Особенности реализации средства централизованного управления КСЗ для ЗОСРВ «Нейтрино»

Шаронов Дмитрий Александрович

АО НИИ ЦПС, г. Тверь

16 октября 2024 г.

Немного о нас

- Центр Систем и Средств Защиты Информации, АО НИИ ЦПС, г. Тверь
- Занимаемся разработкой средств защиты информации (СрЗИ) и систем защиты информации (СЗИ) с 1995 года.
- К наиболее известным продуктам относятся:
  - АПКЗИ "Ребус-1.0"
  - АПКЗИ "Лабиринт-М"
  - АПКЗИ "Ребус-М"
  - АПКДЗ "Тверца Зетта-М"
  - ПК "Ребус-СОВ"
  - АПК "Ребус-СДЗ"

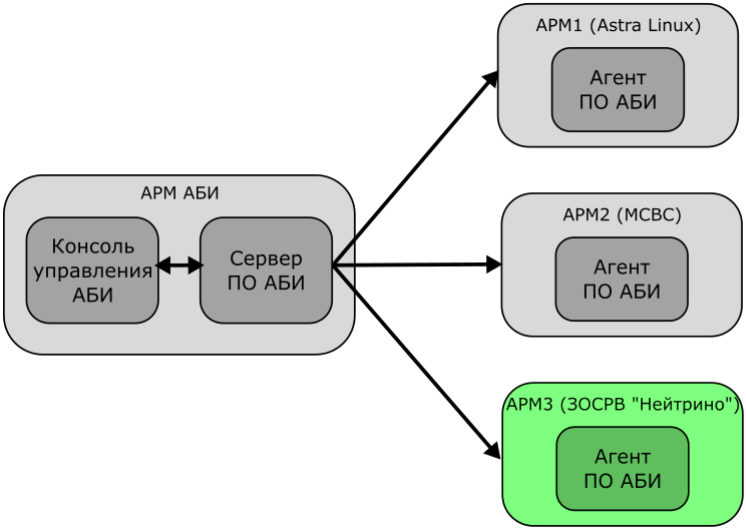
Типовые задачи, решаемые с помощью СЗИ

- Централизованное управление из графического интерфейса.
- Управление пользователями и их паролями.
- Управление разграничением доступа к защищаемым ресурсам.
- Управление событиями безопасности.
- Управление машинными носителями информации.
- Сигнализация о фактах и попытках несанкционированного доступа.
- Управление различными видами блокировок (пользователей, программ, устройств).
- Контроль целостности (как СрЗИ, так и пользовательских данных).
- Резервное копирование и восстановление.
- Тестирование работоспособности СрЗИ.
- Управление средствами антивирусной защиты.

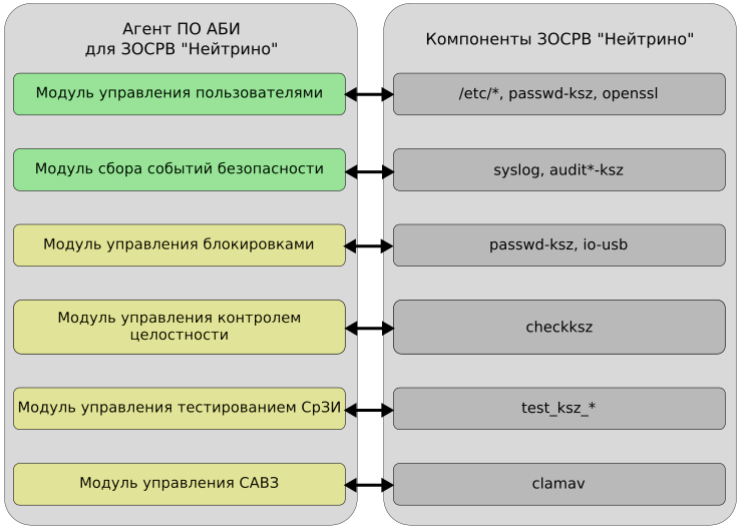
Проблемы, возникающие в гетерогенных сетях

- Разный набор параметров при управлении пользователями.
- Отличия в механизмах разграничения доступа к ресурсам.
- Отличия в системе журналирования и аудита (набор и формат сообщений).
- Различия в реализации прочих встроенных механизмов безопасности (управление блокировками, контроль целостности, резервное копирование и восстановление).
- Разные средства антивирусной защиты.

