Технологии QNX и КПДА в России

Санкт-Петербург, 23 ноября 2016

«Обновления средств защиты информации в программных изделиях КПДА»

Алексей Ермолинский, ООО «СВД Встраиваемые Системы»

СВД Встраиваемые Системы

SWD Software

Сертификат ЗОСРВ «Нейтрино»

Сертификация ЗОСРВ «Нейтрино» в 2016 году

- **Изделие получило сертификат соответствия №3385 от 27 октября 2016 года в системе сертификации МО РФ.**
- Изделие соответствует:

- требованиям 3-го класса защищенности согласно РД СВД
- требованиям 2-го класса защищенности согласно РД МЭ;
- 2-му уровню контроля отсутствия НДВ;
- требованиям на соответствие реальных и декларируемых возможностей.

Руководящие документы

- Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»;
- Устанавливает классификацию средств МЭ по уровню контроля информационных потоков при взаимодействии ЭВМ и **АС** – 5 классов защищенности;
- Класс защищенности МЭ определяет класс защищенности **АС**, при котором обеспечивается безопасное взаимодействие **АС** с внешней средой;

Переход от РД МЭ к РД АС

Соответствие РД МЭ и РД АС:

- для АС 1Д – МЭ 5 класса;
- для АС 1Г – МЭ 4 класса;
- для АС 1В – МЭ 3 класса;
- для АС 1Б – МЭ 2 класса;
- для АС 1А – МЭ 1 класса;

С 2016 года ЗОСРВ «Нейтрино» включает в себя программный комплекс межсетевого экранирования ПК МЭ на базе пакетного фильтра PF для аппаратных платформ ARMLE, ARMLE-V7, MIPSBE, MIPSLE, PPCBE, PPCBE-SPE.

С 1 декабря 2016 года сертификация средств межсетевого экранирования в системе сертификации ФСТЭК будет выполнятся только на соответствие новым требованиям, на основе стандарта «Общие критерии».

Программный комплекс межсетевого экранирования

Компоненты, входящие в состав ПК МЭ:

- библиотеки **lsm-pf-v4-ksz.so**, **lsm-pf-v6-ksz.so** – поддержка базовых функций ПК МЭ;
- библиотека **lsm-nlf-ksz.so** – поддержка фильтрации на канальном и сетевом уровнях;
- библиотека **af_http.so** – поддержка фильтрации на прикладном уровне;
- утилита управления пакетным фильтром **pfctl_ksz**;
- сервис регистрации фильтруемых пакетов **pflogd_ksz**;
- утилита чтения журнала событий **pf_auditprinter_ksz**;
- утилита сигнализации попыток нарушения правил фильтрации **pf_auditnotifier_ksz**.

Программный комплекс межсетевого экранирования

Основные функции ПК МЭ:

- Фильтрация на сетевом, транспортном, прикладном, канальном уровне. В т.ч. Qnet, IPX (и др. по признаку EtherType), по MAC-адресу, по содержимому кадра;
- Трансляция сетевых адресов (NAT);
- Идентификация/аутентификация администратора МЭ;
- Регистрация и учет фильтруемых пакетов, а также устанавливаемых соединений;
- Регистрация действий администратора МЭ;
- Сигнализация нарушений правил фильтрации;
- Контроль целостности компонентов МЭ.

Обновления ЗОСРВ «Нейтрино»

Основные обновления ЗОСРВ «Нейтрино», включенные в состав КСЗ (помимо ПК МЭ):

- Поддержка **ГОСТ 34.11-2012 -** замена устаревшего алгоритма подсчета КС ГОСТ 34.11-94 и хэширование паролей в подсистеме и/а по новому стандарту;
- Ограничено количество попыток входа в систему;
- Добавлена возможность блокировки системы при бездействии пользователя и по комбинации клавиш (хранитель экрана);
- Улучшена функциональность менеджера аудита безопасности (в т.ч. запись журнал аудита блоками заданного размера);
- Часть событий записывает PID в журнал аудита;
- Улучшена функциональность КЦ и панели управления КСЗ.

