СВД Встраиваемые Системы

Алексей Ермолинский, СВД ВС

Комплекс средств защиты ЗОСРВ «Нейтрино»

Классификация

Изделие КПДА.10964-01 (ЗОСРВ «Нейтрино):

- выполнено согласно РД СВТ по 3-му классу ЗИ от НСД и 2-му уровню контроля отсутствия НДВ;
- имеет сертификат соответствия №1740 от 20.12.2011;
- отвечает требованиям приказа №058 МО РФ;
- позволяет создавать АС класса защищенности до 1Б включительно.

Классификация

Класс защищенности 1Б это:

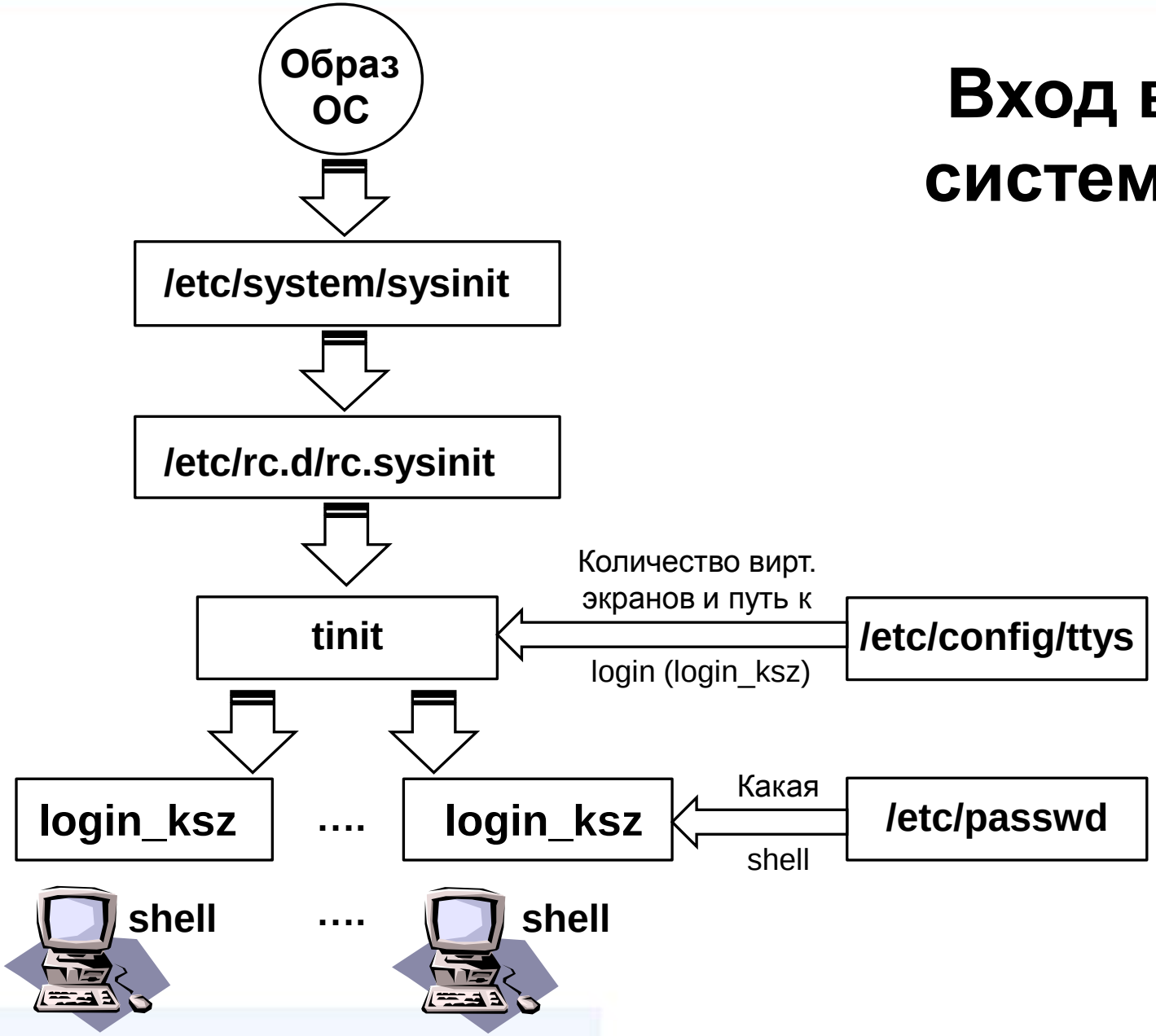
- СВТ не ниже 3-го класса;
- обработка информации, содержащей ГТ;
- уровень конфиденциальности – до СС;
- одновременно обрабатывается от НС до СС;
- не все пользователи имеют доступ ко всей информации.

СВД Встраиваемые Системы

Подсистемы КСЗ

Подсистема управления доступом

Вход в систему



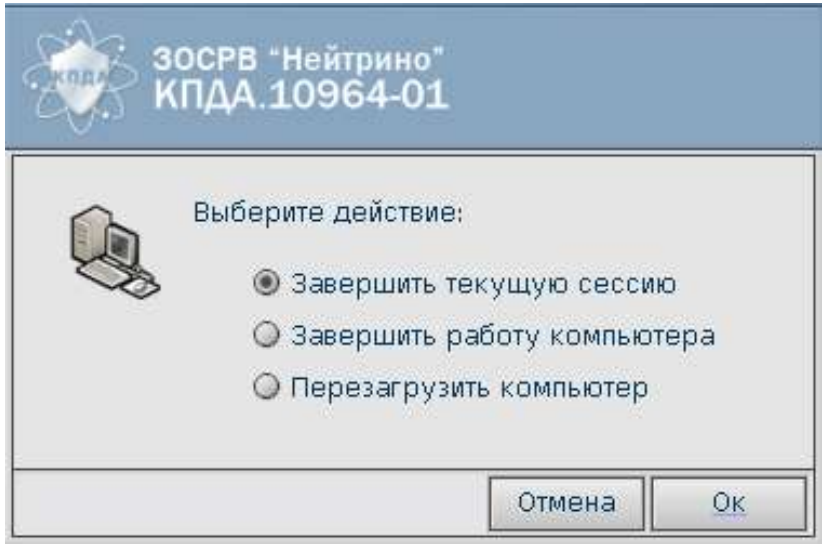
Вход в систему

- графическая утилита, реализующая вход в систему пользователей в сессии Photon;

- осуществляет регистрацию событий входа в журнале аудита КСЗ;
- есть консольный аналог.

Выход из системы

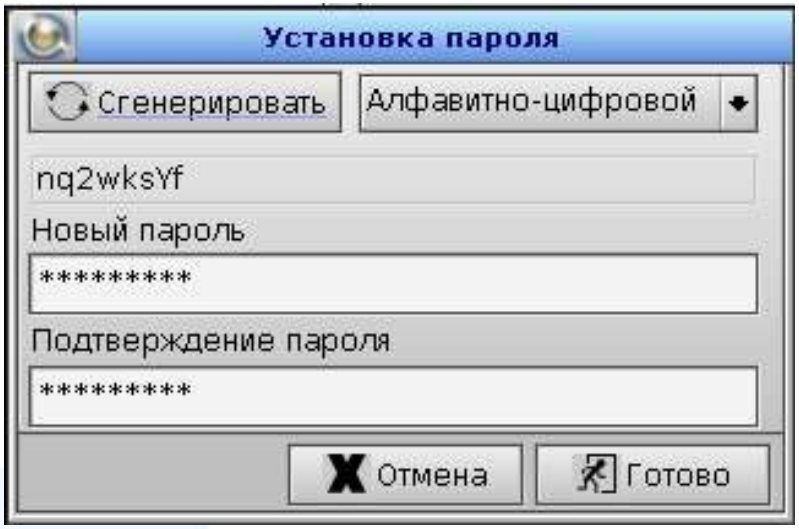
- графическая утилита, реализующая закрытие сессии Photon (выход из системы);



- осуществляет регистрацию событий выхода в журнале аудита КСЗ;
- есть консольный аналог.

