Программно-аппаратные средства обеспечения информационной безопасности

Лекция № 8

Комплексная система защиты информации Панцирь-К

Рахманенко И.А.

План

- КСЗИ Панцирь-К. Серверная и клиентские части
- Идентификация и аутентификация пользователей
- Контроль и разграничение доступа
- Аудит
- Дополнительные возможности

КСЗИ Панцирь-К

Возможности:

- Идентификация и аутентификация: Console, flash, eToken USB, …
- Разграничение и аудит действий пользователей и приложений
- Контроль целостности
- Гарантированное удаление
- Шифрование: 3DES, AES, DES, ГОСТ 28147-89 …

КСЗИ Панцирь-К. Серверная и клиентские части.

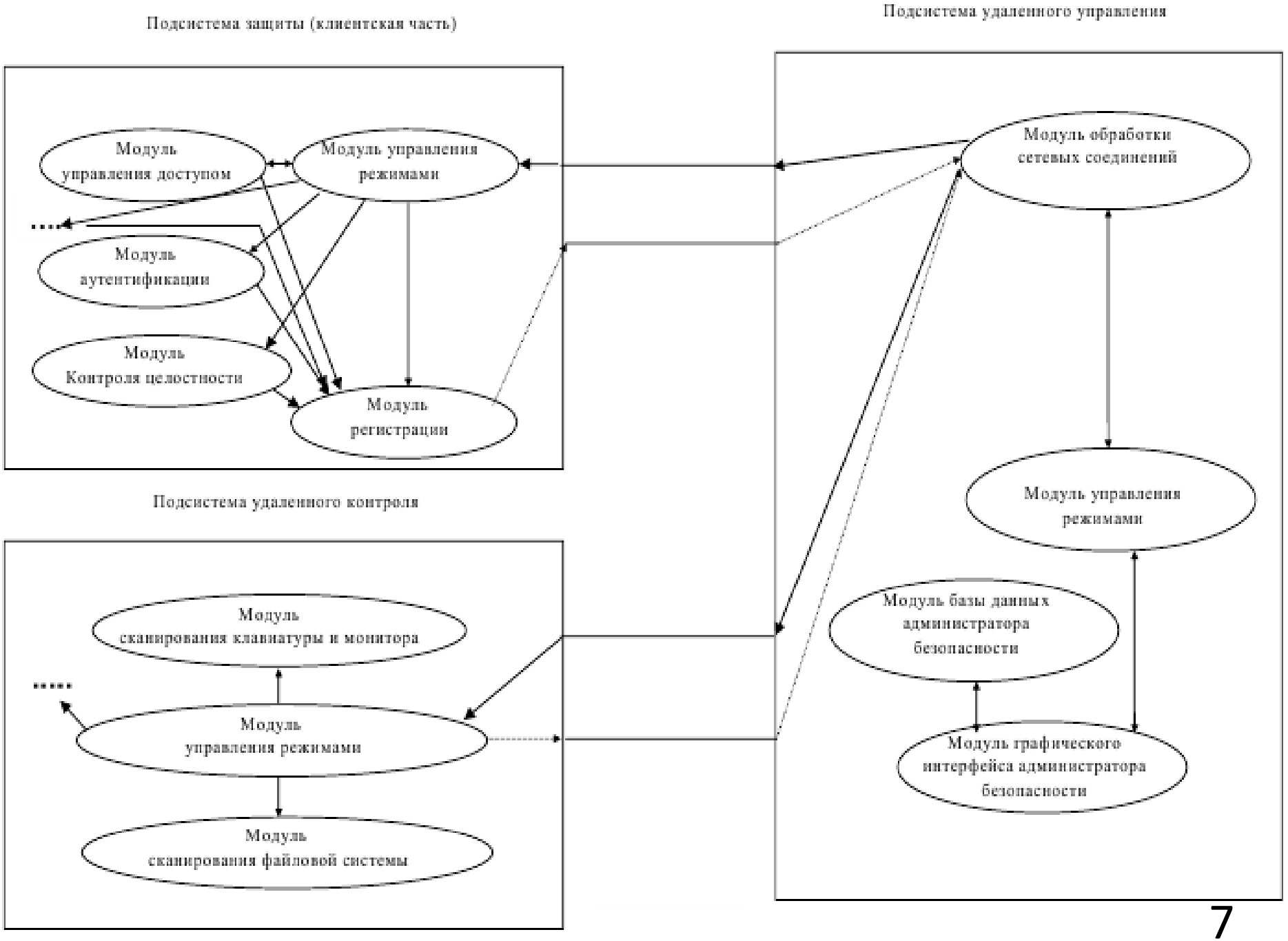
Варианты использования КСЗИ

- Автономный – реализуется локальное администрирование КСЗИ.

- Сетевой – сервер + клиенты.

Общая схема КСЗИ

- Подсистема защиты рабочих станций и информационных серверов (клиент);
- Подсистема удаленного контроля рабочих станций и информационных серверов;
- Подсистема удаленного управления механизмами защиты рабочих станций и серверов (сервер).


Подсистема защиты (клиентская часть)
Модуль управления доступом
Модуль управления режимами
Модуль аутентификации
Модуль Контроля целостности
Модуль регистрации
Подсистема удаленного управления
Модуль обработки сетевых соединений
Модуль управления режимами
Модуль базы данных администратора безопасности
Модуль графического интерфейса администратора безопасности
Подсистема удаленного контроля
Модуль сканирования клавиатуры и монитора
Модуль управления режимами
Модуль сканирования файловой системы

Структура клиентской части

- Модуль аутентификации.
- Модуль управления доступом.
- Модуль управления подключением устройств.
- Модуль регистрации.
- Модуль контроля целостности.
- Модуль противодействия ошибкам и закладкам в системном и функциональном программном обеспечении.
- Модуль очистки памяти, кодирования и шифрования данных.
- Другие

Подсистема удаленного контроля рабочих станций и информационных серверов

- Модуль сканирования клавиатуры и монитора.
- Модуль сканирования файловой системы.
- Модуль управления режимами.

Модуль сканирования клавиатуры и монитора

- Периодический (синхронный) визуальный контроль.
- Асинхронно-синхронный визуальный контроль.
- Асинхронный (разовый по запросу администратора) визуальный контроль.
- Асинхронный (непрерывный) визуальный контроль.

Модуль сканирования файловой системы

- Удаленный доступ к файловой системе защищаемого объекта

Сервер безопасности

- Обеспечивает централизованное управление клиентской частью защиты КСЗИ.

Сервер безопасности. Модули

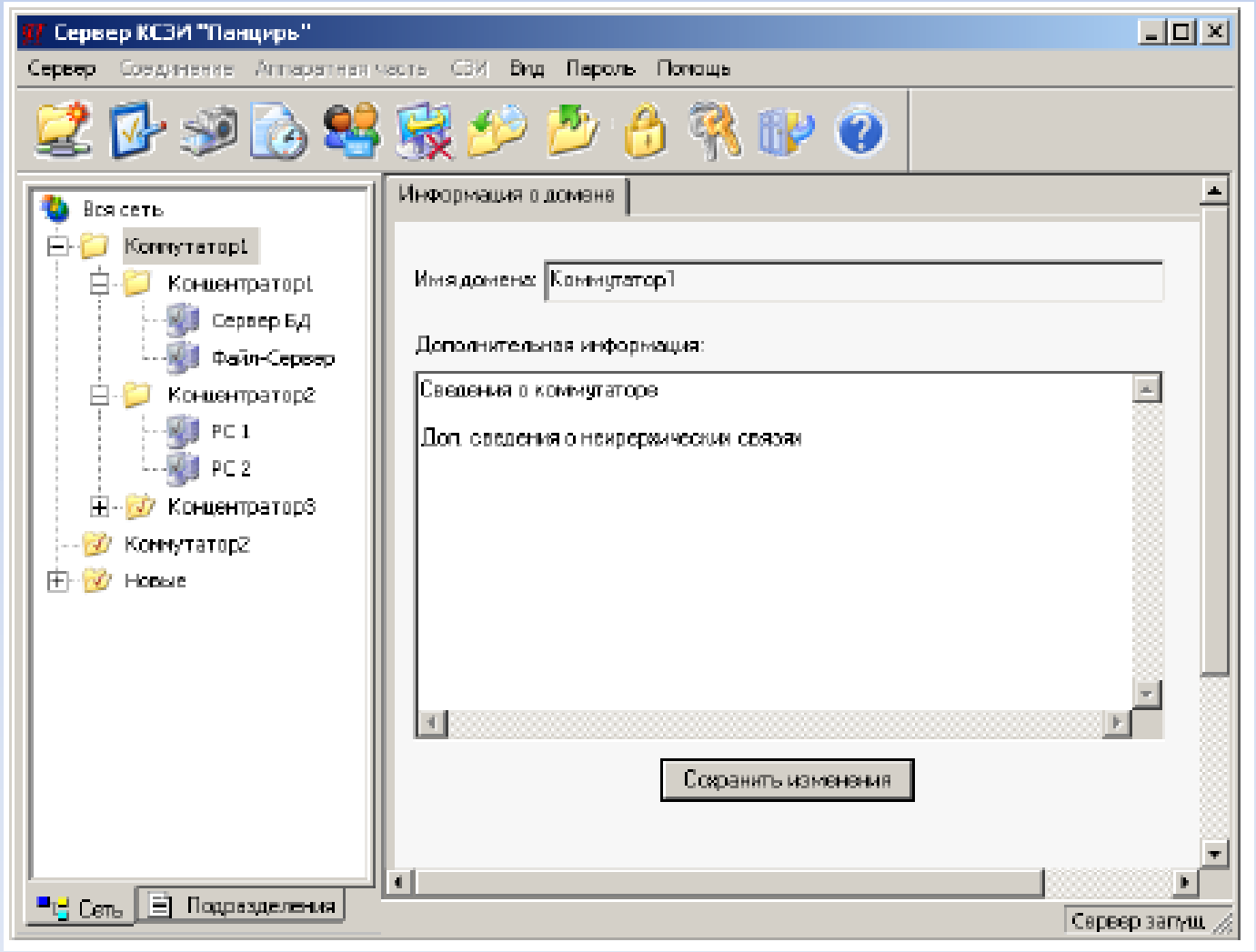
- Модуль обработки сетевых соединений
- Модуль доступа базы данных
- Модуль графического интерфейса
- Модуль управления режимами

Сервер безопасности. Интерфейс

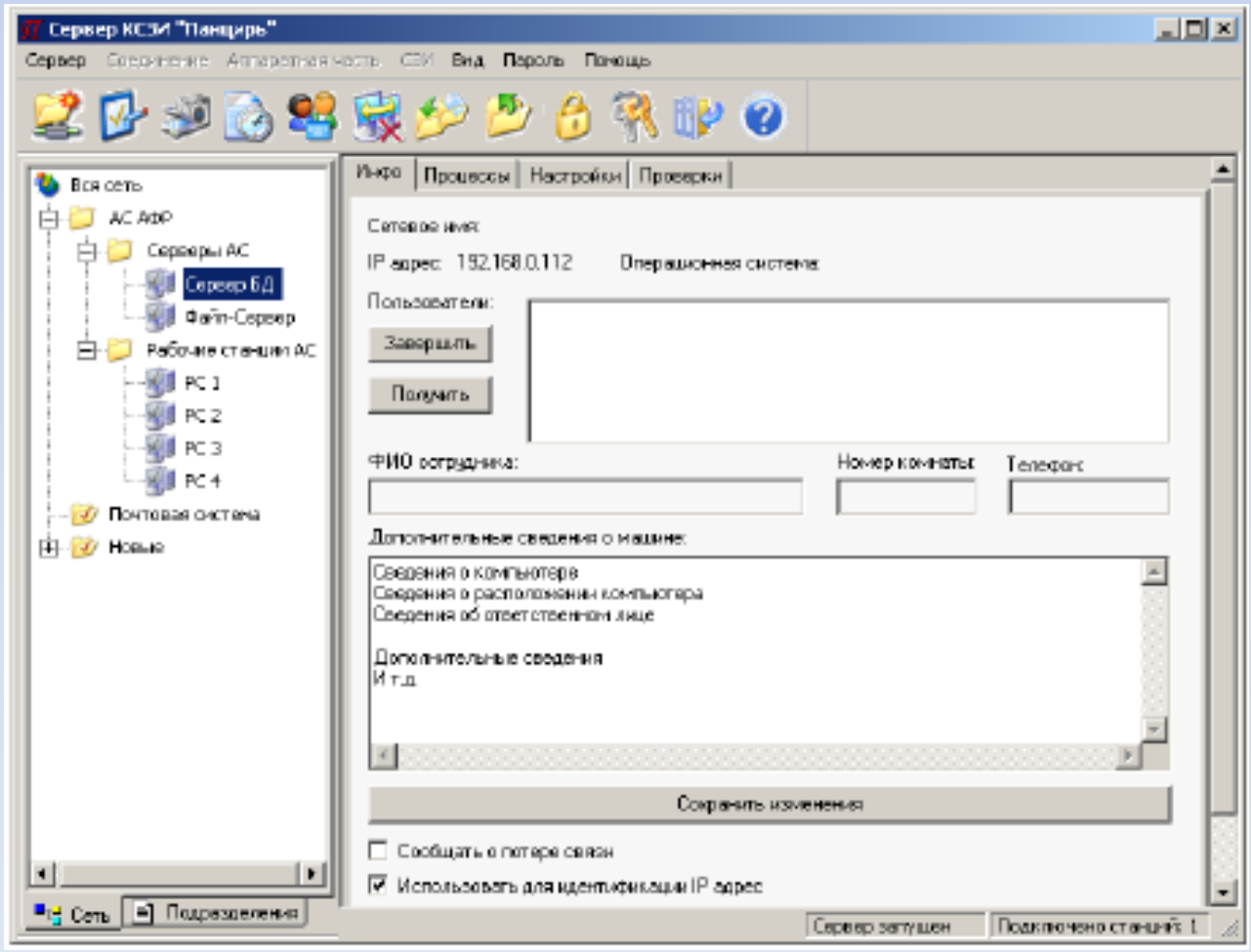
Представление на основе структуры ЛВС:

- Отображение иерархической структуры защищаемой ЛВС;
- Отображение функциональной структуры защищаемой ЛВС;
- Комбинированное отображение.