Обновления ЗОСРВ «Нейтрино»

Основные обновления ЗОСРВ «Нейтрино», включенные в состав базовых компонентов:

- Поддержка аппаратных платформ ARMLE-V7 и PPCBE-SPE;
- Поддержка загрузки PXE для bootpd;
- Добавлена виртуальная клавиатура для Photon;
- Добавлены графические драйверы: devg-haswell.so, devg-lx800.so, devg-ruby.so, devg-radeonhd.so, devg-valleyview.so, часть других обновлена;
- Обновлен сетевой стек и часть сетевых драйверов;
- Обновлены системные утилиты (например, awk, patch, tar, fdisk и др.);
- Исправлены часовые пояса.

Обновления ЗОСРВ «Нейтрино»

Основные обновления ЗОСРВ «Нейтрино», включенные в установочный диск:

- Обновлена библиотека Qt (версия 4.8.7 и 5.5.0 вместо 4.7.1);
- Включен браузер Qupzilla версии 1.8.6;
- Включена кроссплатформенная реализация API OpenGL версии 10.3.1 (mesa3d);
- Добавлен мультимедийный фреймворк Gstreamer версии 1.6.0;
- Оптимизирован алгоритм установки компонентов ЗОСРВ «Нейтрино» в автоматизированном режиме;
- Доработана локализация при установке.

Руководящие документы

Стандарт «Общие критерии» (Common Criteria):

- Полное название - общие критерии оценки защищенности информационных технологий;
- Стандарт не предъявляет требований к конкретному типу средства защиты – используется совокупность требований безопасности ИТ «на все случаи жизни»;
- Требования безопасности разделяются на функциональные требования (функции безопасности - и/а, аудит и т.д.) и требования доверия (разработка, тестирование, эксплуатация и т.д.)
- Национальный стандарт на основе общих критериев:

- ГОСТ Р ИСО/МЭК 15408-01 – введение и общая модель;
- ГОСТ Р ИСО/МЭК 15408-02 – функциональные требования;
- ГОСТ Р ИСО/МЭК 15408-03 – требования доверия;

Классы функциональных требований безопасности:

FAU – аудит безопасности;

FCO – безопасность связи (неотказуемость приема-передачи);

FCS – криптография;

FDP – защита данных пользователя;

FIA – идентификация и аутентификация;

FMT – управление безопасностью (группы, роли, права);

FPR – приватность;

FPT – защита функций безопасности;

FRU – использование ресурсов (отказоустойчивость);

FTA – доступ к объекту оценки (управление сеансами);

FTP – доверенный маршрут (канал);

Руководящие документы

Профиль защиты (ПЗ) и задание по безопасности (ЗБ):

- ПЗ представляет собой набор требований по безопасности из списка функциональных требований ГОСТ Р ИСО/МЭК 15408-02;
- Профиль может быть разработан как для конкретного продукта, так и для отдельной подсистемы защиты или класса продуктов (ОС, САВЗ, МЭ и т.д.);
- Механизмы защиты, описанные в профиле, называются функциями безопасности объекта (ФБО)
- Профиль защиты может быть разработан самостоятельно и зарегистрирован в регистрационном органе;
- Существуют уже разработанные ФСТЭК профили защиты;
- При сертификации системы разработчиком предоставляется задание по безопасности (ЗБ) – описание того, как требования выбранного профиля защиты реализуются в конкретном продукте.

Профили защиты

Для разработки ПЗ и ЗБ ФСТЭК выпущены следующие документы:

- Руководство по разработке профилей защиты и заданий по безопасности;
- Безопасность информационных технологий. Руководство по формированию семейств профилей защиты;
- Безопасность информационных технологий. Руководство по регистрации профилей защиты;
- Положение по разработке профилей защиты и заданий по безопасности.

Профили защиты

В настоящее время ФСТЭК разработаны профили защиты для следующих средств:

- Средств антивирусной защиты
- Средств доверенной загрузки;
- Систем обнаружения вторжений уровня сети;
- Систем обнаружения вторжений уровня узла;
- Средств контроля подключения съемных МНИ;
- Средств контроля отчуждения (переноса) информации со съемных МНИ;
- Средств межсетевого экранирования;

Готовятся к регистрации профили защиты для операционных систем в защищенном исполнении.

