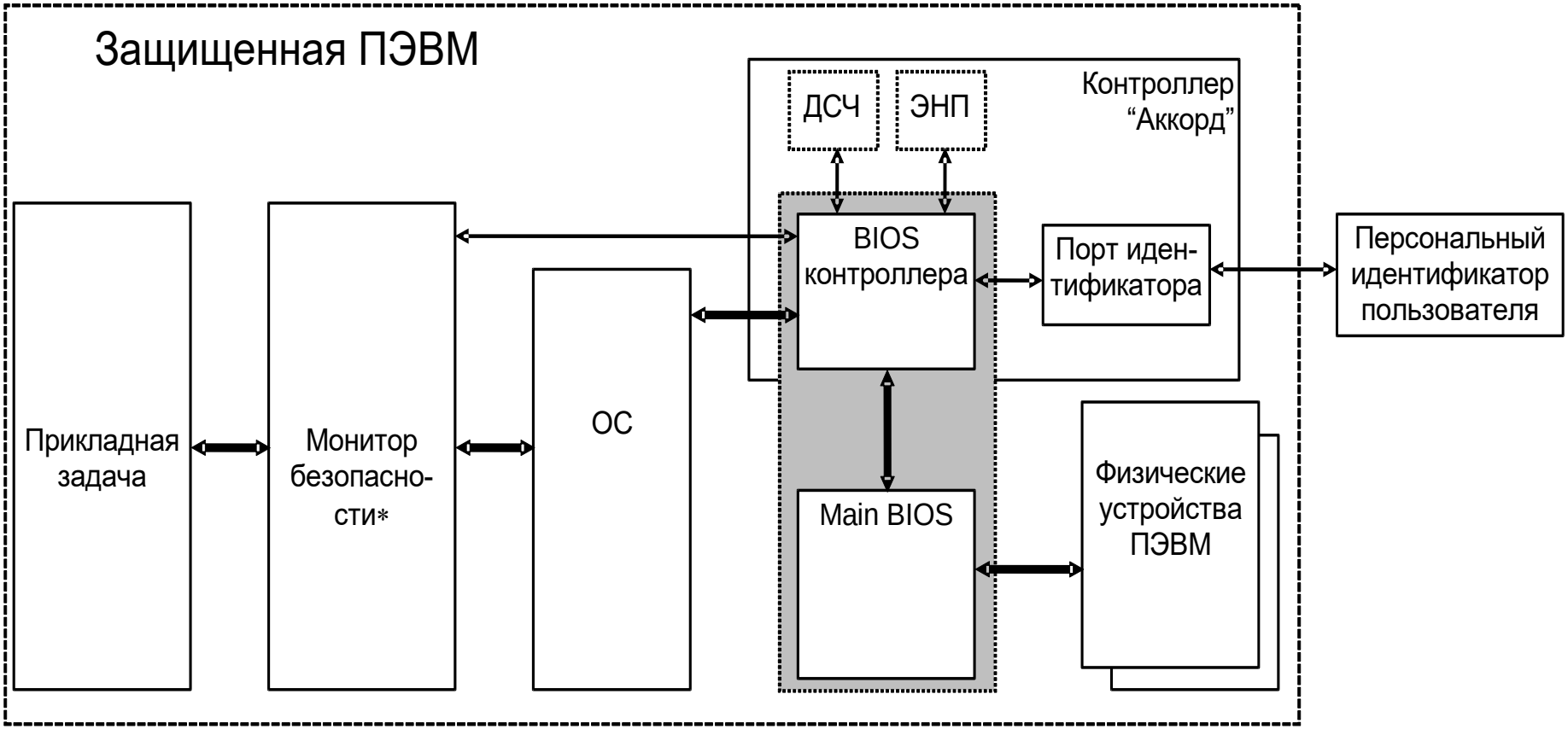
- Статический список (проверка выполняется однократно в начале сеанса, а далее с периодичностью, заданной администратором)
- Динамический список, проверка по которому выполняется при каждой загрузке контролируемого файла в оперативную память.