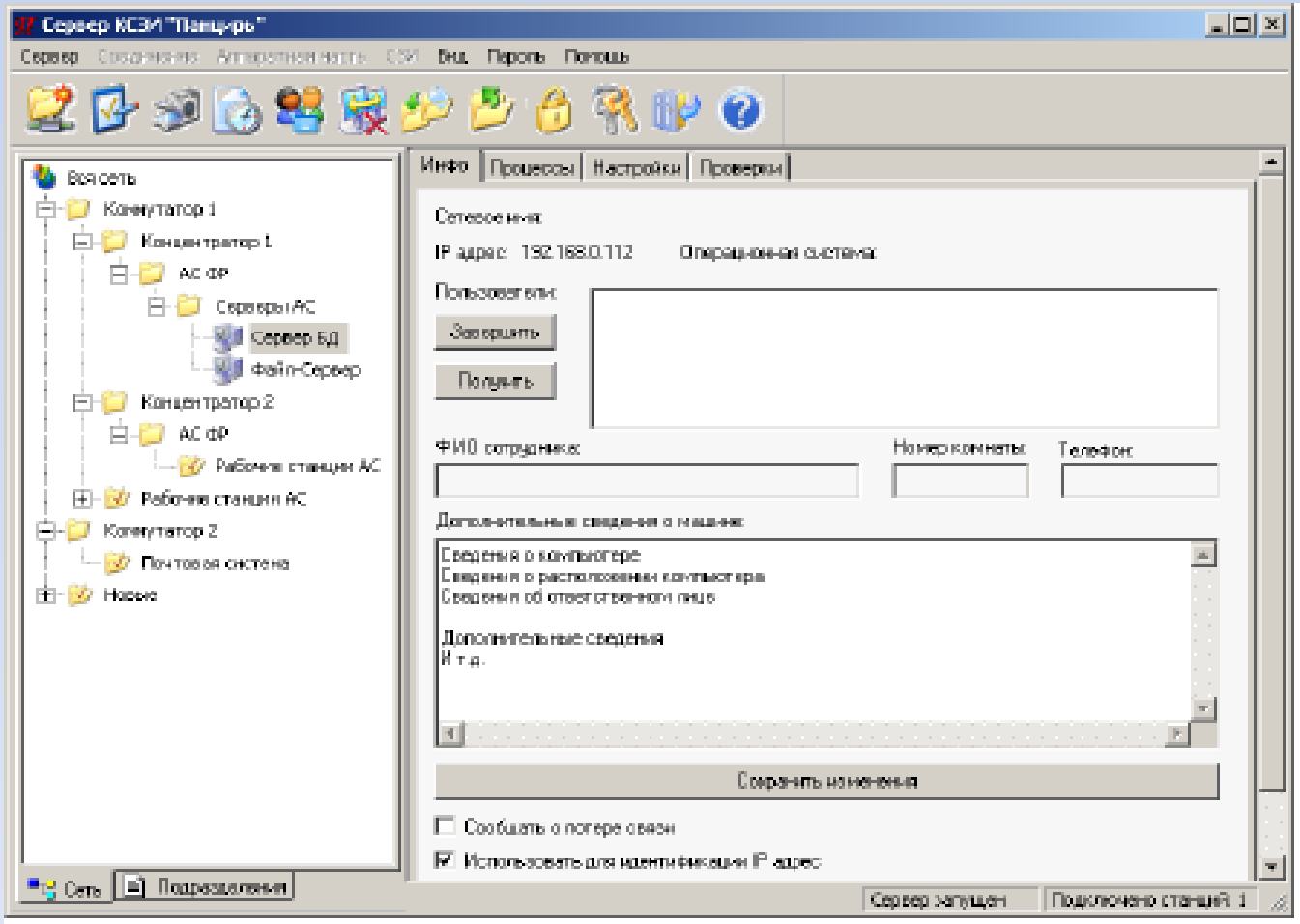
Сервер безопасности. Интерфейс



Сервер безопасности. Интерфейс



Сервер безопасности. Интерфейс

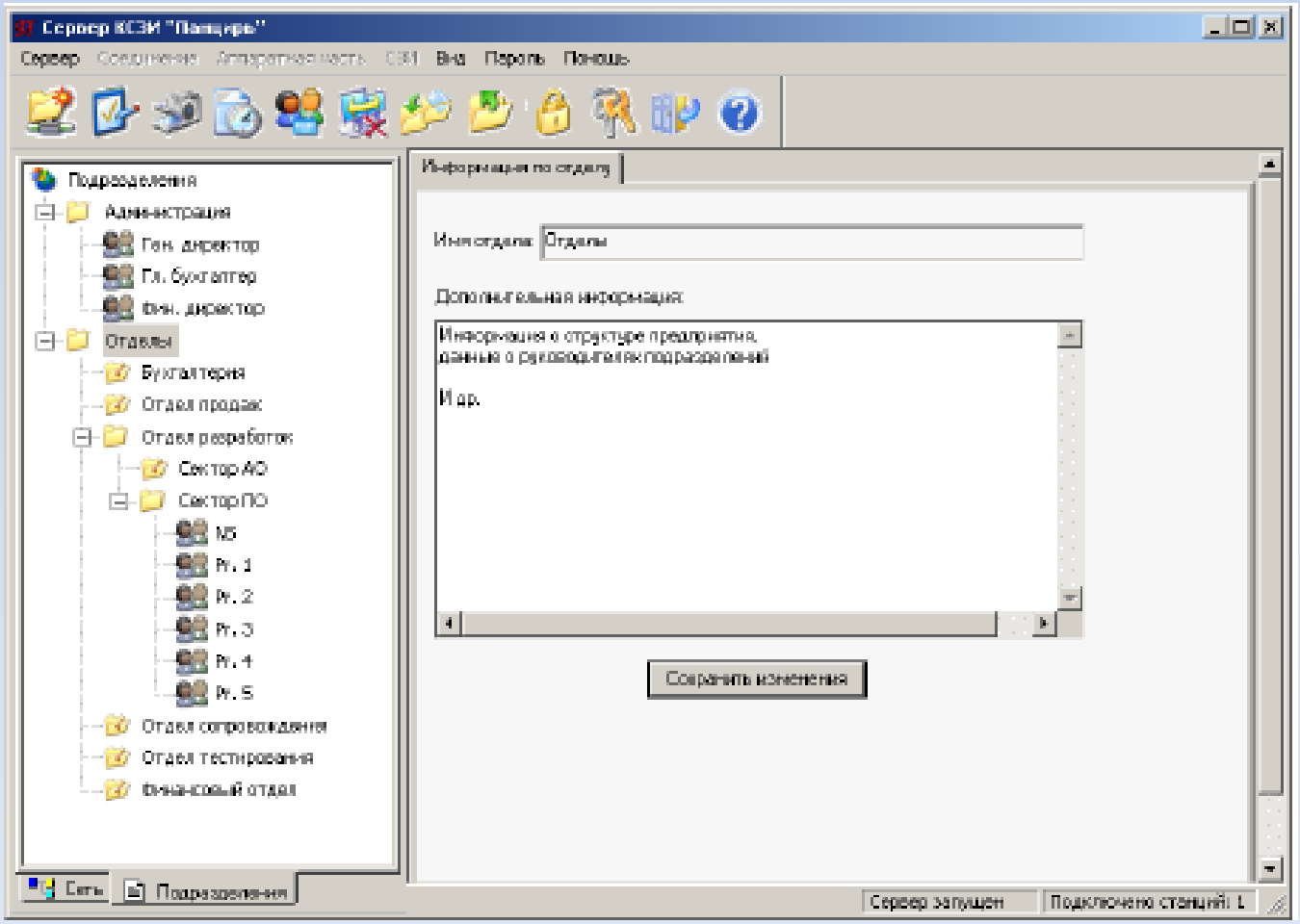


Сервер безопасности. Интерфейс

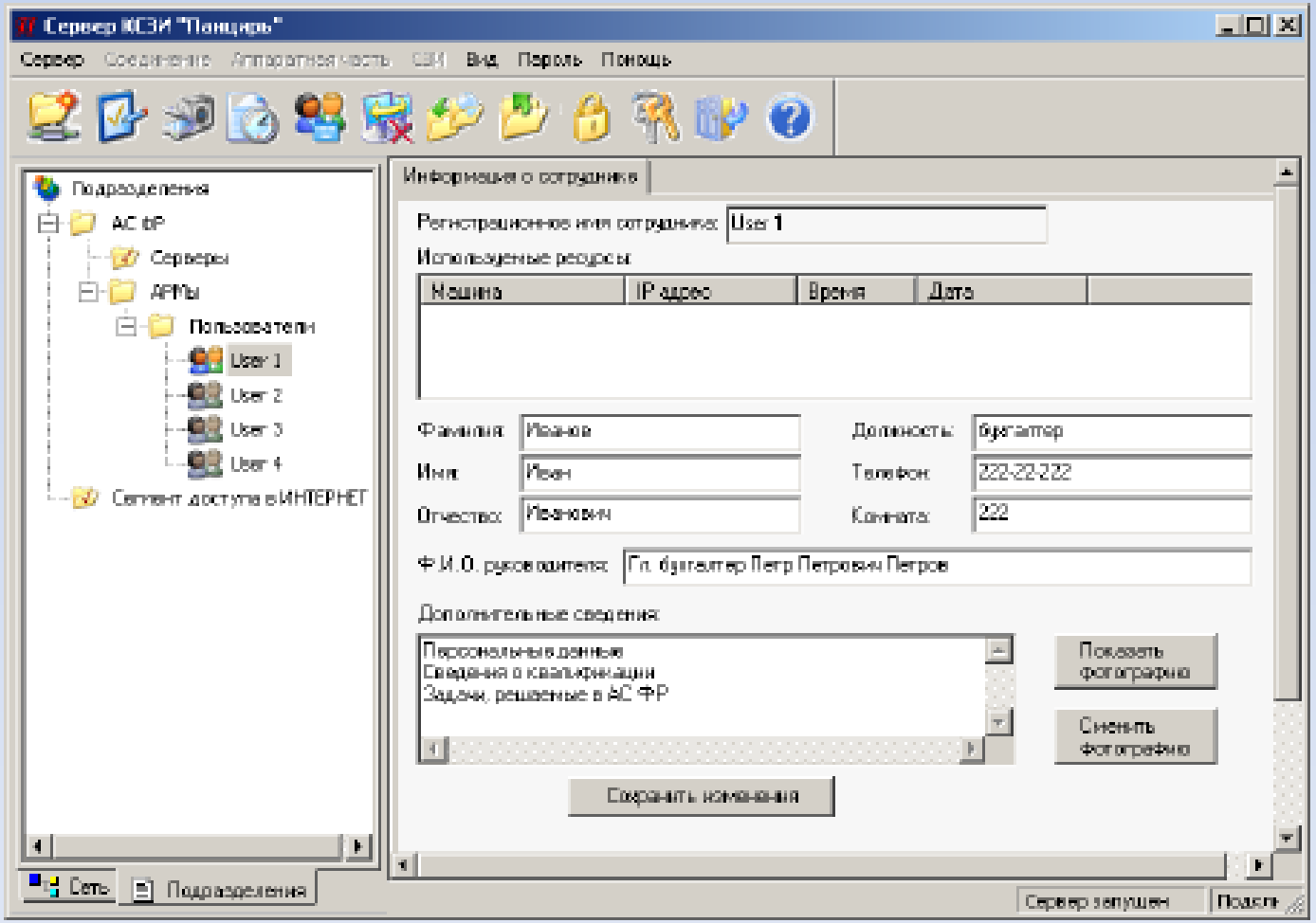
Представление на основе информации о пользователях:

- Отображение иерархической структуры пользователей на предприятии;
- Отображение функциональной принадлежности пользователей к АС;
- Отображение территориального расположения пользователей.

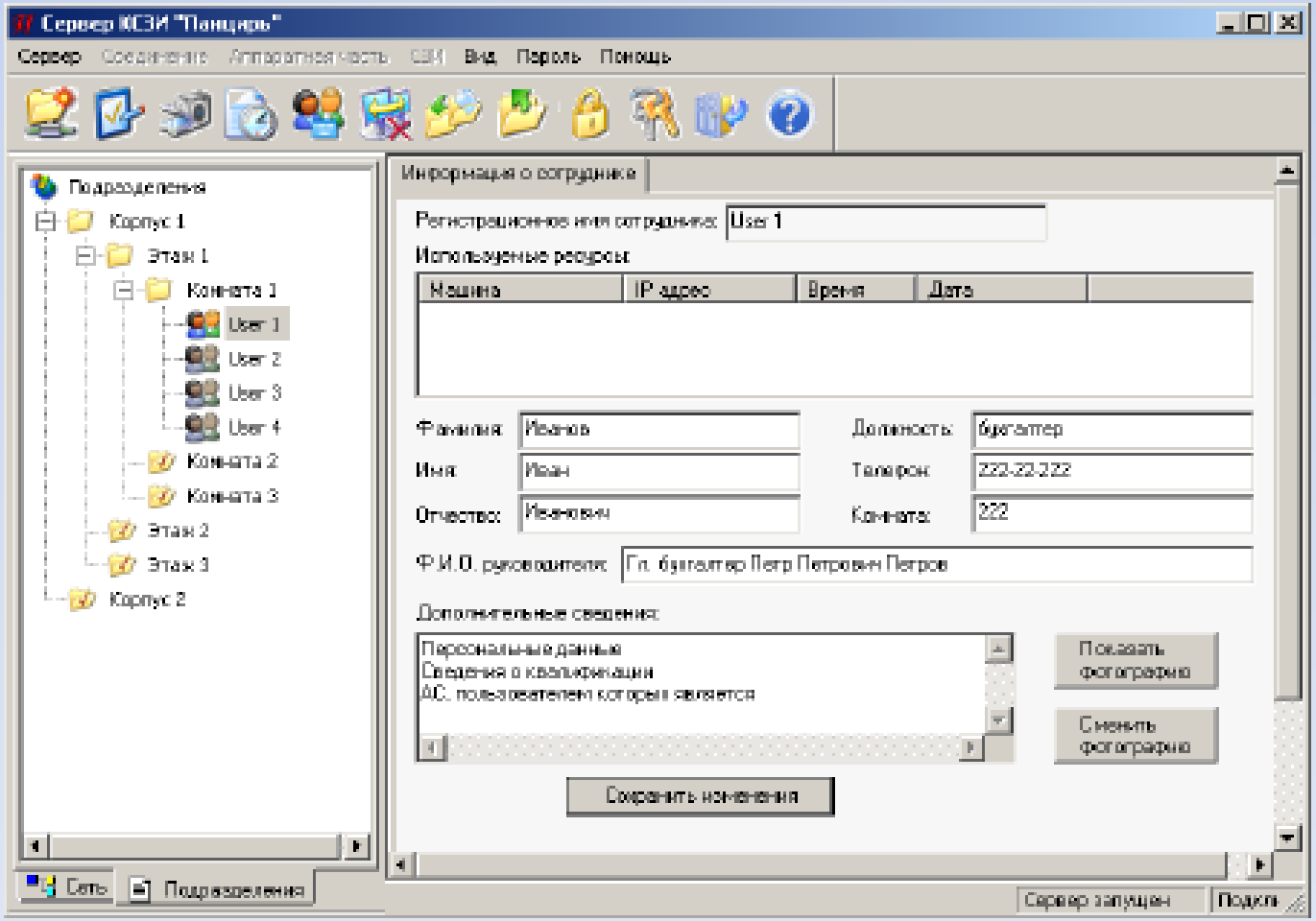
Отображение иерархической структуры пользователей



Отображение функциональной принадлежности пользователей



Отображение территориального расположения пользователей



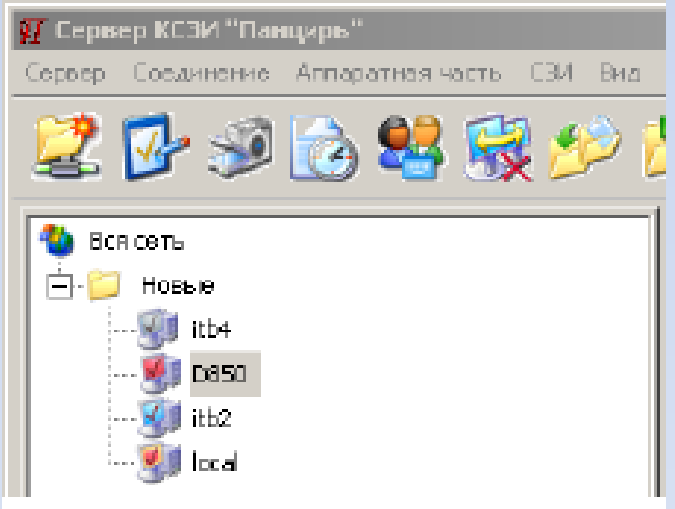
Состояния АС

1) станция выключена или не подключена к сети;

2) станция подключена к сети, но при соединении аутентификация не прошла;

3) станция подключена к сети, но КСЗИ на ней не активна;

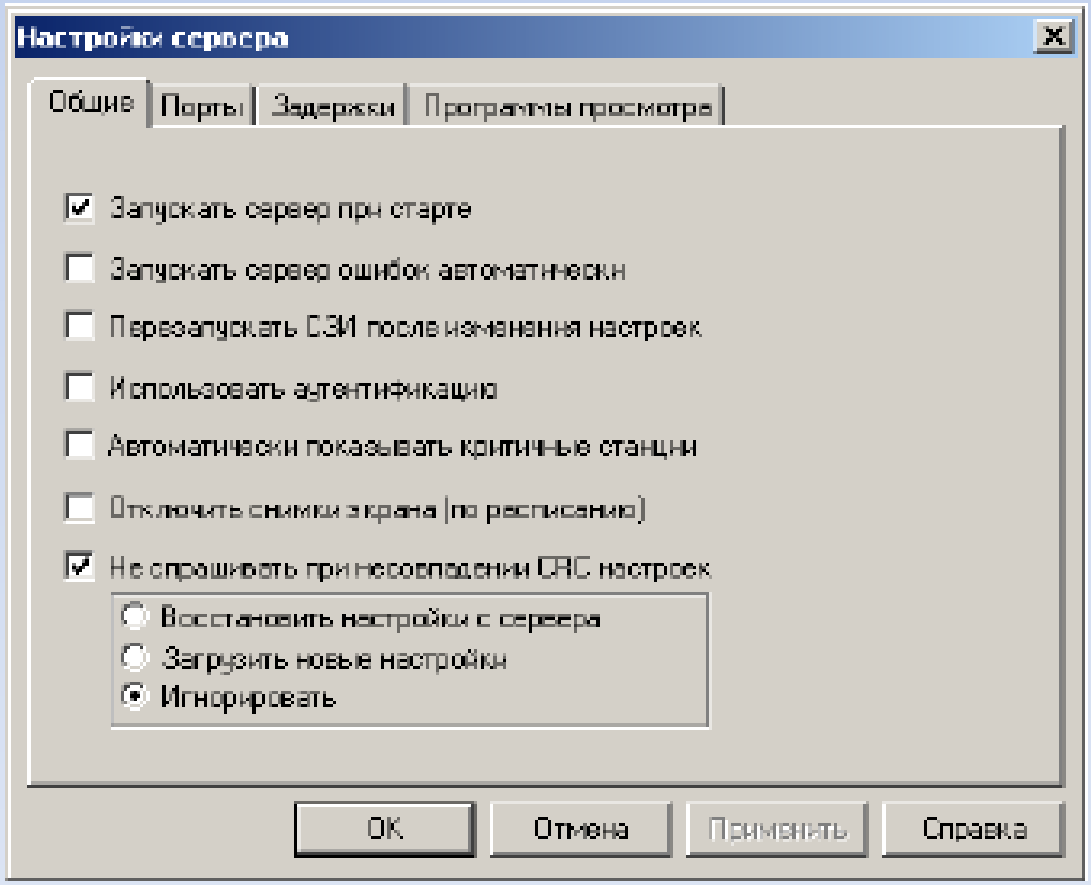
4) станция подключена к сети и на ней активна КСЗИ.



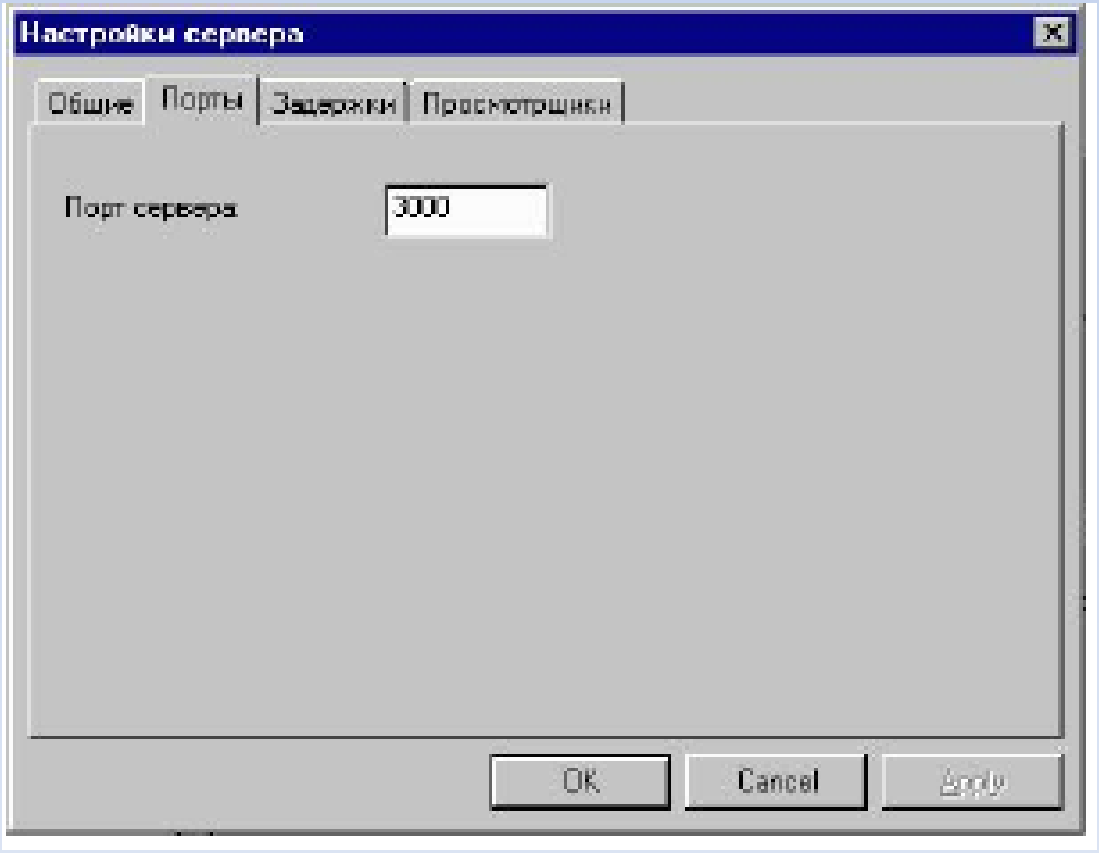
Настройки сервера. Общие

- Запускать сервер при старте
- Запускать сервер ошибок автоматически
- Перезапускать СЗИ после изменения настроек
- Использовать аутентификацию
- Автоматически показывать критичные станции
- Отключить снимки экрана (по расписанию)
- Не спрашивать при несовпадении CRC настроек

