



Алексей Ермолинский, СВД ВС
Комплекс средств защиты
ЗОСРВ «Нейтрино»



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

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



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.



Подсистемы КСЗ

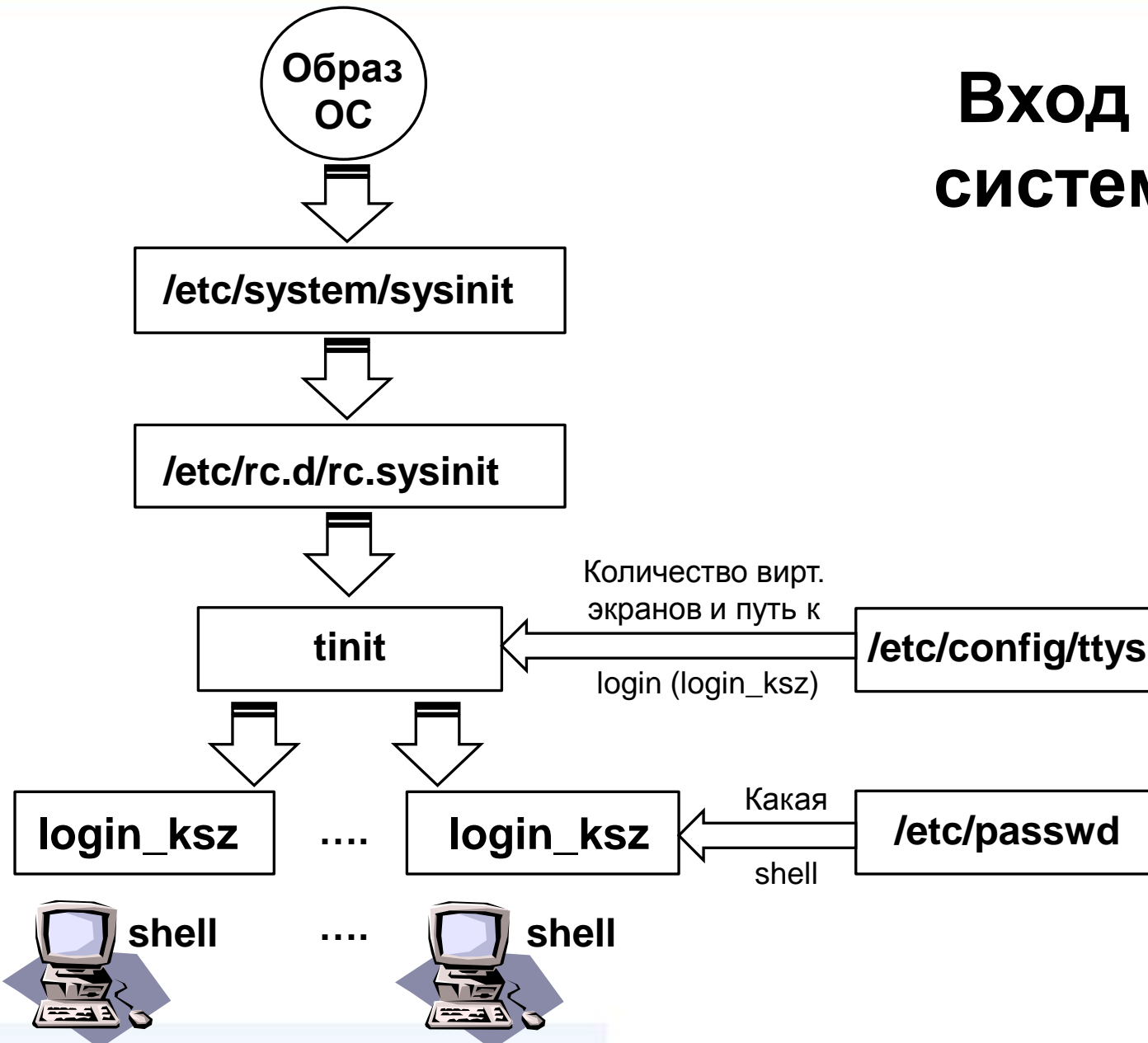




Подсистема управления доступом