Защитные функции комплекса

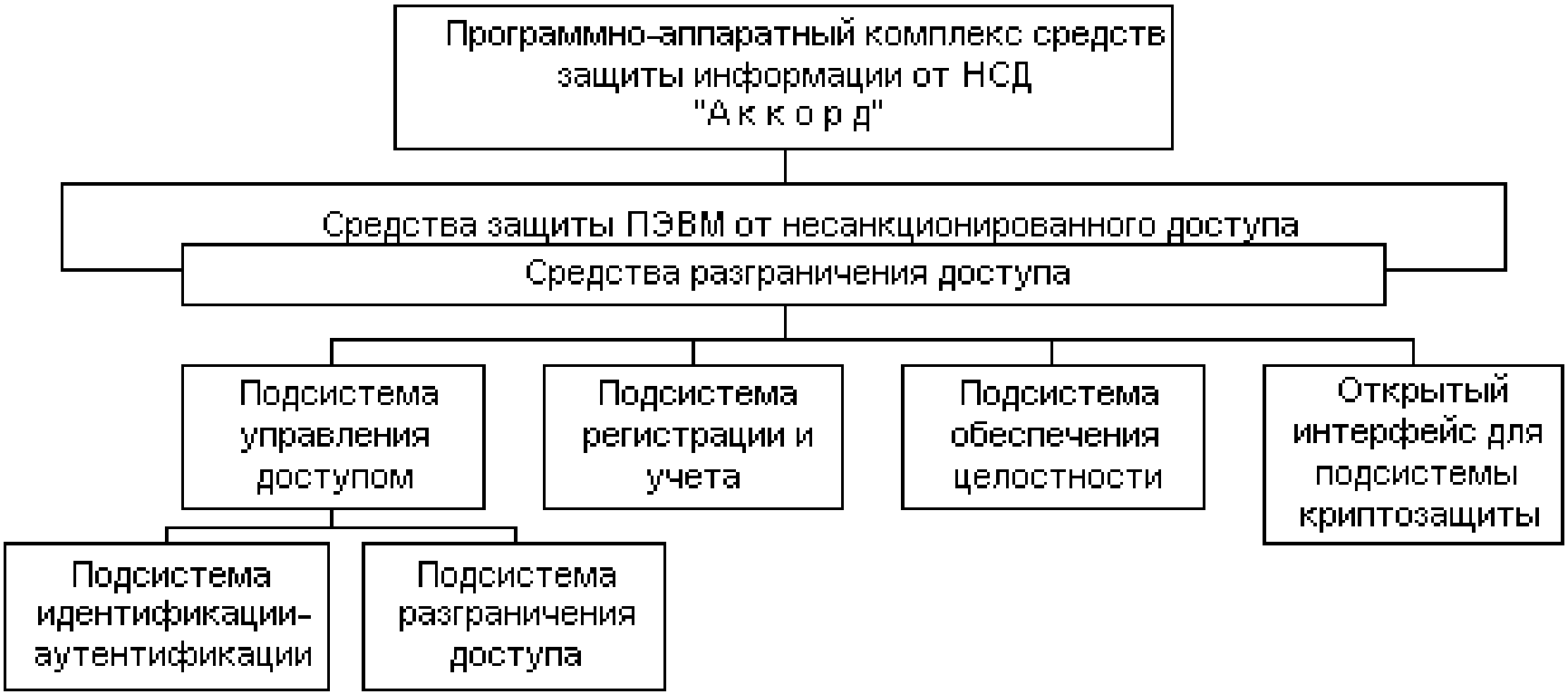
11) Создание изолированной программной среды за счет использования защитных механизмов комплекса;

12) Встраивание или совместное использование других средств защиты информации, в том числе криптографических;

Построение СЗИ



Подсистемы


Программно-аппаратный комплекс средств защиты информации от НСД "А к к о р д"
Средства защиты ПЭВМ от несанкционированного доступа
Средства разграничения доступа
Подсистема управления доступом
Подсистема регистрации и учета
Подсистема обеспечения целостности
Открытый интерфейс для подсистемы криптозащиты
Подсистема идентификации-аутентификации
Подсистема разграничения доступа

Подсистема управления доступом

- Защита от посторонних пользователей обеспечивается процедурами идентификации и аутентификации.
- Ограничение запуска программ и использования данных на основе дискреционного и мандатного управления доступом.

Подсистема регистрации и учета

- Предназначена для регистрации в системном журнале различных событий, происходящих в ПЭВМ.
- При регистрации событий в системном журнале регистрируются:
  - дата и время события;
  - пользователь, осуществляющий регистрируемое действие;
  - действия пользователя (сведения о входе/выходе пользователя из системы, запусках программ, событиях НСД, изменении полномочий и др.)