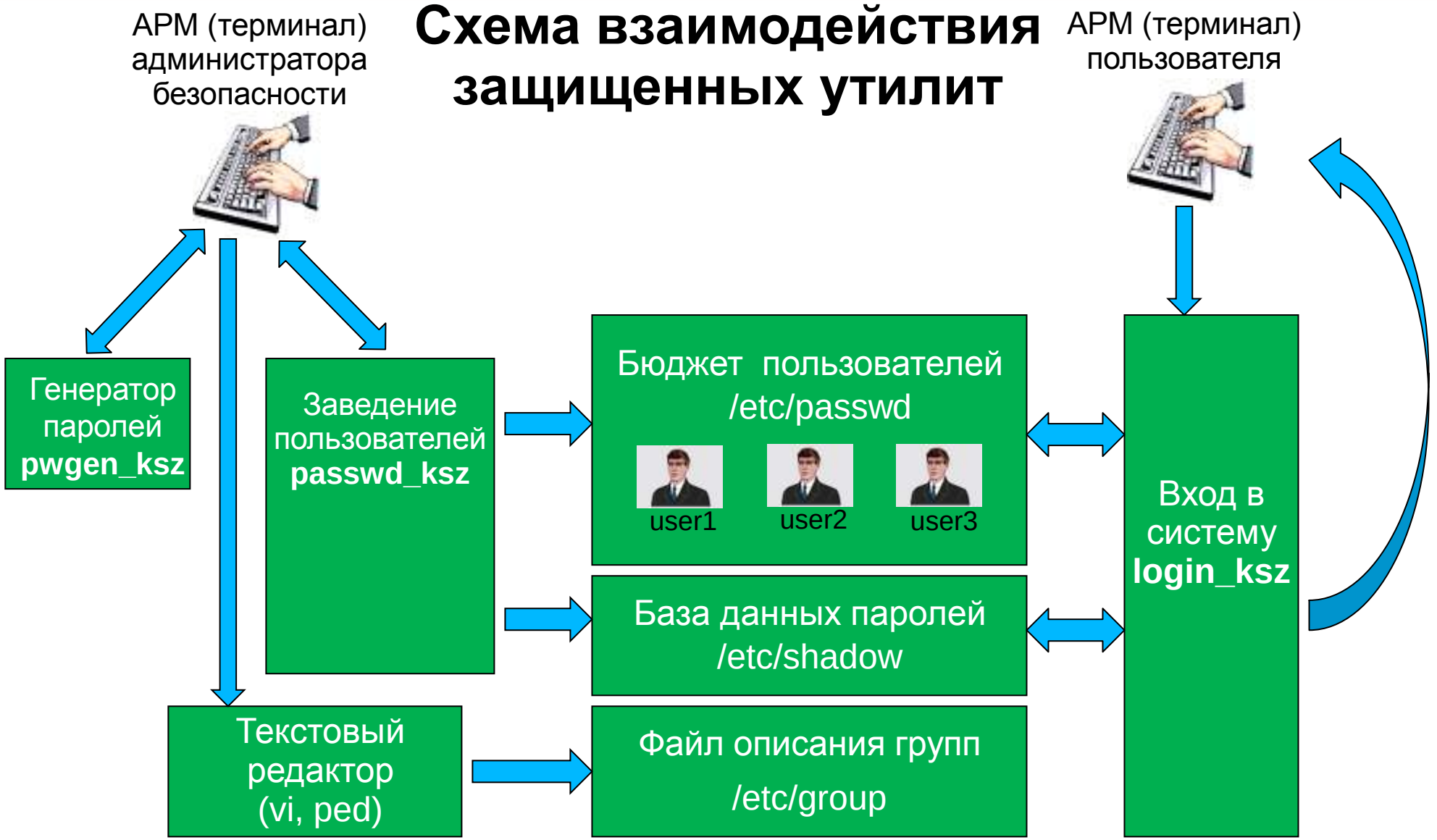
Парольная политика

- Пароли пользователей – не менее 8-ми символов;
- Генерация паролей трех уровней сложности:
  - ✓ простые (только цифры);
  - ✓ средней сложности (цифры и символы);
  - ✓ повышенной сложности (с использованием спецсимволов).



Подсистема управления доступом

Схема взаимодействия защищенных утилит

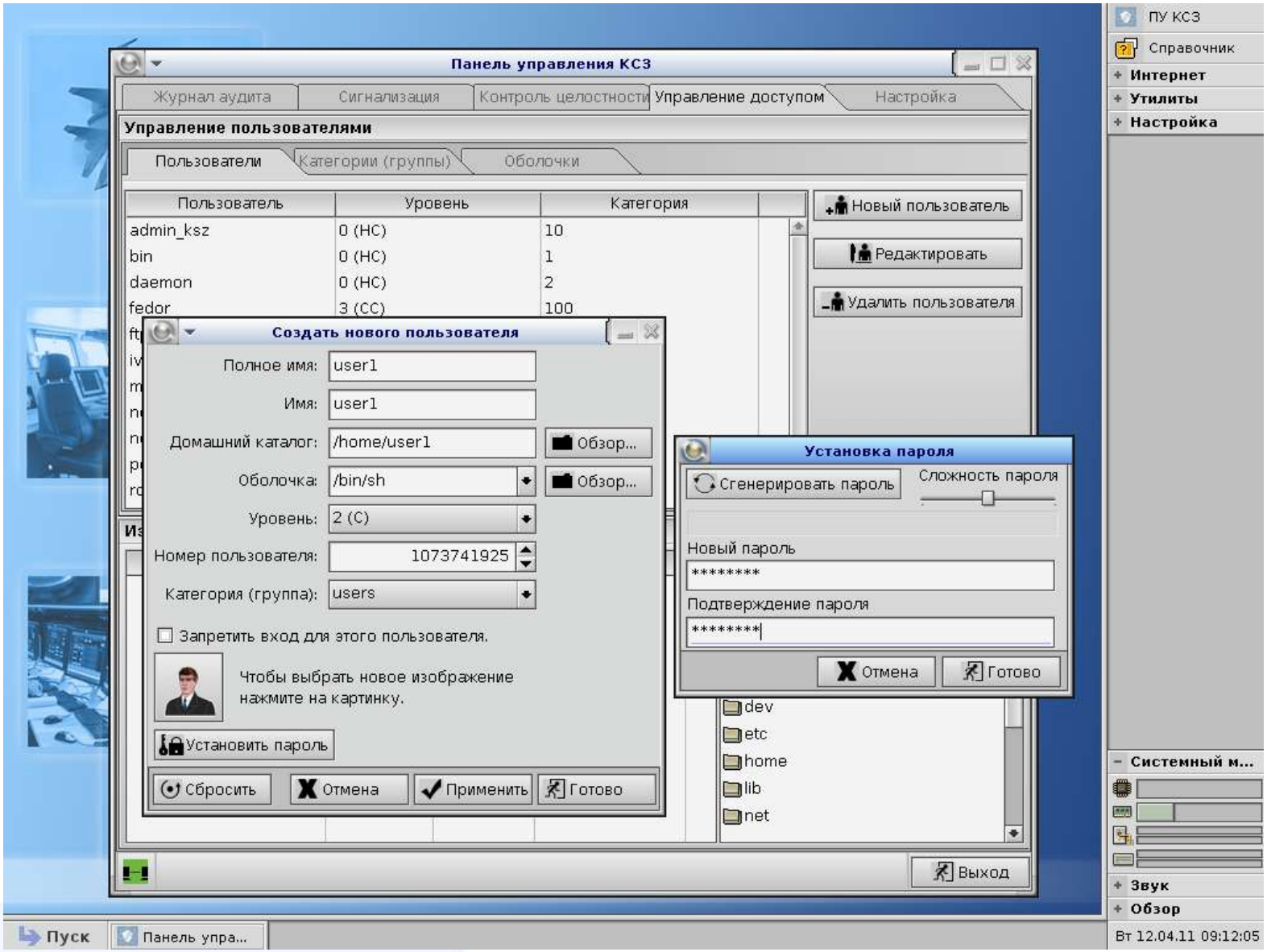


Идентификация объектов

- идентификация ЭВМ – по имени хоста (hostname), IP-адресу и/или имени узла (дескриптору);
- идентификация узлов сети ЭВМ – по имени узла (дескриптору);
- идентификация каналов связи – по номеру интерфейса (en0, en1 и т.д.) или MAC-адресу;
- внешних устройств – по Device ID;
- программ, файлов, каталогов и т.д. по именам.