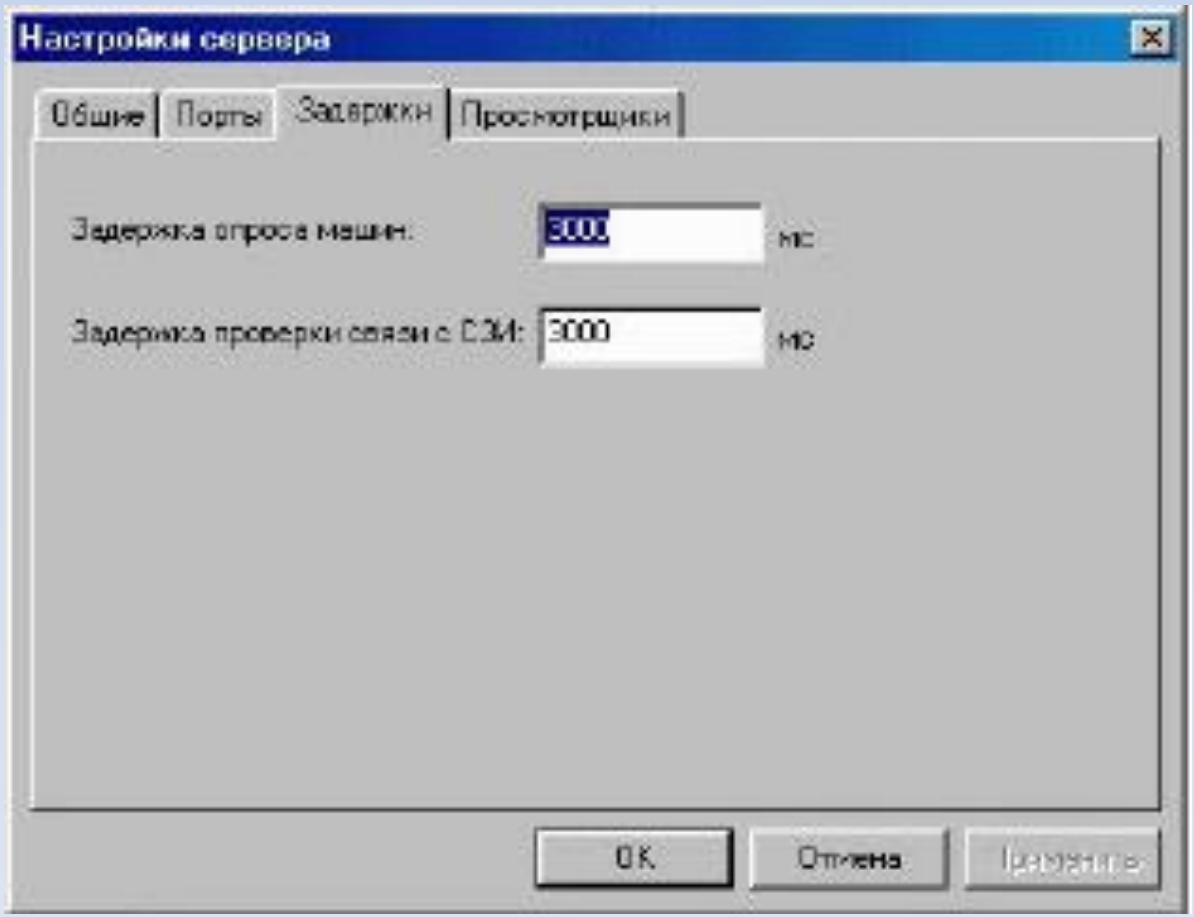
Настройки сервера. Общие



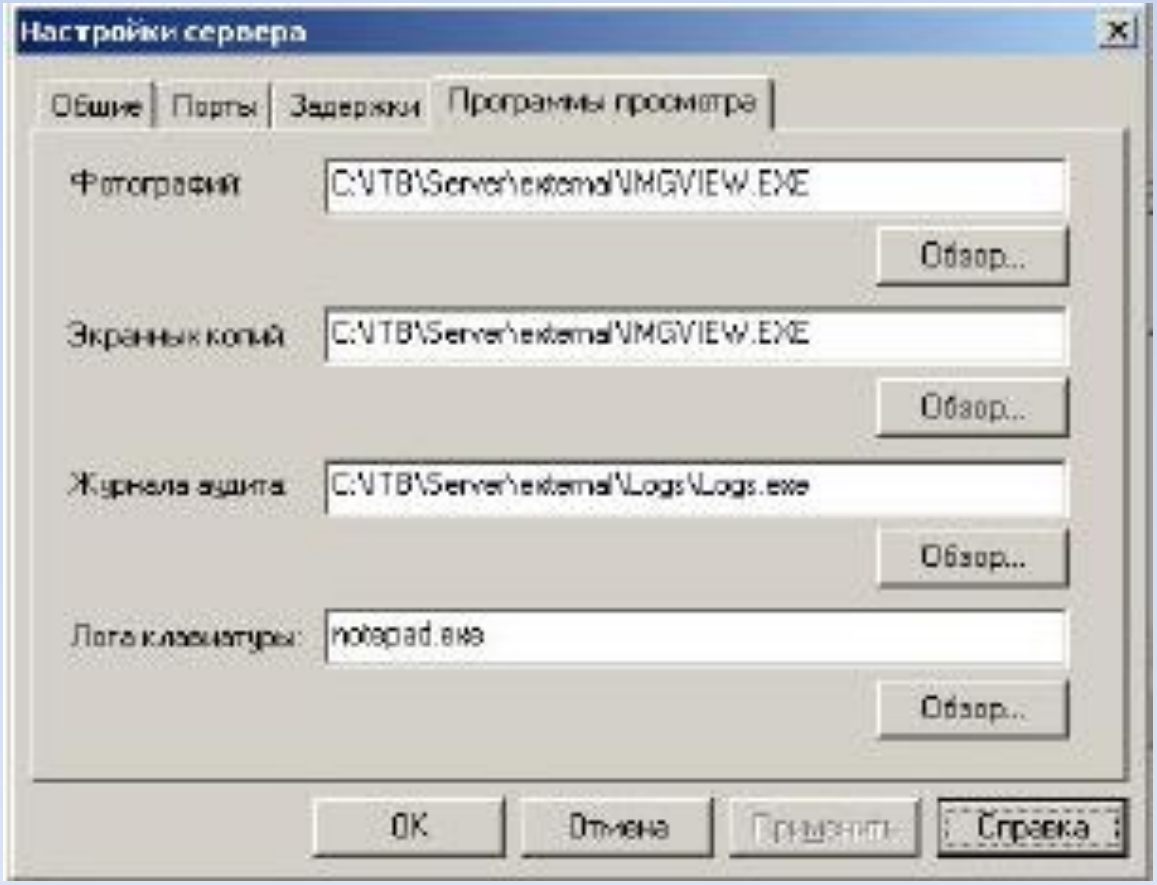
Настройки сервера. Порты



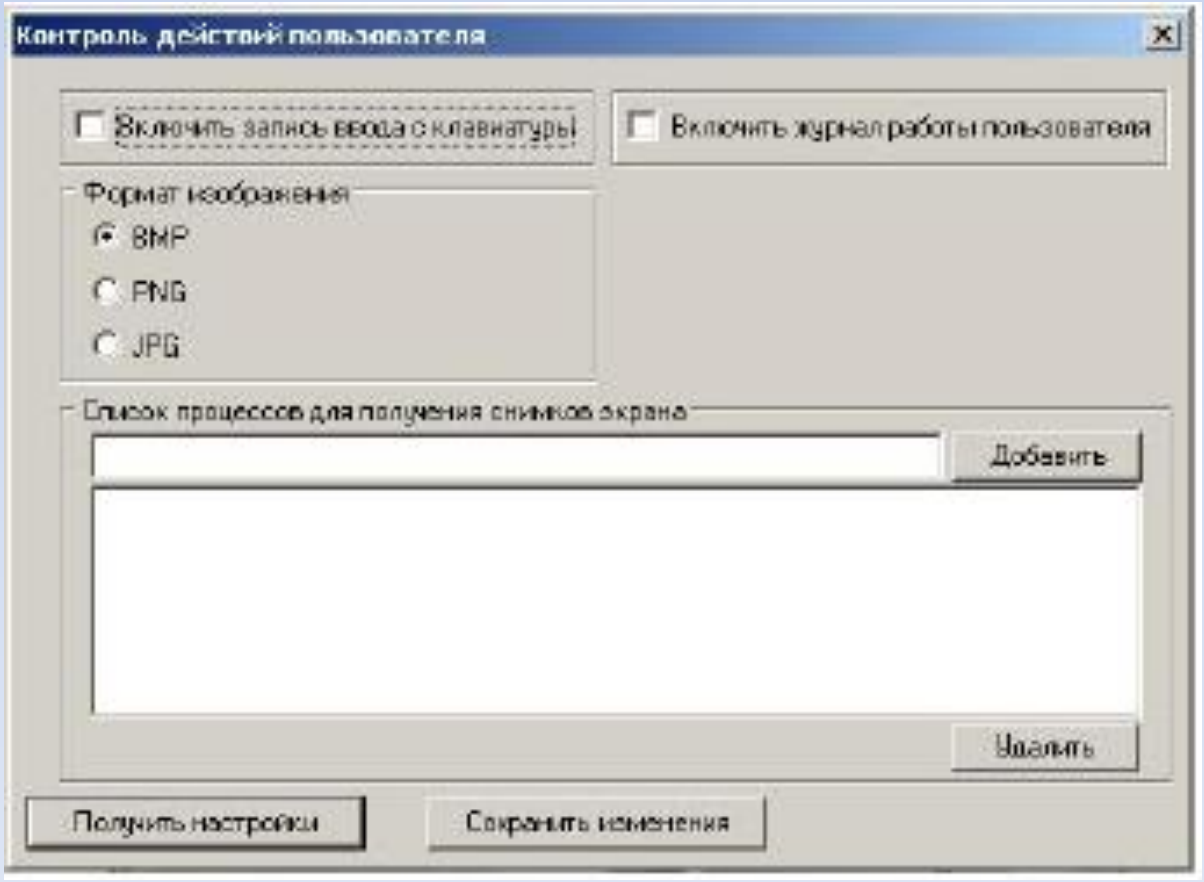
Настройки сервера. Задержки



Настройки сервера. Просмотрщики



Удаленная настройка параметров



Профили пользователей

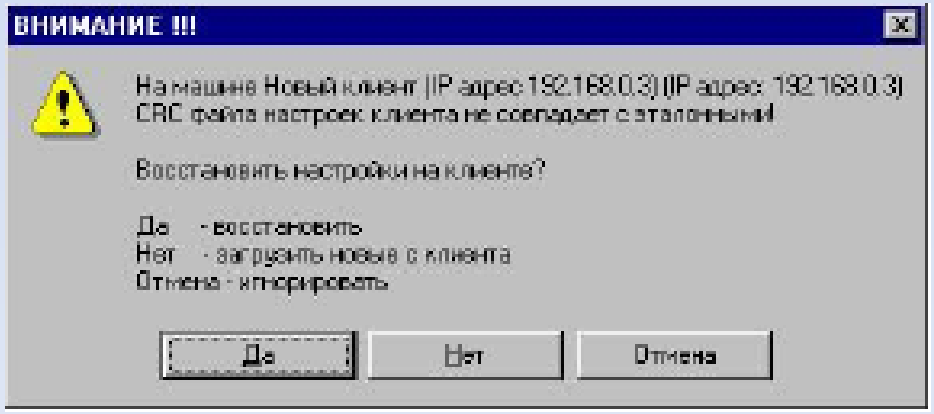
- Необходимы при добавлении новых пользователей, если основные настройки для них совпадают с настройками уже имеющихся пользователей

Профили пользователей

- Управление доступом к файловой системе, к разделяемым сетевым ресурсам, к съемным накопителям (дисковод, CD-ROM)
- Управление доступом к реестру ОС
- Управление доступом к Буферу Обмена
- Управление доступом к сетевым ресурсам по протоколу TCP/IP и др.
- Общие настроек клиентской части КСЗИ.

Синхронизация настроек

- Все настройки хранятся и на серверной и на клиентских частях!
- Кроме текущих настроек клиентских частей, на сервере хранятся копии последних 16 изменений настроек

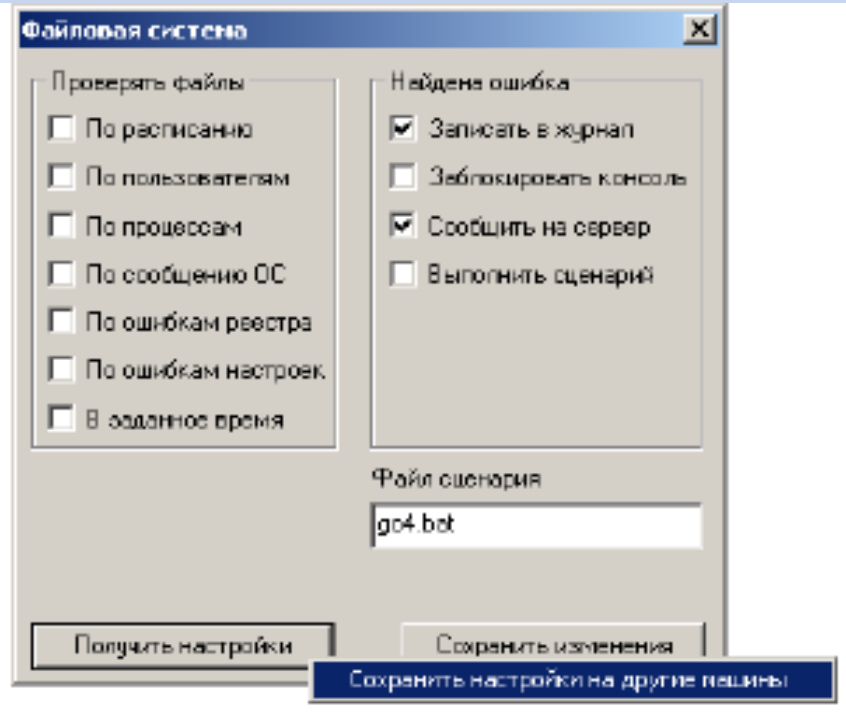


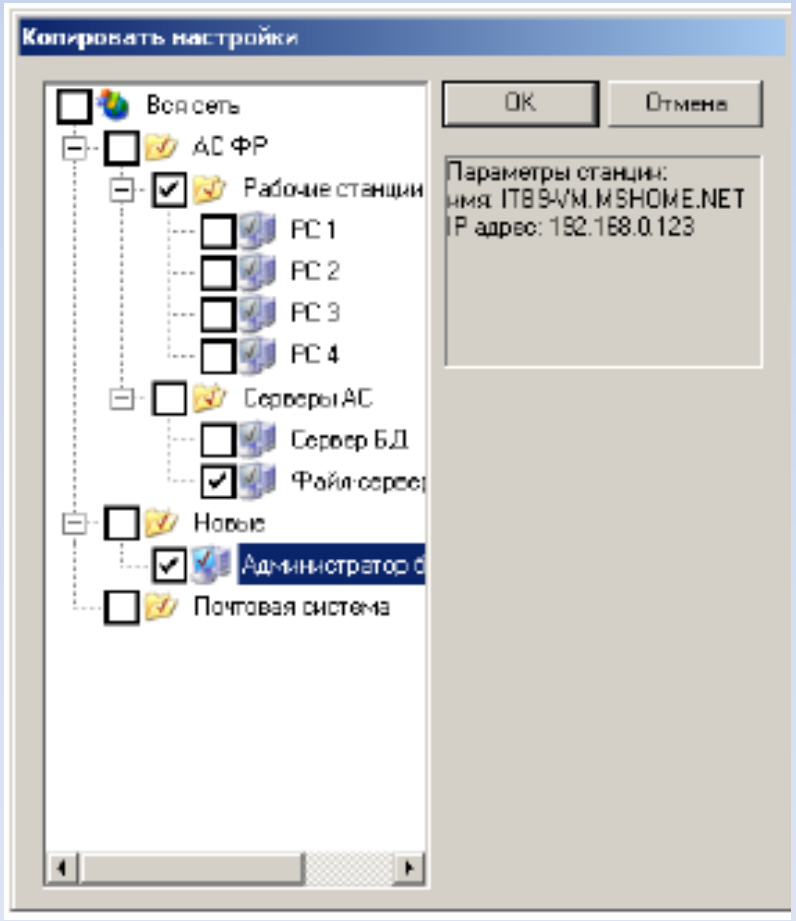
Синхронизация настроек

- Возможность синхронизации части настроек

Файл настроек	Описание
Tcpctrl.ini	Настройки управления доступом к сети по протоколу TCP/IP
Filectrl.ini	Настройки управления доступом к файловой системе, к разделяемым сетевым ресурсам, к съемным накопителям (дисковод, CD-ROM)
Regctrl.ini	Настройки управления доступом к реестру ОС
Printer.ini	Настройки управления доступом к принтерам
Dirlink.ini	Настройки доступа к временным каталогам пользователей КСЗИ
Clipctrl.ini	Настройки управления доступом к Буферу Обмена
Devctrl.ini	Настройки управления подключения устройств
Impctrl.ini	Настройки управления олицетворением субъектов доступа
Uparam.cfg	Настройки параметров учетных записей пользователей
Settings.set	Остальные настройки клиентской части КСЗИ

Тиражирование настроек





Контроль защищенности

- Информация о текущем пользователе
- Управление процессами на удаленной станции
- Проверки
- Мониторинг консоли

Информация о текущем пользователе

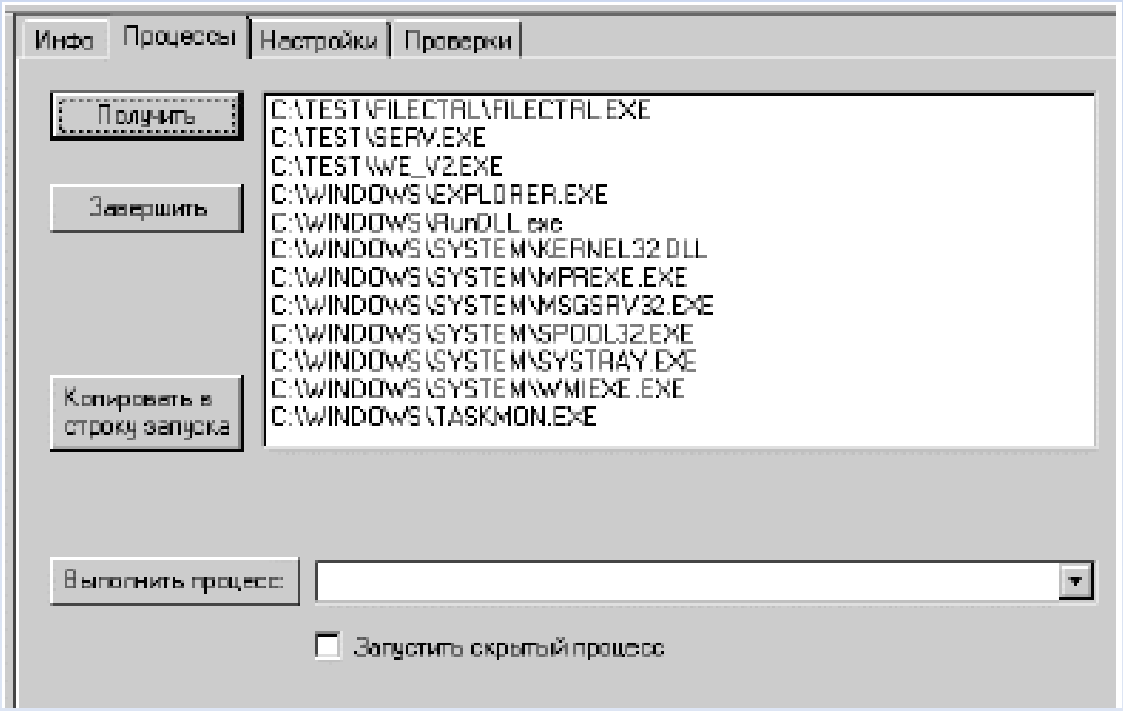
Отображает, какой пользователь в данный момент работает на удаленной станции, информацию о нем и рабочей станции

Имеется 2 опции:

- Сообщать о потери связи
- Использовать для идентификации IP адрес

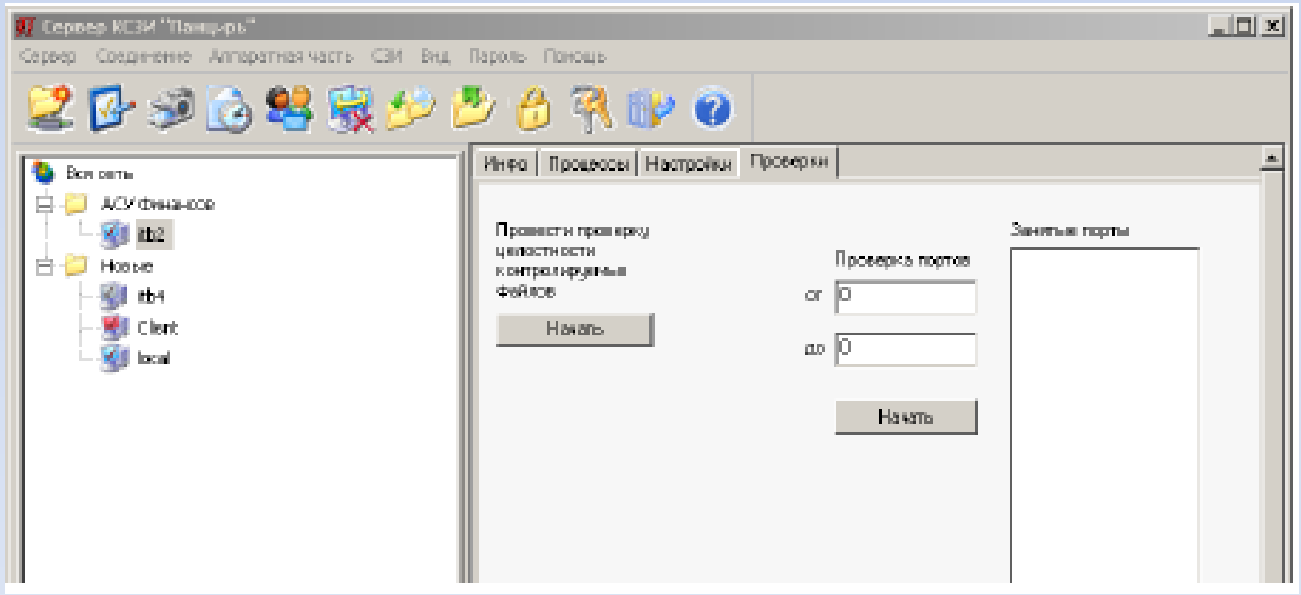
Управление процессами на удаленной станции

- Возможность запуска и завершения процессов, в т. ч. скрытых



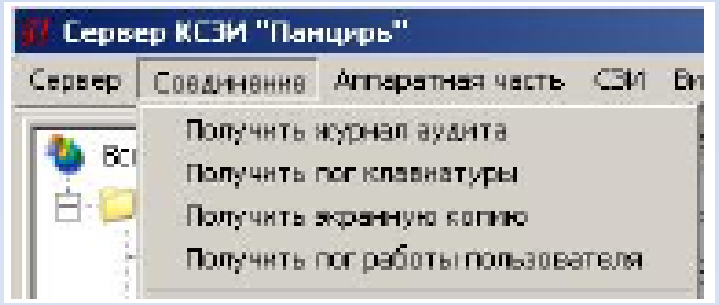
Проверки

- Целостности файловой системы
- Открытых портов



Мониторинг консоли

- Получить лог клавиатуры
- Получить экранную копию
- Получить лог работы пользователя

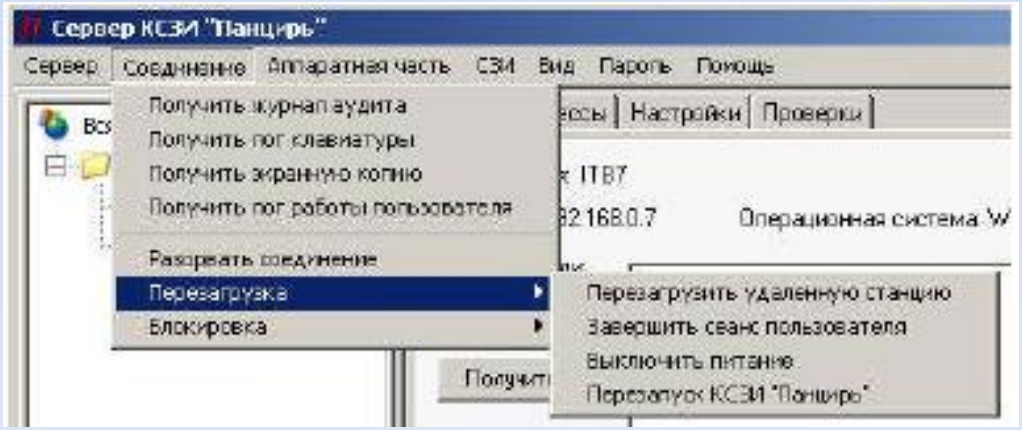


Управление соединением с удаленной станцией

- Перезагрузка
- Блокирование и приостановка
- Настройка соединения

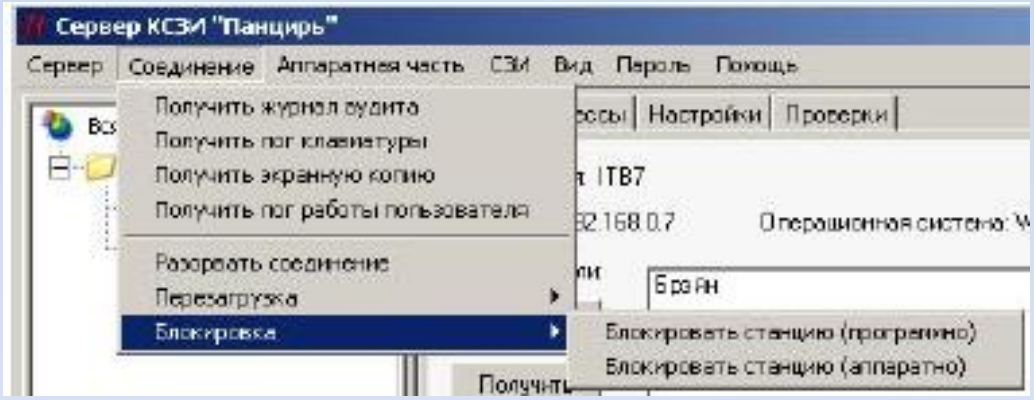
Меню «Перезагрузка»

