Технологии QNX и КПДА в России

Москва, 24 апреля 2019

«Новые требования безопасности информации к ОС и их реализация в ЗОСРВ «Нейтрино»

Алексей Ермолинский, ООО «СВД Встраиваемые Системы»

СВД Встраиваемые Системы

SWD Software

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;

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 ГОСТ Р 57628-2017;
- 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;
- Операционных систем в защищенном исполнении.

Руководящие документы

Требования безопасности к ОС:

- Утверждены приказом ФСТЭК России от 19 августа 2016 г. № 119;
- Установлено 6 классов защиты ОС. Классы 3, 2, 1 могут использоваться в ИС, обрабатывающих ГТ (С, СС, ОВ);
- По функциональному назначению ОС разделяются на тип А, Б, В – ОС общего назначения, встраиваемая ОС, ОС реального времени

	6	5	4	3	2	1
Тип А	ИТ.ОС.А6.П3	ИТ.ОС.А5.П3	ИТ.ОС.А4.П3	ИТ.ОС.А3.П3	ИТ.ОС.А2.П3	ИТ.ОС.А1.П3
Тип Б	ИТ.ОС.Б6.П3	ИТ.ОС.Б5.П3	ИТ.ОС.Б4.П3	ИТ.ОС.Б3.П3	ИТ.ОС.Б2.П3	ИТ.ОС.Б1.П3
Тип В	ИТ.ОС.В6.П3	ИТ.ОС.В5.П3	ИТ.ОС.В4.П3	ИТ.ОС.В3.П3	ИТ.ОС.В2.П3	ИТ.ОС.В1.П3

Функциональные требования

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);

Требования доверия

Классы (семейства) требований доверия:

ADV_ARC – архитектура безопасности;

ADV_FSP – функциональная спецификация;

ADV_IMP – представление реализации;

ADV_SPM – модель политики безопасности;

ALC_FLR – устранение недостатков;

ALC_FPU – обновление ПО;

AGD – руководства по эксплуатации;

ATE – тестирование;

AVA_VAN – анализ уязвимостей;

AVA_CCA – анализ скрытых каналов;

AMA_SIA – влияние обновлений на безопасность.

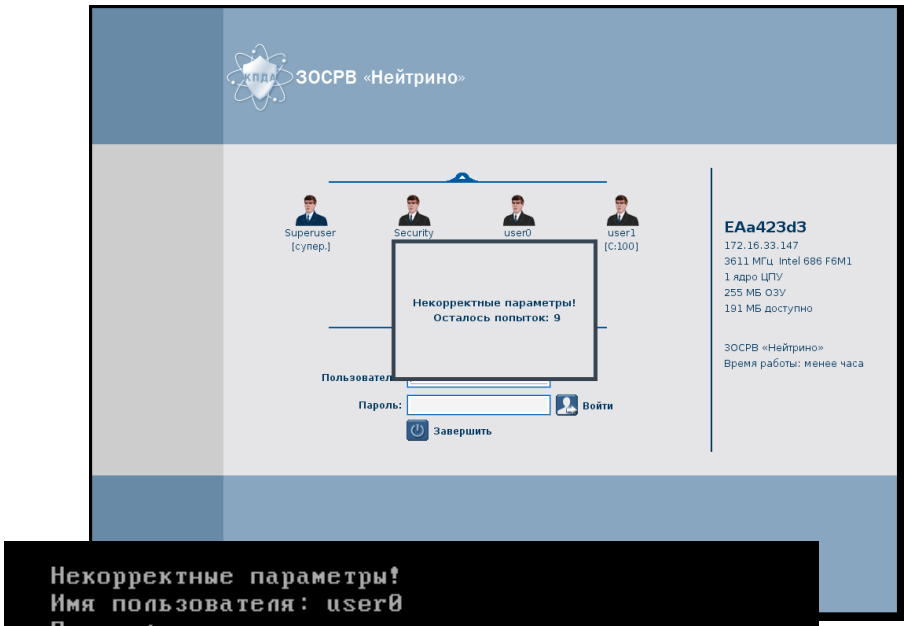
Функции безопасности

В ЗОСРВ «Нейтрино» реализованы следующие функции защиты:

- Идентификация и аутентификация
- Управление доступом;
- Регистрация событий безопасности;
- Ограничение программной среды;
- Изоляция процессов;
- Защита памяти;
- Контроль целостности;
- Обеспечение надежного функционирования;
- Фильтрация сетевого потока;
- Маркирование документов

Идентификация и аутентификация

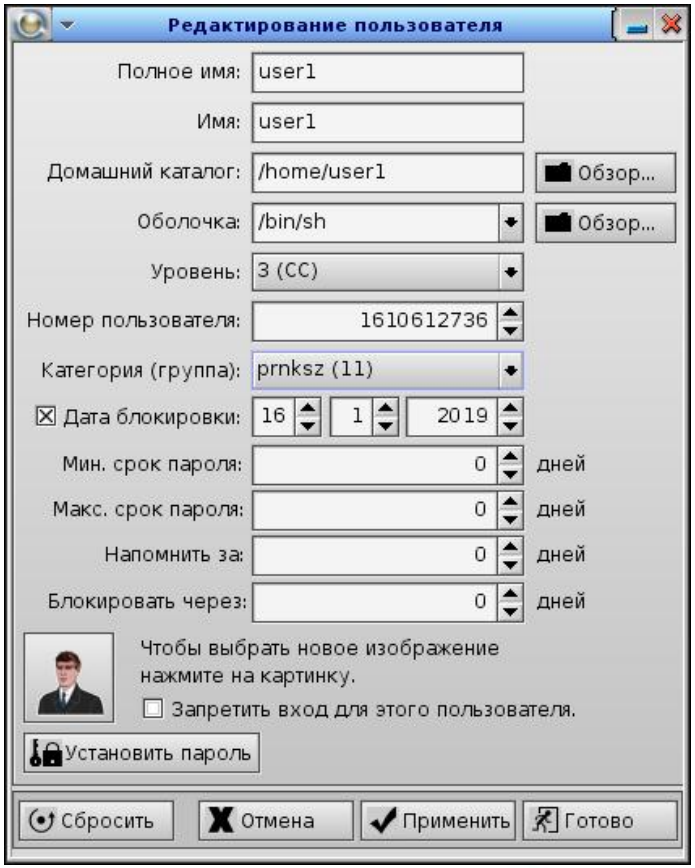
Блокирование и срок действия учетной записи: Опции –m (количество попыток) и –d (интервал между попытками) для login_ksz и phlogin2_ksz




```
Некорректные параметры!
Имя пользователя: user0
Пароль:

Некорректные параметры!

Вход в систему отклонен!
_
```



СВД Встраиваемые Системы

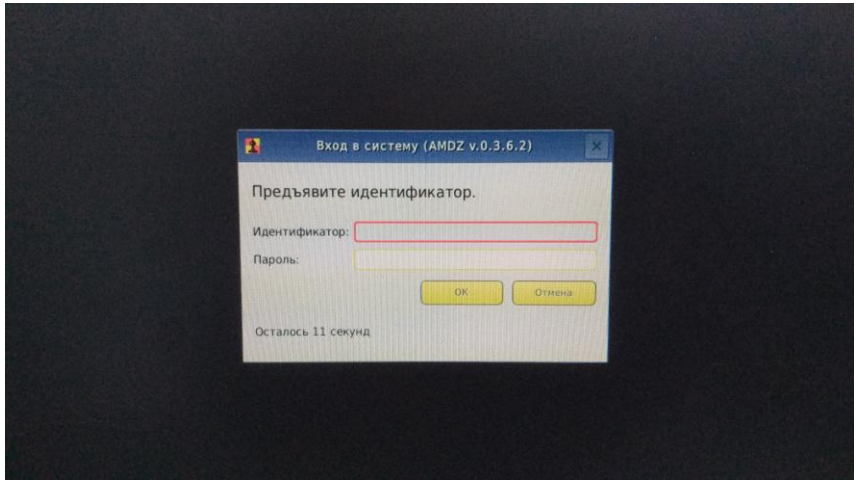
SWD Software

Идентификация и аутентификация

Двухфакторная аутентификация (FIA_UAU.5):

Использование персональных идентификаторов, например, «Шипка».