СВД Встраиваемые Системы

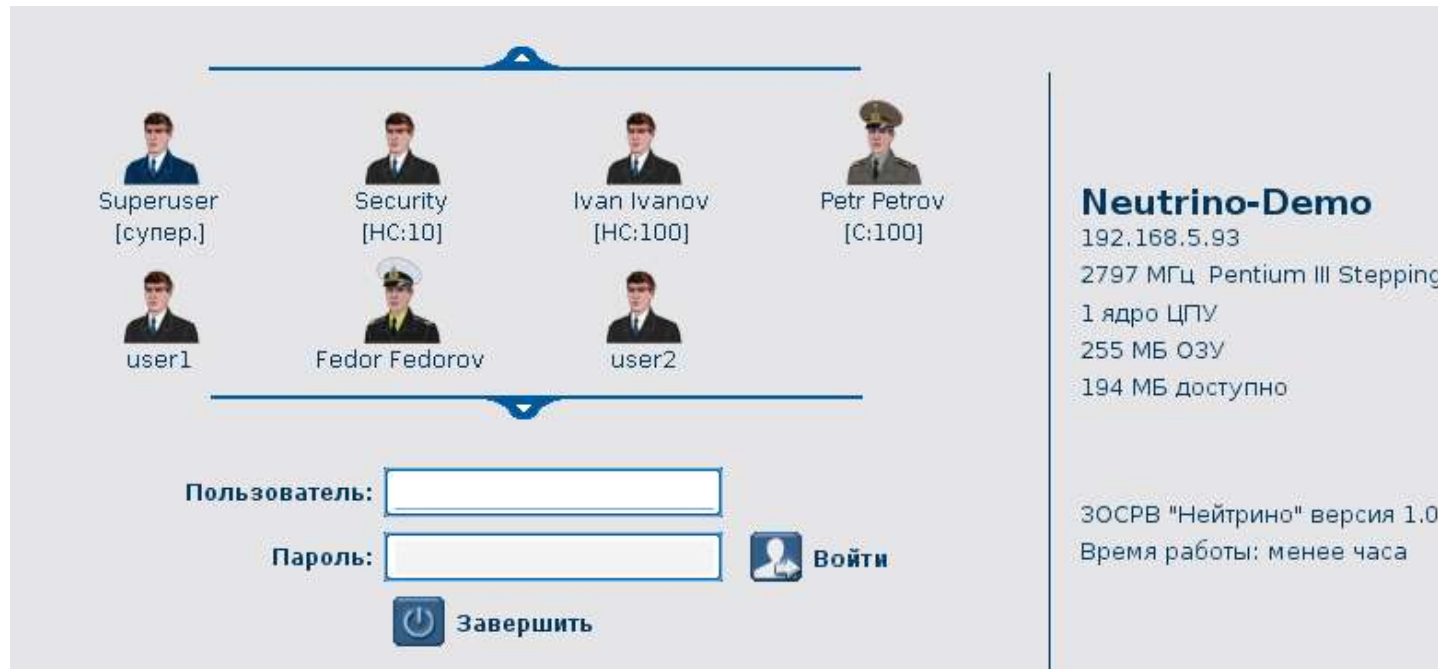
Вход в систему





Вход в систему

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

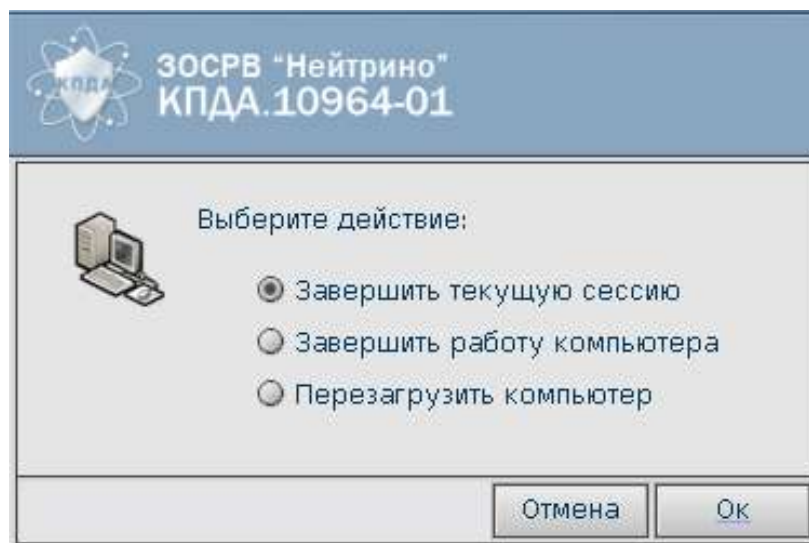


- ❑ осуществляет регистрацию событий входа в журнале аудита КСЗ;
- ❑ есть консольный аналог.



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).