- Перезагрузить удаленную станцию
- Завершить сеанс пользователя
- Выключить питание
- Перезапуск КСЗИ



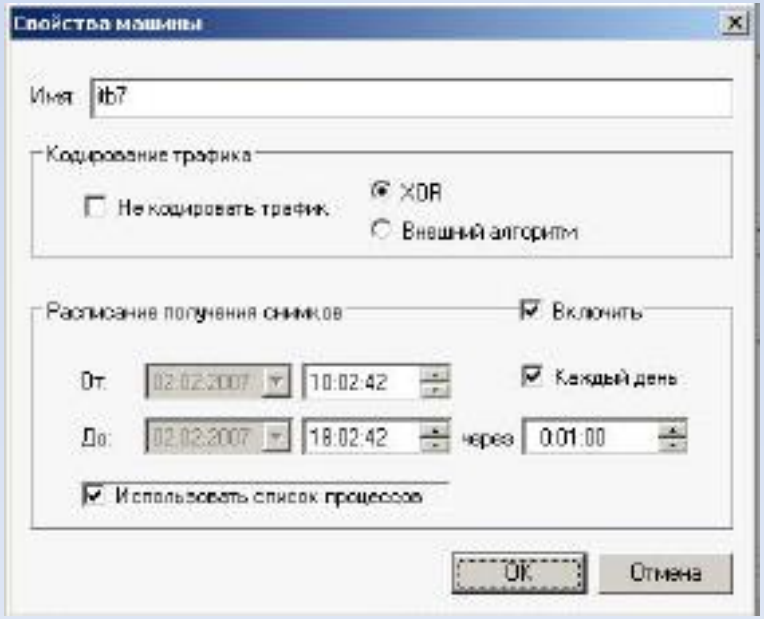
Меню «Блокировка»

- Блокировать станцию (программно)
- Блокировать станцию (аппаратно)



Настройка соединения

- Настройки клиента и сервера должны быть согласованы друг с другом!
- Ключ шифрования хранится в реестре

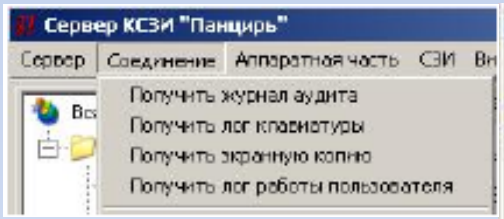


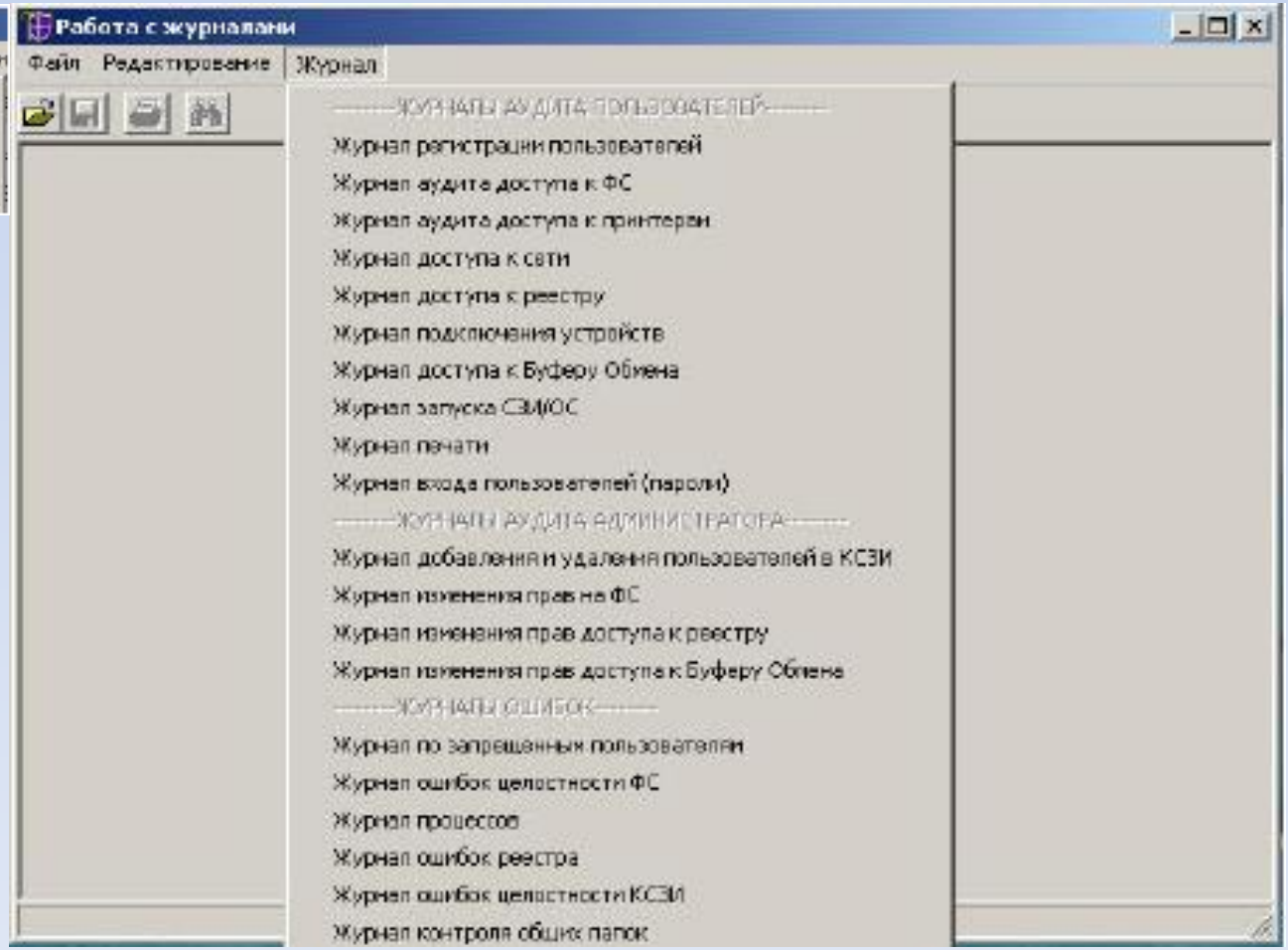
Аудит

Наблюдение за событиями:

- Механизм регистрации событий
- Механизм передачи сообщений об НСД и ошибках функционирования КСЗИ

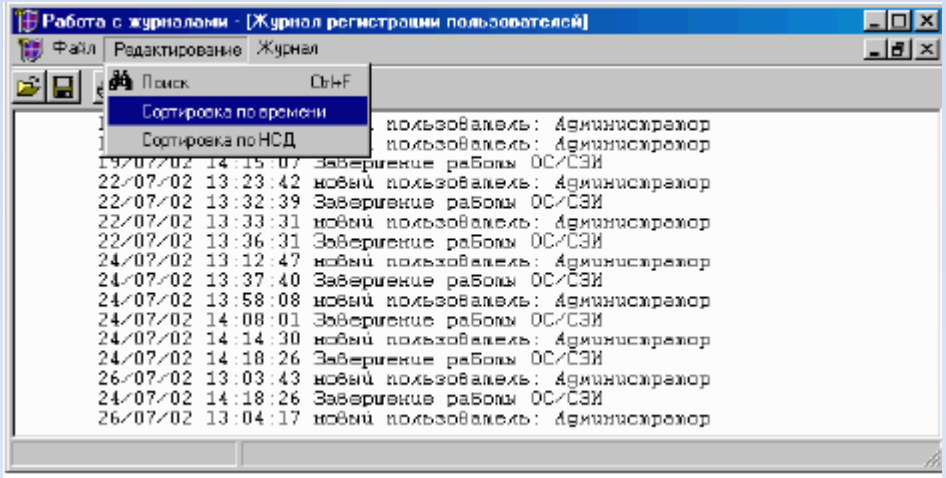
Работа с журналами аудита





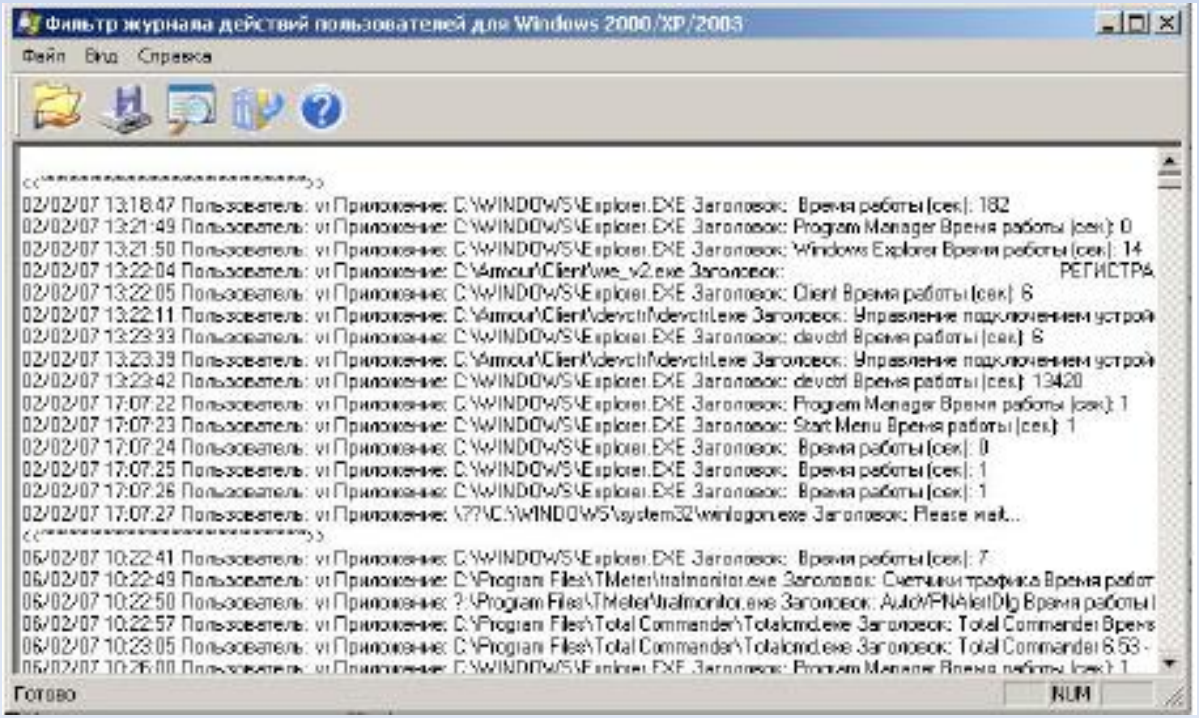
Работа с журналами аудита

- Поиск по сообщению
- Фильтрация по событиям НСД
- Фильтрация по времени



Работа с логом пользователя

- Статистика по работе пользователя со всеми, или отдельной программой за заданный интервал времени

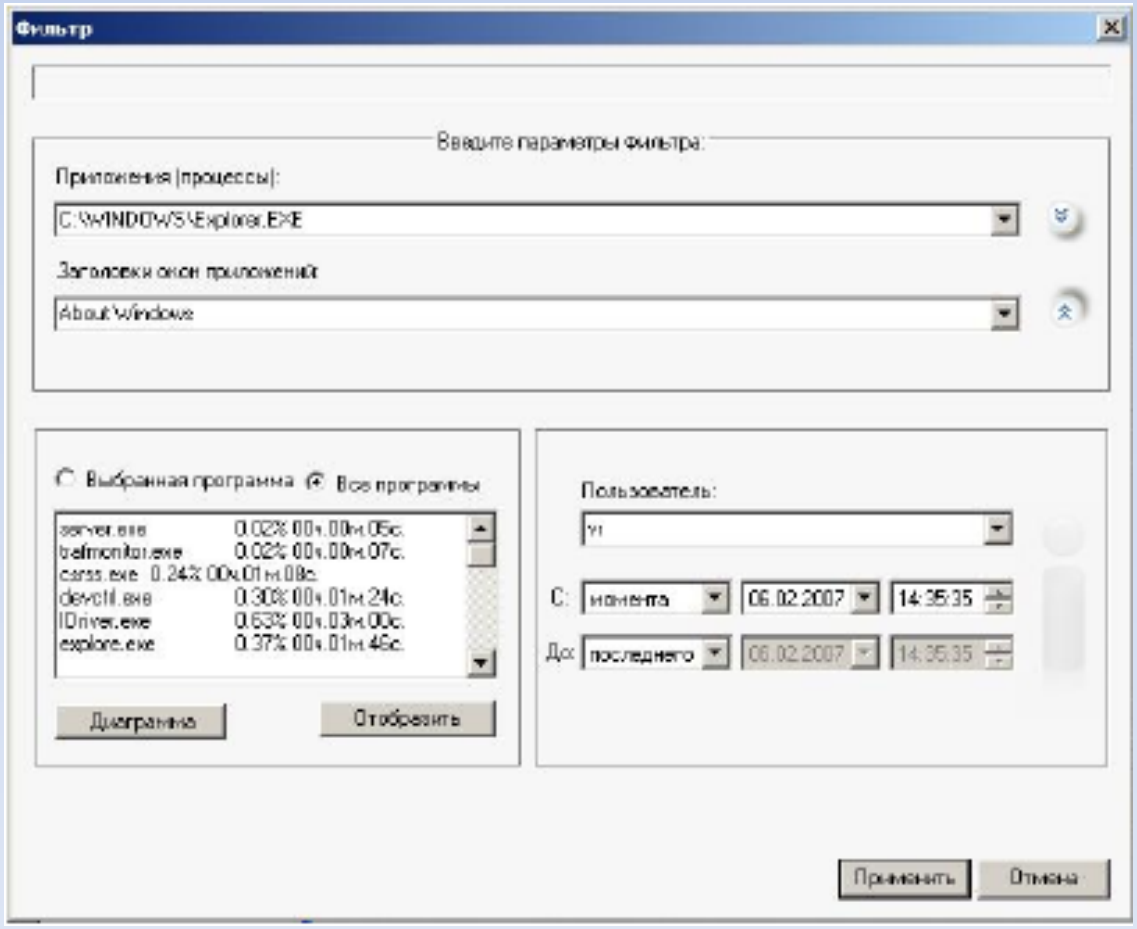


Работа с логом пользователя

Фильтрация :

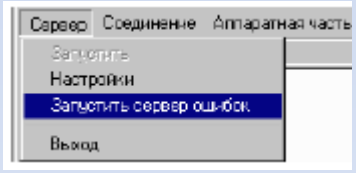
- Приложения (процессы);
- Заголовки окон приложений;
- Пользователь;
- Дата.

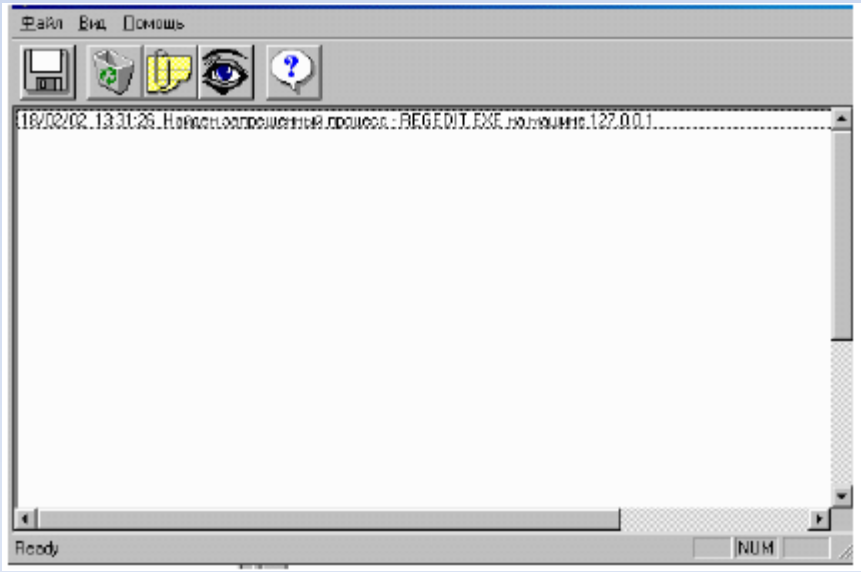
Работа с логом пользователя



Работа с сервером ошибок

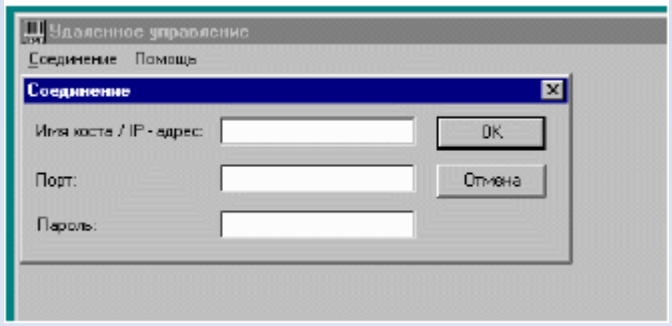
- Сообщения об ошибках, допущенных механизмами, реализующими разграничение доступа к ресурсам.

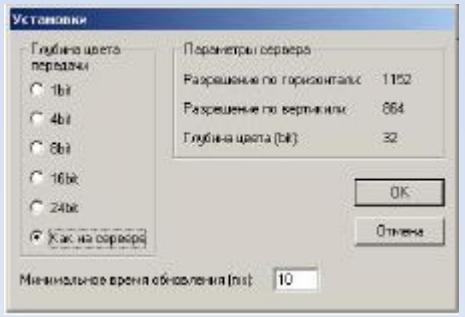




Удаленное управление рабочей станцией

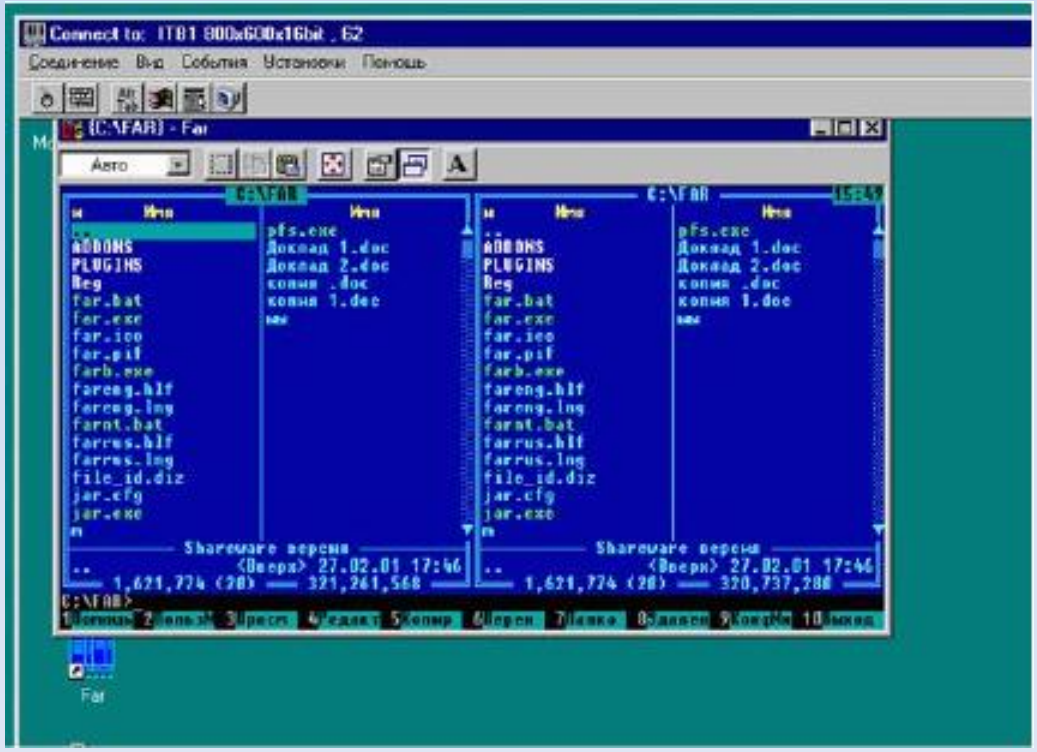
- Находится в каталоге RemoteAccess
- На клиенте должен быть запущен процесс client.exe (для удаленного управления)





Удаленное управление рабочей станцией

- Клиент удаленного управления запускается с правами текущего пользователя



КСЗИ «Панцирь-К». Идентификация и аутентификация пользователей

Механизмы идентификации и аутентификации

- Аутентификация пользователей и администратора безопасности при доступе в систему
- Аутентификация пользователей при доступе к критичным локальным или разделенным в сети файловым объектам
- Аутентификация ответственного лица при запуске сетевых служб (приложений)