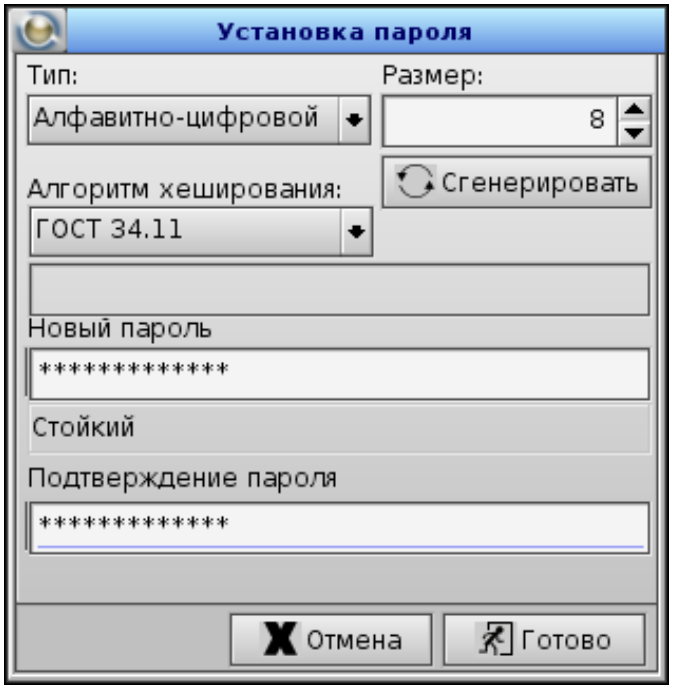
Факторы:
- знание (пароль);
- владение (USB-ключ);



Идентификация и аутентификация

Верификация секретов:

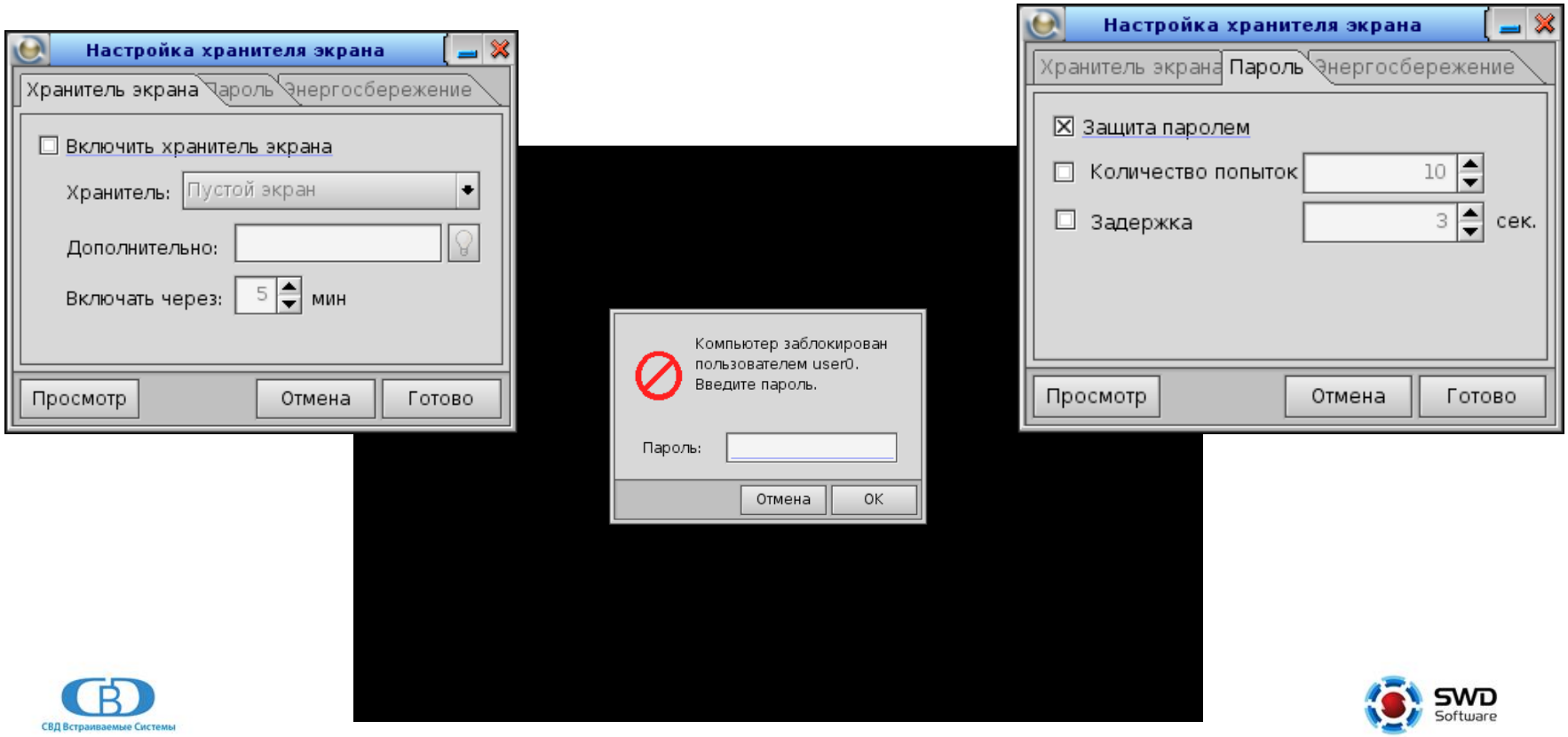
Генерация стойких паролей и проверка на стойкость



