Технологии QNX и КПДА в России

Санкт-Петербург, 30 октября 2018

«Настройка средств доверенной загрузки в ЗОСРВ «Нейтрино»

Алексей Ермолинский, ООО «СВД Встраиваемые Системы»

СВД Встраиваемые Системы

SWD Software

Руководящие документы

Требования безопасности информации к операционным системам:

- Утверждены приказом ФСТЭК России от 19 августа 2016 г. №119;
- В части требований к функциям безопасности установлено 6 классов защиты. Классы 3, 2, 1 могут использоваться в ИС, обрабатывающих ГТ (С, СС, ОВ);

По функциональному назначению ОС делятся на:

- Тип А – ОС для СВТ общего назначения (включая мобильные устройства);
- Тип Б – встраиваемая (прошиваемая) ОС для специализированных СВТ;
- Тип В – ОС реального времени.

Функциональные требования

Функциональные требования безопасности (ФТБ) реализуются:

- ❑ Функциями безопасности ОС (и/а, аудит, КЦ, МЭ и т.д.);
- ❑ Функциями безопасности среды функционирования (физическая защита, **доверенная загрузка** и т.д.);

ФТБ определены в требованиях безопасности информации к ОС и профилях защиты.

«Должна быть обеспечена доверенная загрузка ОС (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды)»

Руководящие документы

Требования к средствам доверенной загрузки:

- Утверждены приказом ФСТЭК России от 27 сентября 2013 г. №119;
- В части требований к функциям безопасности установлено 6 классов защиты. Классы 3, 2, 1 могут использоваться в ИС, обрабатывающих ГТ (С, СС, ОВ);

Типы средств доверенной загрузки:

- уровня базовой системы ввода-вывода;
- уровня платы расширения;
- уровня загрузочной записи.

Доверенная загрузка

Аппаратные средства доверенной загрузки:

- Загрузка ОС только с разрешенных носителей (запрет загрузки с Live CD, с USB и т.д.);
- Контроль целостности СЗИ и/или ОС до загрузки ОС;
- Авторизация пользователей до загрузки ОС;
- Регистрация попыток входа в систему;
- Блокирование входа в систему;
- Восстановление разделов, шифрование разделов, маскирующее удаление информации;
- Администрирование СЗИ НСД;
- Реализуется в виде платы расширения или интегрируется в системную плату.

Доверенная загрузка

Некоторые из существующих на рынке СЗИ аппаратных средств доверенной загрузки:

- Аккорд-АМДЗ (ЗАО «ОКБ САПР»);
- АПМДЗ «Соболь» (Код Безопасности);
- АПМДЗ «Цезарь» (ВНИИНС);
- АПКДЗ «Тверца Зетта-М» (ЗАО НИИ ЦПС);
- МДЗ-Эшелон (НПО «Эшелон»).
- Доверенная платформа KWBS N2930 (ООО Фирма «АНКАД»)

СВД Встраиваемые Системы

SWD Software

Тверца-2

Основные функции контроллера Тверца-2 (АПКДЗ «Тверца Зетта М»):

- Блокировка загрузки ЭВМ с внешних носителей информации;
- Авторизация пользователей до загрузки ОС;
- Регистрация попыток входа;
- Блокирование входа при попытках НСД;
- Контроль временного изъятия контроллера из ЭВМ;
- Контроль целостности файлов, маскирующее удаление информации, резервное копирование и восстановления разделов диска до загрузки ОС.

Тверца-2

Интеграция ЗОСРВ «Нейтрино» с контроллером Тверца-2:

- ❑ Сквозная авторизация пользователей (передача данных авторизации от контроллера Тверца-2 подсистеме и/а ЗОСРВ «Нейтрино»);
- ❑ Чтение журнала событий безопасности контроллера Тверца-2 в среде ЗОСРВ «Нейтрино»;
- ❑ Управление пользователями контроллера Тверца-2 в среде ЗОСРВ «Нейтрино»;
- ❑ Добавление пользователей контроллера в ЗОСРВ «Нейтрино»
- ❑ Добавление пользователей ЗОСРВ «Нейтрино» в базу контроллера.