Возможная схема использования ПО АБИ



Механизмы агента ПО АБИ для ЗОСРВ "Нейтрино"2020

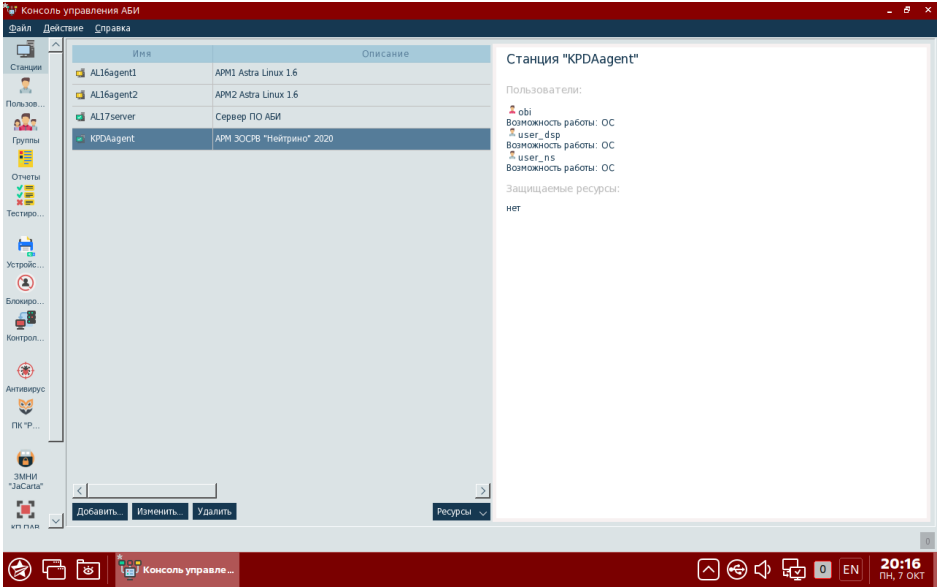


Процесс установки агента ПО АБИ в ЗОСРВ "Нейтрино"2020

