

Особенности реализации средства централизованного управления КСЗ для ЗОСРВ «Нейтрино»

Шаронов Дмитрий Александрович

АО НИИ ЦПС, г. Тверь

16 октября 2024 г.



- 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

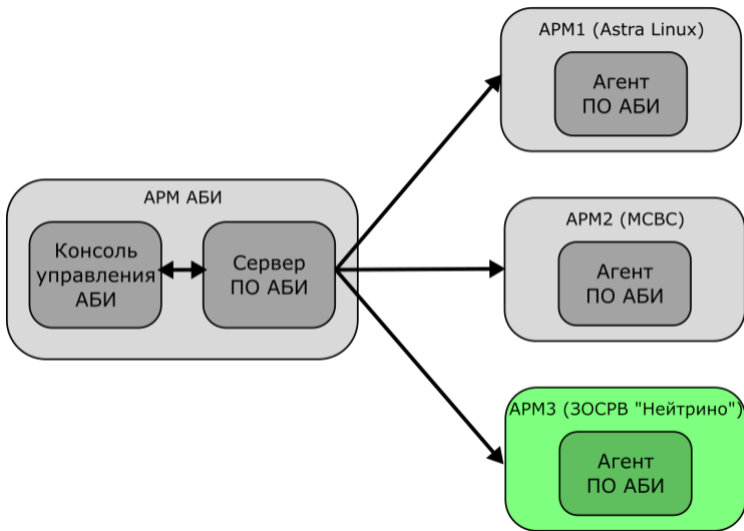
- Централизованное управление из графического интерфейса.
- Управление пользователями и их паролями.
- Управление разграничением доступа к защищаемым ресурсам.
- Управление событиями безопасности.
- Управление машинными носителями информации.
- Сигнализация о фактах и попытках несанкционированного доступа.
- 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.



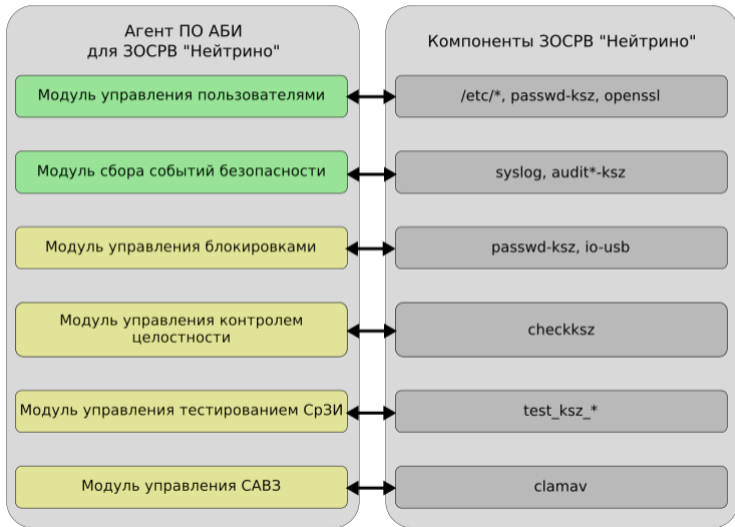
- Разный набор параметров при управлении пользователями.
- Отличия в механизмах разграничения доступа к ресурсам.
- Отличия в системе журналирования и аудита (набор и формат сообщений).
- Различия в реализации прочих встроенных механизмов безопасности (управление блокировками, контроль целостности, резервное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



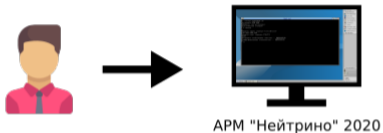
Возможная схема использования ПО АБИ



Механизмы агента ПО АБИ для ЗОСРВ "Нейтрино" 2020



Локальная установка



Удаленная установка



Управление станциями (1)

Контроль АБИ

Файл Действие Справка

Имя	Описание
AL16agent1	APM1 Astra Linux 1.6
AL16agent2	APM2 Astra Linux 1.6
AL17server	Сервер ПО АБИ
KPDAagent	АРМ ЗОСРВ "Нейтрино" 2020