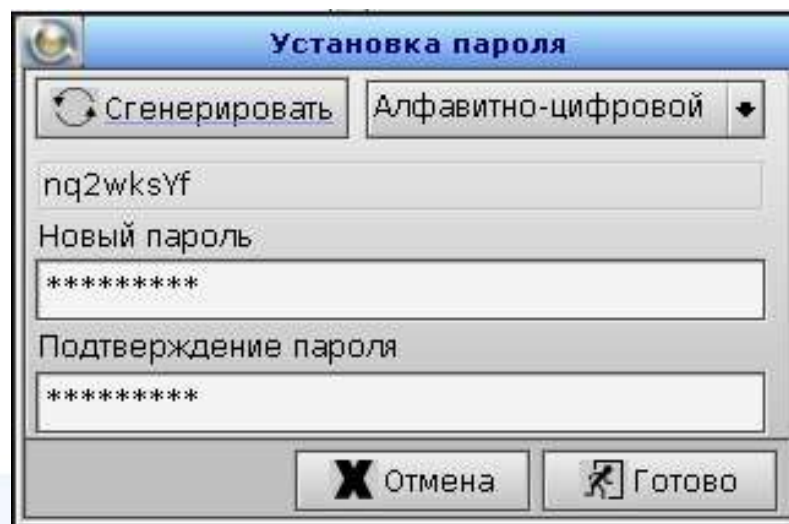
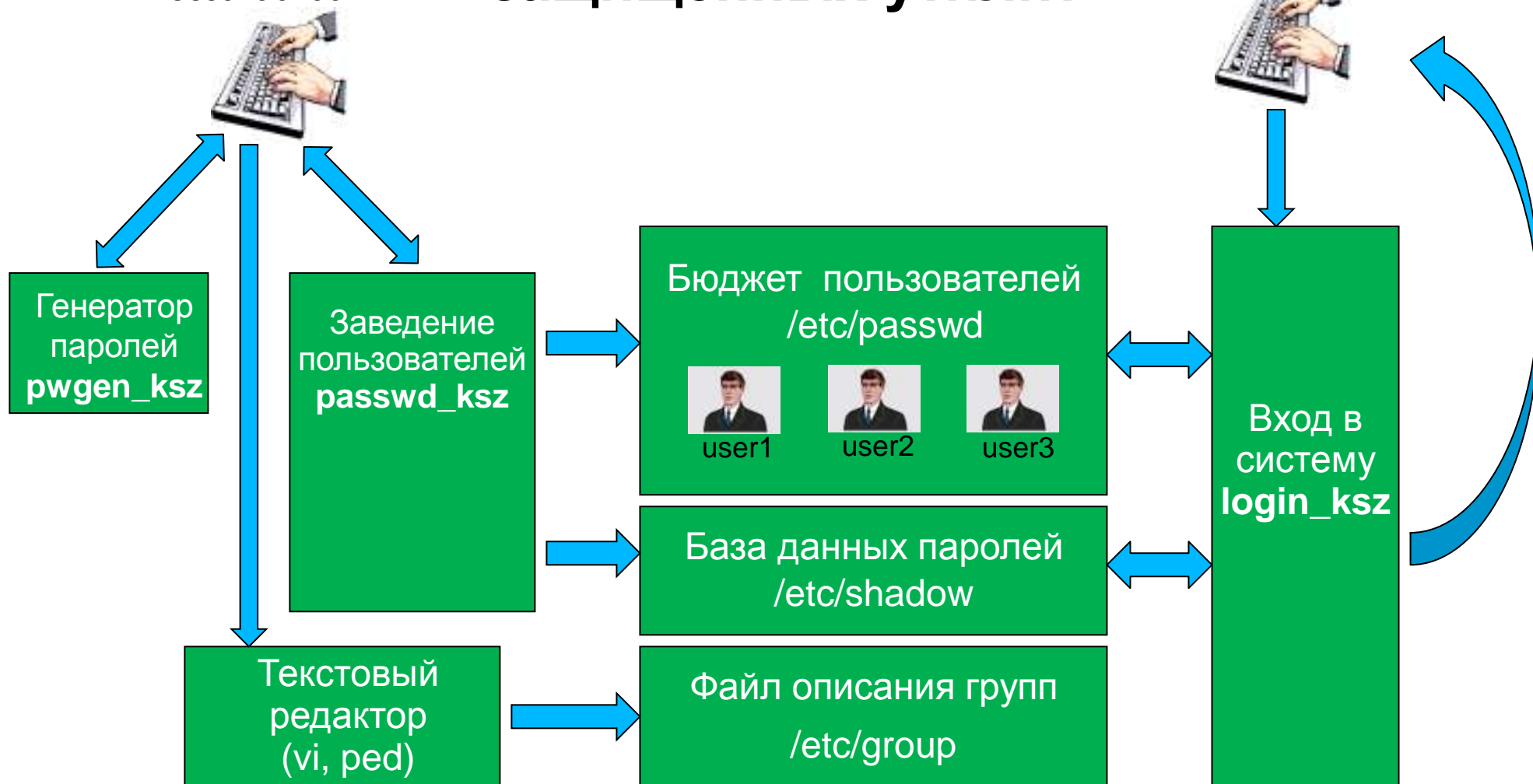




Схема взаимодействия защищенных утилит

АРМ (терминал)
администратора
безопасности

АРМ (терминал)
пользователя





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.



Субъекты матрицы доступа

The screenshot displays the 'Панель управления КСЗ' (Access Control System Control Panel) interface. The main window is titled 'Управление пользователями' (User Management) and contains a table of users. Two dialog boxes are open: 'Создать нового пользователя' (Create new user) and 'Установка пароля' (Password installation).

Table of Users:

Пользователь	Уровень	Категория
admin_ksz	0 (HC)	10
bin	0 (HC)	1
daemon	0 (HC)	2
fedor	3 (CC)	100

Создать нового пользователя (Create new user) dialog:

- Полное имя: user1
- Имя: user1
- Домашний каталог: /home/user1
- Оболочка: /bin/sh
- Уровень: 2 (C)
- Номер пользователя: 1073741925
- Категория (группа): users
- Запретить вход для этого пользователя.
- Установить пароль (checkbox checked)

Установка пароля (Password installation) dialog:

- Сгенерировать пароль (checkbox checked)
- Новый пароль: *****
- Подтверждение пароля: *****

The interface also shows a sidebar with navigation options like 'Интернет', 'Утилиты', and 'Настройка', and a taskbar at the bottom with the 'Пуск' button and the system clock showing 'Вт 12.04.11 09:12:05'.