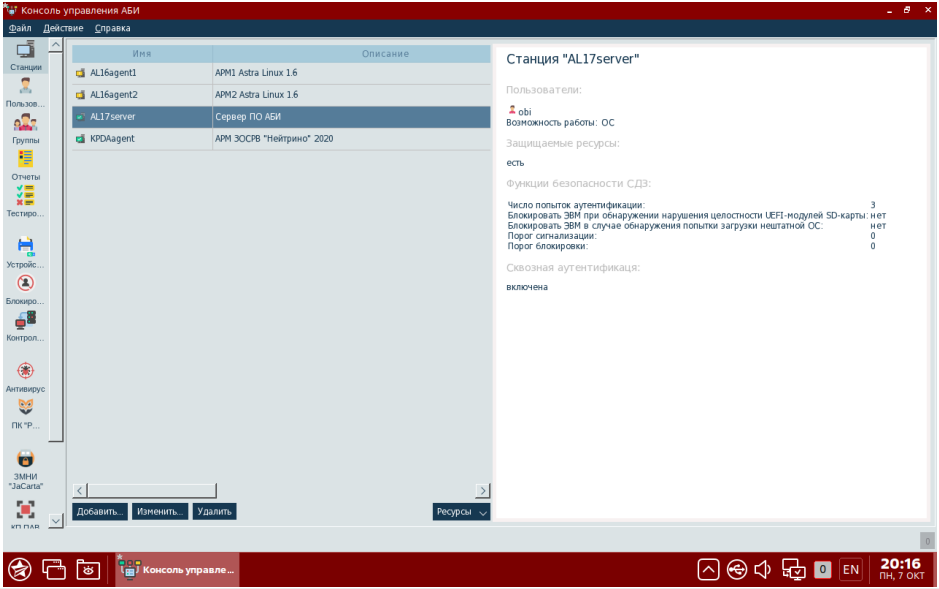
Локальная установка

Удаленная установка

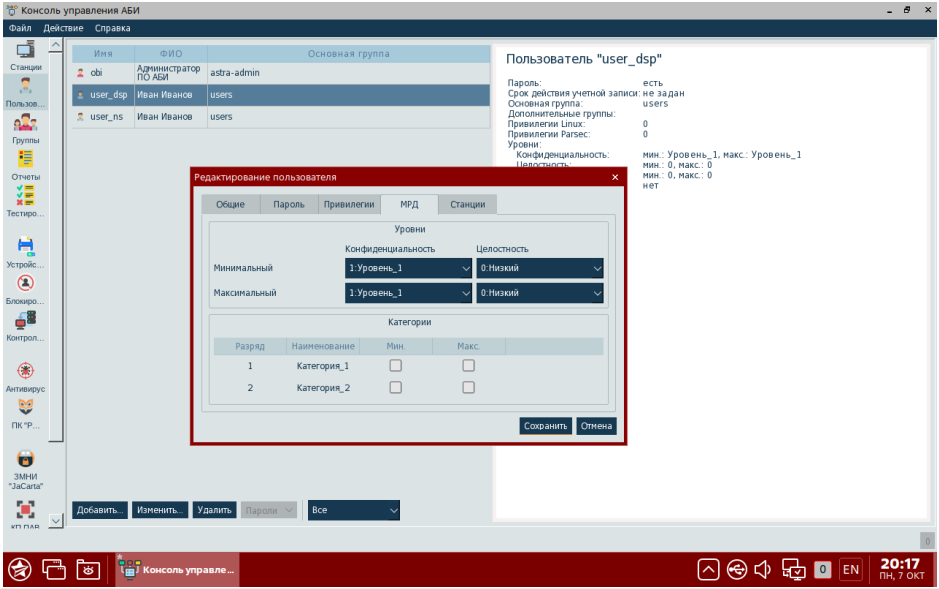
Управление станциями (1)



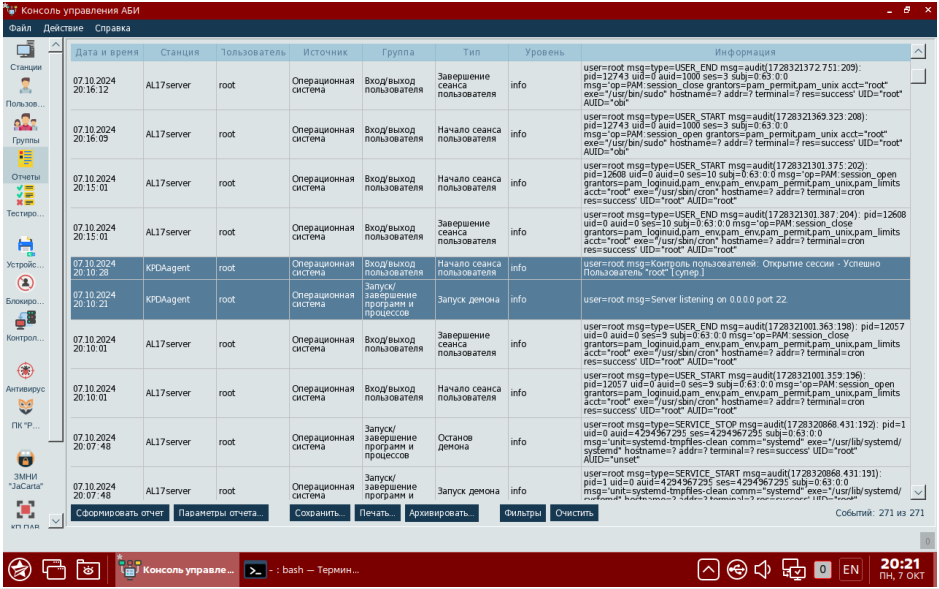
Управление станциями (2)