Станция "KPDAagent"

Пользователи:

- obi
- Возможность работы: ОС
- user_dsp
- Возможность работы: ОС
- user_ns
- Возможность работы: ОС

Защищаемые ресурсы:

нет

Добавить... Изменить... Удалить

Ресурсы

20:16 ПН, 7 ОКТ



Управление станциями (2)

Консоль управления АБИ

Файл Действие Справка

Имя	Описание
AL16agent1	APM1 Astra Linux 1.6
AL16agent2	APM2 Astra Linux 1.6
AL17server	Сервер ПО АБИ
KPDAagent	APM ЗОСРВ "Нейтрино" 2020

Станция "AL17server"

Пользователи:

- obi
Возможность работы: ОС

Защищаемые ресурсы:

есть

Функции безопасности СДЗ:

- Число попыток аутентификации: 3
- Блокировать ЭВМ при обнаружении нарушения целостности UEFI-модулей SD-карты: нет
- Блокировать ЭВМ в случае обнаружения попытки загрузки нештатной ОС: нет
- Порог сигнализации: 0
- Порог блокировки: 0

Сквозная аутентификация:

включена

Добавить... Изменить... Удалить

Ресурсы

20:16 ПН, 7 ОКТ



Управление пользователями

Консоль управления АБИ

Файл Действие Справка

Имя	ФИО	Основная группа
obi	Администратор ПО АБИ	astra-admin
user_dsp	Иван Иванов	users
user_ns	Иван Иванов	users

Пользователь "user_dsp"

Пароль: есть
Срок действия учетной записи: не задан
Основная группа: users
Дополнительные группы:
Привилегия Linux: 0
Привилегия Parsec: 0
Уровни:
Конфиденциальность: мин.: Уровень_1, макс.: Уровень_1
Целостность: мин.: 0, макс.: 0
нет

Редактирование пользователя

Общие Пароль Привилегии МРД Станции

Уровни

	Конфиденциальность	Целостность
Минимальный	1:Уровень_1	0:Низкий
Максимальный	1:Уровень_1	0:Низкий

Категории

Разряд	Наименование	Мин.	Макс.
1	Категория_1	<input type="checkbox"/>	<input type="checkbox"/>
2	Категория_2	<input type="checkbox"/>	<input type="checkbox"/>