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		



Права доступа объектов

Управление правами объекта

Местоположение: /nosec
Символическая ссылка: -
Размер: -
Изменён: Вторник, 19.04.2011 11:22:09

Мандатные права доступа

Уровень: 0 (HC) Владелец: root
Категория (группа): s_users Рекурсивно

Дискреционные права доступа

	Чтение	Запись	Исполнение	
Пользователь	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> SUID бит
Группа	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> SGID бит
Остальные	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> sticky бит

Рекурсивно

Управление правами объекта

Местоположение: /sovsec
Символическая ссылка: -
Размер: -
Изменён: Вторник, 19.04.2011 11:29:03

Мандатные права доступа

Уровень: 3 (CC) Владелец: user2
Категория (группа): ss_users Рекурсивно

Дискреционные права доступа

	Чтение	Запись	Исполнение	
Пользователь	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> SUID бит
Группа	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> SGID бит
Остальные	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> sticky бит

Рекурсивно



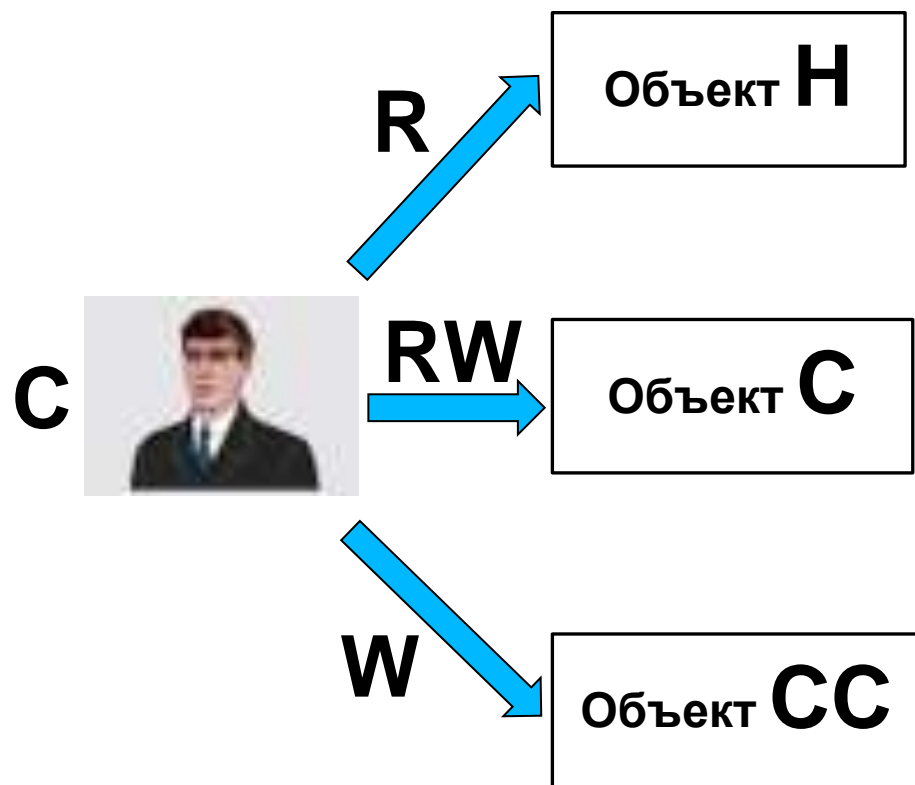
Управление потоками осуществляется с помощью:

- 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



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



Правила управления потоками информации:

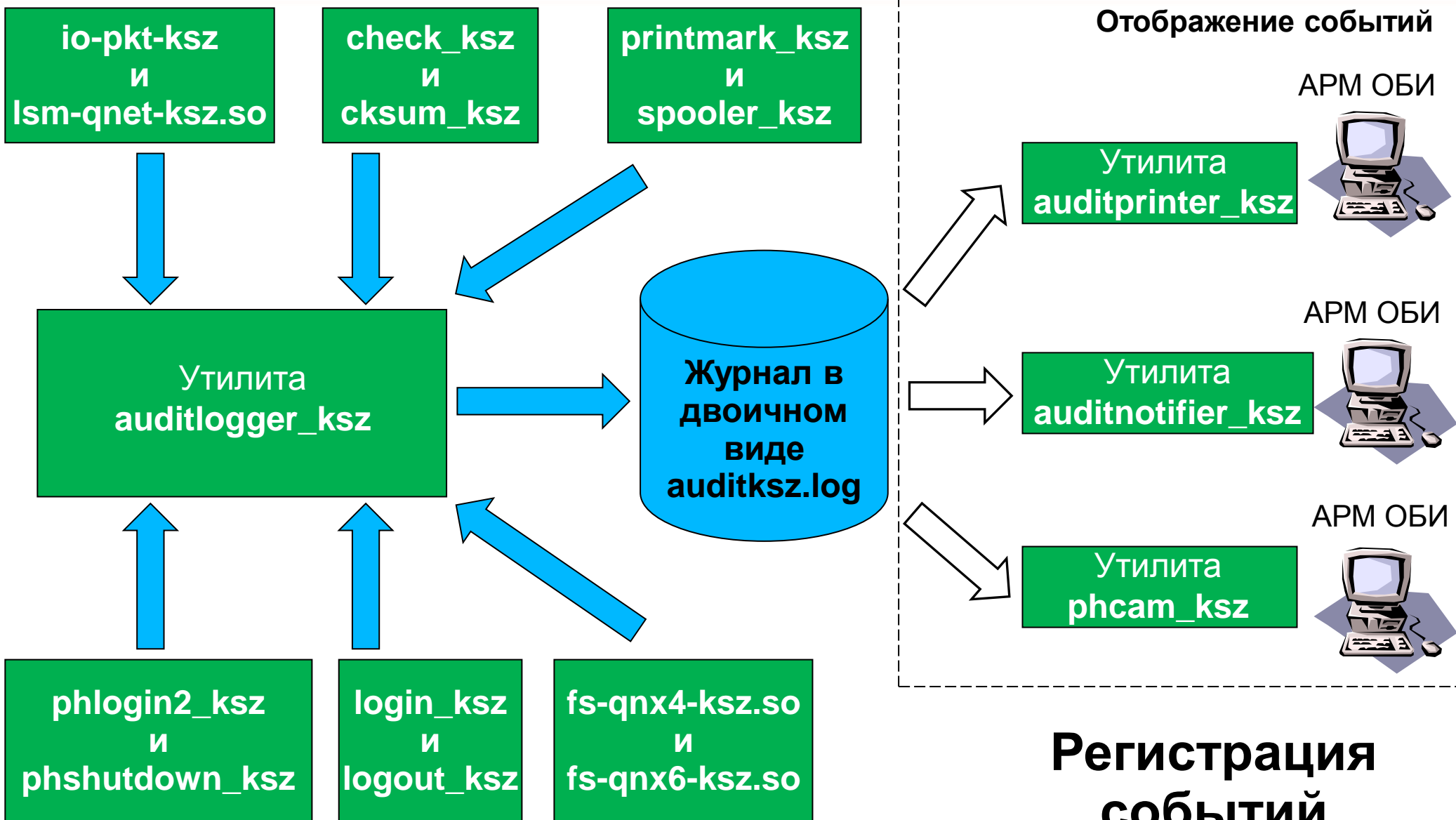
□ субъект имеет право на **чтение** объекта, только если уровень допуска субъекта не ниже грифа объекта и список групп субъекта включает в себя группу (в т.ч. тематическую маску субъекта)