Управление доступом

Блокирование интерактивных сеансов:

Использование «хранителя экрана» при достижении интервала времени бездействия или принудительно



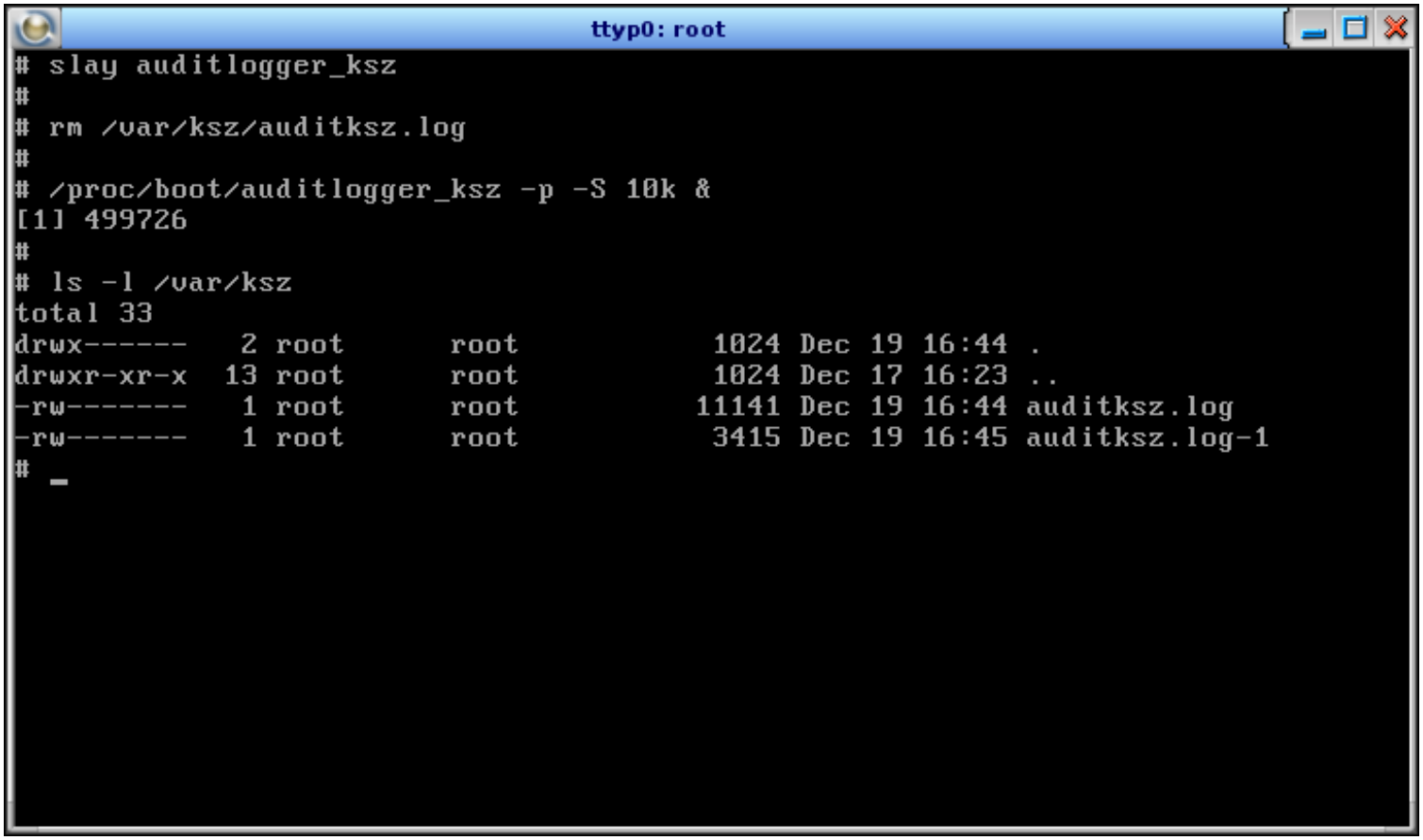
СВД Встраиваемые Системы