Сохранить Отмена

Добавить... Изменить... Удалить Пароли Все

20:17 ПН, 7 ОКТ



Управление событиями безопасности

Консоль управления АБИ

Файл Действие Справка

Дата и время	Станция	Тользователь	Источник	Группа	Тип	Уровень	Информация
07.10.2024 20:16:12	AL17server	root	Операционная система	Вход/выход пользователя	Завершение сеанса пользователя	info	user=root msg=type=USER_END msg=audit(1728321372.751:209): pid=12743 uid=0 auid=1000 ses=3 subj=0 63:0:0 msg='op=PAM: session_close grantors=pam_permit,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success' UID="root" AUID="obi"
07.10.2024 20:16:09	AL17server	root	Операционная система	Вход/выход пользователя	Начало сеанса пользователя	info	user=root msg=type=USER_START msg=audit(1728321369.323:208): pid=12743 uid=0 auid=1000 ses=3 subj=0 63:0:0 msg='op=PAM: session_open grantors=pam_permit,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=? res=success' UID="root" AUID="obi"
07.10.2024 20:15:01	AL17server	root	Операционная система	Вход/выход пользователя	Начало сеанса пользователя	info	user=root msg=type=USER_START msg=audit(1728321301.375:202): pid=12608 uid=0 auid=0 ses=10 subj=0 63:0:0 msg='op=PAM: session_open grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_limits acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success' UID="root" AUID="root"
07.10.2024 20:15:01	AL17server	root	Операционная система	Вход/выход пользователя	Завершение сеанса пользователя	info	user=root msg=type=USER_END msg=audit(1728321301.387:204): pid=12608 uid=0 auid=0 ses=10 subj=0 63:0:0 msg='op=PAM: session_close grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_limits acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success' UID="root" AUID="root"
07.10.2024 20:10:28	KPDAagent	root	Операционная система	Вход/выход пользователя	Начало сеанса пользователя	info	user=root msg=Контроль пользователей. Открытие сессии - Успешно Пользователь "root" [cyber]
07.10.2024 20:10:21	KPDAagent	root	Операционная система	Запуск/завершение программ и процессов	Запуск демона	info	user=root msg=Server listening on 0.0.0.0 port 22
07.10.2024 20:10:01	AL17server	root	Операционная система	Вход/выход пользователя	Завершение сеанса пользователя	info	user=root msg=type=USER_END msg=audit(1728321001.363:198): pid=12057 uid=0 auid=0 ses=9 subj=0 63:0:0 msg='op=PAM: session_close grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_limits acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success' UID="root" AUID="root"
07.10.2024 20:10:01	AL17server	root	Операционная система	Вход/выход пользователя	Начало сеанса пользователя	info	user=root msg=type=USER_START msg=audit(1728321001.359:196): pid=12057 uid=0 auid=0 ses=9 subj=0 63:0:0 msg='op=PAM: session_open grantors=pam_loginuid,pam_env,pam_env,pam_permit,pam_unix,pam_limits acct="root" exe="/usr/sbin/cron" hostname=? addr=? terminal=cron res=success' UID="root" AUID="root"
07.10.2024 20:07:48	AL17server	root	Операционная система	Запуск/завершение программ и процессов	Останов демона	info	user=root msg=type=SERVICE_STOP msg=audit(1728320868.431:192): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=0 63:0:0 msg='unit=systemd-mpfiles-clean comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"
07.10.2024 20:07:48	AL17server	root	Операционная система	Запуск/завершение программ и процессов	Запуск демона	info	user=root msg=type=SERVICE_START msg=audit(1728320868.431:191): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=0 63:0:0 msg='unit=systemd-mpfiles-clean comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' UID="root" AUID="unset"

Сформировать отчет Параметры отчета... Сохранить... Печать... Архивировать... Фильтры Очистить

Событий: 271 из 271

0

Консоль управле... - : bash - Термин...

20:21 ПН, 7 ОКТ



Управление тестированием СрЗИ

Имя станции	Самотестирование ПО АБИ	Тестирование механизма контроля целостности	Тестирование антивируса	Проверка соответствия матрице доп
AL16agent1	Не выполнялось	Не выполнялось	Не выполнялось	Не выполнялось
AL16agent2	Не выполнялось	Не выполнялось	Не выполнялось	Не выполнялось
AL17server	07.10.2024 20:22:41 Выполнено	07.10.2024 20:22:41 Выполнено	07.10.2024 20:22:45 Выполнено	07.10.2024 20:22:41 Выполнено
KPDAAgent	07.10.2024 20:01:49 Выполнено	07.10.2024 20:01:48 Выполнено	Не выполнялось	Не выполнялось



Управление блокировками

Консоль управления АБИ


Файл Действие Справка

Станция	Тип	Объект	Инициатор	Время	Комментарий
KPDAagent	Пользователь	user_dsp	root	2024-10-07 20:30:57	
KPDAagent	Программа	/bin/bar	root	2024-10-07 20:30:38	
AL16agent2	Пользователь	astra_user	root	2024-10-07 20:32:08	
AL16agent2	Программа	/bin/bar	root	2024-10-07 20:33:54	
AL16agent2	Программа	/bin/foo	root	2024-10-07 20:34:20	
AL16agent1	Пользователь	astra_user	root	2024-10-07 20:31:04	