Подсистема обеспечения целостности

- Предназначена для исключения несанкционированных модификаций (как случайных, так и злоумышленных) программной среды, в том числе программных средств комплекса, обрабатываемой информации, обеспечивая при этом защиту ПЭВМ от внедрения программных закладок и вирусов.

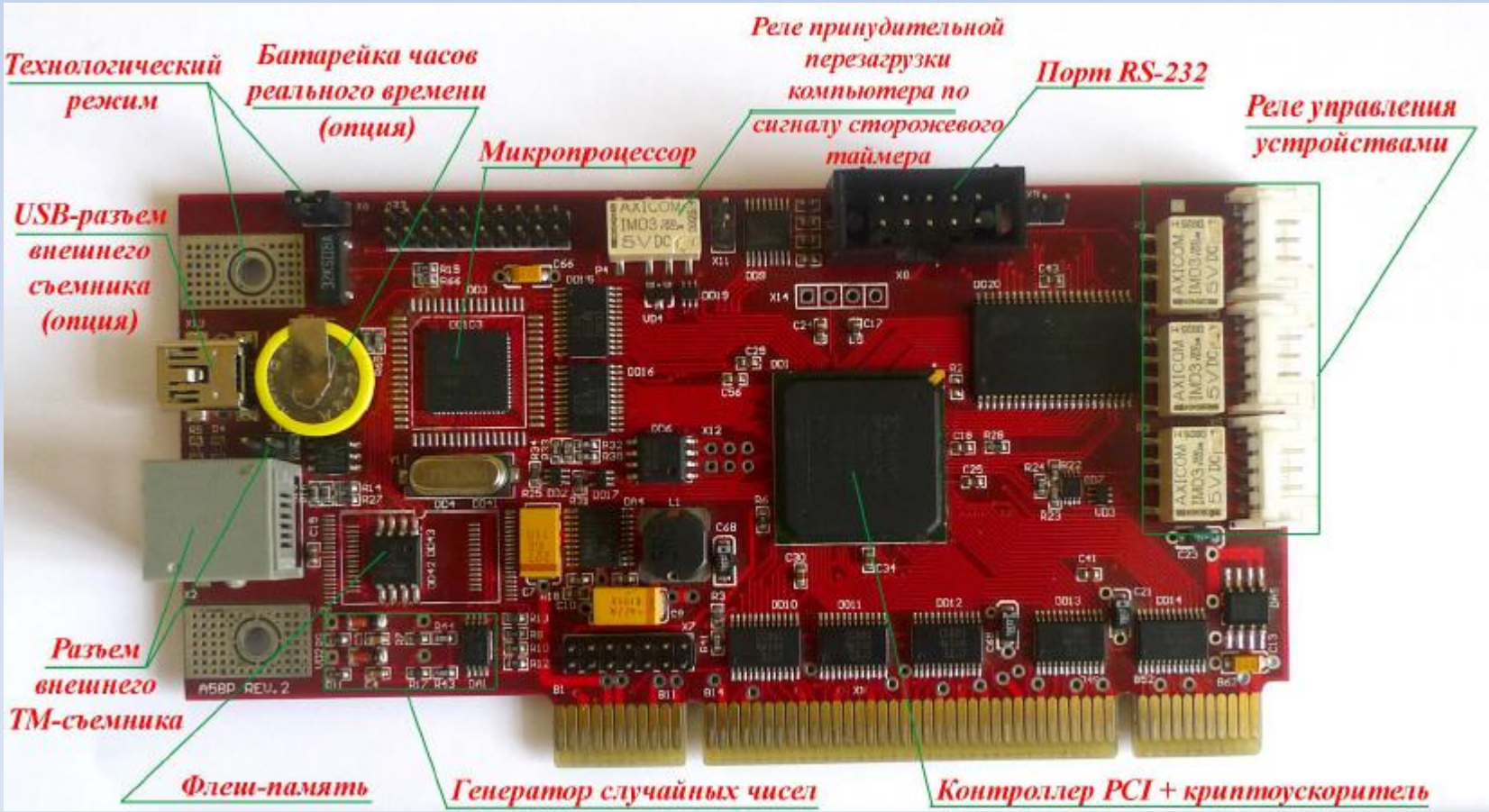
Подсистема обеспечения целостности

Реализуется:

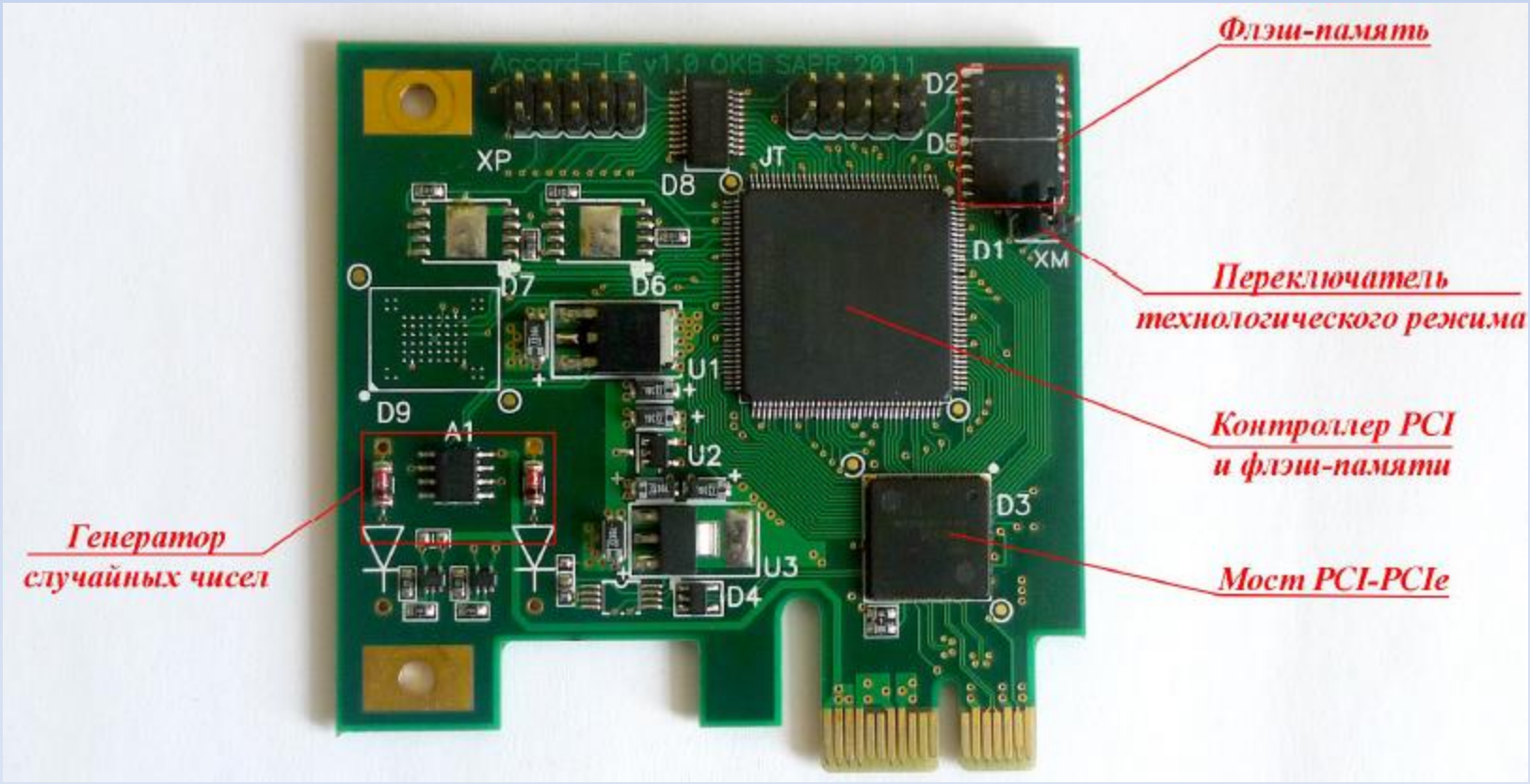
- проверкой целостности назначенных для контроля системных файлов, в том числе КСЗИ НСД, пользовательских программ и данных;
- контролем обращения к операционной системе напрямую;
- исключением возможности использования ПЭВМ без контроллера комплекса;
- механизмом создания замкнутой программной среды, запрещающей запуск привнесенных программ и исключающей несанкционированный выход в ОС.