Пакет поддержки контроллера «Тверца-2»

Пакет поддержки контроллера «Тверца-2» для ЗОСРВ «Нейтрино» содержит компоненты:

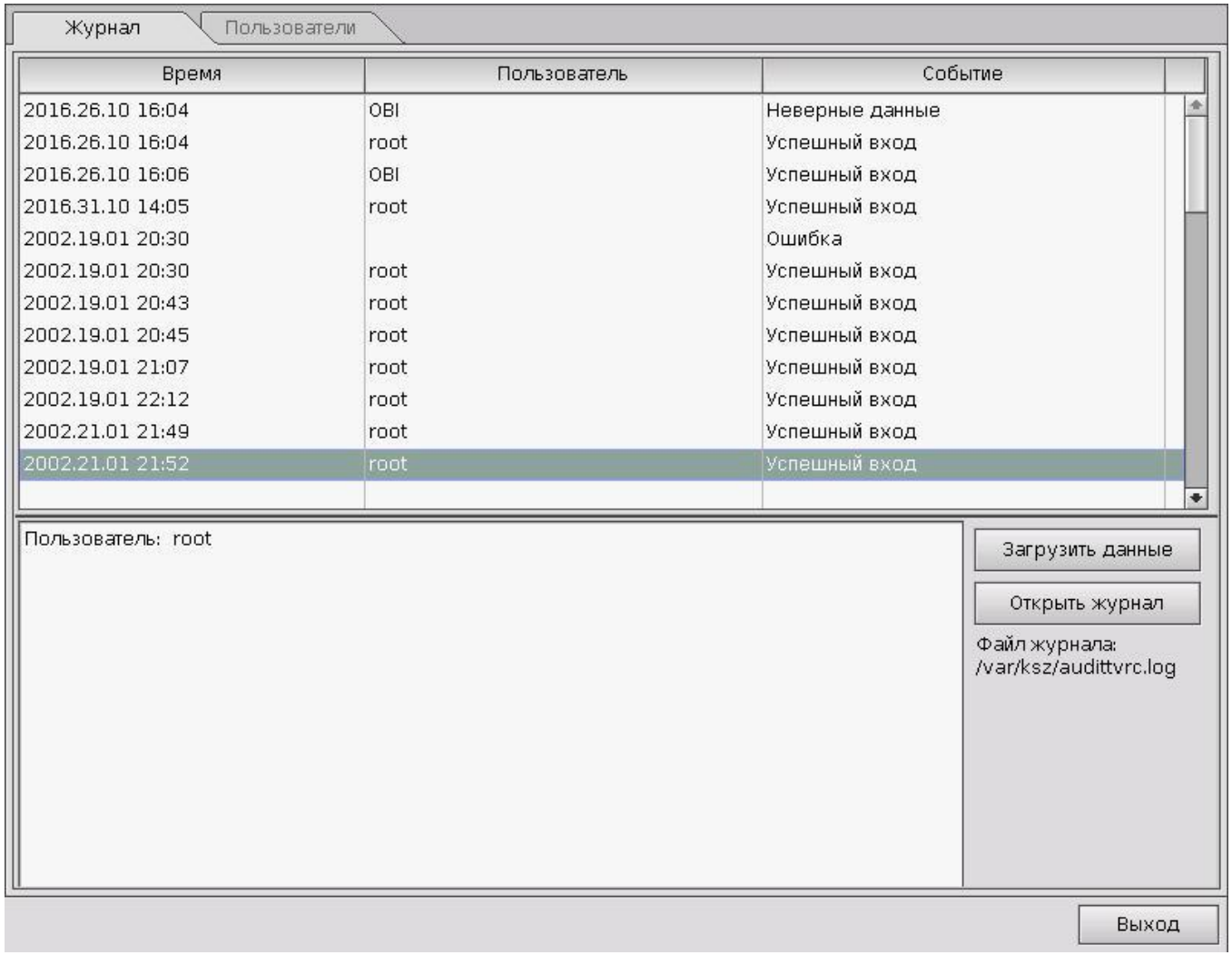
- драйвер работы с контроллером **devt-tvrc** (поддерживаются шины PCI Express, Mini PCI Express, Half Mini PCI Express и M.2);
- доработанный модуль **phlogin2_ksz** обеспечивает сквозную авторизацию пользователей;
- графическая утилита работы с журналом событий и учетными записями пользователей (панель управления Тверца-2, ПУ Тверца-2) **tvrc_cam**.