СВД Встраиваемые Системы

SWD Software

Руководящие документы

Профили защиты средств межсетевого экранирования:

- Определены в информационном сообщении «Об утверждении методических документов, содержащих профили защиты межсетевых экранов» ФСТЭК России от 12 сентября 2016 года;
- В части требований к функциям безопасности установлено 6 классов защиты МЭ. Классы 3, 2, 1 могут использоваться в ИС, обрабатывающих ГТ (С, СС, ОВ);
- По функциональному назначению МЭ разделяются на тип А, Б, В, Г, Д

	6	5	4	3	2	1
Тип А	ИТ.МЭ.А6.П3	ИТ.МЭ.А5.П3	ИТ.МЭ.А4.П3	ИТ.МЭ.А3.П3	ИТ.МЭ.А2.П3	ИТ.МЭ.А1.П3
Тип Б	ИТ.МЭ.Б6.П3	ИТ.МЭ.Б5.П3	ИТ.МЭ.Б4.П3	ИТ.МЭ.Б3.П3	ИТ.МЭ.Б2.П3	ИТ.МЭ.Б1.П3
Тип В	ИТ.МЭ.В6.П3	ИТ.МЭ.В5.П3	ИТ.МЭ.В4.П3	ИТ.МЭ.В3.П3	ИТ.МЭ.В2.П3	ИТ.МЭ.В1.П3
Тип Г	ИТ.МЭ.Г6.П3	ИТ.МЭ.Г5.П3	ИТ.МЭ.Г4.П3	-	-	-
Тип Д	ИТ.МЭ.Д6.П3	ИТ.МЭ.Д5.П3	ИТ.МЭ.Д4.П3	-	-	-

Руководящие документы

Профили защиты средств антивирусной защиты:

- Определены в информационном сообщении «Об утверждении требований к средствам антивирусной защиты» ФСТЭК России от 30 июля 2012;
- В части требований к функциям безопасности установлено 6 классов защиты САВЗ. Классы 3, 2, 1 могут использоваться в ИС, обрабатывающих ГТ (С, СС, ОВ);
- По функциональному назначению САВЗ разделяются на тип А, Б, В, Г

	6	5	4	3	2	1
Тип А	ИТ.САВЗ.А6.ПЗ	ИТ.САВЗ.А5.ПЗ	ИТ.САВЗ.А4.ПЗ	ИТ.САВЗ.А3.ПЗ	ИТ.САВЗ.А2.ПЗ	ИТ.САВЗ.А1.ПЗ
Тип Б	ИТ.САВЗ.Б6.ПЗ	ИТ.САВЗ.Б5.ПЗ	ИТ.САВЗ.Б4.ПЗ	ИТ.САВЗ.Б3.ПЗ	ИТ.САВЗ.Б2.ПЗ	ИТ.САВЗ.Б1.ПЗ
Тип В	ИТ.САВЗ.В6.ПЗ	ИТ.САВЗ.В5.ПЗ	ИТ.САВЗ.В4.ПЗ	ИТ.САВЗ.В3.ПЗ	ИТ.САВЗ.В2.ПЗ	ИТ.САВЗ.В1.ПЗ
Тип Г	ИТ.САВЗ.Г6.ПЗ	ИТ.САВЗ.Г5.ПЗ	ИТ.САВЗ.Г4.ПЗ	ИТ.САВЗ.Г3.ПЗ	ИТ.САВЗ.Г2.ПЗ	ИТ.САВЗ.Г1.ПЗ

Программный комплекс антивирусной защиты (ПК АВЗ):

- Функционирует под управлением ЗОСРВ «Нейтрино» КПДА.10964-01 и ЗОСРВ «QNX» КПДА.00002-01;
- Имеет децимальный номер КПДА.94201-01;
- Сертифицирован по общим критериям на соответствие требованиям профиля защиты ИТ.САВЗ.Б2.ПЗ, а также по второму уровню контроля отсутствия НДВ и на соответствие реальных и декларируемых в документации функциональных возможностей.
- Соответствует требованиям приказа №058 МО РФ
- Может применяться на серверах сетевых информационных систем.

Доверенная загрузка

Аппаратные средства доверенной загрузки:

- ❑ Загрузка ОС только с установленных носителей (запрет загрузки с Live CD, с USB и т.д.);
- ❑ Контроль целостности СЗИ и/или ОС до загрузки ОС;
- ❑ Авторизация пользователей (в т.ч. с помощью аппаратных ключей) до загрузки ОС;
- ❑ Регистрация попыток входа в систему;
- ❑ Блокирование входа в систему;
- ❑ Восстановление разделов, шифрование разделов, маскирующее удаление информации;
- ❑ Администрирование СЗИ НСД.

