



# Технологии QNX и КПДА в России

Санкт-Петербург, 30 октября 2018

«Настройка средств доверенной загрузки в ЗОСРВ  
«Нейтрино»

Алексей Ермолинский, ООО «СВД Встраиваемые Системы»

## 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 профилям 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»)

# 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»

Журнал Пользователи

| Время            | Пользователь | Событие         |
|------------------|--------------|-----------------|
| 2016.26.10 16:04 | OBi          | Неверные данные |
| 2016.26.10 16:04 | root         | Успешный вход   |
| 2016.26.10 16:06 | OBi          | Успешный вход   |
| 2016.31.10 14:05 | root         | Успешный вход   |
| 2002.19.01 20:30 |              | Ошибка          |
| 2002.19.01 20:30 | root         | Успешный вход   |
| 2002.19.01 20:43 | root         | Успешный вход   |
| 2002.19.01 20:45 | root         | Успешный вход   |
| 2002.19.01 21:07 | root         | Успешный вход   |
| 2002.19.01 22:12 | root         | Успешный вход   |
| 2002.21.01 21:49 | root         | Успешный вход   |
| 2002.21.01 21:52 | root         | Успешный вход   |

Пользователь: root

Загрузить данные

Открыть журнал

Файл журнала:  
/var/ksz/auditvrc.log

Выход

# Управление пользователями контроллера «Тверца-2»

The screenshot displays a web-based user management interface. At the top, there are two tabs: 'Журнал' (Journal) and 'Пользователи' (Users), with 'Пользователи' being the active tab. The main area is divided into a table of users and a sidebar with control buttons.

| Пользователь | Статус        |
|--------------|---------------|
| user1        | пользователь  |
| OBIZ         | администратор |
| user2        | администратор |
| user3        | пользователь  |
| root         | администратор |
| OB1          | администратор |

Buttons on the right sidebar:

- Загрузить список пользователей
- Добавить пользователя
- Редактировать
- Удалить пользователя
- Добавить пользователя в систему
- Добавить пользователя из системы

Below the table, a detailed view of the selected 'root' user is shown:

Пользователь: root  
Пароль: \*\*\*\*\*  
Статус: администратор  
Время действия пароля: 00.00 - 23.59  
Разрешенные дни недели: Пн Вт Ср Чт Пт Сб Вс  
Лимит действия пароля: 2020.12.31

Подготовленный пароль: \*\*\*\*\*  
Лимит действия пароля: 0000.00.00

There is a checkbox labeled 'Показывать пароль' (Show password) which is currently unchecked.

A 'Выход' (Exit) button is located at the bottom right of the interface.

# Управление пользователями контроллера «Тверца-2»

**Добавить пользователя**

Идентификатор пользователя:

Статус пользователя: Пользователь ▾

Разрешенные дни работы:         
Пн Вт Ср Чт Пт Сб Вс

Разрешенное время работы:  ч.  м.  
по  ч.  м.

Пароль:

Подготовленный пароль:

**Портировать пользователя.**

Имя:

Полное имя:

Домашний каталог:

Оболочка:

Уровень:

Номер пользователя:

Категория (группа):

# 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

Добавить пользователя   Удалить пользователя   Добавить группу   Удалить группу   Применить   Форматировать БД   Выход

**Пользователи**

- Администраторы
  - Гл.Администратор
- Обычные

**Журнал**

**Аппаратура**

**Диски**

**Файлы**


**Реестр**

**Настройки**

**Инфо**

### Настройки пользователя: Гл.Администратор

**Персональные параметры**

Идентификатор:  

Пароль:

**Параметры авторизации**

Блокировать запись пользователя

**Данные аутентификации**

Дата начала срока действия АИП\_АНП:

Дата окончания срока действия АИП\_АНП:

Дата начала срока действия пароля:

Дата окончания срока действия пароля:

Количество неудачных попыток доступа:

Общее количество всех попыток доступа:

**Параметры пароля**

Минимальная длина:  символов

Время действия:  дней

Попыток для смены:

**Кто может менять пароль**

Только администратор

Пользователь и администратор

# Контроль целостности аппаратных средств в Аккорд-АМДЗ

Поставить/снять все группы Сохранить список оборудования Пересчитать список оборудования Выход

Пользователи  
Журнал  
Аппаратура  
Диски  
Файлы  
Реестр  
Настройки  
Инфо  
База данных

**CPU**

Контролировать группу

| Результат | Устройство                                | Наименование   | Частота                                      |
|-----------|---|--|--|
| OK        | <input checked="" type="checkbox"/> CPU-0 | <input checked="" type="checkbox"/> Intel(R) Core(TM) i5-35... | <input checked="" type="checkbox"/> 3411 MHz |