Подсистема управления доступом

Субъекты матрицы доступа



Идентификаторы процесса (пользователя)

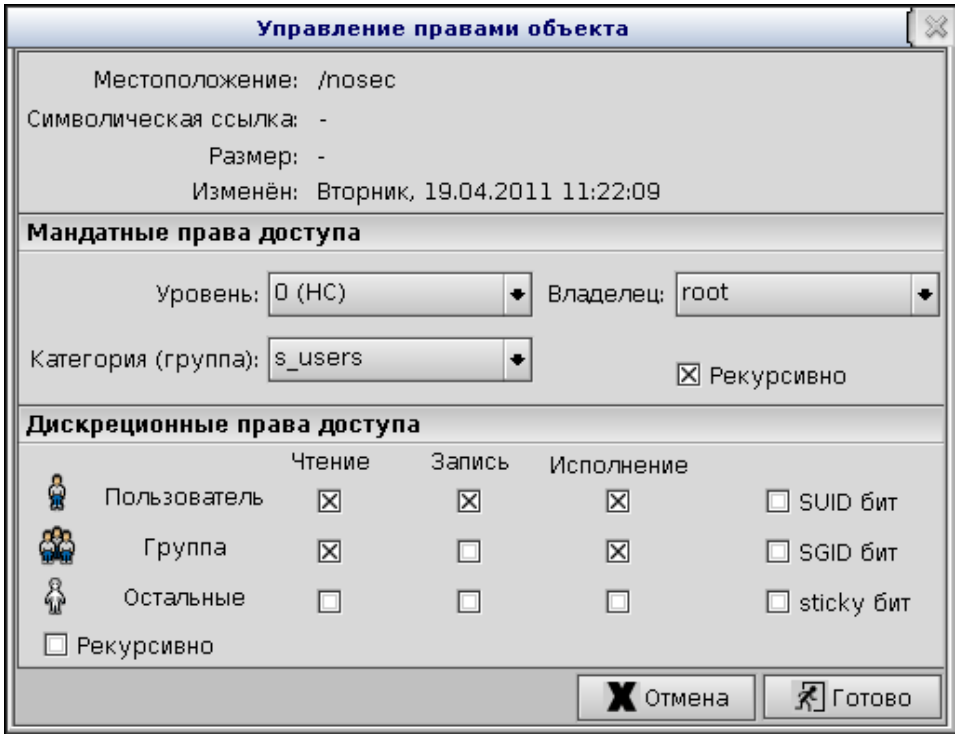
- Реальный идентификатор пользователя (uid)
- Реальный идентификатор группы (gid)
- Эффективный идентификатор пользователя (euid)
- Эффективный идентификатор группы (egid)

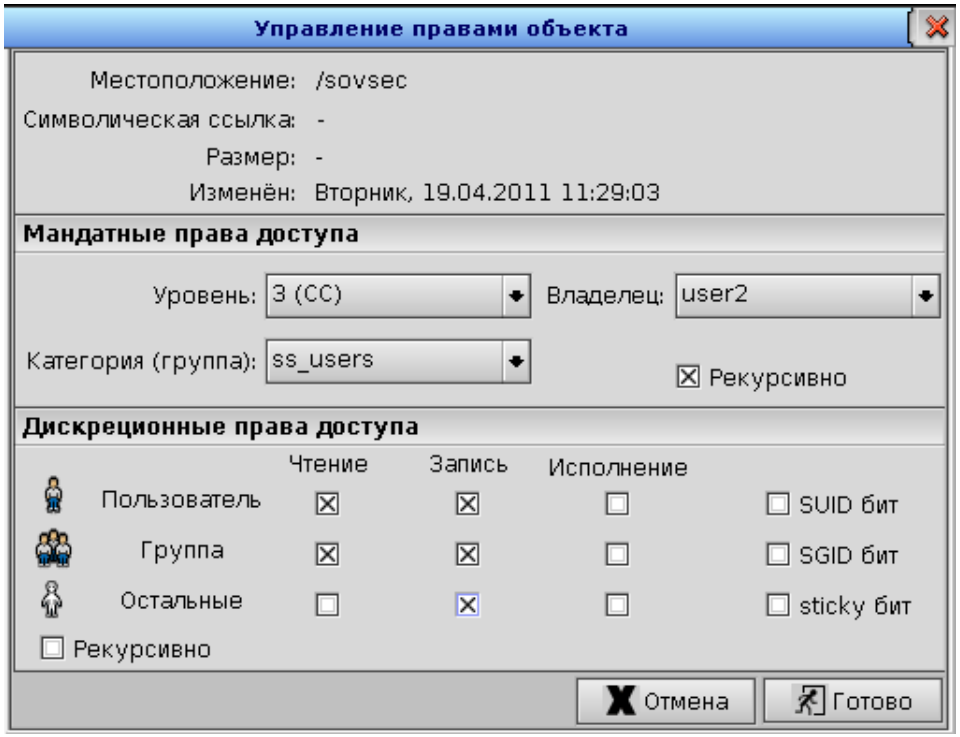
Структура st_mode

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Тип файла				Set uid	Set gid	reserved	r	w	x	r	w	x	r	w	x
							владелец			группа			остальные		

Подсистема управления доступом

Права доступа объектов





Подсистема управления доступом

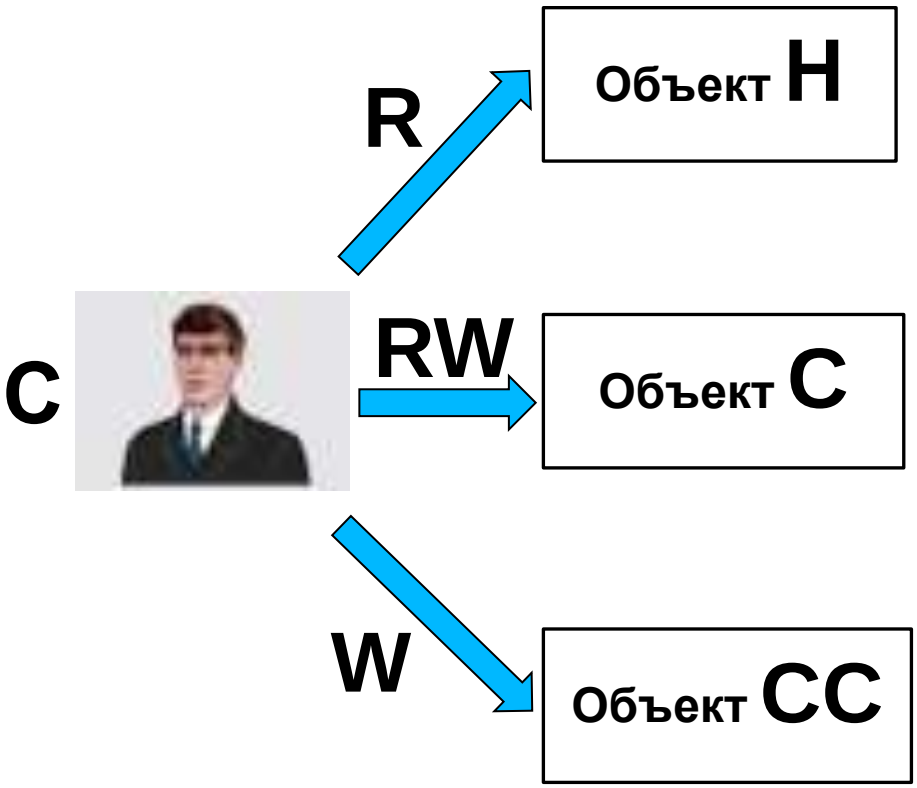
Управление потоками осуществляется с помощью:

- уровней доверия субъектов (пользователей, процессов, программ). Определяются идентификатором пользователя;
- меток конфиденциальности объектов. Определяются идентификатором пользователя-владельца объекта.

Уровень доверия	Условное наименование	Значение uid/euid
0 (минимальный)	Несекретно	1-536870911
1	ДСП	536870912-1073741823
2	С	1073741824-1610612735
3 (максимальный)	СС	1610612736-2147483647

Подсистема управления доступом

Права доступа к объектам с различными грифами при условии совпадения групповой принадлежности



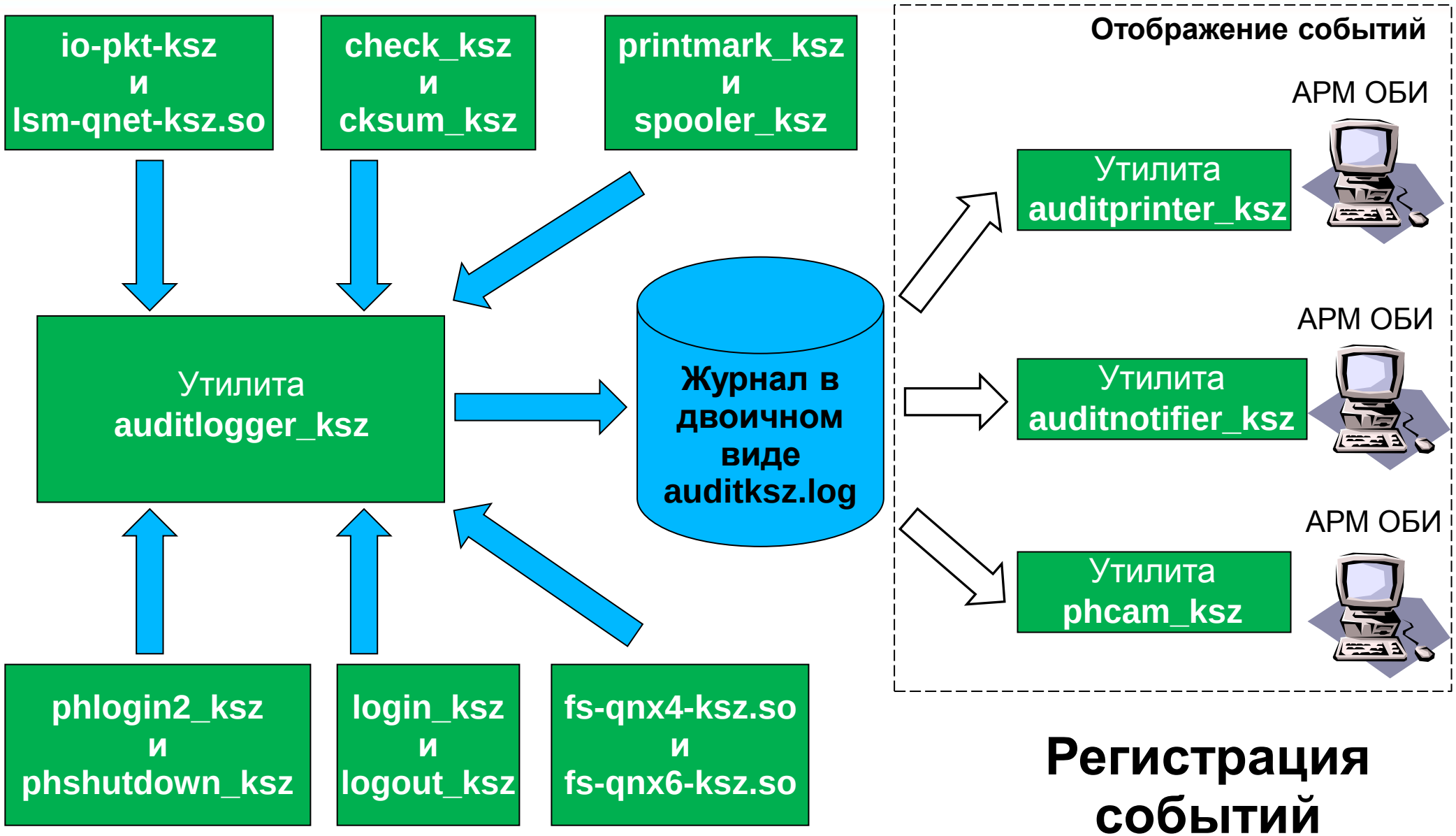
Правила управления потоками информации:

- субъект имеет право на **чтение** объекта, только если уровень допуска субъекта не ниже грифа объекта **и** список групп субъекта включает в себя группу (в т.ч. тематическую маску субъекта)

- субъект имеет право на **запись** в объект, только если уровень допуска субъекта не выше, чем гриф объекта и группа субъекта совпадает с группой объекта

СВД Встраиваемые Системы

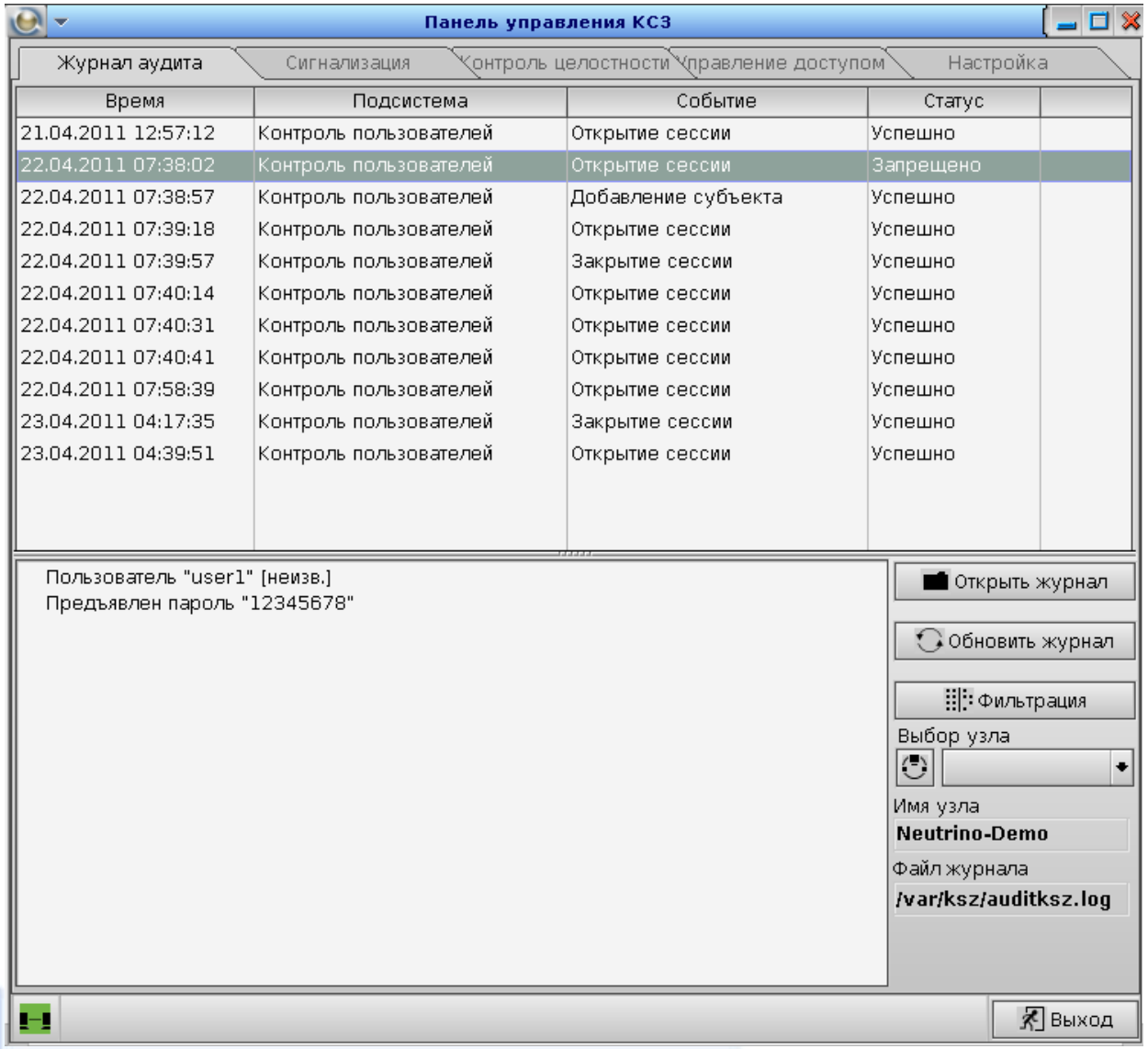
Подсистема регистрации и учета

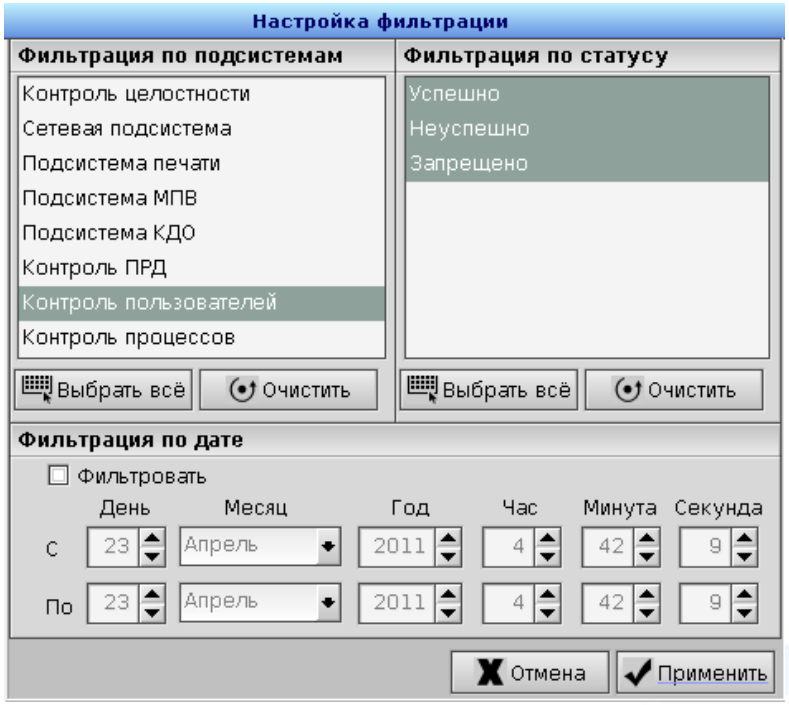


Регистрация событий безопасности

Подсистема регистрации и учета

Вход/выход





СВД Встраиваемые Системы

Подсистема регистрации и учета

АРМ ОБИ

АРМ исполнителя

АРМ ОБИ

Текстовый редактор (файл)

Журнал аудита

/etc/printers конф.