Доверенная загрузка

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.

Доверенная загрузка

Интеграция ЗОСРВ «Нейтрино» с АПКДЗ «Тверца Зетта М»:

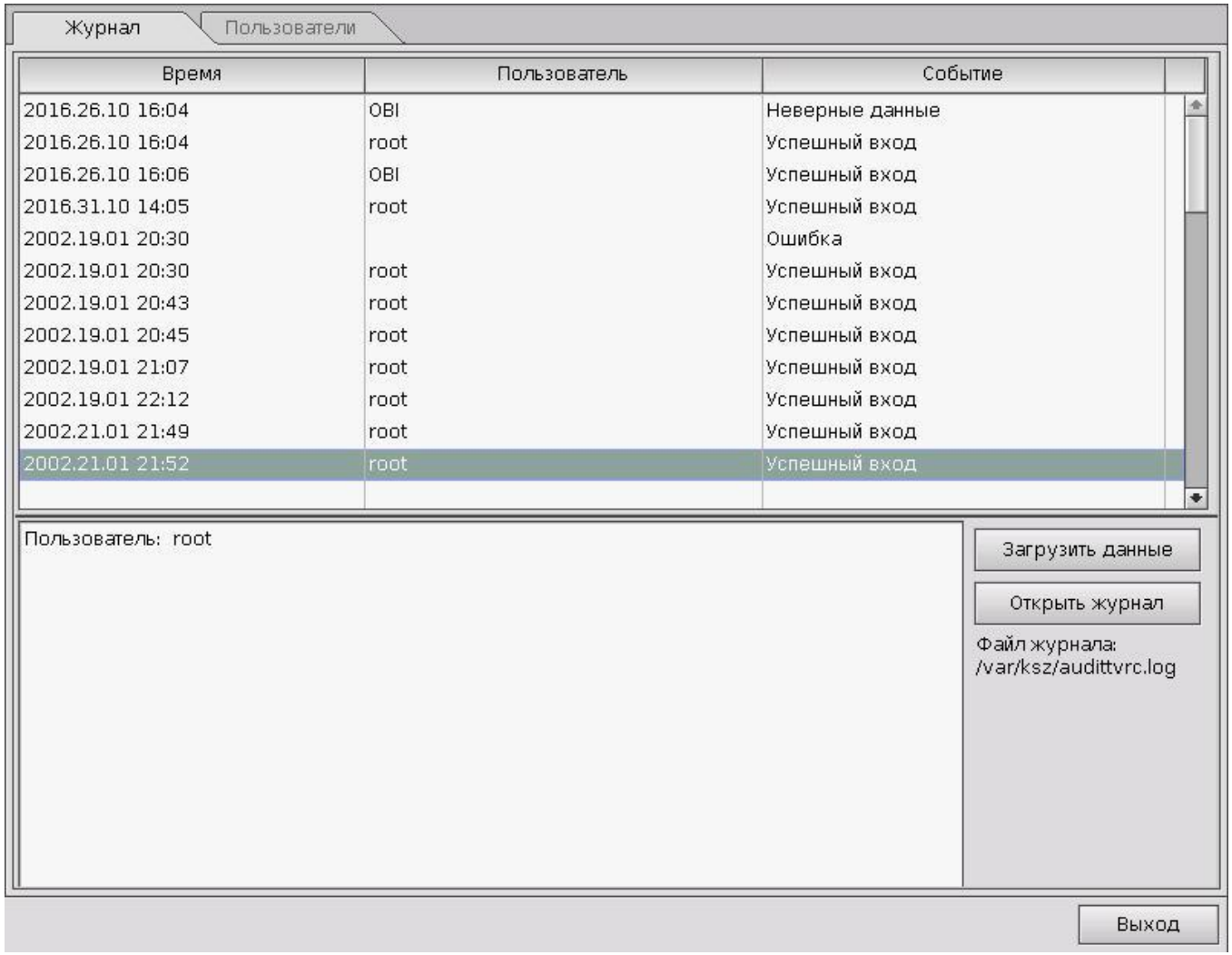
- Сквозная авторизация пользователей (передача данных авторизации от контроллера Тверца-2 подсистеме и/а ЗОСРВ «Нейтрино»);
- Чтение журнала событий безопасности контроллера Тверца-2 в среде ЗОСРВ «Нейтрино»;
- Управление пользователями контроллера Тверца-2 в среде ЗОСРВ «Нейтрино»;
- Добавление пользователей 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**;
- графическая утилита работы с журналом событий и учетными записями пользователей (панель управления Тверца-2, ПУ Тверца-2) **tvrc_cam**;