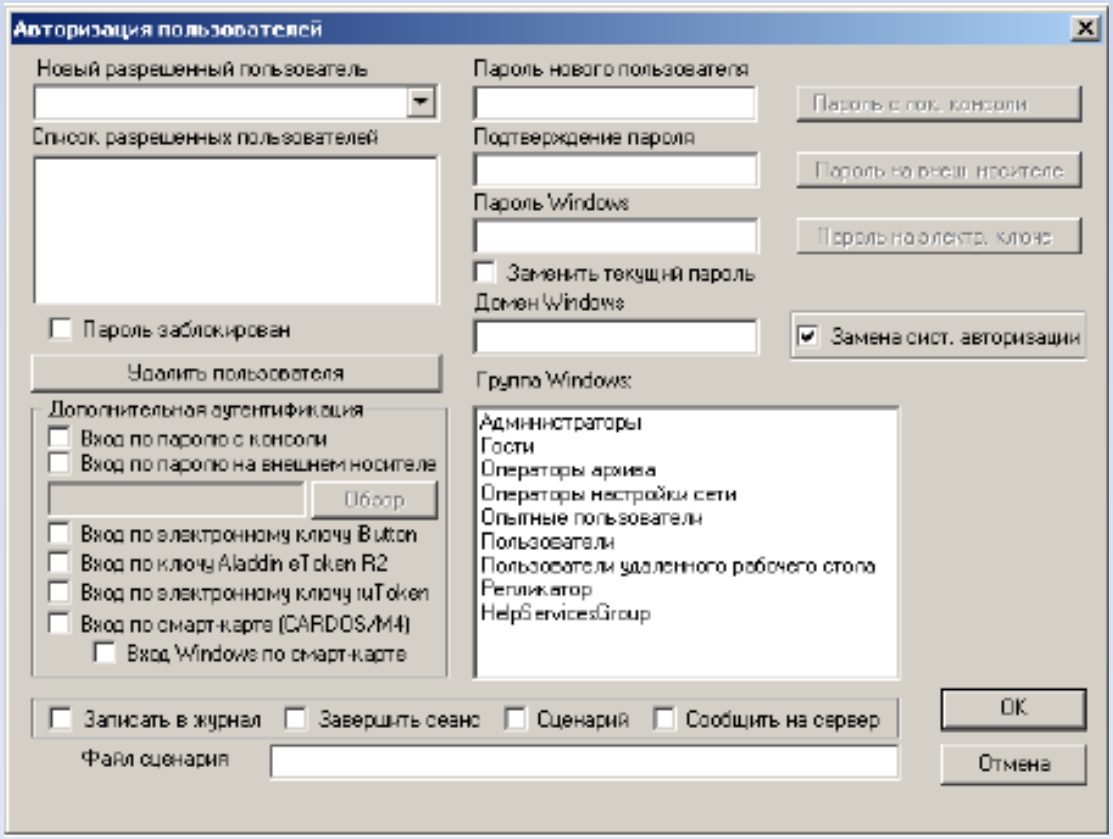
Режимы авторизации

Два режима авторизации:

- Одноуровневый (СКЗИ)
- Двухуровневый (СКЗИ + штатные средства)

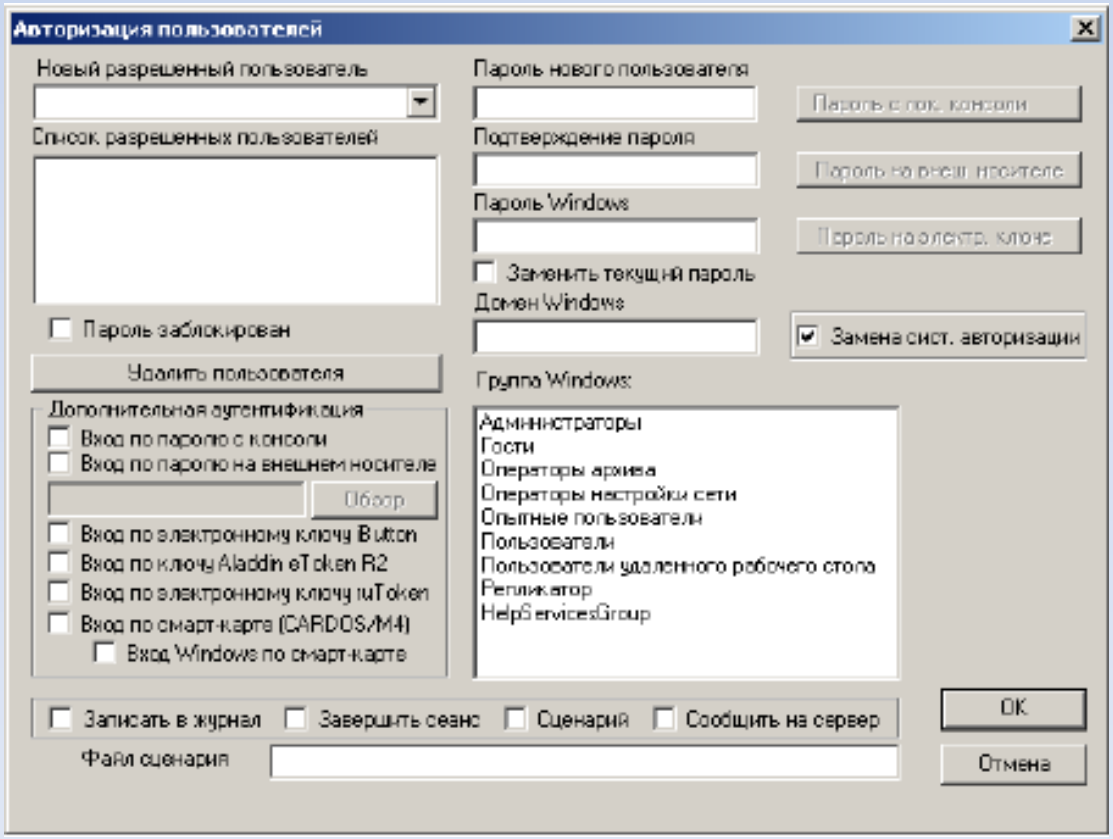
Настройка механизма авторизации

- Переключение режимов авторизации - флаг “Замена системной авторизации”



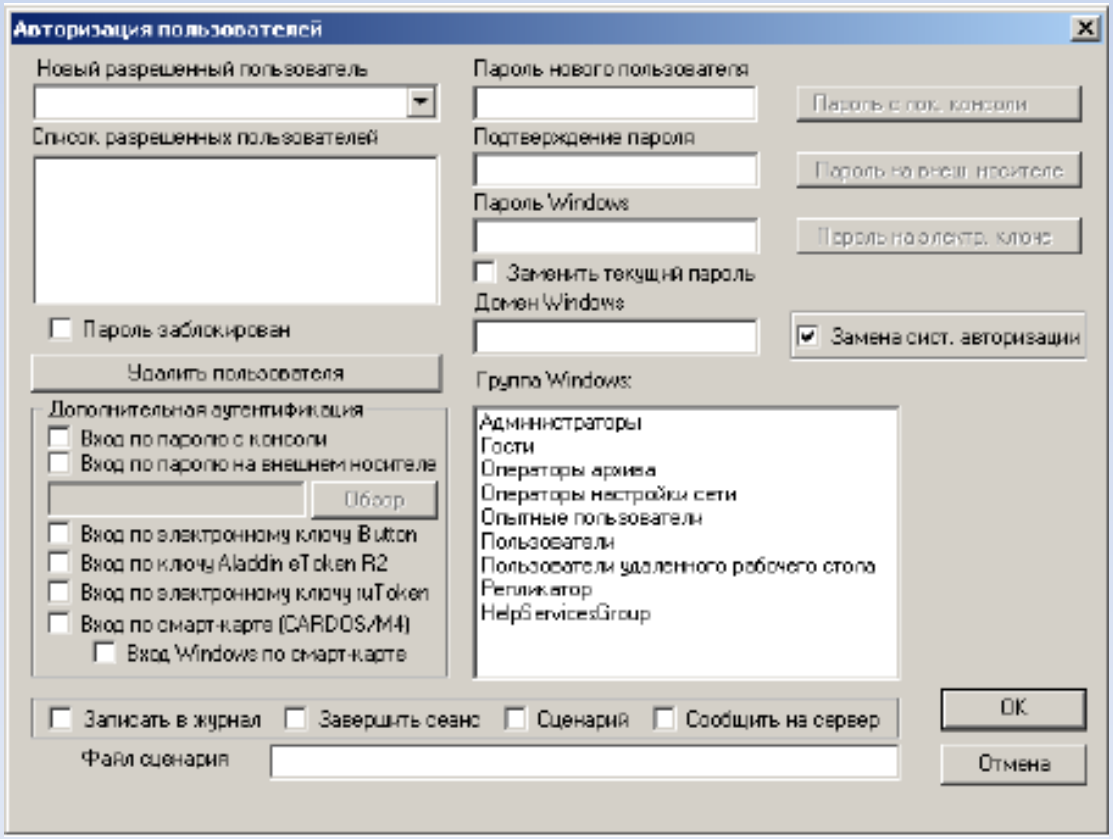
Настройка механизма авторизации

1. В окне «Авторизация пользователей» указать способ аутентификации



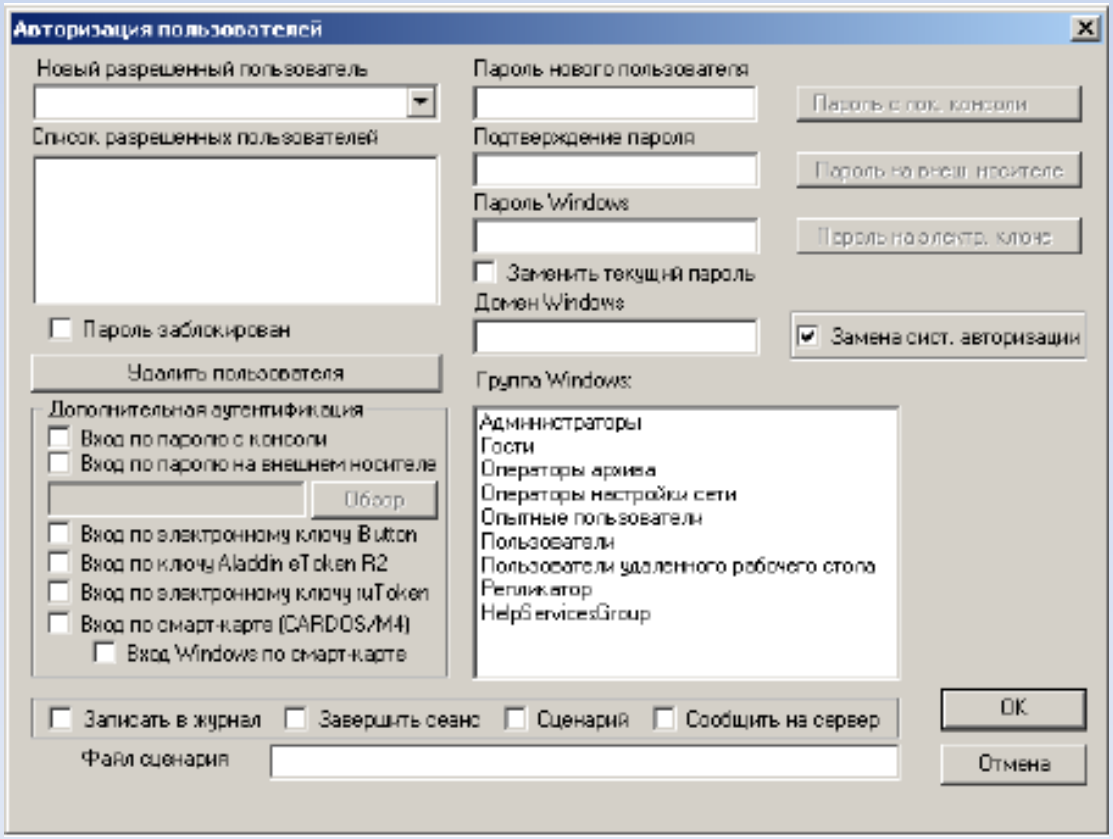
Настройка механизма авторизации

2. В списке «Новый разрешенный пользователь» выбрать пользователя



Настройка механизма авторизации

3. Ввести пароль (СКЗИ + Windows)

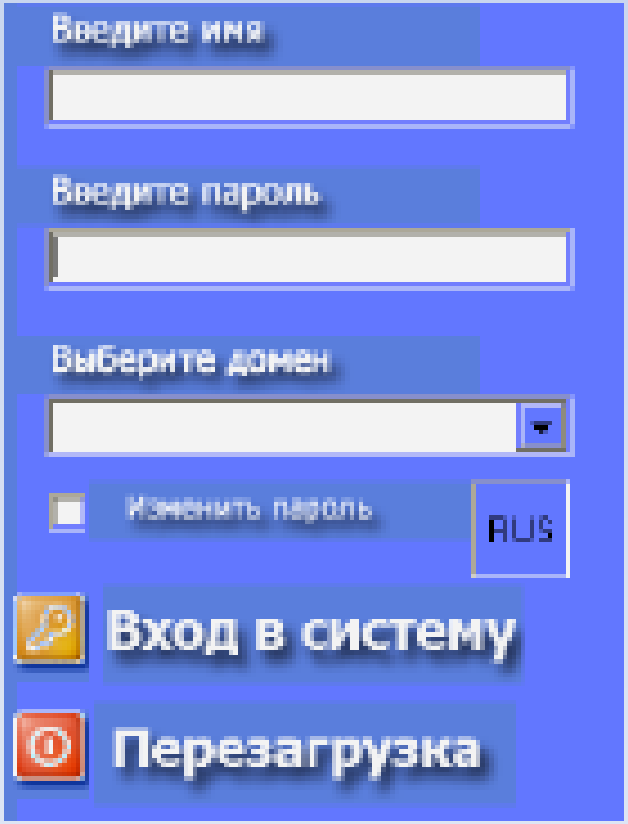


Способы входа

- Вход по паролю с консоли
- Вход по паролю на внешнем носителе
- Вход по электронному ключу i-Button
- Вход по ключу Aladdin eToken R2
- Вход по электронному ключу ruToken
- Вход по смарт-карте (CARDOS/M4)

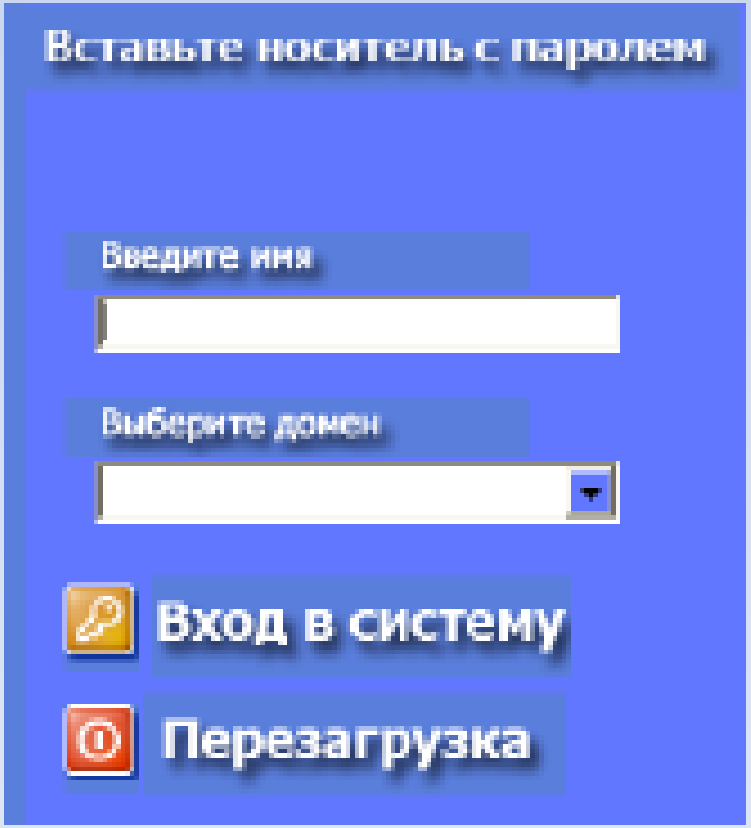
Вход в систему

- Окно авторизации:



Ввод пароля с внешнего носителя

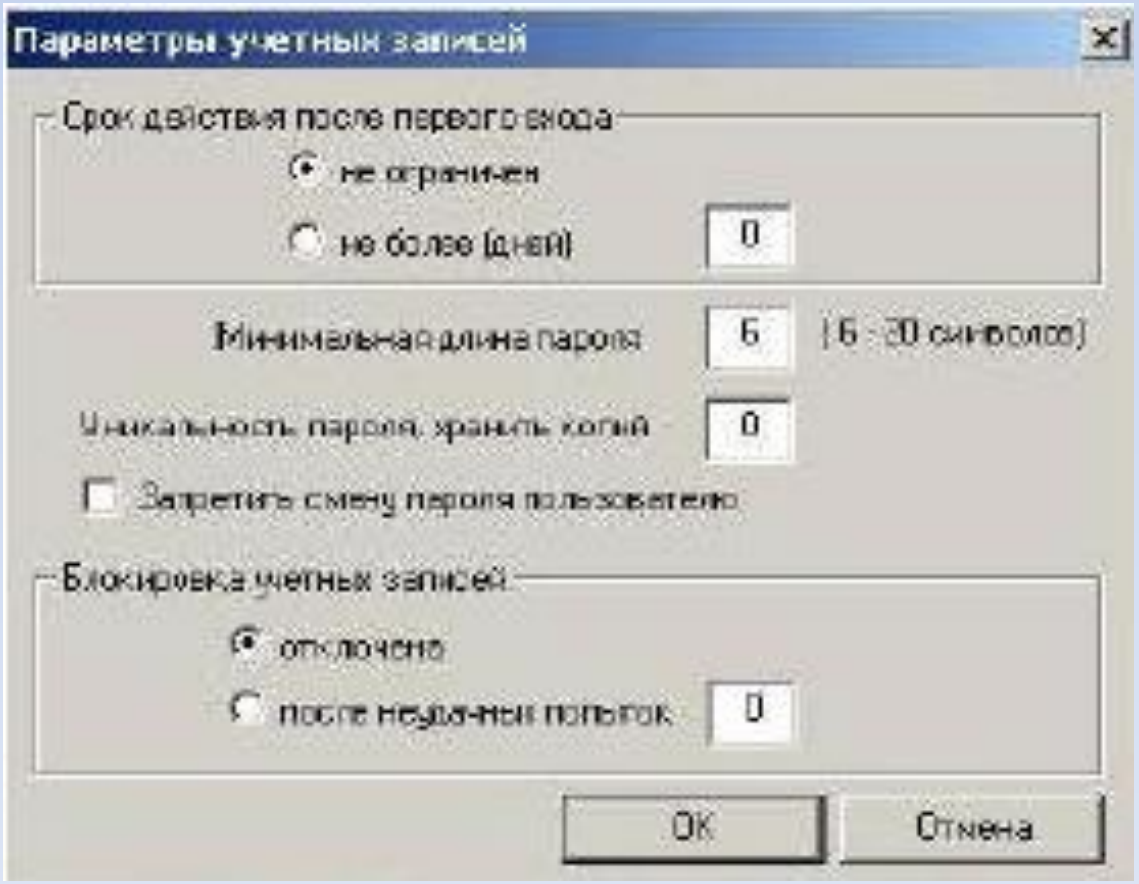
- Окно авторизации:



Ограничения на пароль

- Длина пароля (от 6 до 20 символов)
- Количество попыток ввода неверного пароля
- Запрет смены пароля пользователем
- Срок действия пароля с момента первого входа пользователя (от 0 до 999 дней)
- Уникальность пароля (хранится до 9 последних паролей)

Ограничения на пароль



РАЗГРАНИЧЕНИЕ ДОСТУПА К ФАЙЛОВОЙ СИСТЕМЕ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

Разграничение доступа к ФС

Виды файловых объектов:

- Файлы на жестком диске;
- Удаленные файловые объекты (разделенные в сети);
- Файловые объекты на внешних носителях.

Основные принципы разграничения доступа к ФС

- Только администратор может назначать (изменять) права доступа субъекта к объекту, такой сущности, как “Владелец” не существует;
- Две политики контроля доступа к ресурсам – разрешительная и запретительная.;
- Права доступа назначаются субъектам, а не присваиваются объектам в качестве их атрибутов;
- Для любого субъекта доступа может быть реализована собственная разграничительная политика;

Основные принципы разграничения доступа к ФС

- Для каждого устанавливаемого типа доступа может быть использована собственная разграничительная политика «Разрешенные для…», либо «Запрещенные для…»;
- Типы доступа к ресурсам - «Чтение», «Запись», «Выполнение»;
- Объект, задается своим полнопутевым именем (логический диск, каталог, подкаталог, файл), либо используются маски;
- Разграничения действуют иерархически, права нижестоящего объекта наследуются у вышестоящего, если для него не заданы собственные права доступа;

Основные принципы разграничения доступа к ФС

- В качестве самостоятельных субъектов доступа в КСЗИ используются две сущности: «ПОЛЬЗОВАТЕЛЬ» и «ПРОЦЕСС». Права для субъекта процесс могут назначаться эксклюзивно и совместно с правами пользователя;
- Субъект доступа «ПРОЦЕСС» задается своим полнопутевым именем. Для задания объекта могут использоваться маски;
- Для прав доступа субъекта «ПРОЦЕСС» используется механизм наследования.

Правила назначения прав доступа

Чтобы задать разграничения субъекту (процессу или пользователю) необходимо выполнить следующие действия:

1. Задать имя субъекта, для которого устанавливаются разграничения.
2. Выбрать тип доступа к ресурсу.
3. Задать полнопутевое имя объекта.