Плата контроллера «Аккорд-5МХ»

Плата контроллера «Аккорд-5.5»



Плата контроллера «Аккорд-LE»



Организационные меры, необходимые для применения комплекса

- Наличие администратора безопасности информации – 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 комплекса в СВТ(РС), эксплуатацию и контроль правильности использования СВТ(РС) с внедренным комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса;

Организационные меры, необходимые для применения комплекса

- Разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.).
- Физическая охрана СВТ (АС) и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера Комплекса;

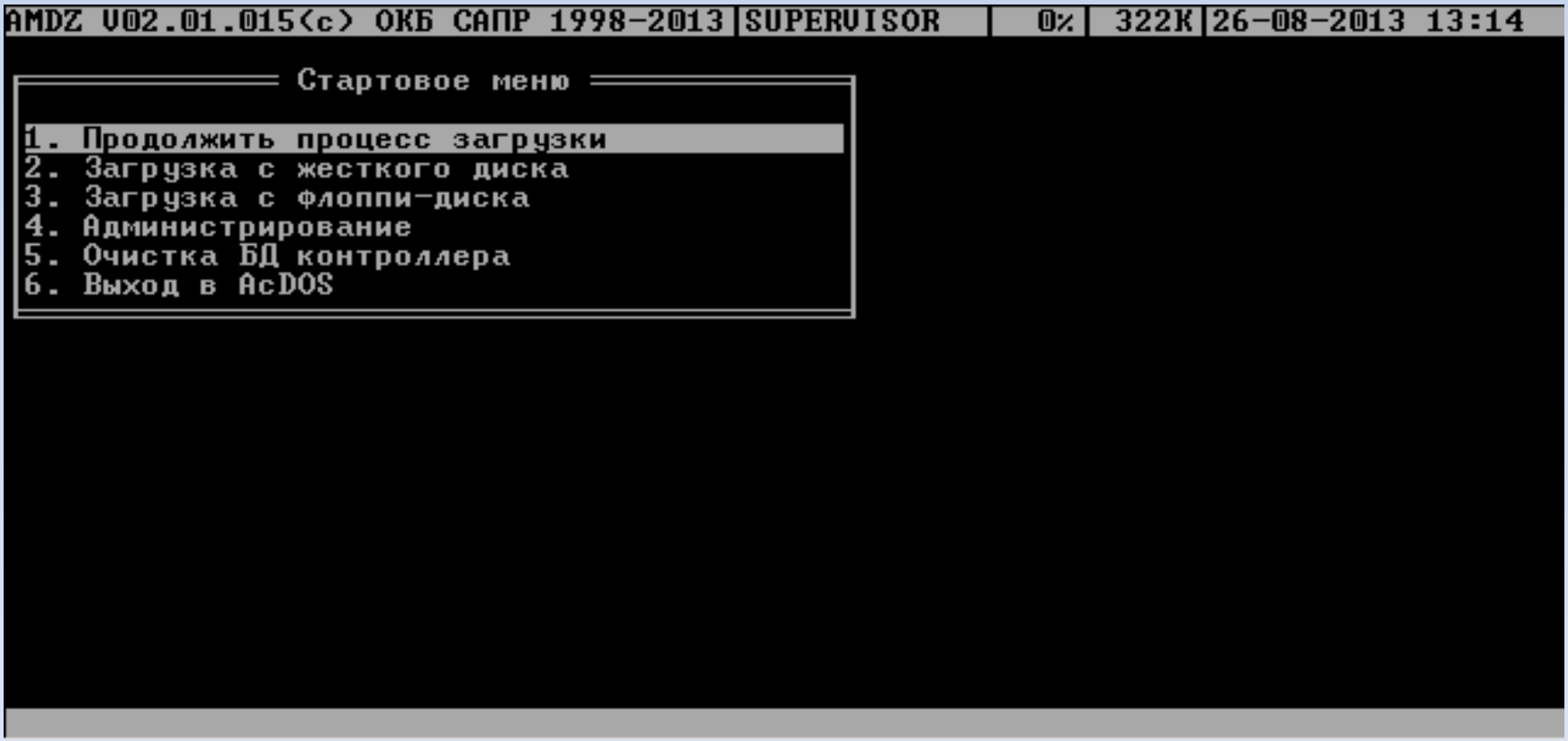
Организационные меры, необходимые для применения комплекса

- Использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации (ГСЗИ);
- Периодическое тестирование средств защиты комплекса.