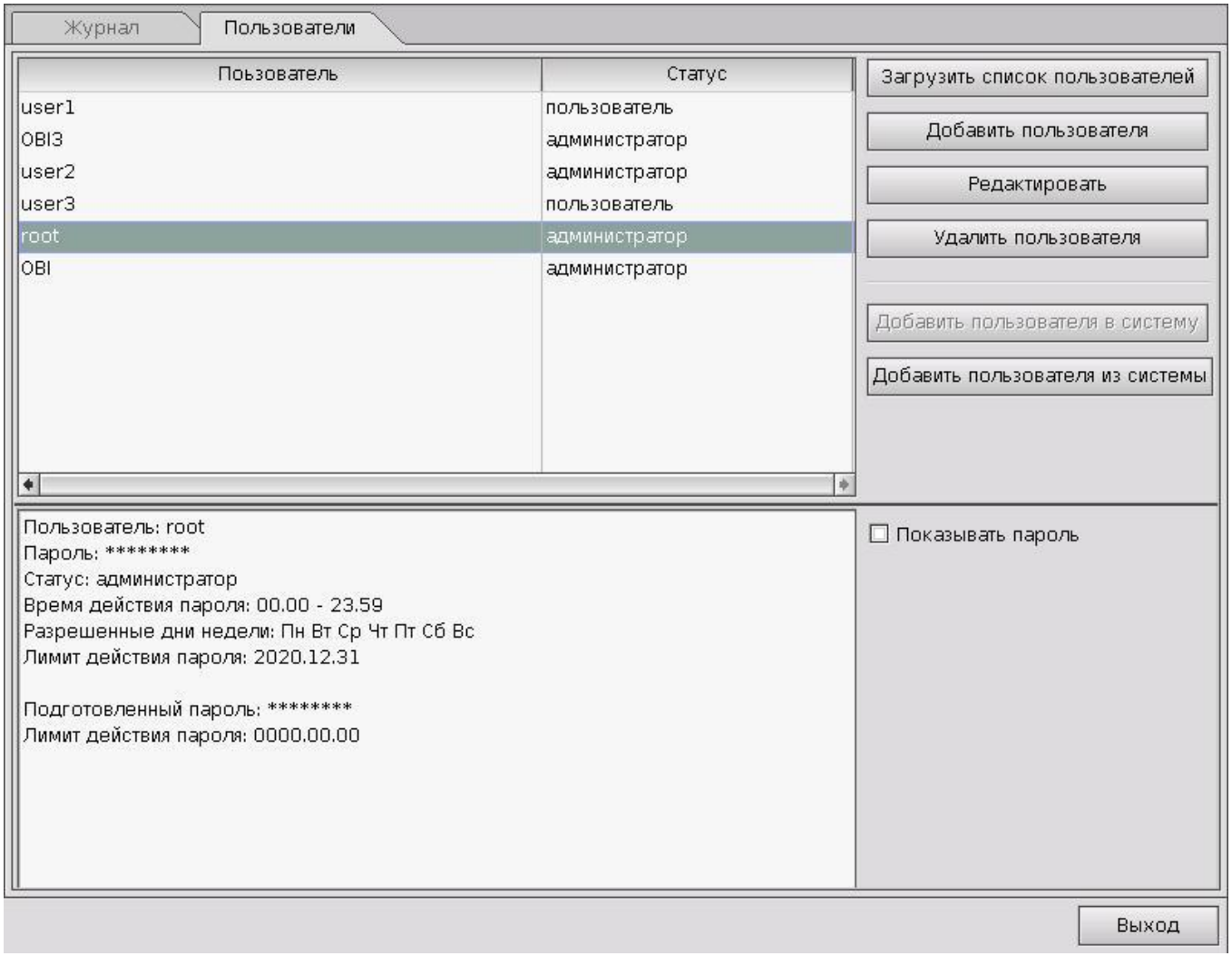
Журнал событий контроллера «Тверца-2»