Настройка доверенной загрузки

Настройка доверенной загрузки в ЗОСРВ «Нейтрино»:

- ❑ инициализация устройства **/dev/tvrc** (запуск драйвера **devt-tvrc** из образа или через **rc.local**);
- ❑ передача параметра **–t** утилите **phlogin2_ksz** для сквозной авторизации (в скрипте **ph**);
- ❑ администрирование учетных записей (импорт, экспорт, создание пользователей) в Панели управления Тверца-2 (утилита **tvrc_cam**).

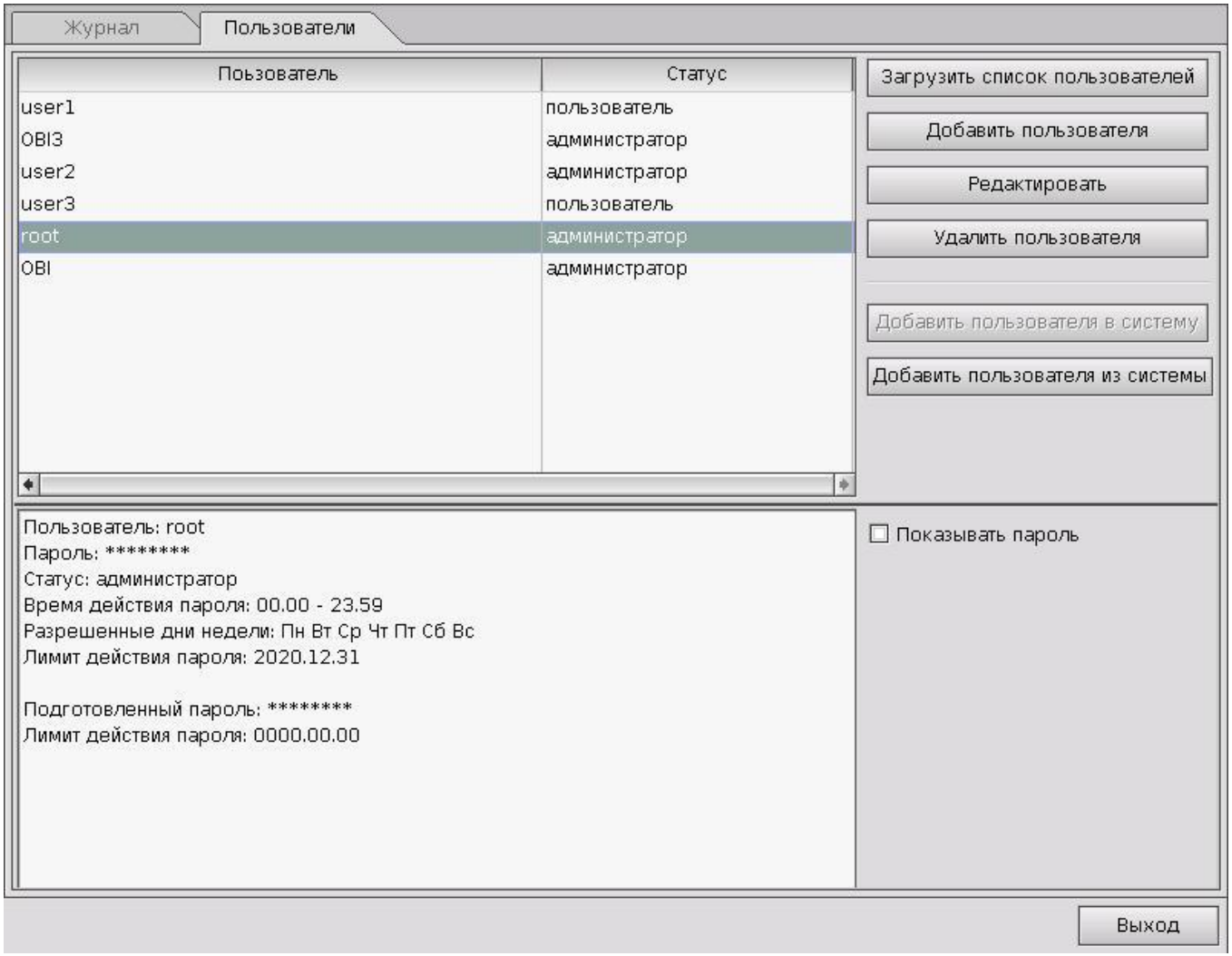
Журнал событий контроллера «Тверца-2»