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



Подсистема регистрации и учета

СВД Встраиваемые Системы



**Регистрация
событий
безопасности**



Подсистема регистрации и учета

СВД Встраиваемые Системы

Вход/выход

Панель управления КСЗ

Журнал аудита | Сигнализация | Контроль целостности | Управление доступом | Настройка

Время	Подсистема	Событие	Статус
21.04.2011 12:57:12	Контроль пользователей	Открытие сессии	Успешно
22.04.2011 07:38:02	Контроль пользователей	Открытие сессии	Запрещено
22.04.2011 07:38:57	Контроль пользователей	Добавление субъекта	Успешно
22.04.2011 07:39:18	Контроль пользователей	Открытие сессии	Успешно
22.04.2011 07:39:57	Контроль пользователей	Закрытие сессии	Успешно
22.04.2011 07:40:14	Контроль пользователей	Открытие сессии	Успешно
22.04.2011 07:40:31	Контроль пользователей	Открытие сессии	Успешно
22.04.2011 07:40:41	Контроль пользователей	Открытие сессии	Успешно
22.04.2011 07:58:39	Контроль пользователей	Открытие сессии	Успешно
23.04.2011 04:17:35	Контроль пользователей	Закрытие сессии	Успешно
23.04.2011 04:39:51	Контроль пользователей	Открытие сессии	Успешно

Пользователь "user1" [неизв.]
Предъявлен пароль "12345678"

Открыть журнал

Обновить журнал

Фильтрация

Выбор узла

Имя узла
Neutrino-Demo

Файл журнала
/var/ksz/auditksz.log

Выход

Настройка фильтрации

Фильтрация по подсистемам	Фильтрация по статусу
Контроль целостности	Успешно
Сетевая подсистема	Неуспешно
Подсистема печати	Запрещено
Подсистема МПВ	
Подсистема КДО	
Контроль ПРД	
Контроль пользователей	
Контроль процессов	

Выбрать всё | Очистить

Фильтрация по дате

Фильтровать

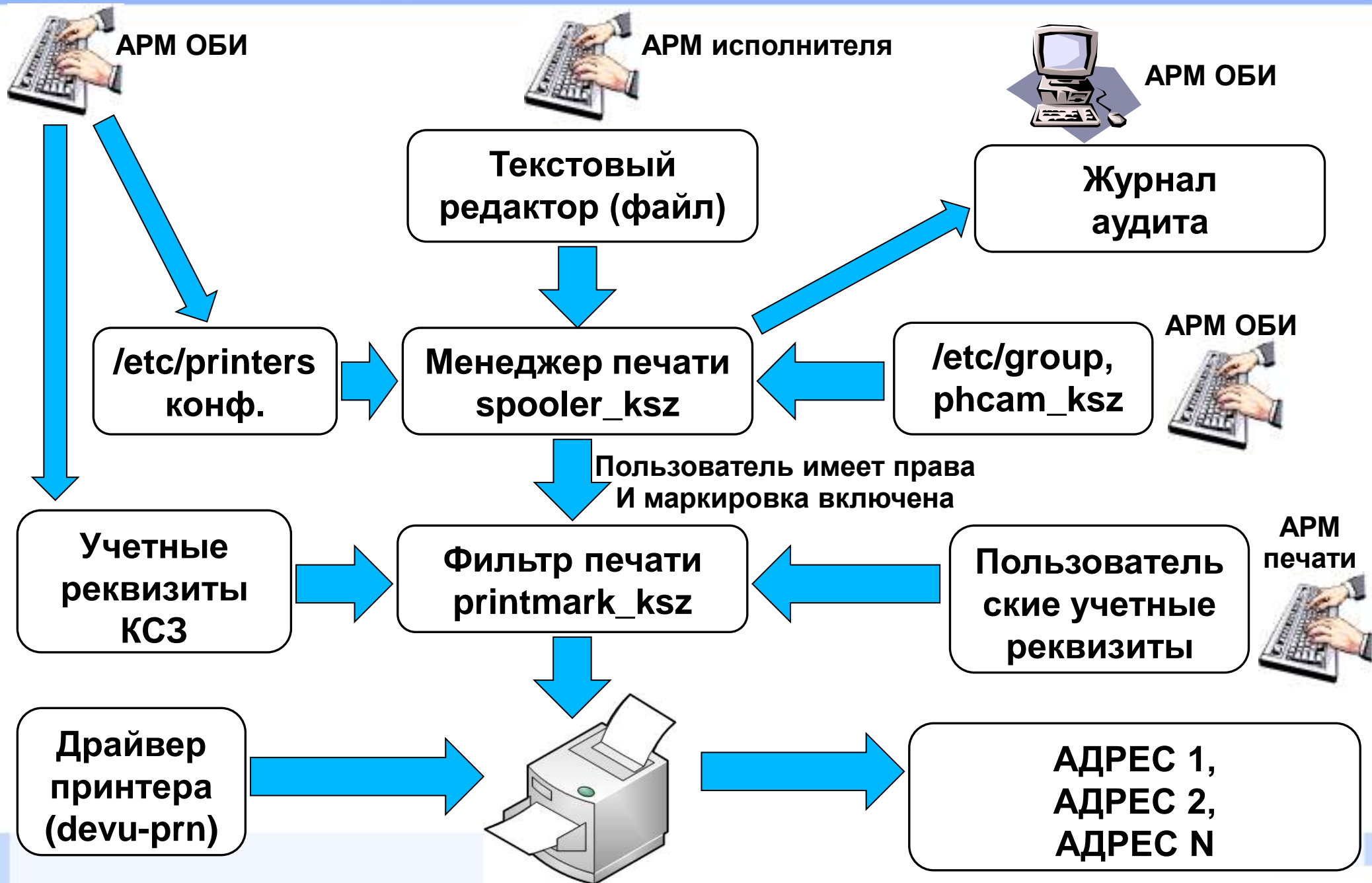
День	Месяц	Год	Час	Минута	Секунда
с 23	Апрель	2011	4	42	9
По 23	Апрель	2011	4	42	9