СВД Встраиваемые Системы

SWD Software

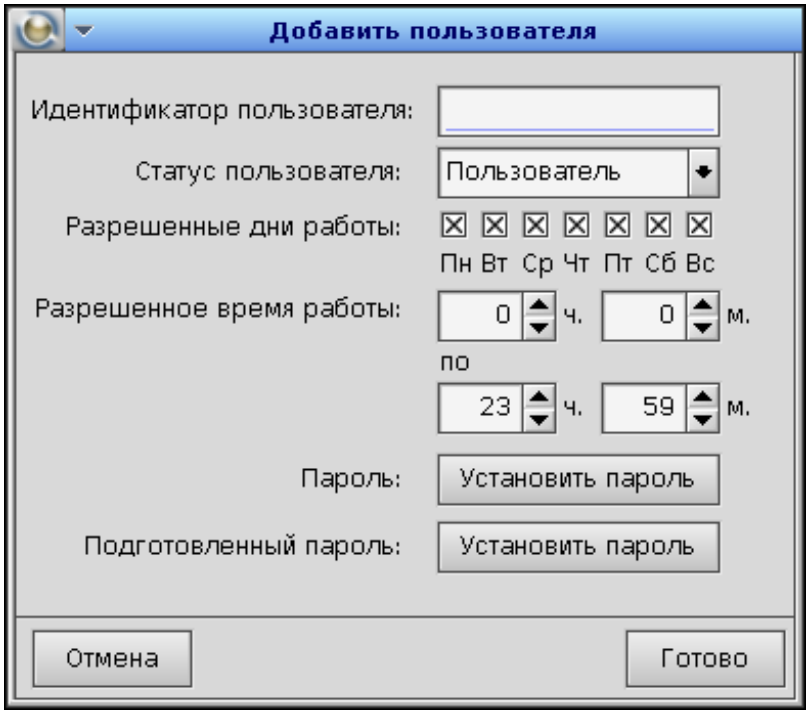
Управление пользователями контроллера «Тверца-2»

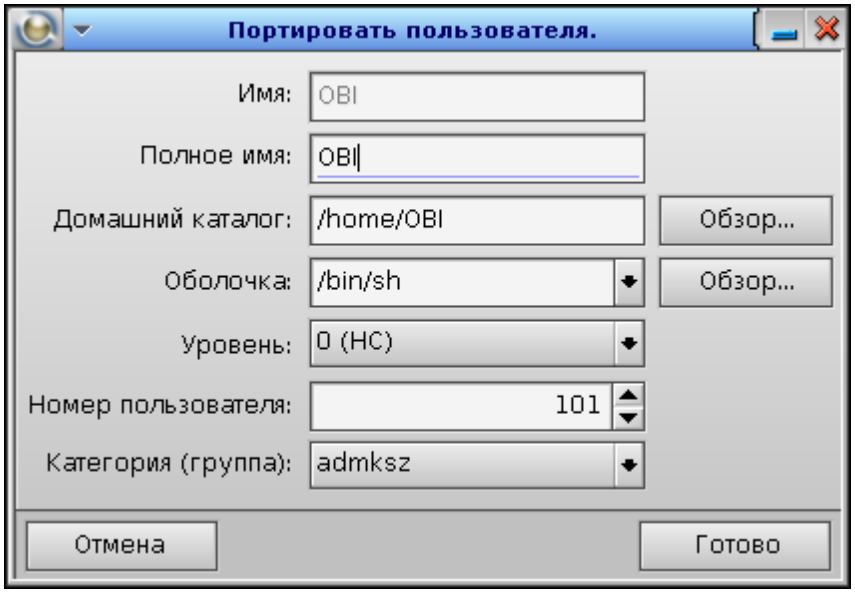


СВД Встраиваемые Системы

SWD Software

Управление пользователями контроллера «Тверца-2»