СВД Встраиваемые Системы

SWD Software

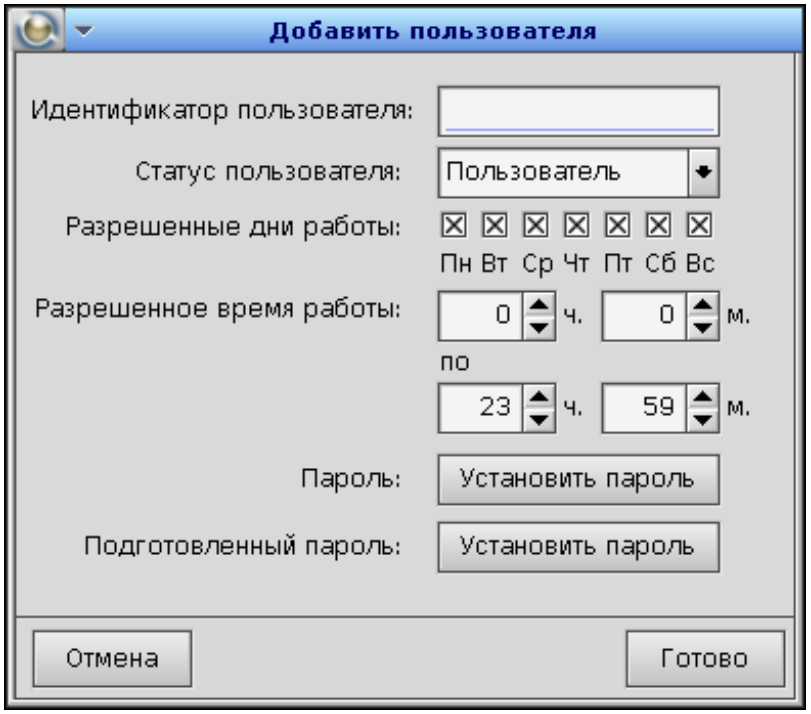
Управление пользователями контроллера «Тверца-2»

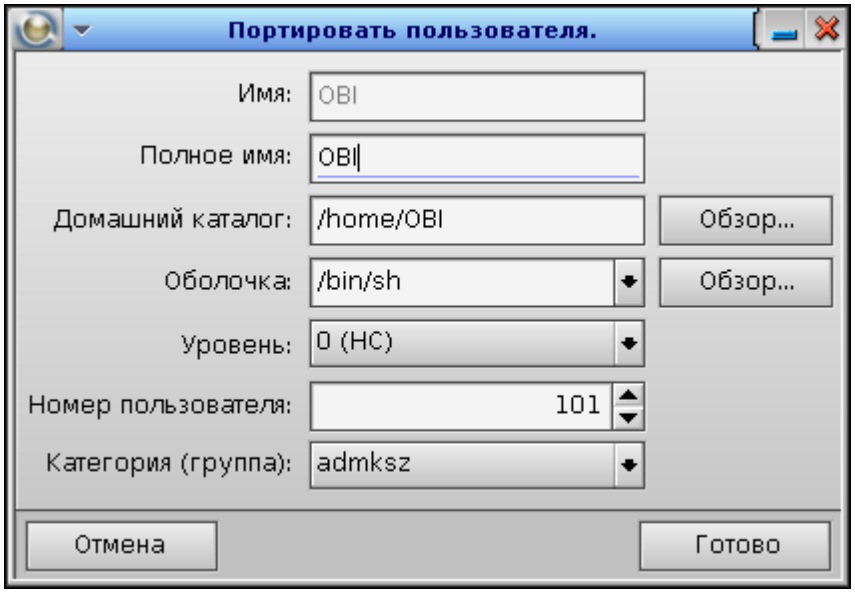


СВД Встраиваемые Системы

SWD Software

Управление пользователями контроллера «Тверца-2»