Установка комплекса

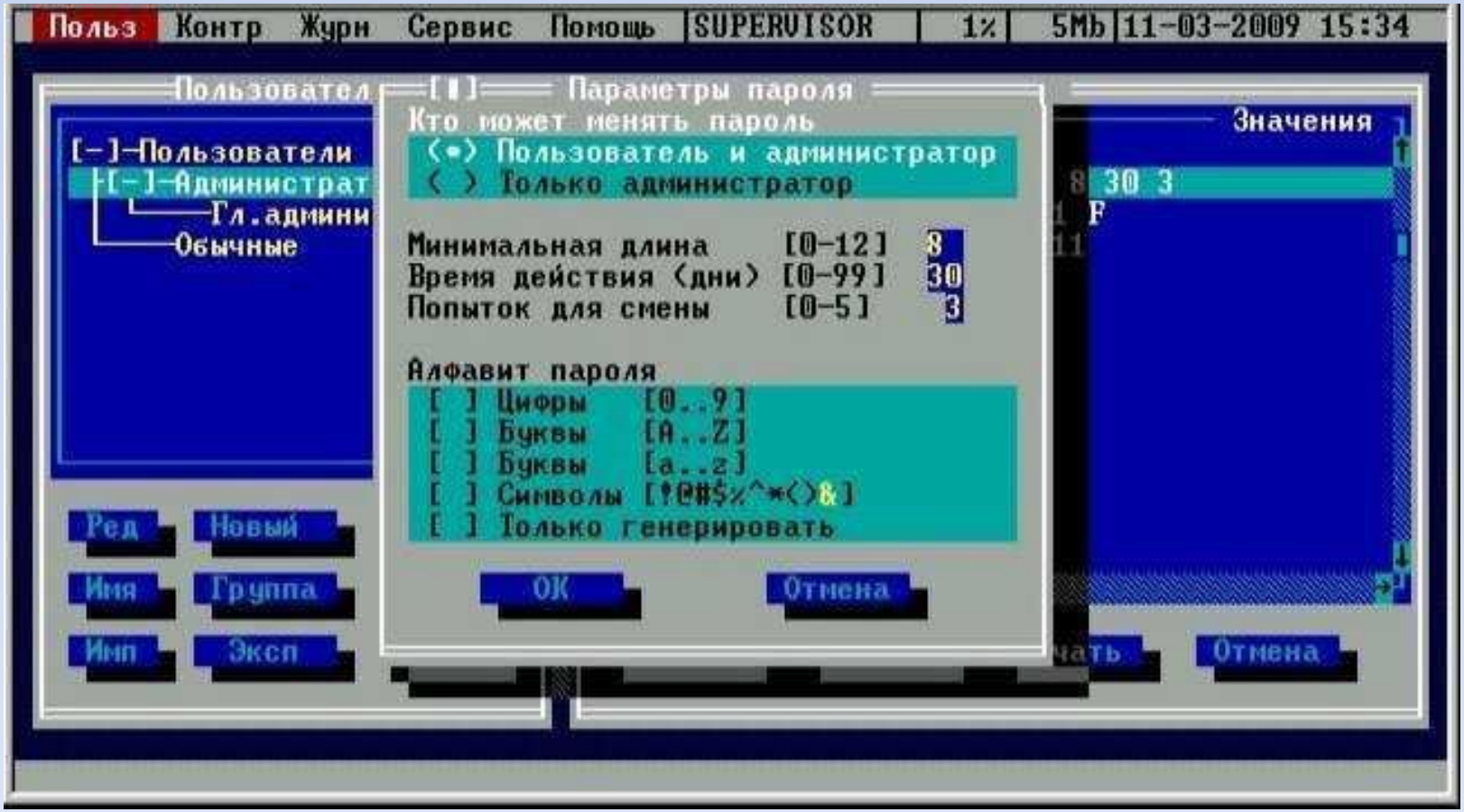
1. Установка платы контроллера в свободный слот ПЭВМ;
2. Подсоединение контактного устройства (съемника информации);
3. Регистрация администратора БИ, настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ;
4. Регистрация пользователей, назначение пользователям персональных идентификаторов, паролей и времени доступа;
5. Назначение списка дисков, файлов, разделов реестра, контролируемых на целостность (подробнее см. «Руководство администратора», входящее в комплект поставки комплекса).