Правила действия разрешений. Разрешительная политика

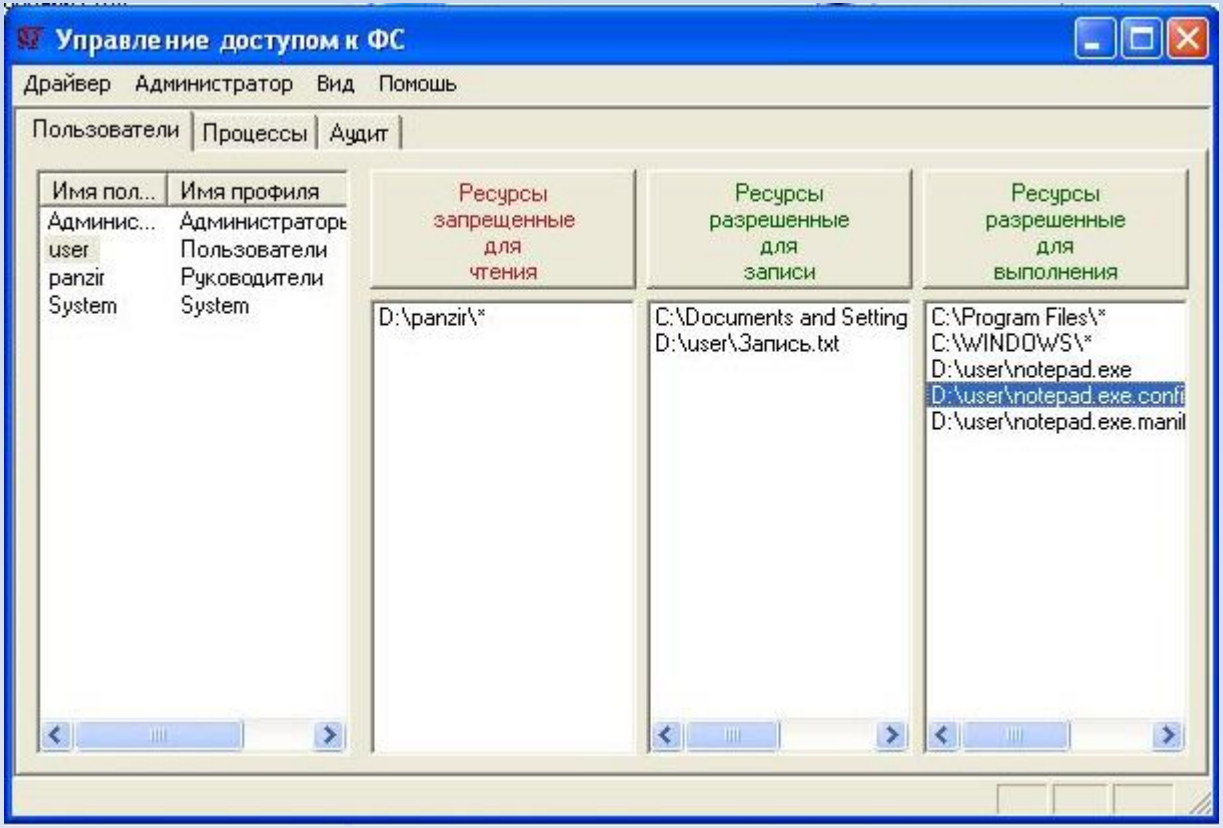
Папка, которой выдаются разрешения: C:\doc\

Разрешение / Права доступа	Чтение	Запись	Выполнение
Обзор	+	+	+
Чтение	+	+	+
Создание, модификация, удаление	-	+	-
Выполнение	-	+	+

Правило настройки разграничений

1. Задаются ресурсы, разрешенные для записи (при этом они автоматически разрешаются и для чтения),
2. Задаются ресурсы, разрешенные для выполнения (при этом они автоматически разрешаются и для чтения),
3. Задаются ресурсы, разрешенные для чтения (которые при этом не разрешаются для записи и выполнения).

Правила действия разрешений. Разграничение доступа пользователей



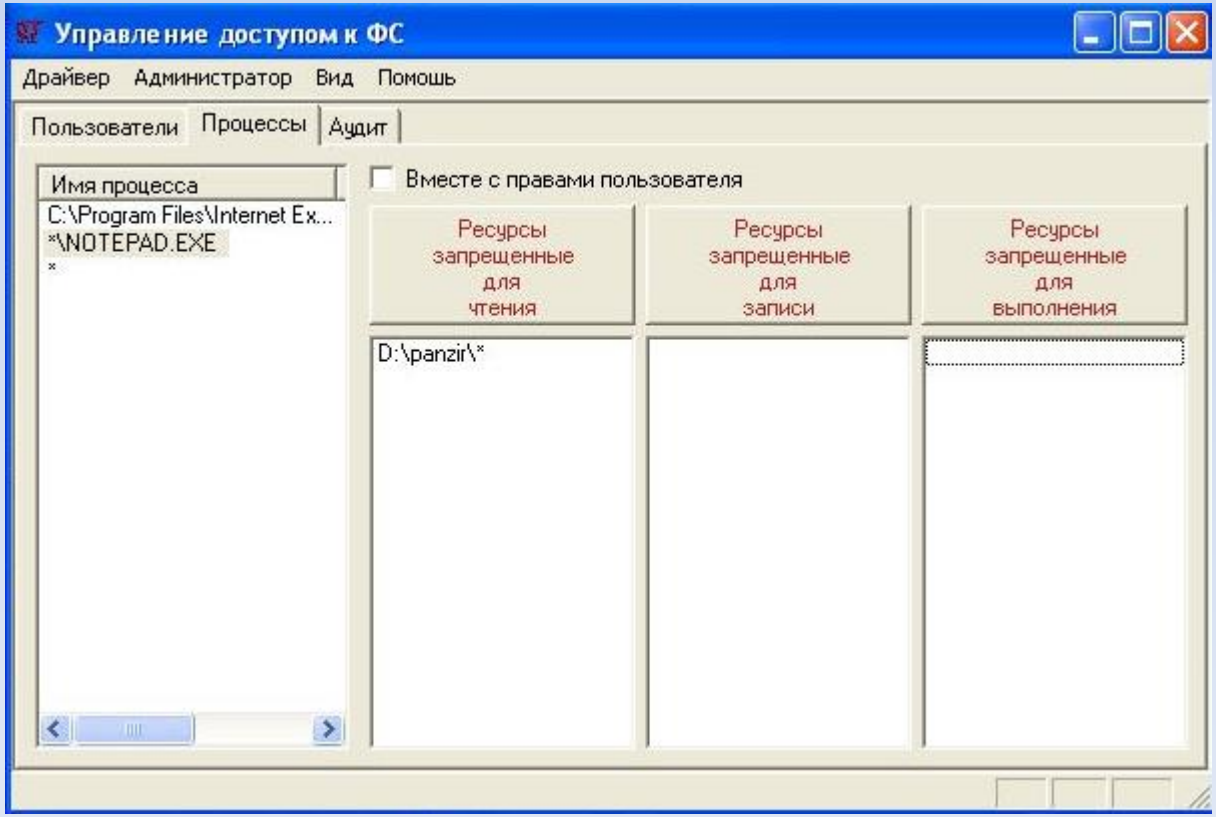
Правила действия разрешений. Запретительная политика

Папка, которой запрещаются действия: C:\doc\
Права доступа для этой папки:

Запрещение / Права доступа	Чтение	Запись	Выполнение
Обзор	-	+	+
Чтение	-	+	+
Создание, модификация, удаление	-	-	+
Выполнение	-	+	-

Ко всем остальным ресурсам, разрешен ПОЛНЫЙ доступ!

Правила действия разрешений. Разграничение доступа процессов



Создание масок

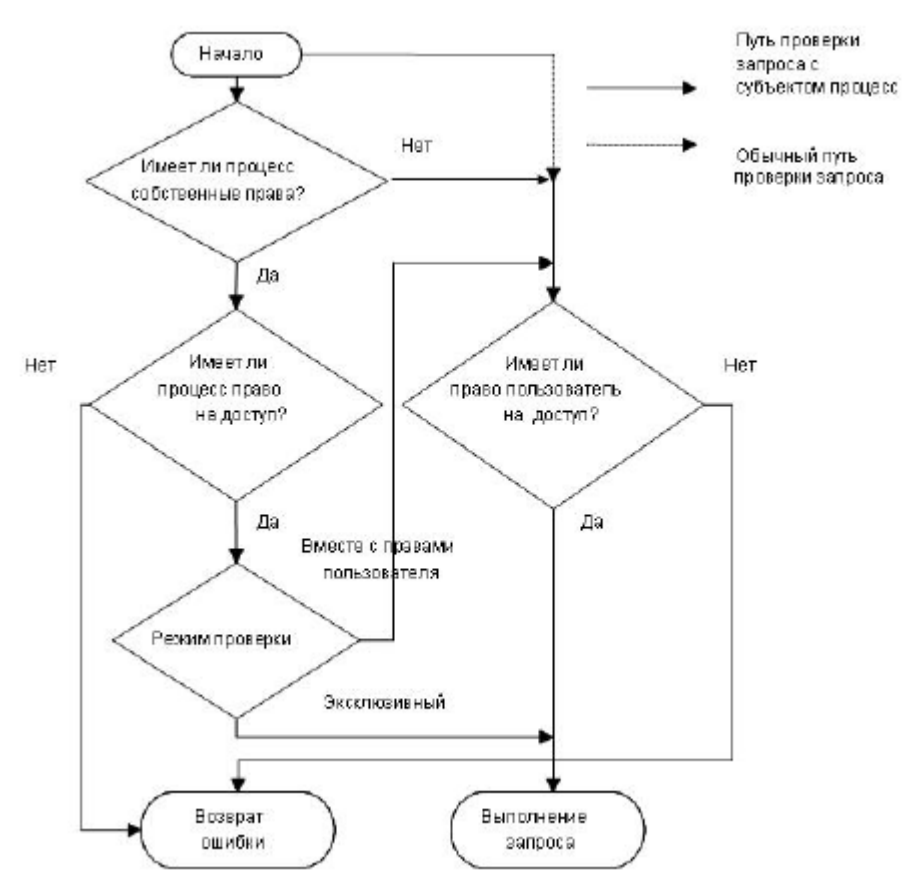
Процессы и объекты могут задаваться маской:

- * - любая последовательность символов;
- ? - любой символ;
- [набор символов] - любой символ входящий в набор;
- [!набор символов] или
- [^набор символов] - любой символ не входящий в набор.

Создание масок. Примеры

- c:*
  - (c:\, c:\aaa, c:\user\user1\aaa)
- *user*
  - (c:\user1\b, d:\users\user2)
- c:*asd.txt
  - (c:\user1\asd.txt, c:\aaaasd.txt)
- c:\user?\[!abcg-z]rr.txt
  - (c:\user1\drr.txt)

Алгоритм контроля доступа к ресурсам



Пример настройки файловой системы для пользователя System

Субъект доступа	Ресурсы		
Пользователи	Разрешённые для чтения	Разрешённые для записи и чтения	Разрешённые для выполнения
System	C:	C:\Documents and Settings	C:\Program Files C:\Winnt (WINDOWS) C:\СЗИ НСД
Процессы	Запрещенные для чтения	Запрещенные для записи и чтения	Запрещенные для выполнения
C:\СЗИ НСД			
C:\WINNT (WINDOWS)\system32\winlogon.exe			
C:\WINNT (WINDOWS)\system32\lsass.exe			
C:\WINNT (WINDOWS)\system32\csrss.exe			
C:\WINNT (WINDOWS)\system32\svchost.exe			
C:\WINNT (WINDOWS)\system32\services.exe			

Механизм обеспечения замкнутости программной среды

- Обеспечение замкнутости программной среды позволяет ограничивать возможности по запуску на компьютере деструктивных программ как локально, так и из сети.
- Осуществляется путем определения пользователям и процессам списка санкционированных программ

Способы организации замкнутой программной среды

- Задание списка разрешенных процессов (системных и прикладных) с возможностью запуска только тех процессов, которые отнесены к разрешенным.
- Задание папок, откуда разрешается запускать программы (с запретом записи и модификации в них файлов).

Способы организации замкнутой программной среды

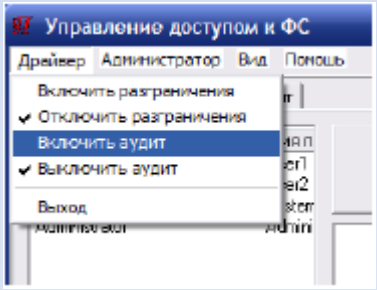
- Разграничение прав доступа к запуску скриптов
- Дополнительный анализ содержимого файлов (поиск признаков исполняемого файла)

Разграничение прав доступа к разделяемым сетевым ресурсам

- Разграничение удаленного доступа к сетевым разделяемым ресурсам в сети Microsoft выполняется в том же интерфейсе, возможности разграничения доступа совпадают

Аудит событий ФС

- Реализован механизм выборочной регистрации – регистрироваться доступ к объектам, задаваемым администратором безопасности. Для этого необходимо заполнить список контролируемых объектов.



Аудит событий ФС

- Все действия администратора безопасности по изменению прав доступа к рассматриваемым объектам защиты фиксируются и записываются в файле fileadm.log в каталоге Filectrl КСЗИ.

РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕЕСТРУ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

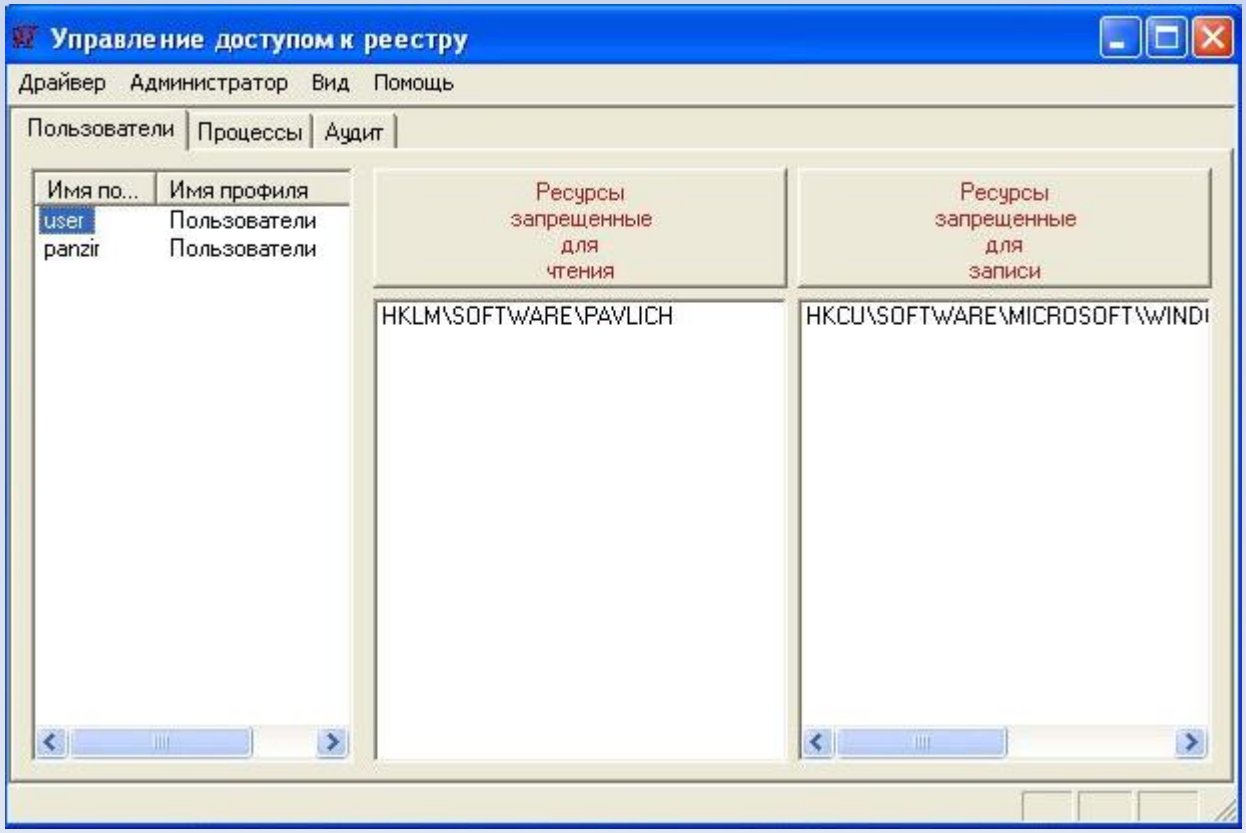
Разграничение доступа к реестру

Механизм полностью унифицирован с механизмом управления доступом к ФС:

- Разрешительная и запретительная разграничительные политики
- Разграничение для процессов и пользователей.

Отличие – типы доступа “Запись” и “Чтение”

Разграничение доступа к реестру



Аудит событий доступа к реестру

- Выборочный аудит - регистрируется доступ только к заданным объектам реестра ОС.
- Регистрация изменений прав доступа к реестру

ПЕРЕНАЗНАЧЕНИЕ ПУТЕЙ К КАТАЛОГАМ

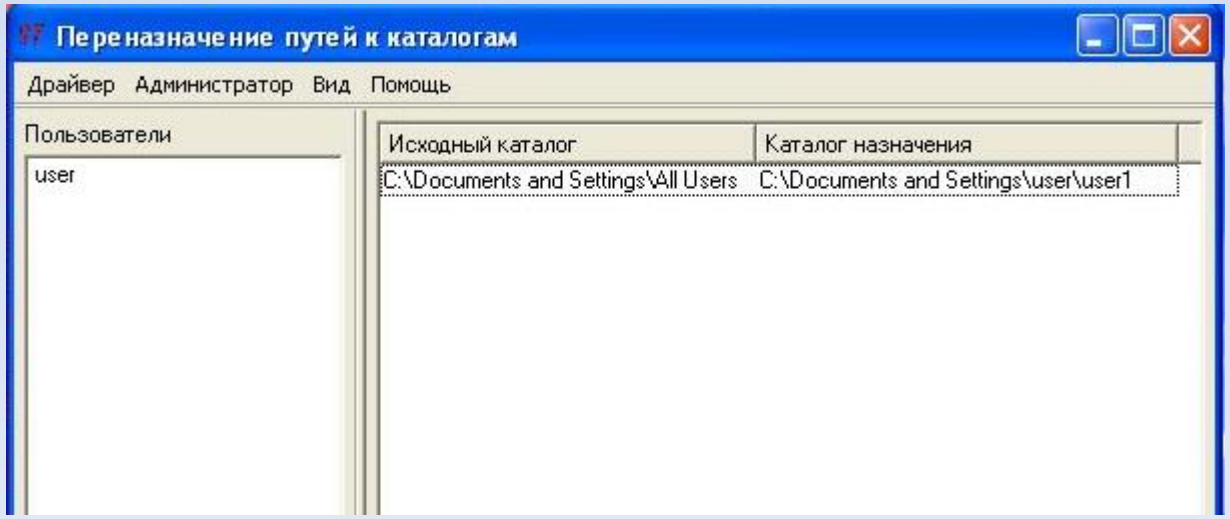
КСЗИ «Панцирь-К». Контроль и разграничение доступа

Переназначение путей каталогам

- КСЗИ позволяет разделять между пользователями неразделяемые системой и приложениями каталоги.
- Некоторые каталоги являются общими для всех пользователей (например \Documents and Settings\All Users\)

Переназначение путей каталогам

- Для каждого неразделяемого каталога запросы перенаправляются в назначенный пользователю каталог.
- Необходимо заранее скопировать содержимое!

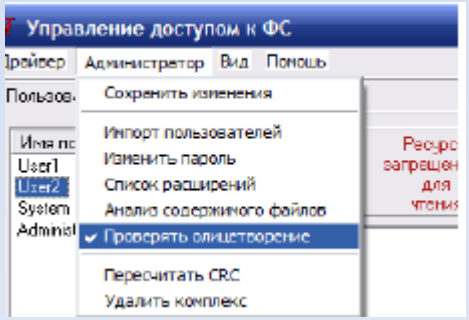


КОНТРОЛЬ ОЛИЦЕТВОРЕНИЯ СУБЪЕКТОВ ДОСТУПА

КСЗИ «Панцирь-К». Контроль и разграничение доступа

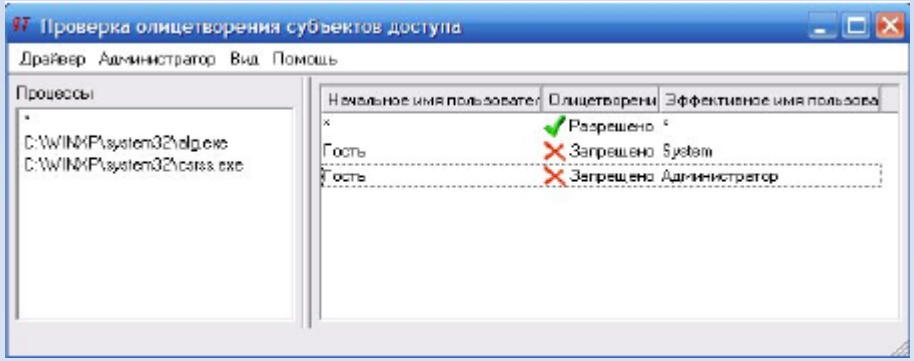
Контроль сервисов олицетворения

- При запросе доступа к защищаемому ресурсу анализируется, было ли запрещенное олицетворение потоком, запросившим ресурс, и если было, КСЗИ отказывает ему в доступе к ресурсу
- Пример – запуск программы с правами администратора



Переназначение путей каталогам

- Возможно разрешение и запрещение олицетворения отдельным пользователям
- Применяется к файловой системе и реестру



УПРАВЛЕНИЕ ДОСТУПОМ К СЕТИ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

Управление доступом к сети

- Реализуется разграничение доступа пользователей и процессов к сетевым ресурсам.
- Предназначен для защиты доступа к сети Internet и Intranet, для изоляции информационных потоков в ЛВС.