СВД Встраиваемые Системы

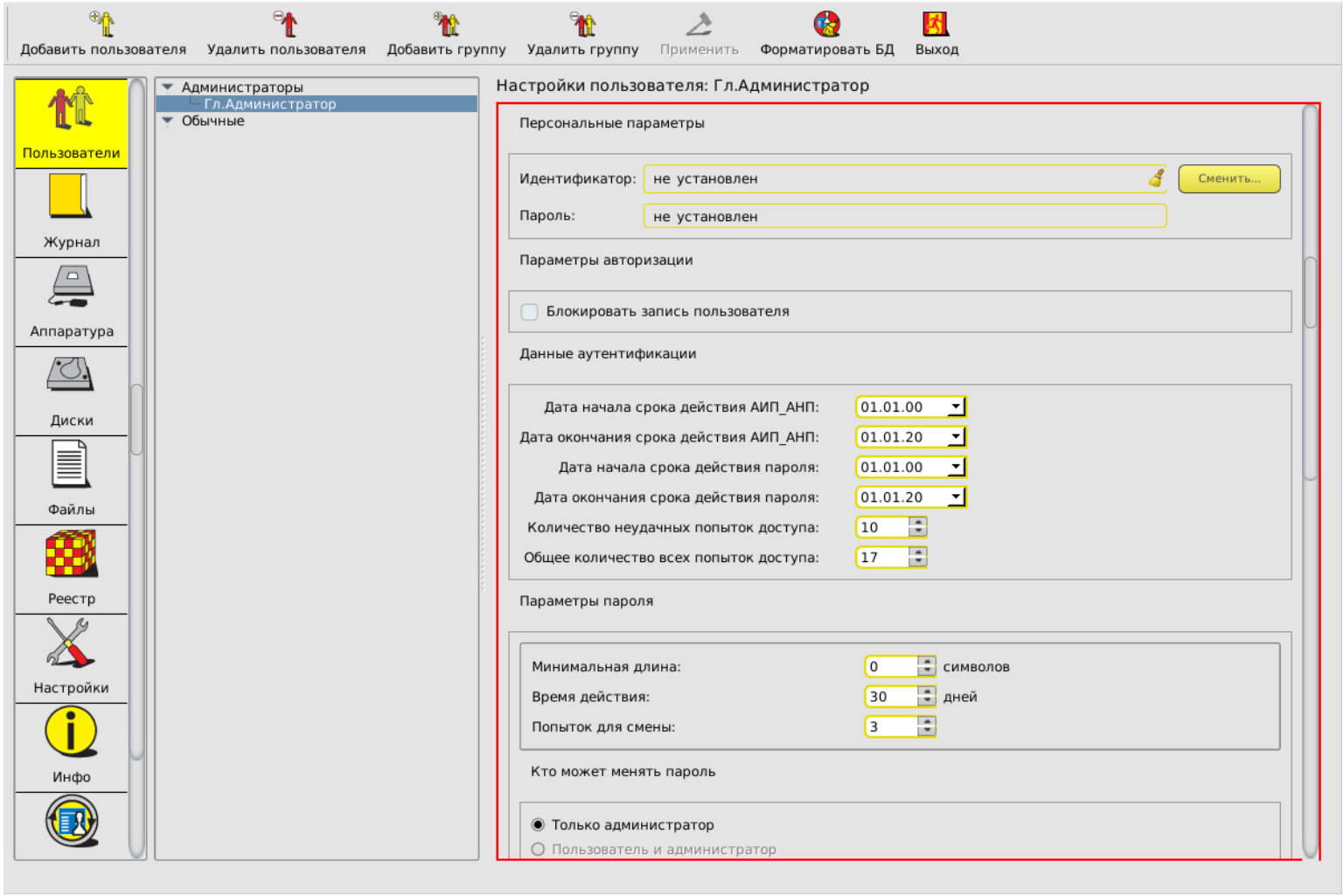
SWD Software

Аккорд-АМДЗ

Основные функции комплекса Аккорд-АМДЗ (на базе контроллера Аккорд GX):

- Блокировка загрузки ЭВМ с внешних носителей информации;
- Аутентификация пользователей, в т.ч. с помощью персонального идентификатора «Шипка»;
- Контроль целостности аппаратных средств;
- Контроль целостности объектов ФС (в т.ч. QNX4 и QNX6);
- Регистрация событий безопасности;
- Администрирование комплекса с помощью встроенного ПО.