Стартовое меню администратора



Главное меню администратора

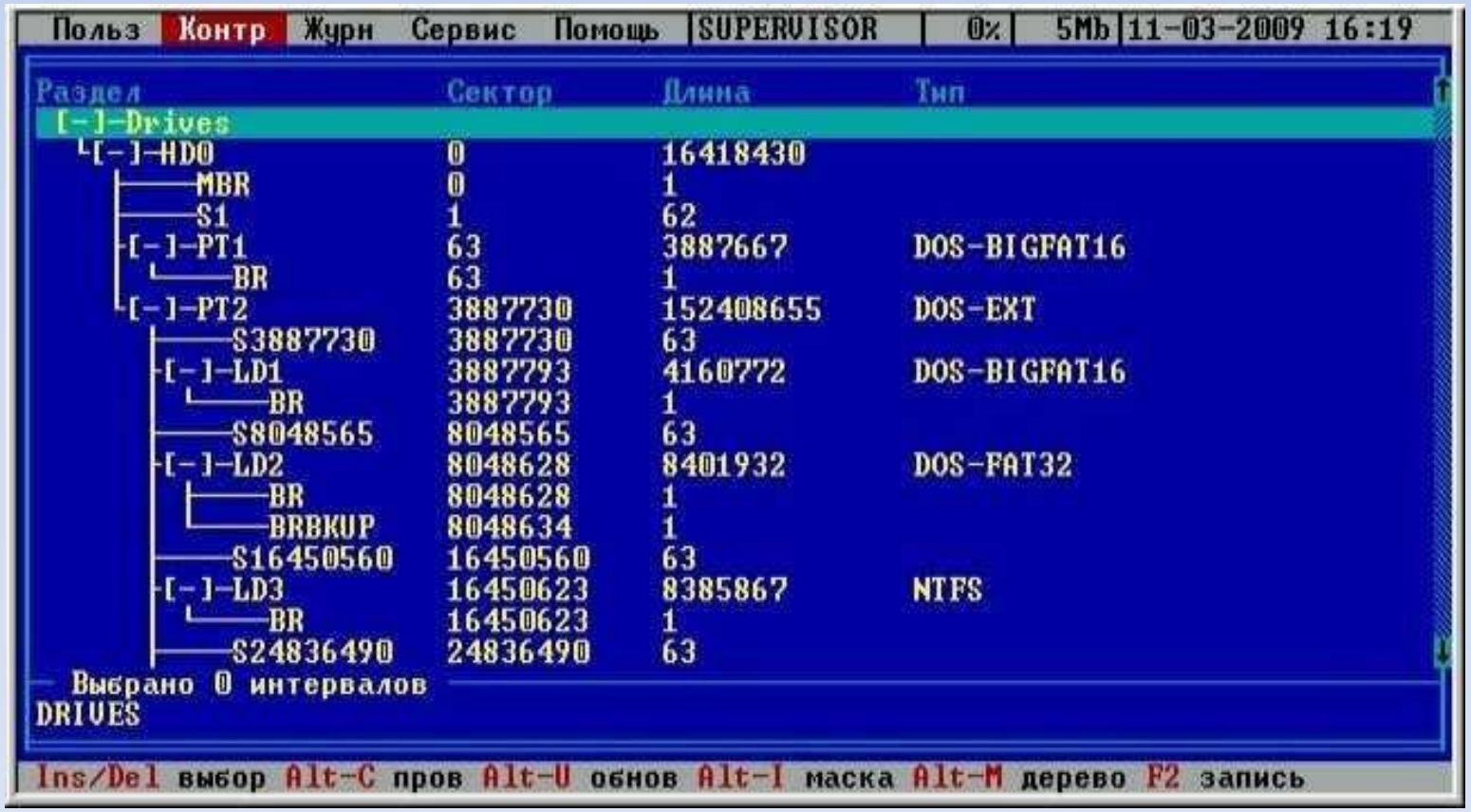
Параметры пароля



Функция управления внешними устройствами

Окно контроля аппаратной части компьютера

Окно контроля служебных областей диска



Дерево разделов и ключей реестра

Рассмотренные вопросы

- ПАК “Соболь”
- Установка комплекса “Соболь”
- СЗИ НСД Аккорд АМДЗ