SWD Software

Регистрация событий безопасности

Действия при переполнении журнала:

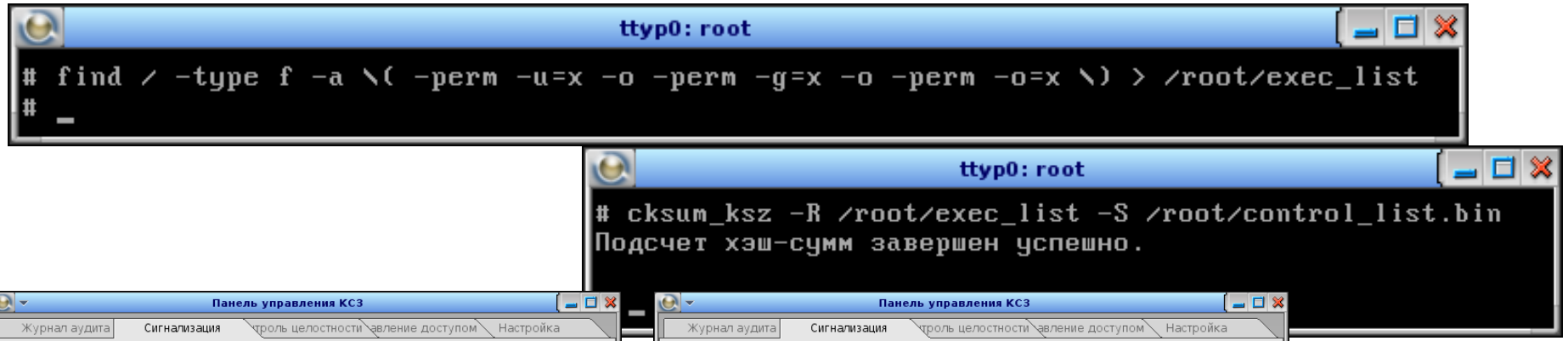
Опции –S (размер) и –p (разбивать на блоки) менеджера аудита auditlogger_ksz