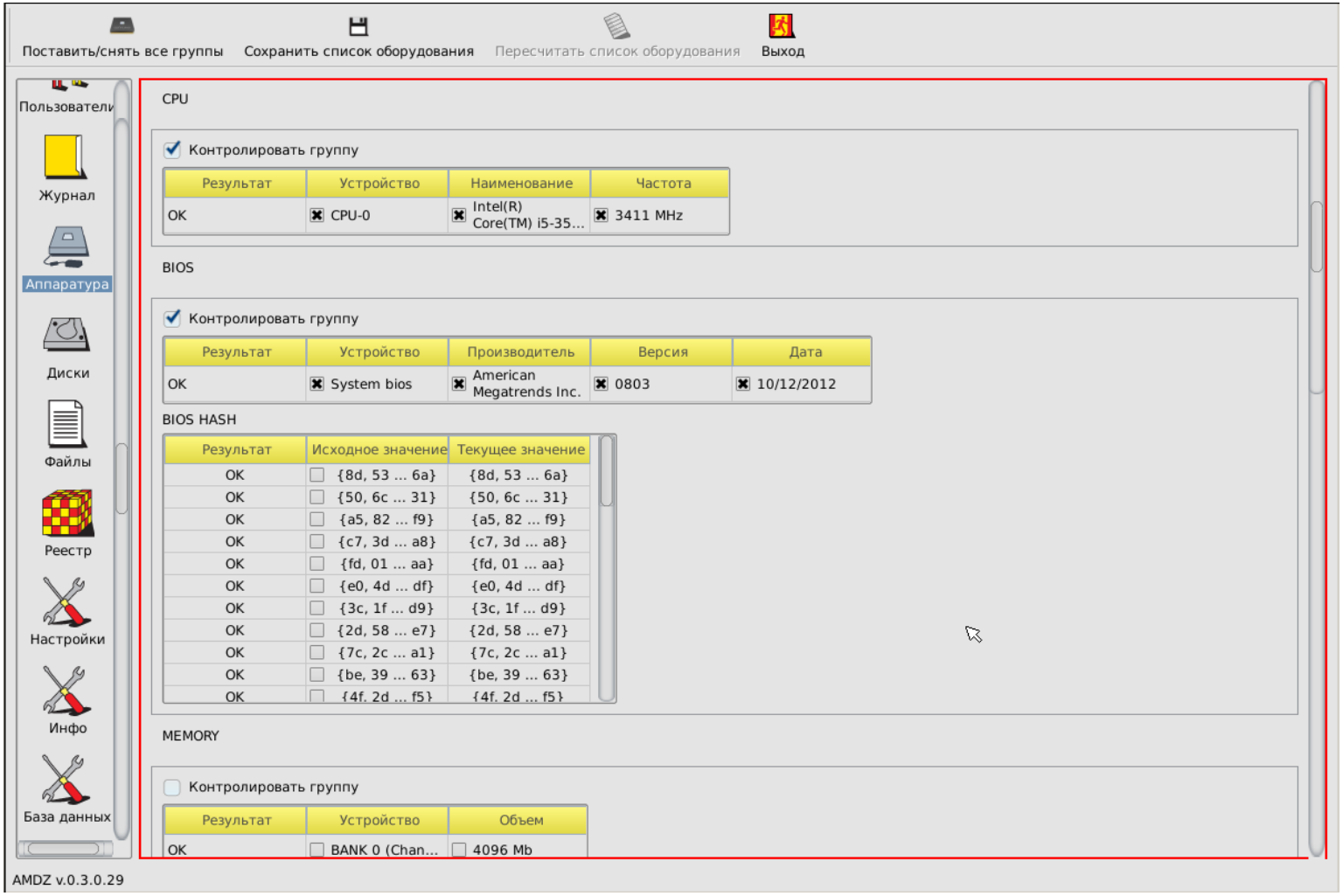
Графический интерфейс администрирования Аккорд-АМДЗ