Управление доступом к сети

Субъектами доступа являются:

- пользователи;
- процессы которые могут обращаться к сетевым ресурсам.

Управление доступом к сети

Объектами доступа являются:

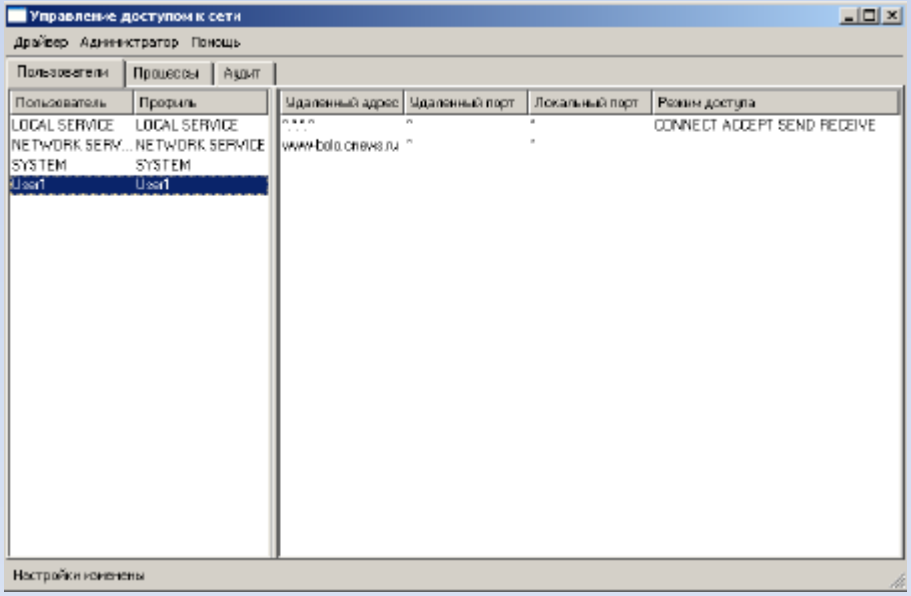
- IP-адреса удаленных ресурсов;
- сетевые имена удаленных ресурсов;
- локальные порты (сетевые службы), с которых может осуществляться доступ к удаленным ресурсам;
- удаленные порты, к которым может осуществляться доступ на удаленных компьютерах.

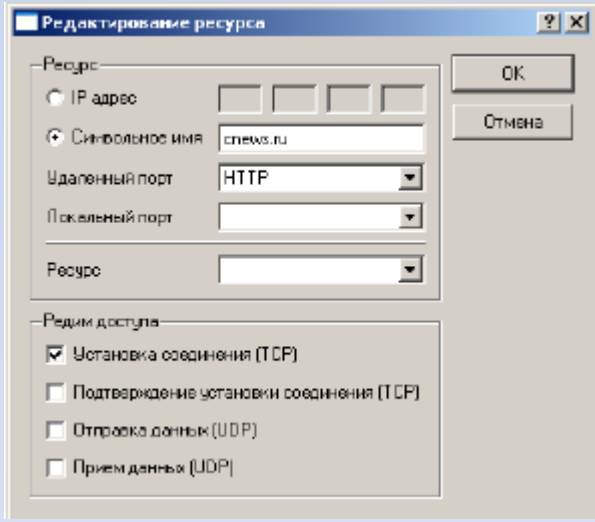
Управление доступом к сети

Настраиваемые типы доступа:

- право на установку исходящего соединения (для протокола TCP);
- право на подтверждение установки входящего соединения (для протокола TCP);
- право на отправку данных без установления соединения (для протокола UDP);
- право на получение (прием) данных без установления соединения (для протокола UDP).

Управление доступом к сети





УПРАВЛЕНИЕ ПОДКЛЮЧЕНИЕМ УСТРОЙСТВ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

Управление подключением устройств

- КСЗИ реализует контроль подключения (монтирования) устройств.
- Данный механизм должен предотвращать возможность подключения устройств, не являющихся необходимыми для выполнения своих служебных обязанностей пользователями.

Управление подключением устройств

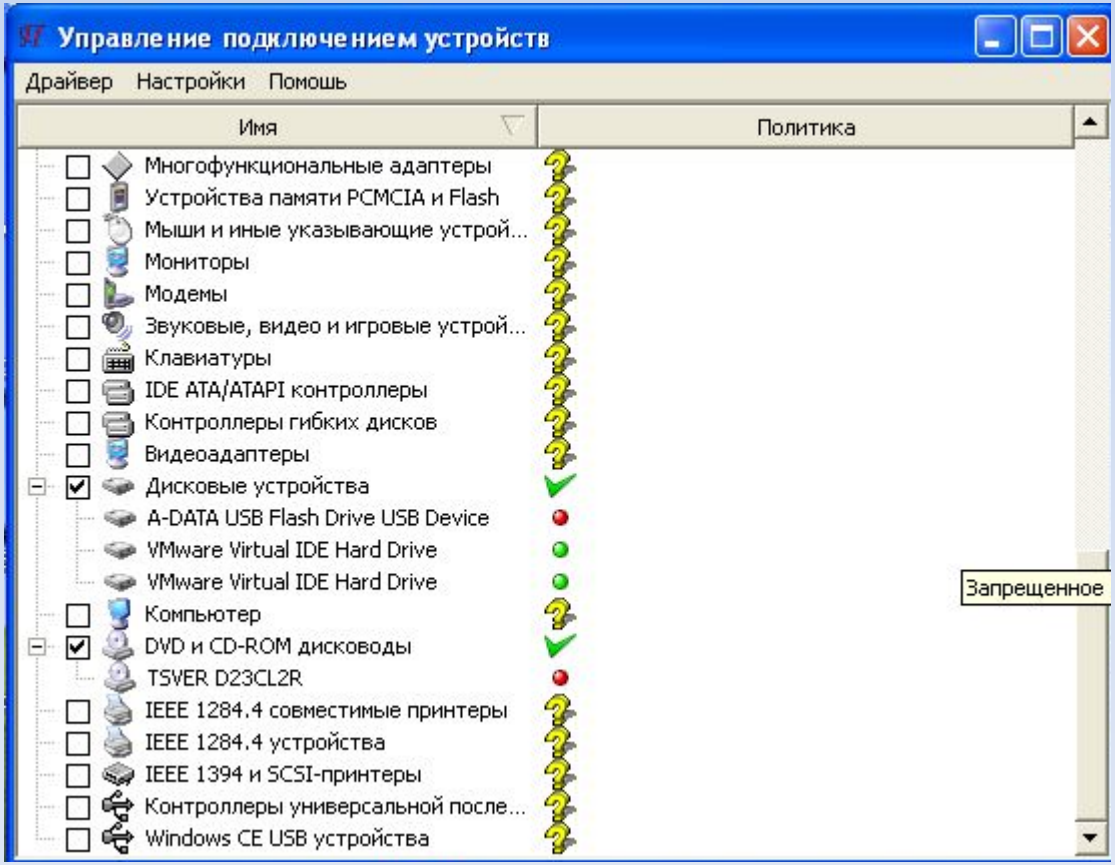
- Возможность контроля подключения устройств по их серийным номерам и по типу устройств.
- Все настройки распространяются на всех пользователей, работающих на локальной машине

Управление подключением устройств

Настройка механизма осуществляется в два этапа:

- задаются классы устройств, подключение устройств к которым следует контролировать
- задаются устройства, запрещенные (разрешенные) для подключения к системе, относящиеся к выбранным классам

Управление подключением устройств



УПРАВЛЕНИЕ ДОСТУПОМ К БУФЕРУ ОБМЕНА

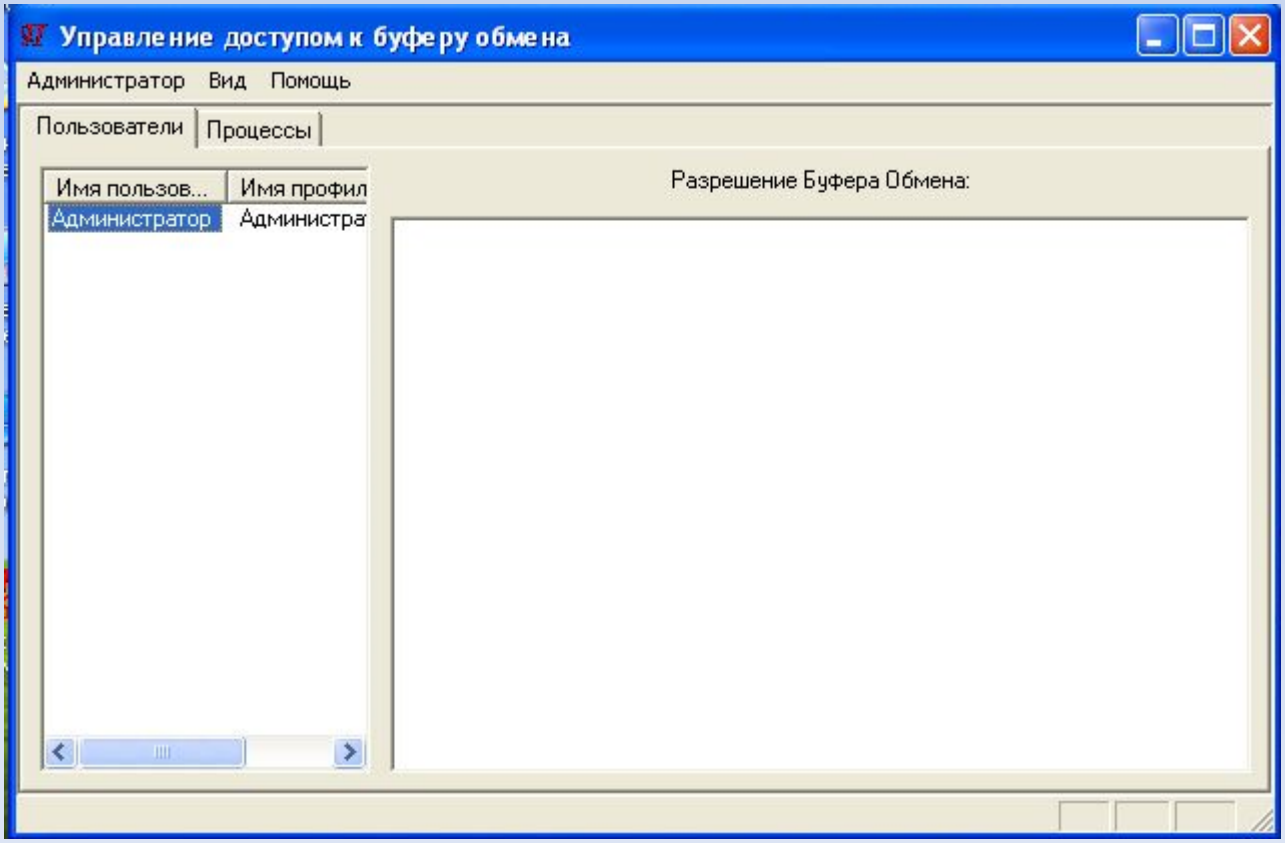
КСЗИ «Панцирь-К». Контроль и разграничение доступа

Управление доступом к буферу обмена

КСЗИ реализует контроль доступа к буферу обмена для пользователей и приложений.

- Windows не обеспечивает разграничение буфера обмена в случае запуска приложение пользователем с правами другого пользователя
- Разграничение буфера обмена необходимо при реализации на защищаемом компьютере обработки категорированных данных.

Управление доступом к буферу обмена



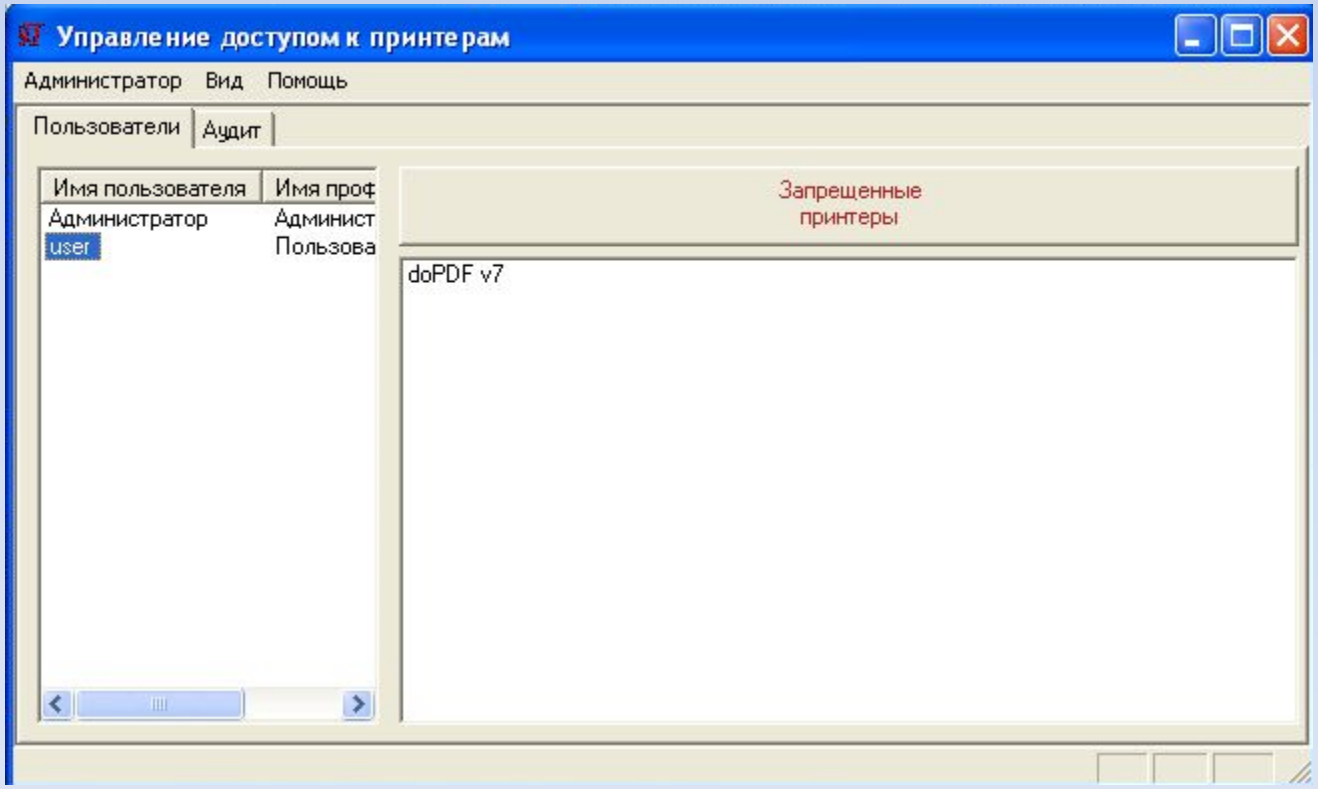
УПРАВЛЕНИЕ ДОСТУПОМ К ЛОКАЛЬНЫМ И СЕТЕВЫМ ПРИНТЕРАМ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

Управление доступом к принтерам

- В КСЗИ реализован собственный диспетчер разграничения прав доступа пользователей к принтерам.
- Разграничение доступа осуществляется к локальным и к сетевым принтерам, драйверы которых установлены на компьютере, на котором осуществляются разграничения.

Управление доступом к принтерам



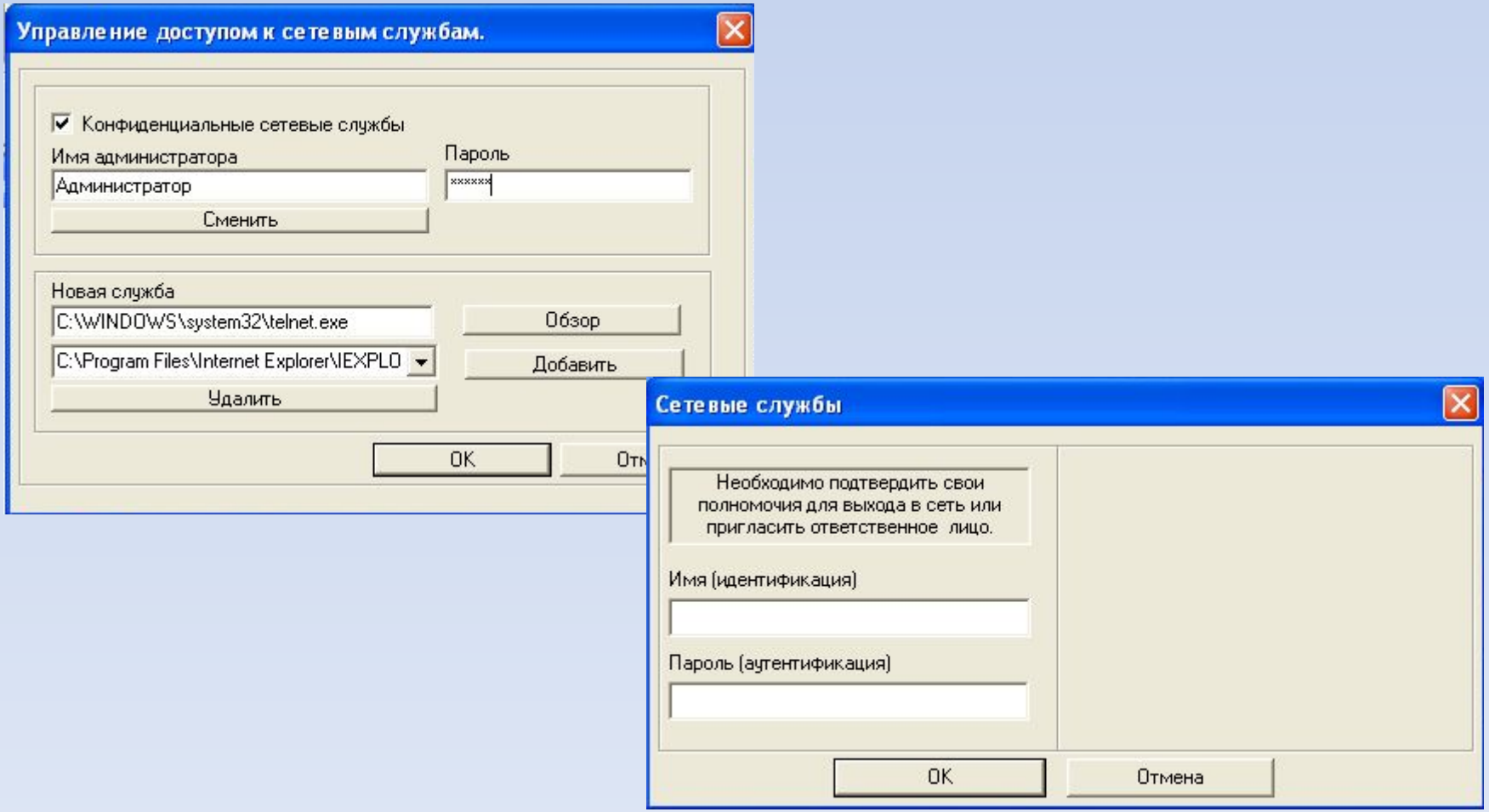
УПРАВЛЕНИЕ ДОСТУПОМ К СЕТЕВЫМ СЛУЖБАМ

КСЗИ «Панцирь-К». Контроль и разграничение доступа

Управление доступом к сетевым службам

- КСЗИ обеспечивает контролируемый доступ пользователей к сетевым службам, реализуя возможность запуска приложения только после авторизации ответственного лица.
- В общем случае данный механизм может применяться не только для авторизованного запуска сетевой службы, но и для авторизованного запуска любого процесса.

Управление доступом к сетевым службам



КСЗИ «Панцирь-К». Аудит событий

Аудит событий

- КСЗИ осуществляет регистрацию основных событий при функционировании защищаемого объекта и реализует иерархическую модель аудита событий информационной безопасности системы.

Уровни аудита

1. Регистрация событий уровней, реализующих разграничительную политику доступа к ресурсам.
2. Регистрация событий уровня, реализующего контроль активности и корректности функционирования механизмов защиты, реализующих разграничительную политику доступа к ресурсам

Типы регистрируемых событий

1 Уровень:

- События, связанные с действиями пользователей по доступу к ресурсам защищаемой системы;
- События, связанные с действиями администратора безопасности по созданию и переназначению прав доступа пользователей к ресурсам защищаемой системы.