СВД Встраиваемые Системы

SWD Software

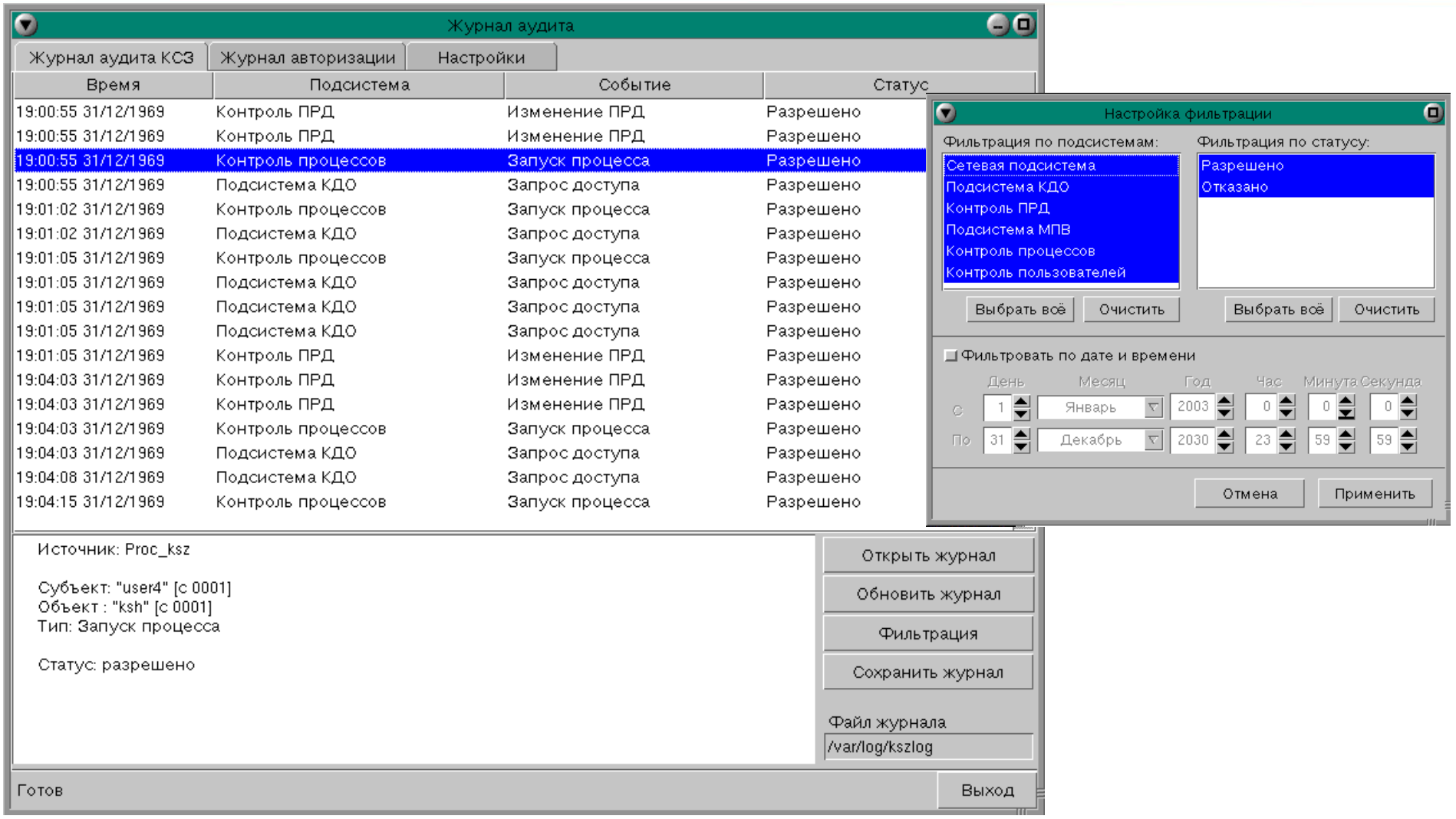
ЗОСРВ «QNX» КПДА.00002-01

В 2017 году планируется проведение инспекционного контроля ЗОСРВ «QNX» КПДА.00002-01

Основные планируемые обновления:

- оптимизация установки целевых систем из архивов дистрибутива;
- добавление опции E0 в микроядро Proc32_ksz;
- работа с журналом событий безопасности в графической оболочке Photon;
- обновление ряда утилит и графических драйверов.