Отмена | Применить



Подсистема регистрации и учета

СВД Встраиваемые Системы





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.

Маркирование документа

Учетный номер документа: 001/нс

Реквизиты АС: Mashburo

ФИО исполнителя: Ivanov

ФИО отправившего на печать: Petrov

Кол-во экземпляров: 2

Адресат экземпляра:

Адресаты: Удалить Добавить

СВД ВС
SWD Software

Номера экземпляров к печати (1,2 или 1-3): 1-2

Отменить Продолжить



Подсистема регистрации и учета

СВД Встраиваемые Системы

Запуск/завершение процессов

Панель управления КСЗ

Журнал аудита | Сигнализация | Контроль целостности | Управление доступом | Настройка

Время	Подсистема	Событие	Статус
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Завершение процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Завершение процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Завершение процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Завершение процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно
23.04.2011 06:14:08	Контроль процессов	Запуск процесса	Успешно

Процесс: "bin/sh":
Субъект: "user1" [C:100]

Открыть журнал

Обновить журнал



Регистрация попыток доступа

Панель управления КСЗ

Журнал аудита | Сигнализация | Контроль целостности | Управление доступом | Настройка

Время	Подсистема	Событие	Статус
29.04.2011 14:13:02	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:02	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:02	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Запрещено
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно
29.04.2011 14:13:03	Подсистема КДО	Запрос доступа	Успешно

Операция: "чтение"
Субъект: "user1" [C:100]
Объект: "/tmp/test" [CC:0]
Источник: "devb-eide"
Тип контроля доступа: мандатный

Открыть журнал
Обновить журнал
Фильтрация



Регистрация изменения полномочия субъектов доступа и статуса объектов доступа

Панель управления КСЗ

Журнал аудита | Сигнализация | Контроль целостности | Управление доступом | Настройка

Время	Подсистема	Событие	Статус
03.05.2011 10:25:07	Подсистема КДО	Запрос доступа	Успешно
03.05.2011 10:25:16	Контроль пользователей	Открытие сессии	Успешно
03.05.2011 10:25:51	Контроль ПРД	Изменение ПРД	Успешно
03.05.2011 10:25:58	Подсистема КДО	Запрос доступа	Успешно
03.05.2011 10:25:58	Подсистема КДО	Запрос доступа	Успешно

Субъект: "root" [супер.]
Объект: "/tmp/test"
ПРД объекта: "user2" [CC:0] Тип доступа: -rwxrwxr-x
Изменение ПРД: "user1" [C:0] Тип доступа: -rwxrwxr-x
Источник: devb-eide

Открыть журнал
Обновить журнал
Фильтрация
Выбор узла
Имя узла: **Neutrino-Demo**
Файл журнала: /var/ksz/auditksz.log

Выход

Панель управления КСЗ

Журнал аудита | Сигнализация | Контроль целостности | Управление доступом | Настройка

Время	Подсистема	Событие	Статус
03.05.2011 10:36:02	Подсистема КДО	Запрос доступа	Успешно
03.05.2011 10:36:02	Подсистема КДО	Запрос доступа	Успешно
03.05.2011 10:36:02	Подсистема КДО	Запрос доступа	Успешно
03.05.2011 10:36:02	Контроль ПРД	Изменение ПРД	Успешно
03.05.2011 10:36:02	Контроль пользователей	Изменение субъекта	Успешно