**BIOS**

Контролировать группу

| Результат | Устройство                                      | Производитель  | Версия                                   | Дата   |
|-----------|---|--|--|--|
| OK        | <input checked="" type="checkbox"/> System bios | <input checked="" type="checkbox"/> American Megatrends Inc. | <input checked="" type="checkbox"/> 0803 | <input checked="" type="checkbox"/> 10/12/2012 |

**BIOS HASH**

| Результат | Исходное значение                        | Текущее значение |
|-----------|--|------------------|
| OK        | <input type="checkbox"/> {8d, 53 ... 6a} | {8d, 53 ... 6a}  |
| OK        | <input type="checkbox"/> {50, 6c ... 31} | {50, 6c ... 31}  |
| OK        | <input type="checkbox"/> {a5, 82 ... f9} | {a5, 82 ... f9}  |
| OK        | <input type="checkbox"/> {c7, 3d ... a8} | {c7, 3d ... a8}  |
| OK        | <input type="checkbox"/> {fd, 01 ... aa} | {fd, 01 ... aa}  |
| OK        | <input type="checkbox"/> {e0, 4d ... df} | {e0, 4d ... df}  |
| OK        | <input type="checkbox"/> {3c, 1f ... d9} | {3c, 1f ... d9}  |
| OK        | <input type="checkbox"/> {2d, 58 ... e7} | {2d, 58 ... e7}  |
| OK        | <input type="checkbox"/> {7c, 2c ... a1} | {7c, 2c ... a1}  |
| OK        | <input type="checkbox"/> {be, 39 ... 63} | {be, 39 ... 63}  |
| OK        | <input type="checkbox"/> {4f, 2d ... f5} | {4f, 2d ... f5}  |

**MEMORY**

Контролировать группу

| Результат | Устройство                               | Объем                            |
|-----------|--|----------------------------------|
| OK        | <input type="checkbox"/> BANK 0 (Chan... | <input type="checkbox"/> 4096 Mb |

AMDZ v.0.3.0.29



# Контроль целостности объектов ФС в Аккорд-АМДЗ

Добавить в СКЦ    Убрать из СКЦ    Сохранить    Пересчитать    Переместить СКЦ с диска на диск    Подключить виртуальный диск    Отключить виртуальный диск    Выход

Пользователи  
Журнал  
Аппаратура  
Диски  
Файлы  
Реестр  
Настройки  
Инфо

| Имя             | Размер | Тип   | Дата измен   |
|-----------------|--------|-------|--------------|
| .boot           |        | Папка | 26.10.18 13  |
| bin             |        | Папка | 24.10.18 10  |
| etc             |        | Папка | 18.06.18 0:0 |
| home            |        | Папка | 24.10.18 10  |
| lib             |        | Папка | 21.05.18 11  |
| opt             |        | Папка | 24.10.18 10  |
| root            |        | Папка | 24.10.18 11  |
| sbin            |        | Папка | 21.05.18 11  |
| brconfig        | 22 Кб  | Файл  | 21.05.18 11  |
| chkdosfs        | 33 Кб  | Файл  | 21.05.18 11  |
| chkfsys         | 50 Кб  | Файл  | 21.05.18 11  |
| chkqnx6fs       | 39 Кб  | Файл  | 21.05.18 11  |
| console load... | 11 Кб  | Файл  | 21.05.18 11  |
| devb-adpu320    | 202 Кб | Файл  | 21.05.18 11  |
| devb-aha8       | 214 Кб | Файл  | 21.05.18 11  |
| devb-ahci       | 70 Кб  | Файл  | 21.05.18 11  |
| devb-btmm       | 29 Кб  | Файл  | 21.05.18 11  |
| devb-cide       | 135 Кб | Файл  | 21.05.18 11  |

| Имя               | Хэш               | Содержимое | Атрибуты                 | Рекурсивно               | Результат |
|-------------------|-------------------|------------|--------------------------|--------------------------|-----------|
| ▼ 028F07771864... |                   |            |                          |                          |           |
| ▼ Раздел 1        |                   |            |                          |                          |           |
| /etc              | 35E4015C4826F5... | ✗          | <input type="checkbox"/> | ✗                        | OK        |
| /shiplist_...     | CACAC3865081E2... | ✗          | ✗                        | <input type="checkbox"/> | OK        |

**Внимание!**

Выберите атрибуты добавления файла/каталога

Контролировать содержимое файлов

Контролировать атрибуты файлов и каталогов

OK    Отмена

Добавить в список контроля целостности

# Спасибо за внимание

**Алексей Ермолинский**  
**Инженер-программист**

Телефон (812) 346-89-56 (доб.124)

Почта [support@kpda.ru](mailto:support@kpda.ru)

Сайт [www.kpda.ru](http://www.kpda.ru)