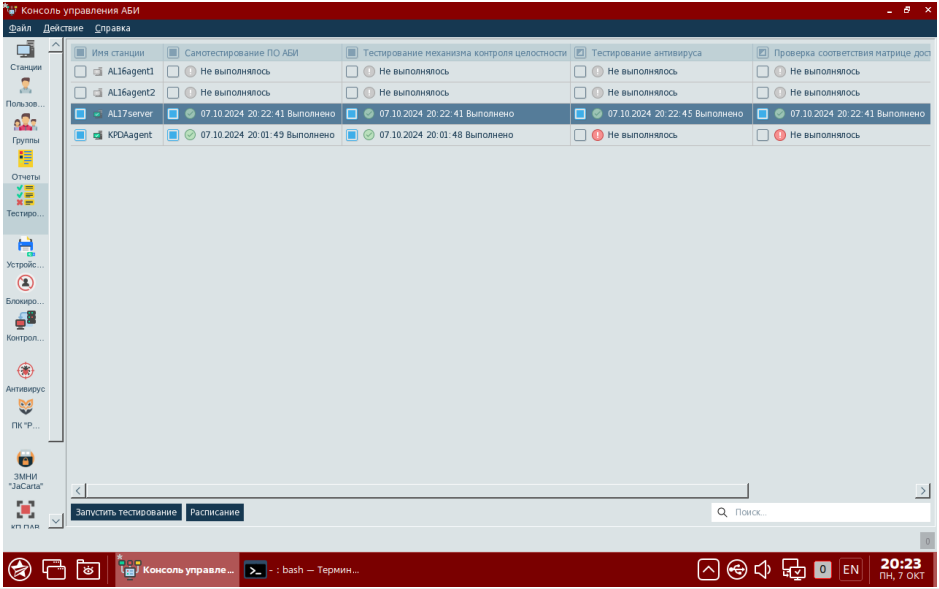
Управление пользователями



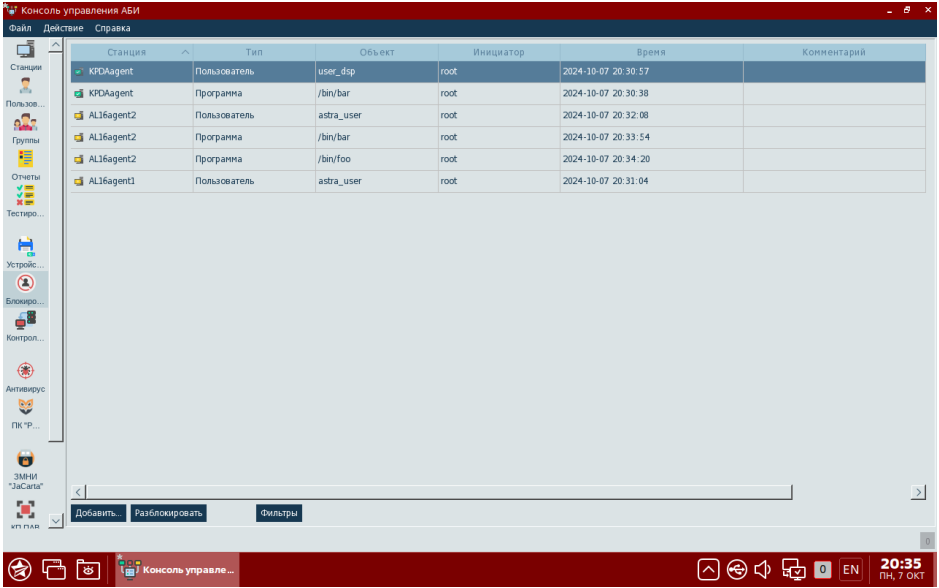
Управление событиями безопасности



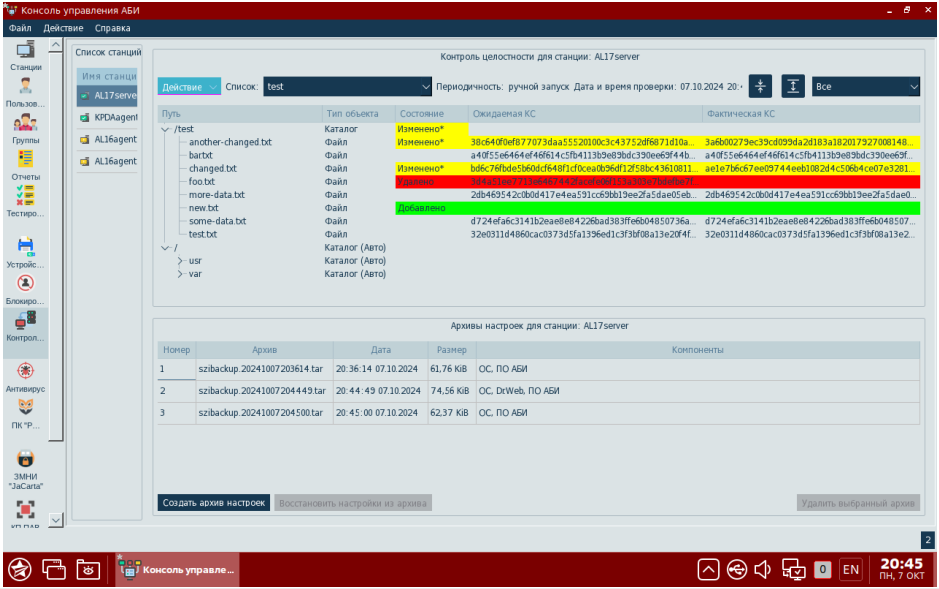
Управление тестированием СрЗИ



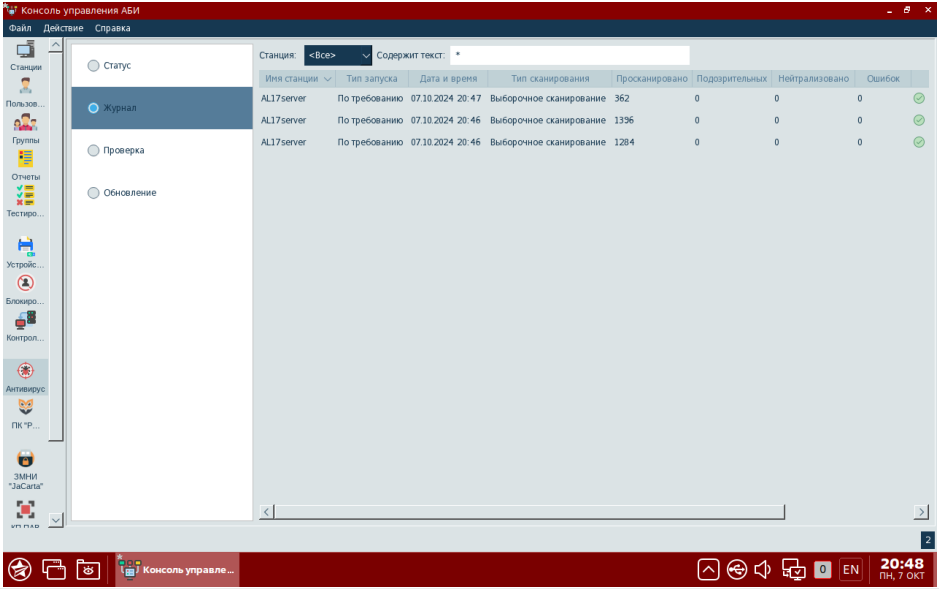
Управление блокировками



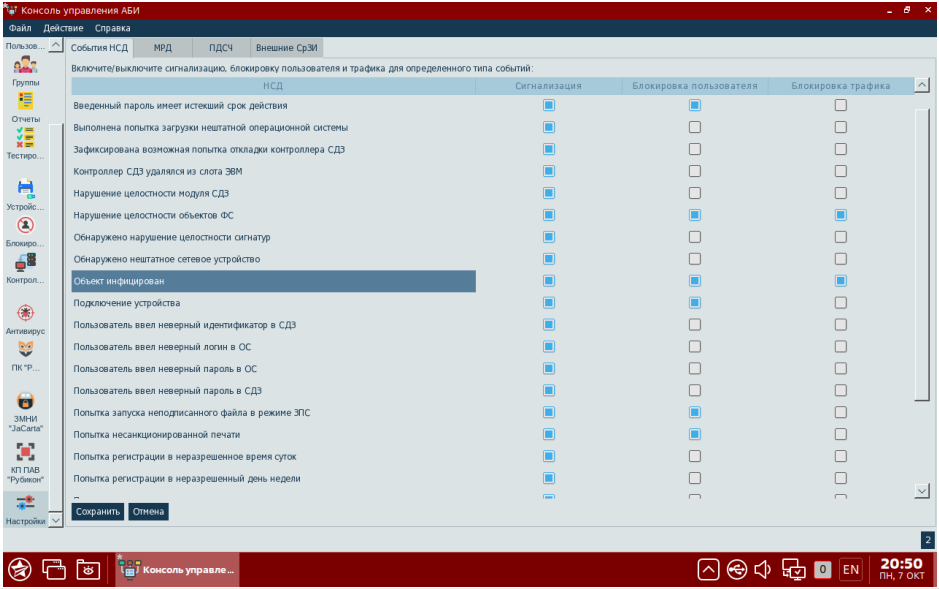
Управление контролем целостности



Управление антивирусом



Управление реакцией на события НСД



Планы

- Завершение реализации заявленного функционала в рамках разработки программного комплекса ПО АБИ.
- Получение сертификатов соответствия требованиям РД НДВ-2 и РДВ в системе сертификации СрЗИ Минобороны России.
- Использование в разрабатываемых СЗИ и доработка функционала после анализа опыта использования на объектах автоматизации.

Спасибо за внимание.