СВД Встраиваемые Системы

SWD Software

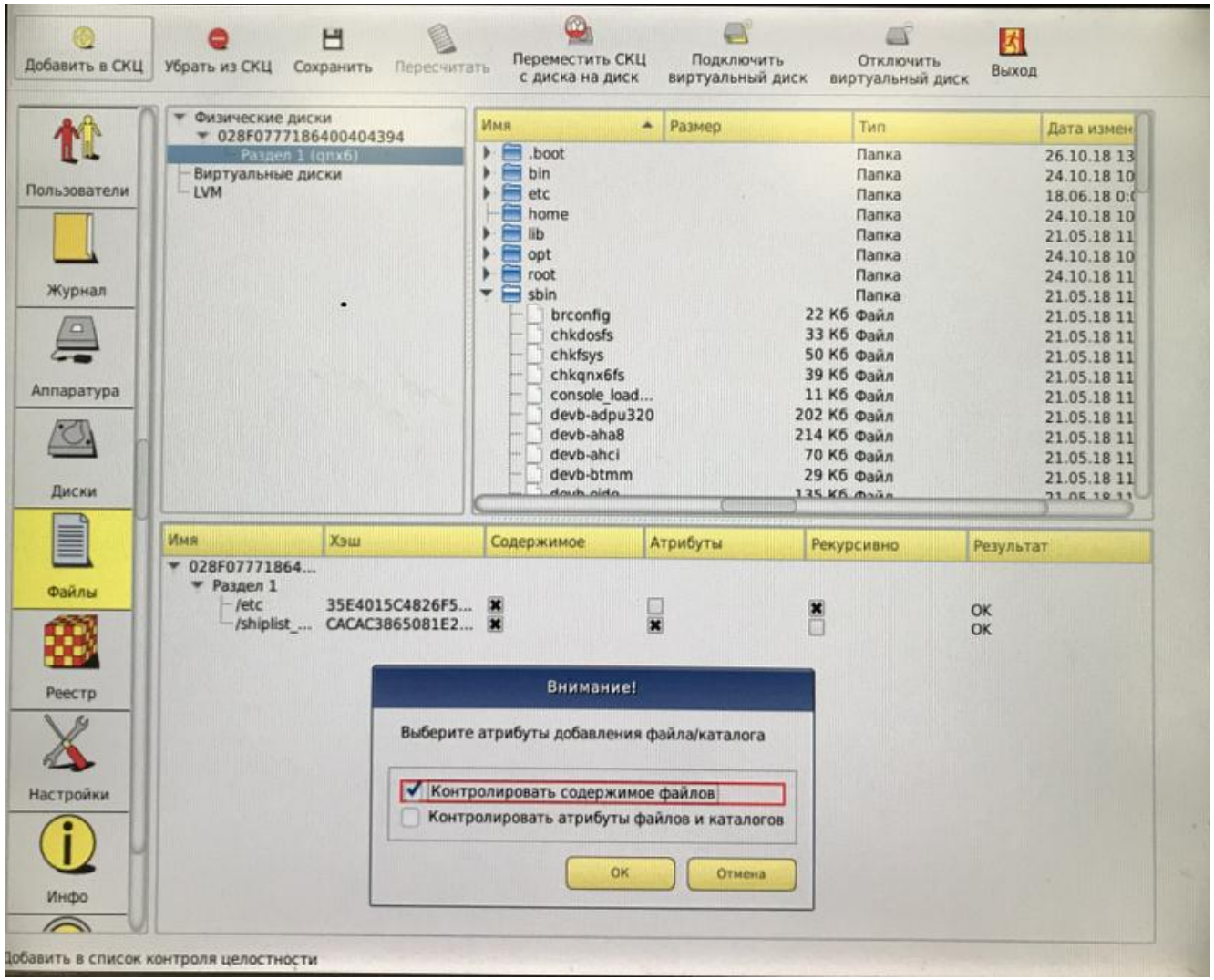
Контроль целостности аппаратных средств в Аккорд-АМДЗ



СВД Встраиваемые Системы

SWD Software

Контроль целостности объектов ФС в Аккорд-АМДЗ



СВД Встраиваемые Системы

SWD Software

Спасибо за внимание

Алексей Ермолинский
Инженер-программист

Телефон (812) 346-89-56 (доб.124)
Почта support@kpda.ru
Сайт www.kpda.ru

СВД Встраиваемые Системы

SWD Software