Менеджер печати spooler_ksz

/etc/group, phcam_ksz

АРМ ОБИ

Пользователь имеет права
И маркировка включена

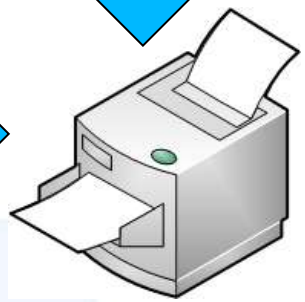
Учетные реквизиты КСЗ

Фильтр печати printmark_ksz

Пользовательские учетные реквизиты

АРМ печати

Драйвер принтера (devu-prn)

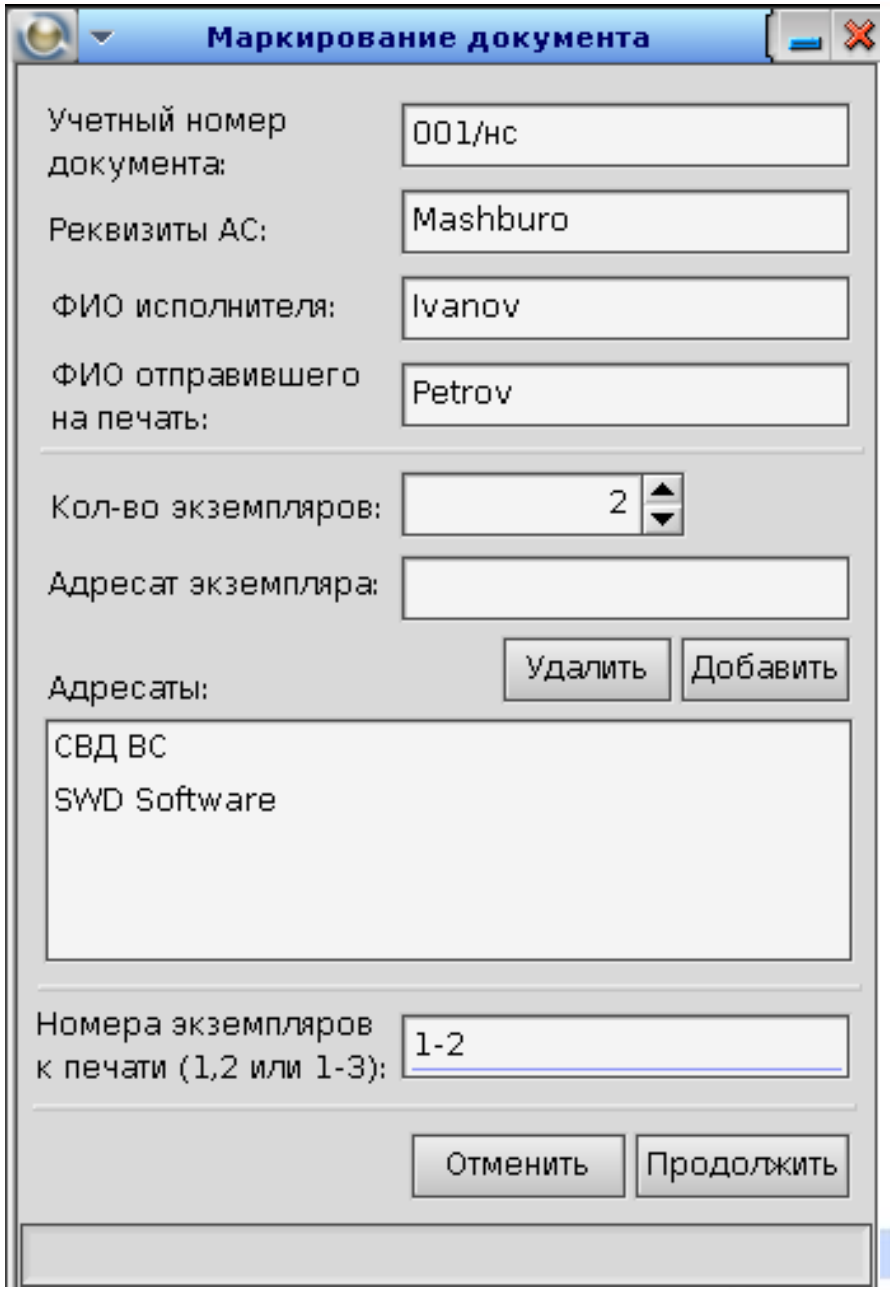


АДРЕС 1,
АДРЕС 2,
АДРЕС N

Подсистема регистрации и учета

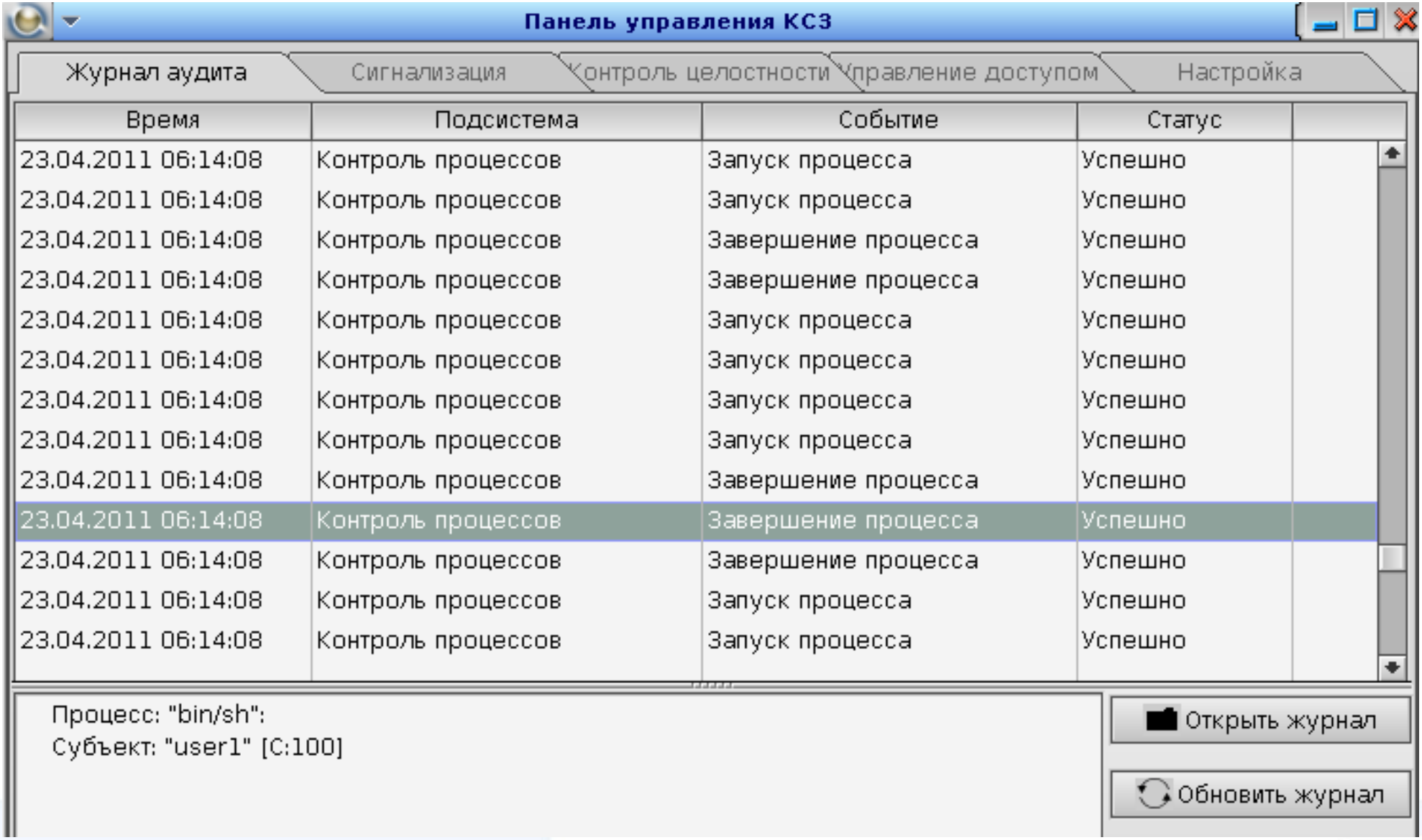
Маркирование документов

- печать конфиденциальных документов доступна только для пользователей из специальной группы;
- маркируются документы с грифом «ДСП» и выше;
- выводится окно для ввода пользовательских реквизитов перед печатью.