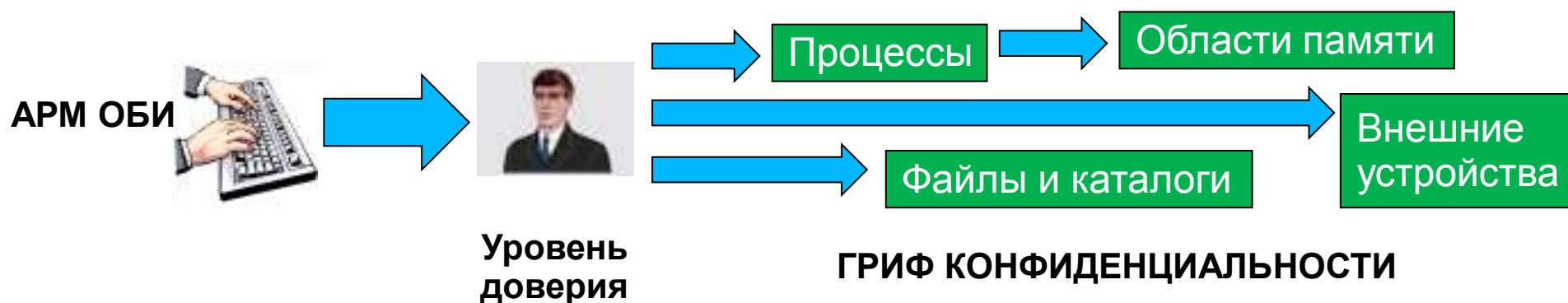
Изменил: "root" [супер.]
Пользователь: "user1" [C:100]
Изменены:
привилегии с [ДСП:100] на [C:100]

Открыть журнал
Обновить журнал
Фильтрация
Выбор узла
Имя узла: **Neutrino-Demo**
Файл журнала: /var/ksz/auditksz.log

Выход



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.



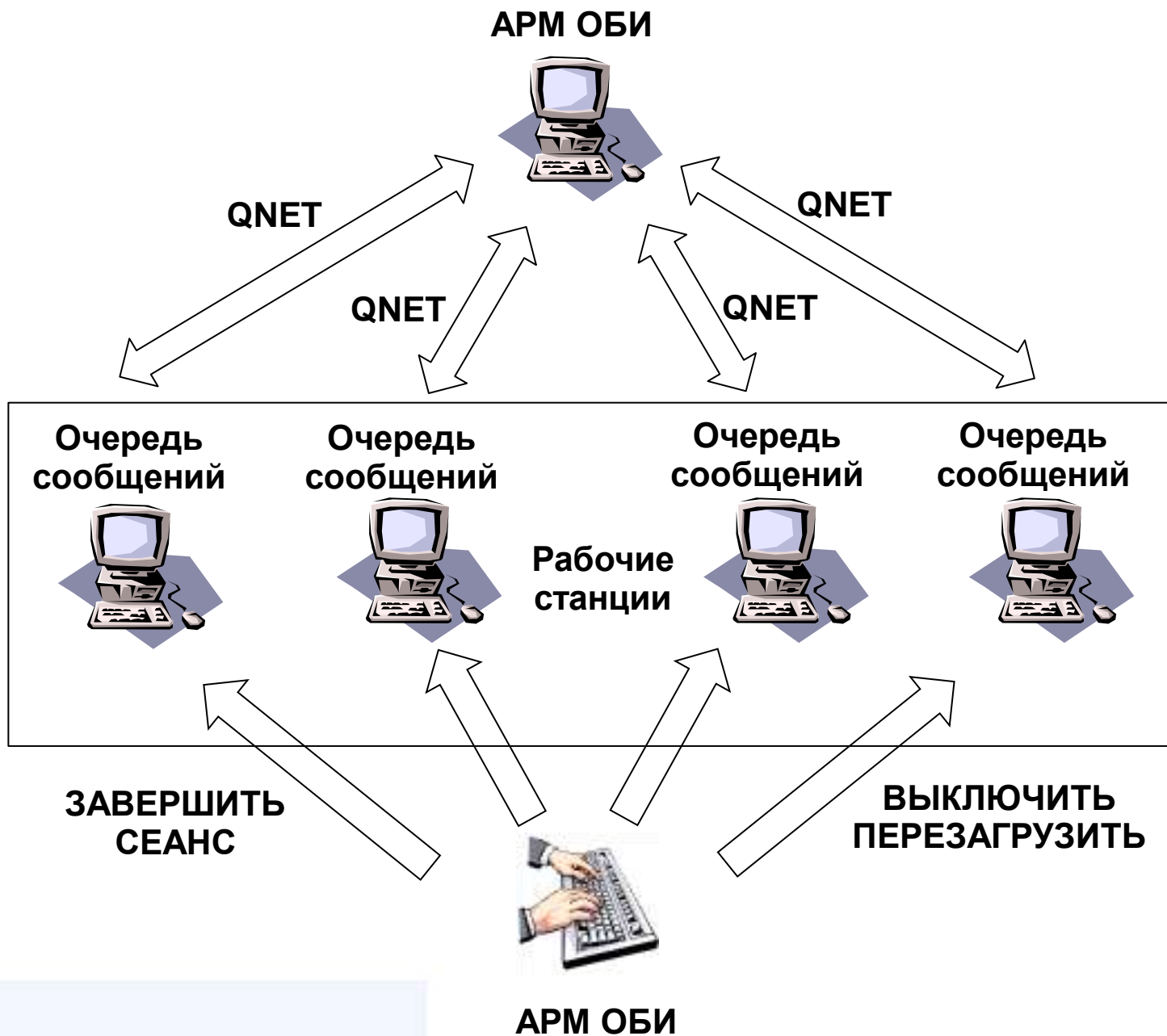
Сигнализация попыток НСД

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 – не редактируемый список, поставляемый вместе с дистрибутивом;
- выполняется в графическом и консольном режиме;
- опционально контроль может быть периодическим;
- результаты КЦ регистрируются в журнале безопасности.