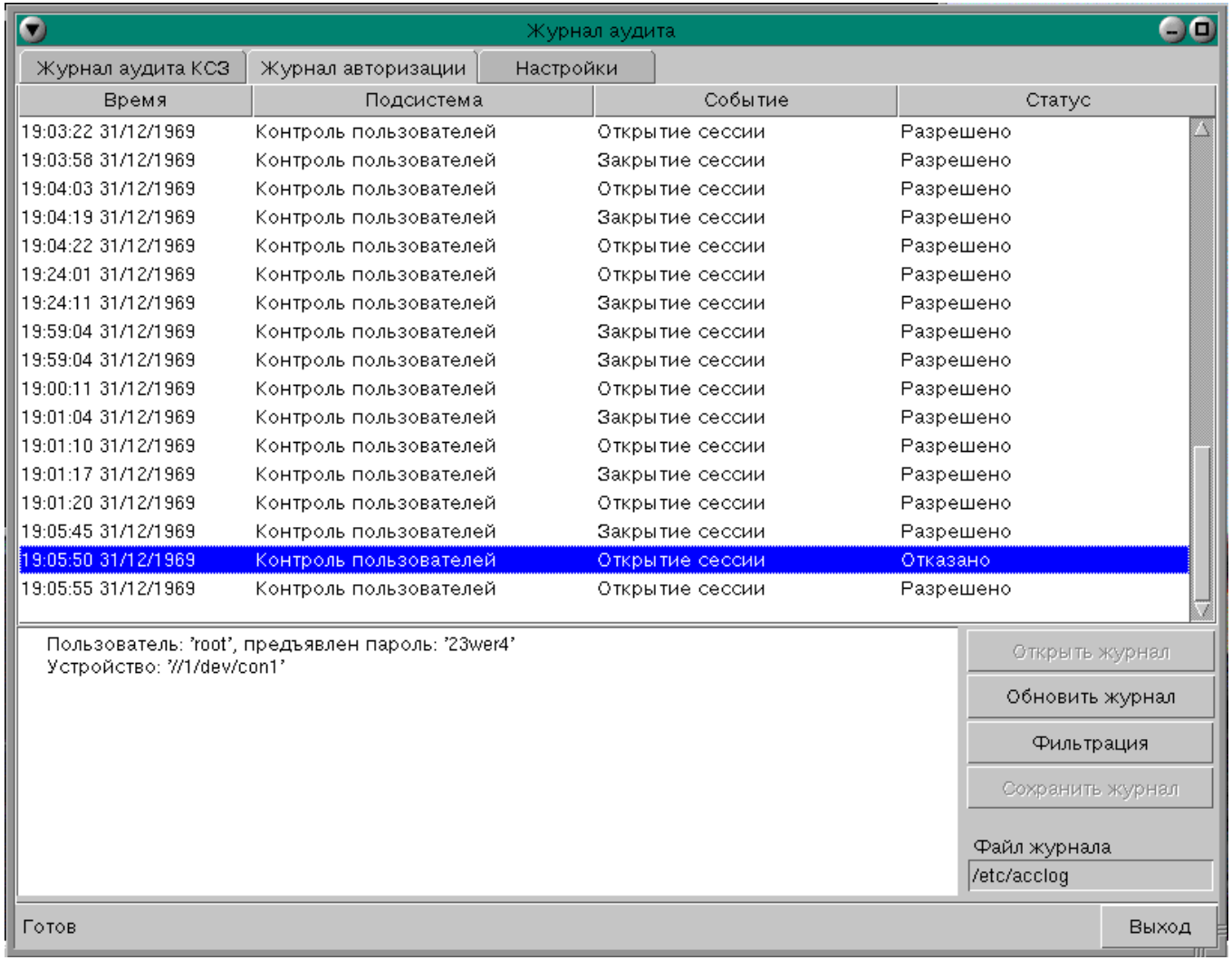
ЗОСРВ «QNX» КПДА.00002-01



СВД Встраиваемые Системы

SWD Software

ЗОСРВ «QNX» КПДА.00002-01



СВД Встраиваемые Системы

SWD Software

Спасибо за внимание

Алексей Ермолинский
Инженер-программист

т. (812) 346-89-56
support@kpda.ru

www.kpda.ru
www.swd.ru

СВД Встраиваемые Системы

SWD Software