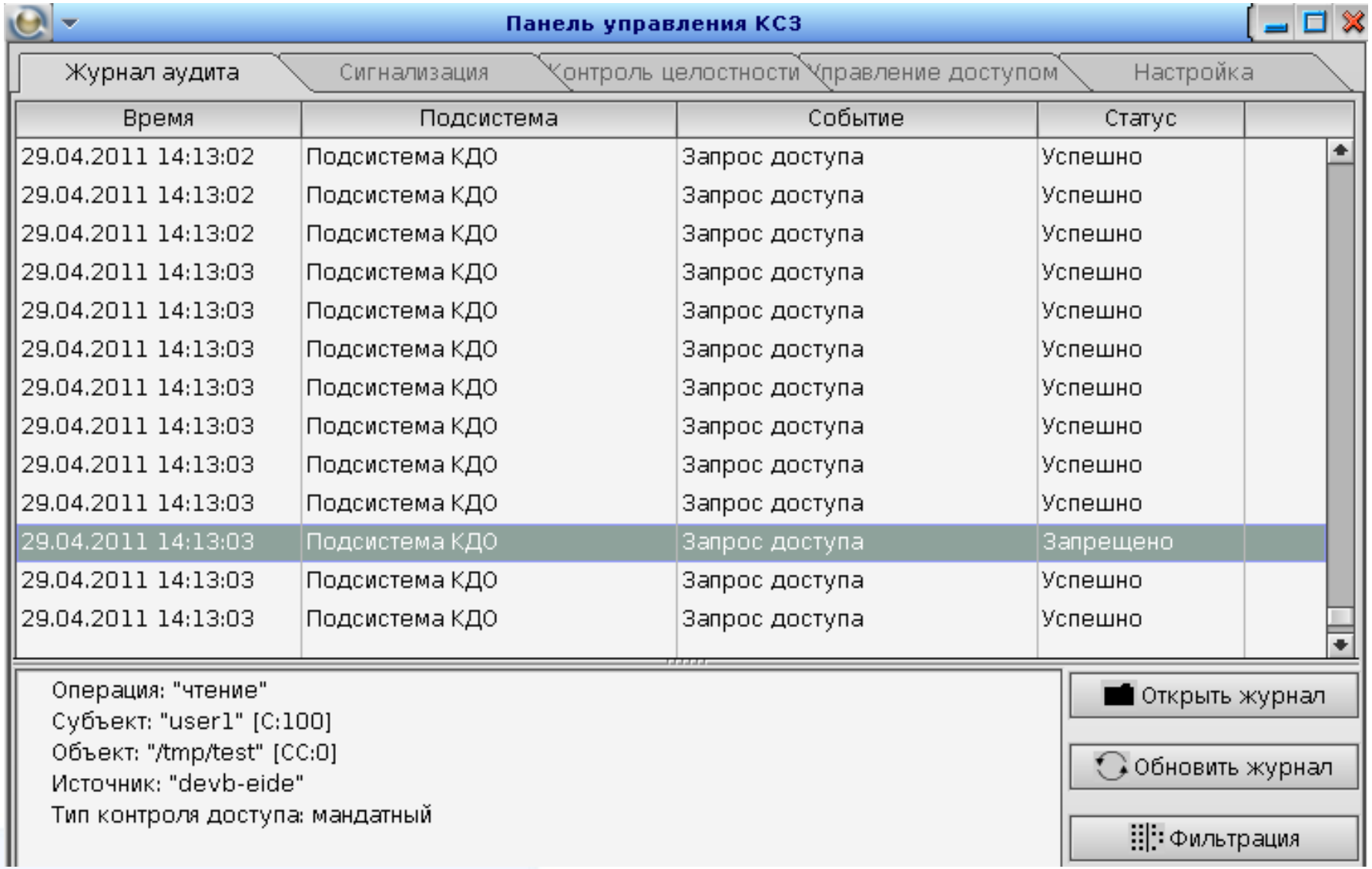
Подсистема регистрации и учета

Запуск/завершение процессов



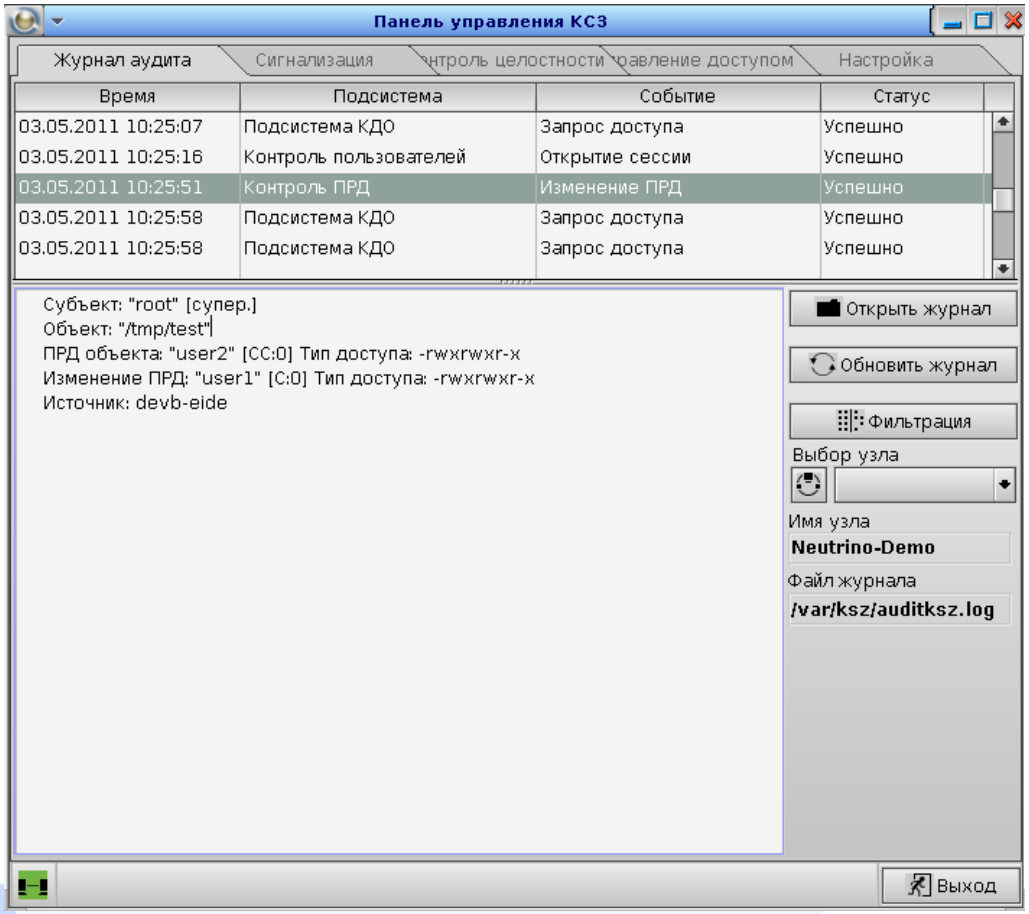
Подсистема регистрации и учета

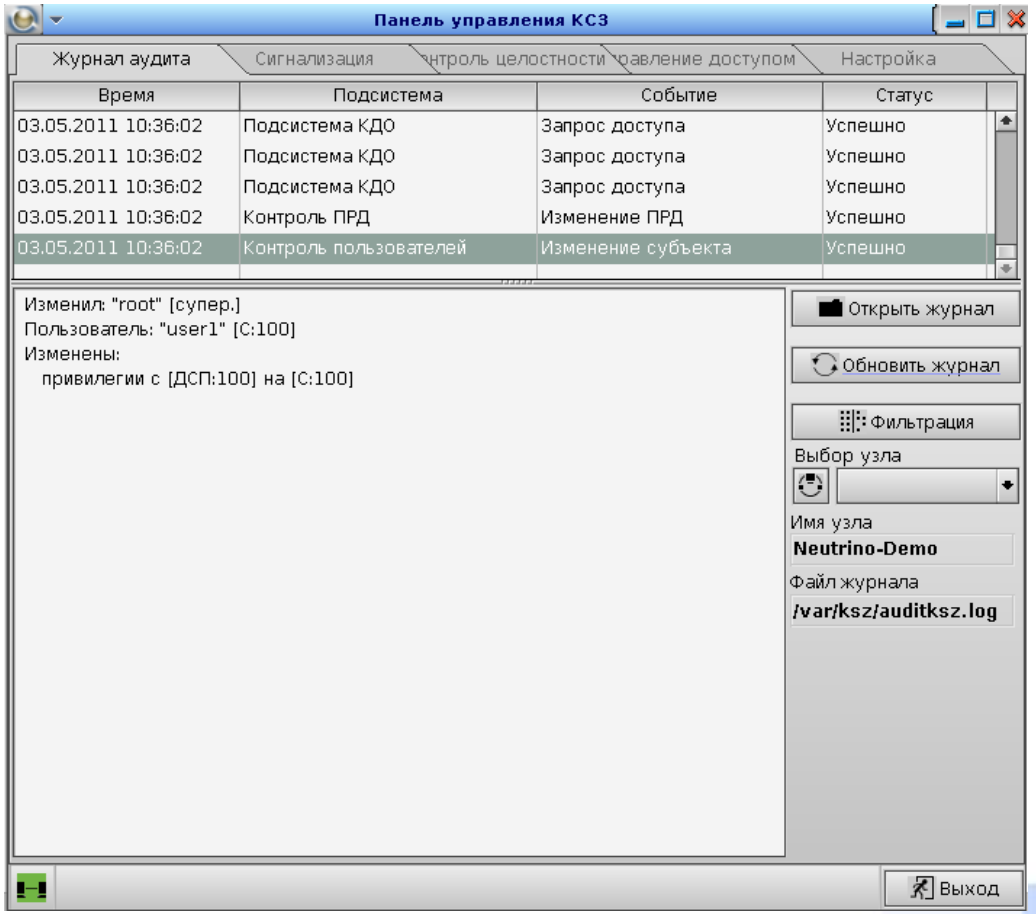
Регистрация попыток доступа



Подсистема регистрации и учета

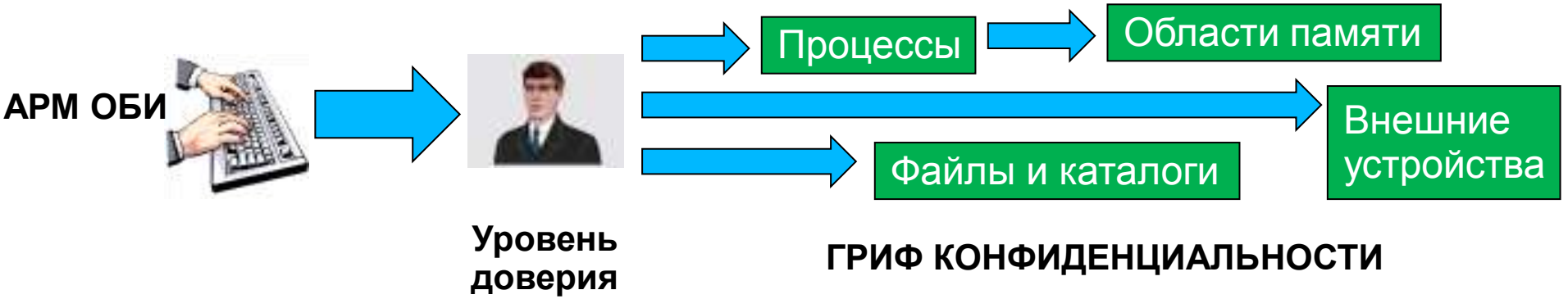
Регистрация изменения полномочия субъектов доступа и статуса объектов доступа





Подсистема регистрации и учета

Автоматический учет создаваемых защищаемых объектов



Очистка освобождаемых областей памяти

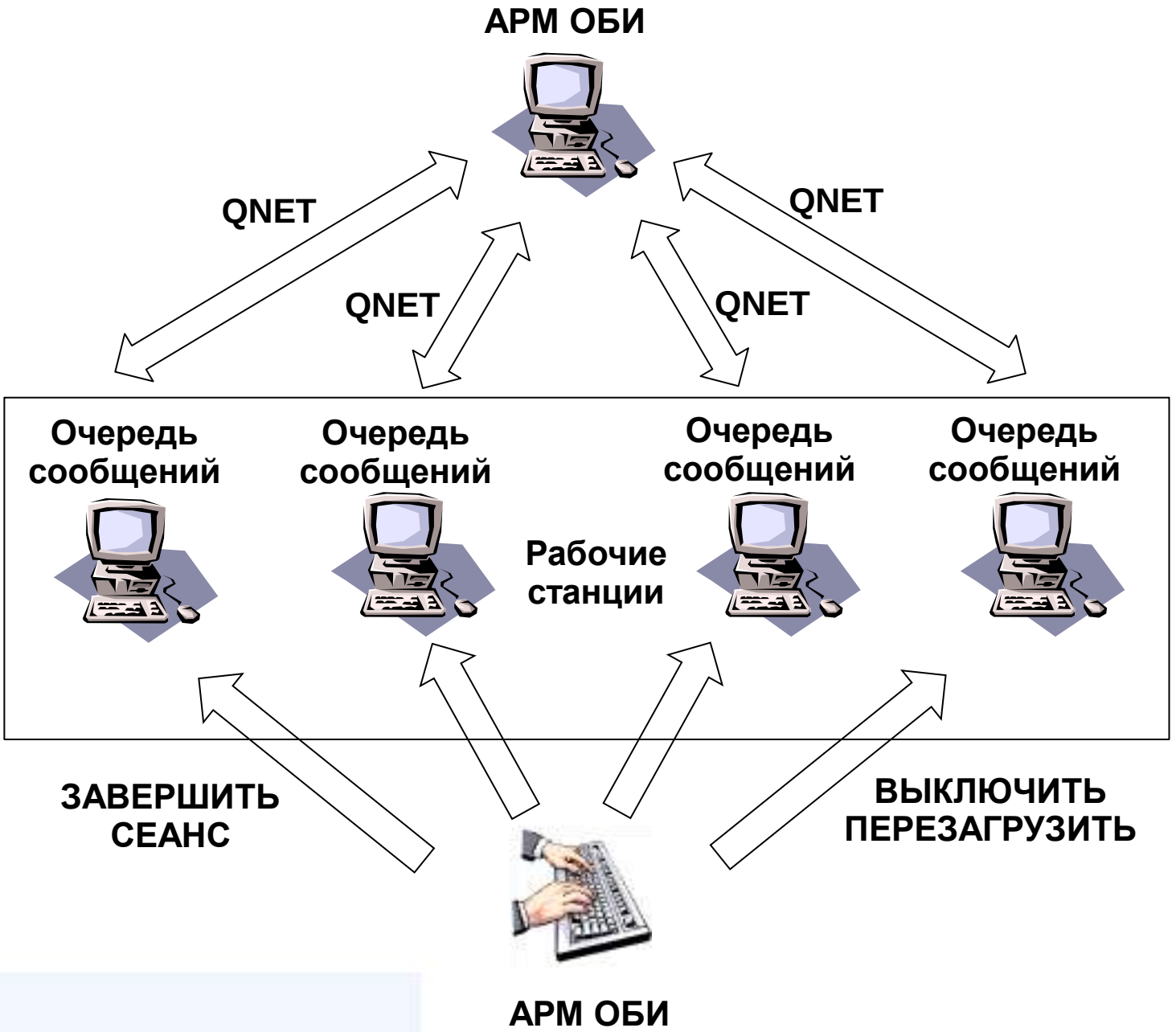
- очистка освобождаемых областей оперативной памяти осуществляется микроядром;
- очистка RAM происходит автоматически при терминировании процессов;
- затирание освобождаемых областей внешней памяти осуществляется драйверами файловых систем;
- затирание освобождаемого места происходит автоматически при удалении файлов;