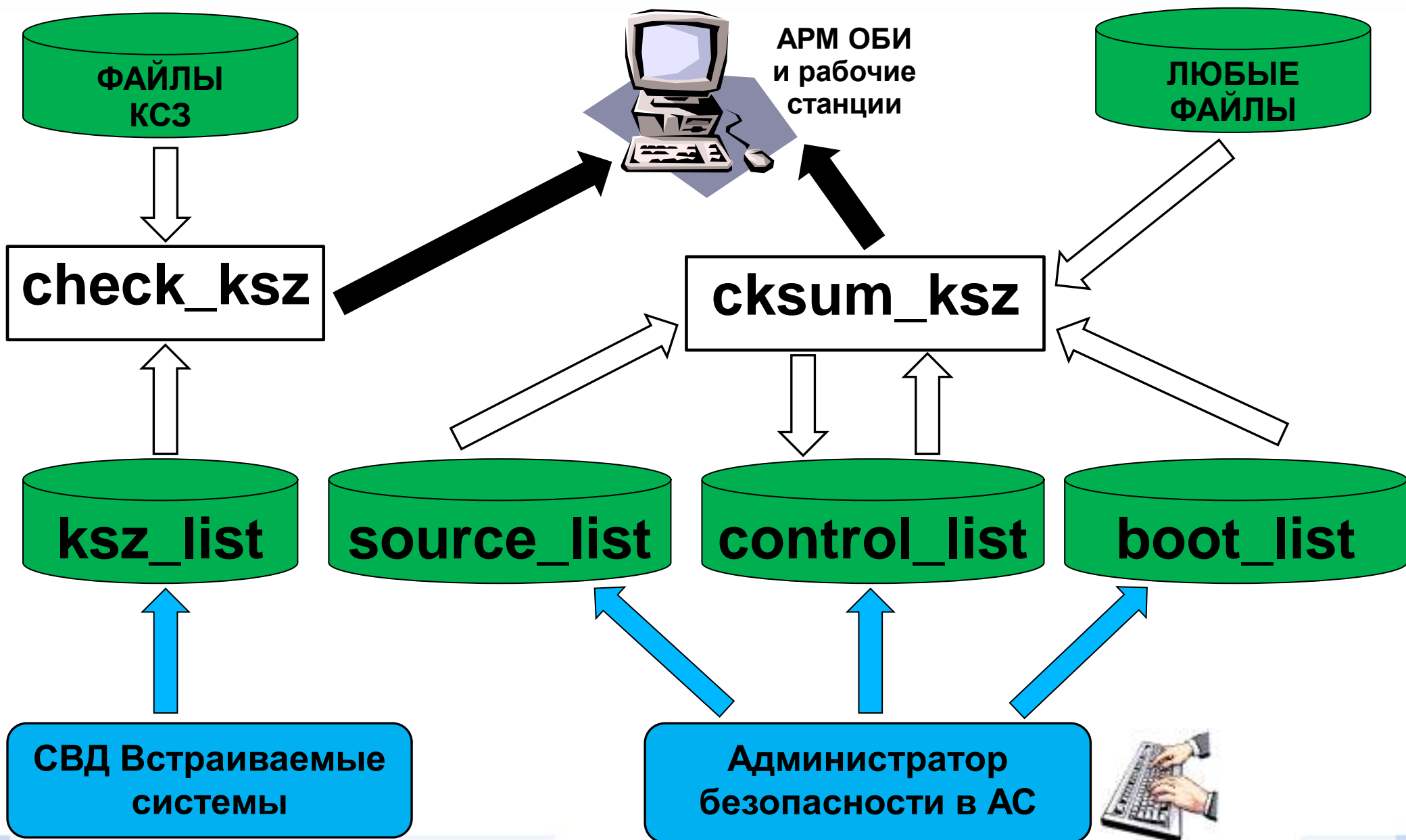
Контроль целостности файлов

- 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.



Подсистема обеспечения целостности

СВД Встраиваемые Системы





Подсистема обеспечения целостности

СВД Встраиваемые Системы

КЦ в ПУ КСЗ

Панель управления КСЗ

Журнал аудита | Сигнализация | **Контроль целостности** | Управление доступом | Настройка

Контроль целостности КСЗ

Статус проверки: **пройдена успешно**

Дата последней проверки: **03/05/11 17:54:03**

Узел: **Neutrino-Demo**

Периодически

Выбор узла

Контроль целостности файлов

Статус проверки: **пройдена успешно**

Дата последней проверки: **03/05/11 17:54:21**

Узел: **Neutrino-Demo**

Периодически

Выбор узла

Контроль целостности файлов

Список контролируемых файлов

- /tmp/test
- /bin/vasa
- /bin/cat
- /bin/chgrp
- /bin/chmod
- /bin/chown
- /bin/confstr
- /bin/cp
- /bin/cpio
- /bin/csplit
- /bin/ctags
- /bin/dd



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.



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