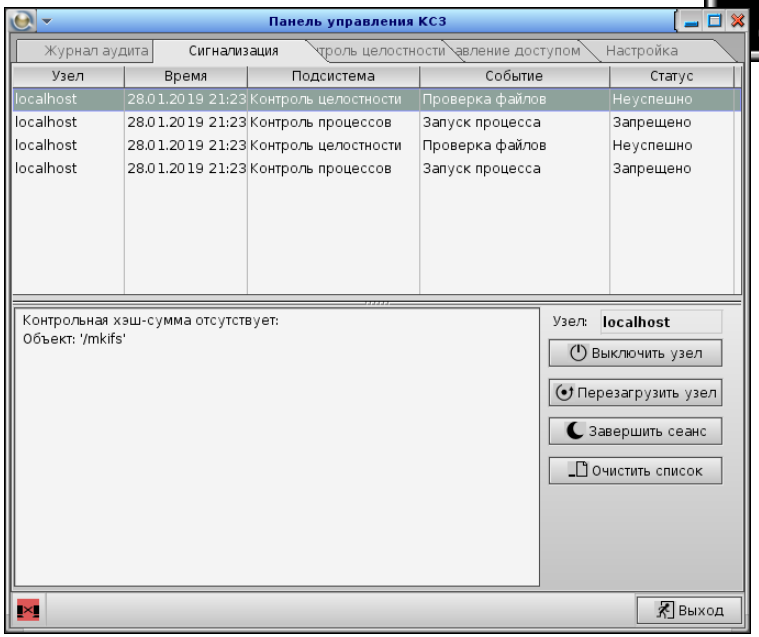


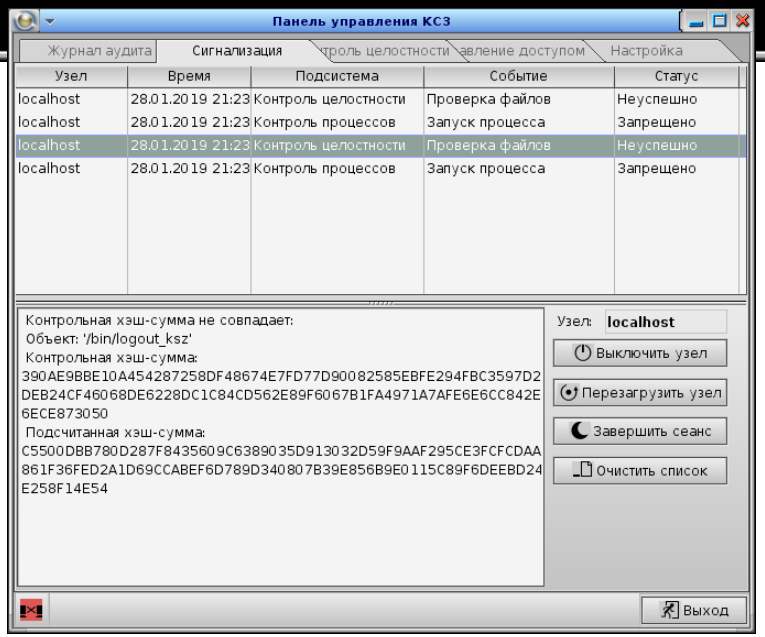
SWD Software

Ограничение программной среды

Перечень компонентов для запуска:
Опция –е микроядра и менеджера процессов procnto-*-ksz







SWD Software

Защита памяти

Многократная перезапись стираемых объектов:

Опция clean драйверов fs-qnx4-ksz.so и fs-qnx6-ksz.so

Перезапись байтами AA55
devb-eide blk auto=partition dos exe=all qnx6 clean=AA55 cam quiet

Перезапись псевдослучайным байтом
devb-eide blk auto=partition dos exe=all qnx6 clean=RR cam quiet

Фильтрация сетевого потока

Фильтрация на основе атрибутов безопасности:

- сетевой адрес (блок адресов);
- сетевой порт;
- физический адрес;
- сетевой и транспортный протокол;
- протоколы прикладного уровня;
- содержимое кадра.

Полное управление информационными потоками:

Поддержка в сетевом менеджере io-pkt-ksz меток конфиденциальности (уровень и категория) в соответствии с ГОСТ Р 58256-2018

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