- очистка памяти может быть опционально однократной или двукратной.

Сигнализация попыток НСД

На всех узлах защищаемой сети запущены:

- защищенный менеджер аудита;
- модуль поддержки защищенной сети Qnet;
- менеджер очередей сообщений **mqueue**;
- на АРМ ОБИ - клиентские утилиты, получающие сообщения от менеджера аудита при попытке НСД;
- администратор безопасности на АРМ ОБИ может воздействовать на АРМ нарушителя;
- сигнализация может выполняться в консольном режиме.

Подсистема регистрации и учета



Контроль целостности КСЗ

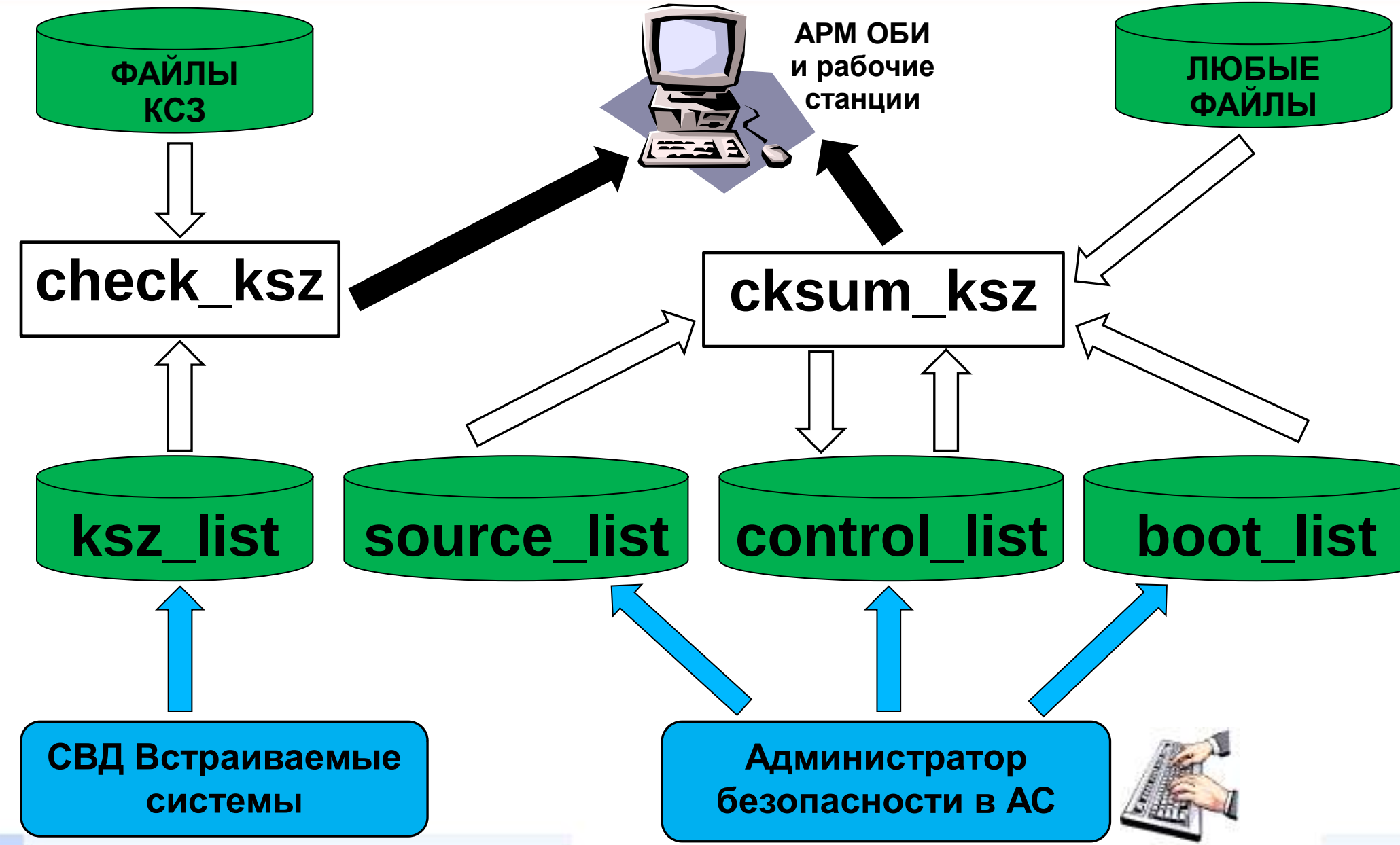
- производится проверка целостности ключевых защищенных компонент КСЗ;
- входные данные – нередактируемый список, поставляемый вместе с дистрибутивом;
- выполняется в графическом и консольном режиме;
- опционально контроль может быть периодическим;
- результаты КЦ регистрируются в журнале безопасности.