Типы регистрируемых событий

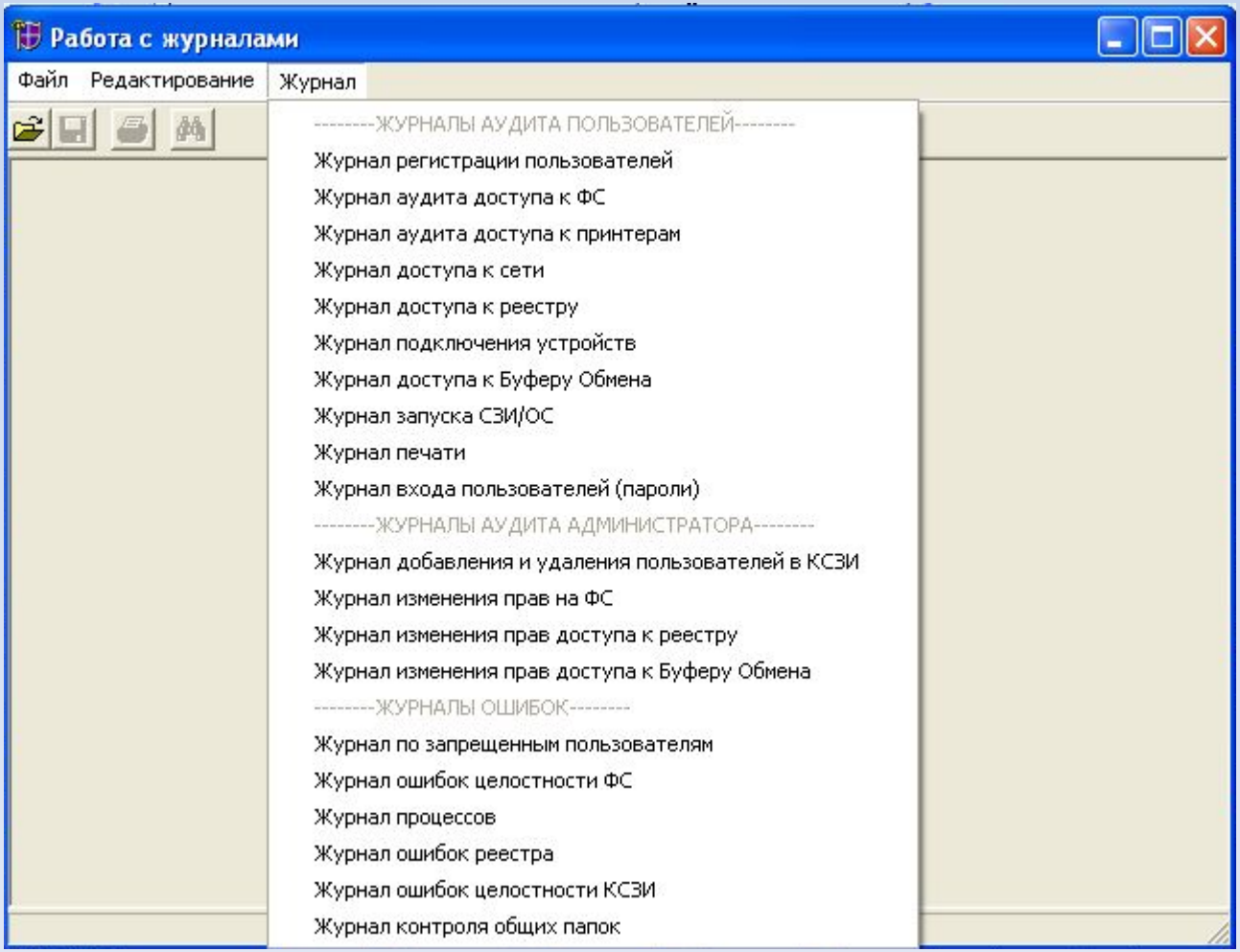
2 Уровень:

- События, связанные с некорректностью функционирования системы разграничения доступа (ошибки доступа)

Информация о событии

- Дата и время;
- Субъект, осуществляющий регистрируемое действие;
- Тип события;
- Результат выполнения и т.д.

Журналы аудита



Журналы аудита

- **Журнал регистрации пользователей** - регистрация входа и завершения работы пользователей в ОС
- **Журнал входа пользователей (пароли)** - регистрация всех (правильных и неправильных) попыток входа и смену действующего пароля пользователей в ОС

Аудит доступа пользователей к ресурсам

- Журнал аудита доступа к ФС
- Журнал доступа к реестру
- Журнал доступа к сети
- Журнал аудита доступа к принтерам
- Журнал подключения устройств
- Журнал доступа к Буферу Обмена

Журналы аудита

- **Журнал запуска СЗИ/ОС** - запуска сервиса КСЗИ и времени последнего цикла обработки событий
- **Журнал печати** - реализует автоматическую регистрацию печати.

Журнал печати

Регистрируются:

- дата и время выдачи (обращения к подсистеме вывода) твердой копии;
- наименование файла документа и уровень конфиденциальности пользователя;
- спецификация устройства выдачи (логическое имя внешнего устройства);
- идентификатор субъекта доступа, запросившего документ;
- объем фактически выданного документа (количество листов).

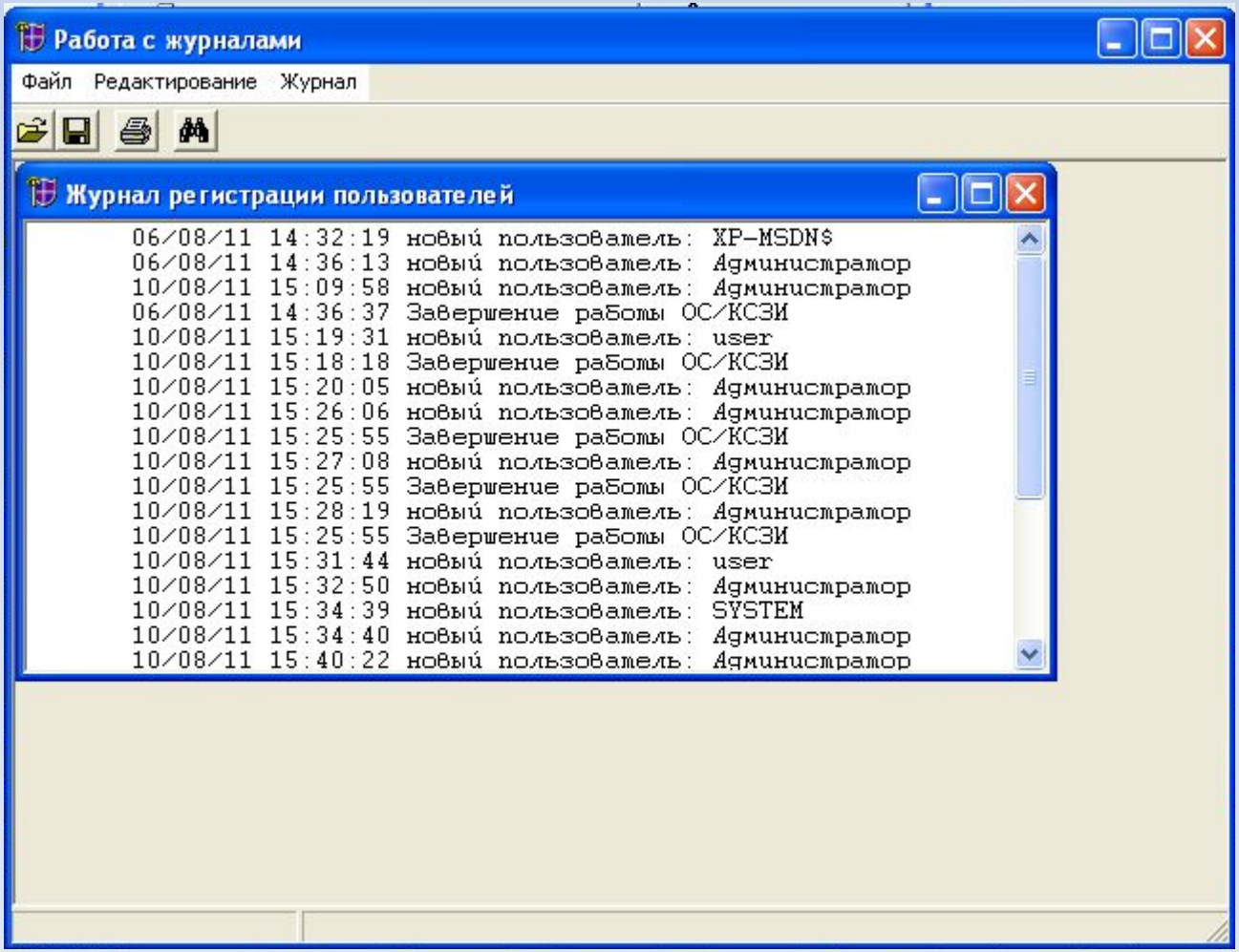
Журналы аудита администратора

- Журнал добавления и удаления пользователей в КСЗИ
- Журнал изменения прав на ФС
- Журнал изменения прав доступа к реестру
- Журнал изменения прав доступа к Буферу Обмена

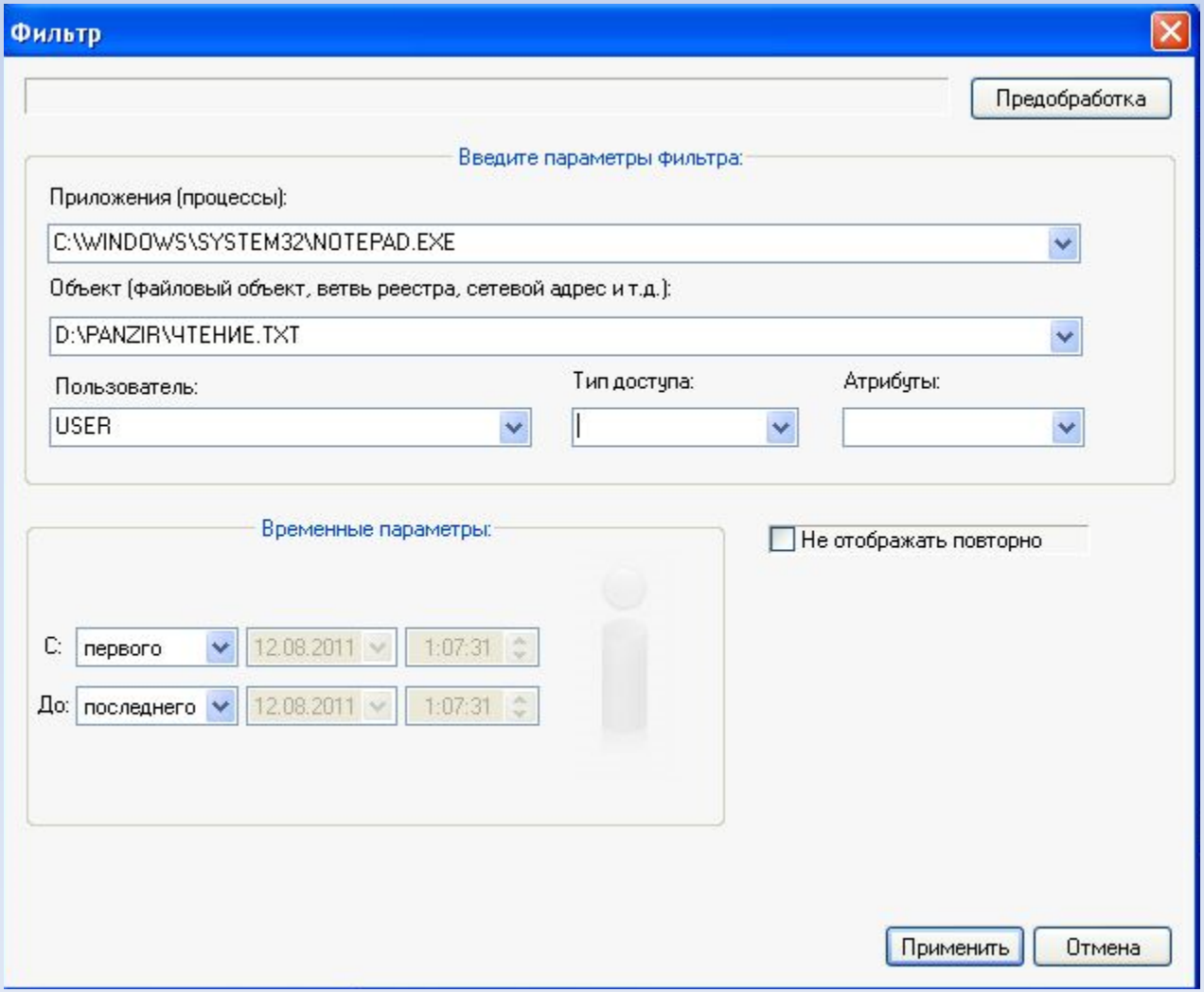
Аудит в КСЗИ


Настройки клиентской части
Системные и дополнительные настройки
Защита данных
Контроль целостности
Разграничение Доступа
Учетные записи
Аудит
Аппаратная защита
ОБРАБОТКА ЖУРНАЛОВ (КОНТРОЛЬ РАЗМЕРА)
РАЗБОР ЖУРНАЛОВ (ФИЛЬТР)
КОНТРОЛЬ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ
OK
Отмена
Справка

Аудит в КСЗИ


Работа с журналами
Файл Редактирование Журнал
Журнал регистрации пользователей
06/08/11 14:32:19 новый пользователь: XP-MSDN$
06/08/11 14:36:13 новый пользователь: Администратор
10/08/11 15:09:58 новый пользователь: Администратор
06/08/11 14:36:37 Завершение работы ОС/КСЗИ
10/08/11 15:19:31 новый пользователь: user
10/08/11 15:18:18 Завершение работы ОС/КСЗИ
10/08/11 15:20:05 новый пользователь: Администратор
10/08/11 15:26:06 новый пользователь: Администратор
10/08/11 15:25:55 Завершение работы ОС/КСЗИ
10/08/11 15:27:08 новый пользователь: Администратор
10/08/11 15:25:55 Завершение работы ОС/КСЗИ
10/08/11 15:28:19 новый пользователь: Администратор
10/08/11 15:25:55 Завершение работы ОС/КСЗИ
10/08/11 15:31:44 новый пользователь: user
10/08/11 15:32:50 новый пользователь: Администратор
10/08/11 15:34:39 новый пользователь: SYSTEM
10/08/11 15:34:40 новый пользователь: Администратор
10/08/11 15:40:22 новый пользователь: Администратор

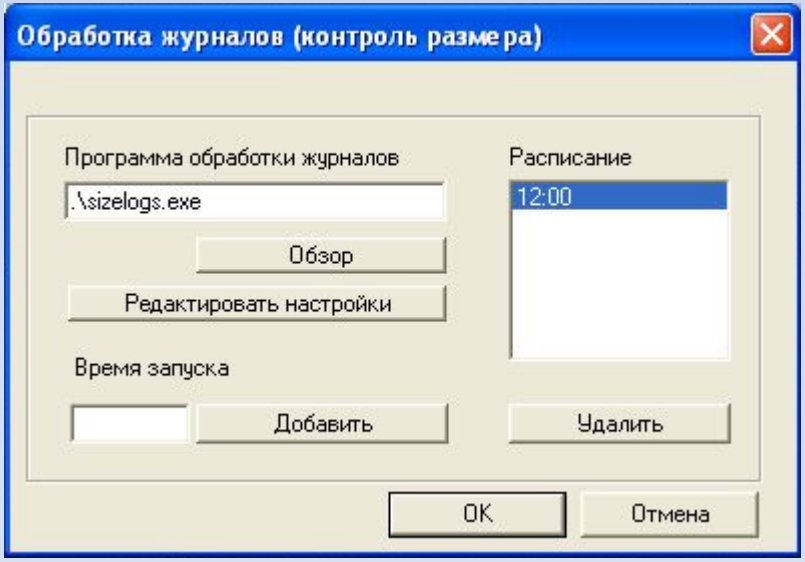
Аудит в КСЗИ


Фильтр
Предобработка
Введите параметры фильтра:
Приложения (процессы):
C:\WINDOWS\SYSTEM32\NOTEPAD.EXE
Объект (файловый объект, ветвь реестра, сетевой адрес и т.д.):
D:\PANZIR\ЧТЕНИЕ.TXT
Пользователь:
USER
Тип доступа:
Атрибуты:
Временные параметры:
Не отображать повторно
С:
первого
12.08.2011
1:07:31
До:
последнего
12.08.2011
1:07:31
Применить
Отмена

Ротация журналов аудита

- Программа ротации позволяет обрезать и очищать журналы, а также делать копии журналов перед (либо после) их очисткой.
- Программа содержит два файла sizelogs.exe и sizelogs.lcmd

Ротация журналов аудита



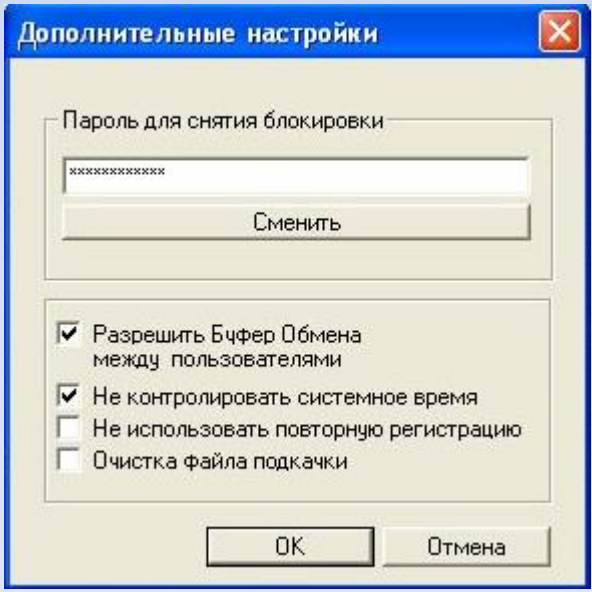
Ротация журналов аудита. Команды

- processlog FILENAME SIZE (BYTE) SIZE (STR) //[-1]
- makebackup FILENAME [NUM]
- externcmd CMDLINE
- externcmdhide CMDLINE
- sleep NUM
- gotostart

КСЗИ «Панцирь-К». Дополнительные возможности

Дополнительные настройки

- Пароль для снятия блокировки
- Разрешить Буфер Обмена между пользователями
- Не контролировать системное время
- Не использовать повторную регистрацию
- Очистка файла подкачки



Сохранение и восстановление настроек

- Тиражирование с помощью сервера
- Копирование настроек вручную
- Файлы настроек - pre.set, filectrl.ini, regctrl.ini, tcpctrl.ini, dirlink.ini, devctrl.ini, impctrl.ini, clipctrl.ini и printer.ini

Дополнительная защита данных

- Шифрование данных «на лету»
- Автоматическое гарантированное удаление остаточной информации
- Разграничение прав доступа к защищаемым объектам
- Скрытие защищаемых объектов файловой системы

Шифрование данных «на лету»

- Шифрование (расшифрование) данных при их сохранении в локальный или удаленный файловый объект.
- Поддерживаются файловые системы NTFS, FAT32 или FAT16.
- Алгоритмы шифрования: XOR, GOST, DES, 3DES, AES, ГОСТ 28147-89.
- СЗД позволяет подключать СКЗИ «Signal-COM CSP» и СКЗИ «КриптоПро CSP».

Гарантированное удаление остаточной информации

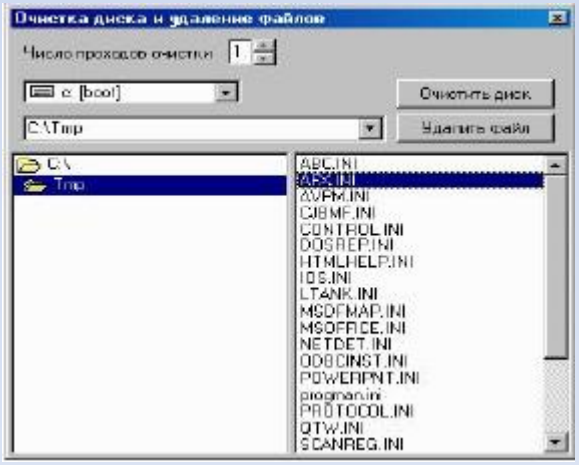
- КСЗИ позволяет осуществлять очистку оперативной и внешней памяти. Очистка производится путем записи маскирующей информации в память при ее освобождении (перераспределении).
- Для модифицируемых файловых объектов система позволяет задавать число «проходов очистки» и вид маскирующей информации, записываемой СЗД в файловый объект.

Варианты автоматического запуска программ очистки оперативной и дисковой памяти

- **По расписанию.**
- **При входе (идентификации) нового пользователя**
- Для реализации функций очистки памяти в состав дистрибутива КСЗИ включены две утилиты “delsec.exe” и “clearam.exe”

Гарантированное удаление файлов с жёсткого диска

- Программа FullDel.exe:
- Удаление файлов
- Очистка диска



Скрытие защищаемых объектов файловой системы

- Скрытие защищаемого файлового объекта;
- Скремблирование имени файлового объекта;
- Кодирование имени файлового объекта.

Механизмы контроля целостности

1. Контроль целостности каталогов и файлов данных (синхронный и асинхронный)
2. Контроль целостности исполняемых файлов (программ перед запуском)
3. Контроль целостности файлов КСЗИ

Дополнительные механизмы контроля печати

- **Механизм маркировки документов**

Автоматический ввод реквизитов документов при печати из программы MS Word (другие программы печати в этом режиме средствами КСЗИ запрещены)

- **Механизм теневого копирования любых печатных документов**

Автоматическое копирование документов при печати из любых программ.

Рассмотренные вопросы

- КСЗИ Панцирь-К. Серверная и клиентские части
- Идентификация и аутентификация пользователей
- Контроль и разграничение доступа
- Аудит
- Дополнительные возможности