Контроль целостности файлов

- производится проверка целостности заданного списка файлов;
- входные данные – список контролируемых файлов, создаваемый администратором безопасности;
- контрольные хэш-суммы рассчитываются по ГОСТ. Р 34.11-94;
- выполняется в графическом и консольном режиме;
- опционально контроль может быть периодическим;
- результаты КЦ регистрируются в журнале безопасности.

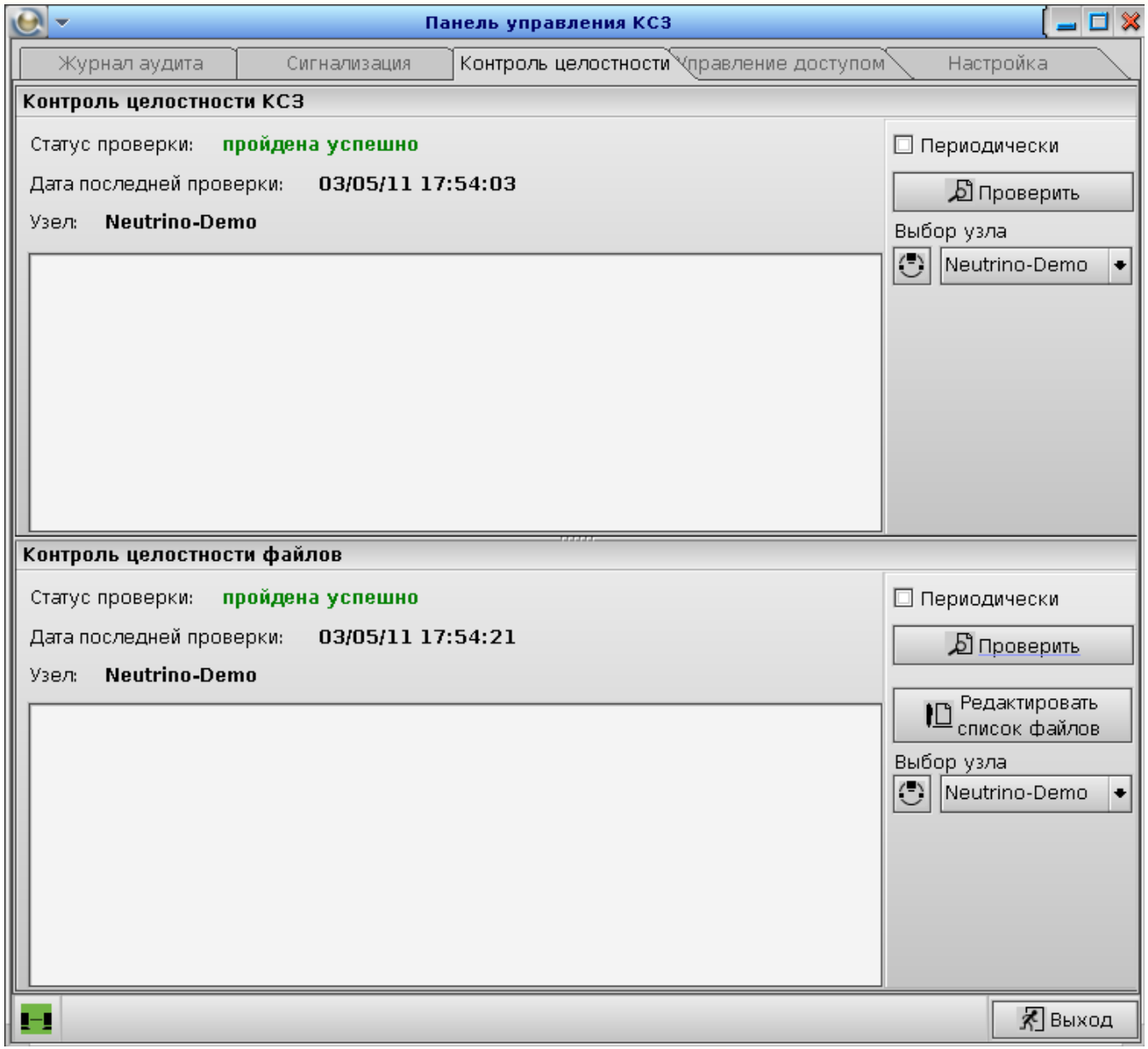
СВД Встраиваемые Системы

Подсистема обеспечения целостности

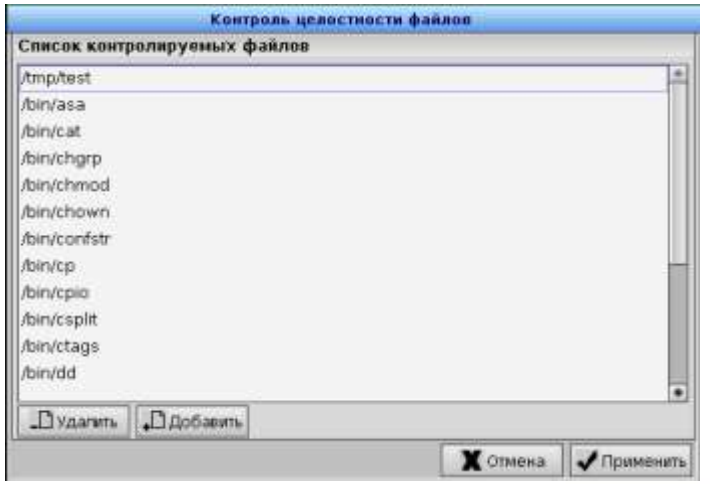


СВД Встраиваемые Системы

Подсистема обеспечения целостности



КЦ в ПУ КСЗ



Оперативный контроль

- один из АРМ защищенной сети - АРМ ОБИ;
- АРМ ОБИ связан по сети Qnet с рабочими станциями;
- администратор безопасности имеет доступ к журналам всех АРМ и отслеживает события НСД;
- воздействие на АРМ нарушителя может быть реализовано командами удаленного управления QNX или функциями ПУ КСЗ;
  - выключить узел;
  - перезагрузить узел;
  - завершить сеанс пользователя.

Подсистема обеспечения целостности

Периодическое тестирование

- затирания удаляемых файлов;
- затирания освобождаемых областей RAM;
- дискреционного разграничения доступа;
- мандатного разграничения доступа;
- механизма изоляции модулей;
- защищенного стека TCP/IP.

Средства восстановления

- создание резервных копий с помощью утилит копирования, сжатия данных и записи на носитель;
- проведение контроля целостности после восстановления;
- тестирование механизмов КСЗ после восстановления.

Спасибо за внимание.

СВД Встраиваемые Системы

www.kpda.ru forum.kpda.ru

sales@kpda.ru support@kpda.ru

Центральный офис:

196066 Санкт-Петербург

Московский проспект, 212А

тел.: (812)373-41-17

факс:(812)373-19-07

Технический офис:

191014 Санкт-Петербург

ул.Госпитальная, д.3

тел./факс:(812)578-02-45