Добавить... Разблокировать Фильтры

0

20:35 ПН, 7 ОКТ



Управление контролем целостности

Консоль управления АБИ

Файл Действие Справка

Список станций

Имя станции

- AL17server
- KPDAagent
- AL16agent
- AL16agent

Контроль целостности для станции: AL17server

Действие: [выпадающий список] Список: test Периодичность: ручной запуск Дата и время проверки: 07.10.2024 20: [иконки] Все [выпадающий список]

Путь	Тип объекта	Состояние	Ожидаемая КС	Фактическая КС
~/test	Каталог	Изменено*		
~/test/another-changed.txt	Файл	Изменено*	38c6400ef877073daa55520100c3c43752df6871d10a...	3a6b00279ec39cd099da2d183a182017927008148...
~/test/bar.txt	Файл		a40f55e6464ef46f614c5fb4113b9e89bdc390ee69f44b...	a40f55e6464ef46f614c5fb4113b9e89bdc390ee69f...
~/test/changed.txt	Файл	Изменено*	bd6c76fbde5b60dcf68f1df0cea0b96df12f58bc43610811	ae1e7b6c57ee09744eeb1082d4c506b4ce07e3281
~/test/foo.txt	Файл	Удалено	3d4a51ee7713e6487442f2acaf609151a303e7b6dfba7f...	
~/test/more-data.txt	Файл		2db469542c0b0d417e4ea591cc69bb19ee2fa5dae05eb...	2db469542c0b0d417e4ea591cc69bb19ee2fa5dae0...
~/test/new.txt	Файл	Добавлено		
~/test/some-data.txt	Файл		d724efa6c3141b2eae8e84226bad383ffe6b04850736a...	d724efa6c3141b2eae8e84226bad383ffe6b048507...
~/test/test.txt	Файл		32e0311d4860cac0373d5fa1396ed1c3f3f08a13e20f4f...	32e0311d4860cac0373d5fa1396ed1c3f3f08a13e2...
~/usr	Каталог (Авто)			
~/var	Каталог (Авто)			

Архивы настроек для станции: AL17server

Номер	Архив	Дата	Размер	Компоненты
1	szibackup_20241007203614.tar	20:36:14 07.10.2024	61,76 KiB	ОС, ПО АБИ
2	szibackup_20241007204449.tar	20:44:49 07.10.2024	74,56 KiB	ОС, DrWeb, ПО АБИ
3	szibackup_20241007204500.tar	20:45:00 07.10.2024	62,37 KiB	ОС, ПО АБИ

Создать архив настроек Восстановить настройки из архива Удалить выбранный архив

2

Консоль управле...

20:45 ПН, 7 ОКТ



Управление антивирусом

Консоль управления АБИ

Файл Действие Справка

Станция: <Все> Содержит текст: *

Статус

Журнал

Проверка

Обновление

Имя станции	Тип запуска	Дата и время	Тип сканирования	Просканировано	Подозрительных	Нейтрализовано	Ошибок
AL17server	По требованию	07.10.2024 20:47	Выборочное сканирование	362	0	0	0
AL17server	По требованию	07.10.2024 20:46	Выборочное сканирование	1396	0	0	0
AL17server	По требованию	07.10.2024 20:46	Выборочное сканирование	1284	0	0	0

2

Консоль управле...

20:48 ПН, 7 ОКТ



Управление реакцией на события НСД

Консоль управления АБИ

Файл Действие Справка

Пользов... ^

События НСД МРД ПДСЧ Внешние СрЭИ

Включите/выключите сигнализацию, блокировку пользователя и трафика для определенного типа событий:

НСД	Сигнализация	Блокировка пользователя	Блокировка трафика
Введенный пароль имеет истекший срок действия	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Выполнена попытка загрузки нештатной операционной системы	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Зафиксирована возможная попытка отладки контроллера СДЗ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Контроллер СДЗ удалялся из слота ЭВМ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Нарушение целостности модуля СДЗ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Нарушение целостности объектов ФС	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Обнаружено нарушение целостности сигнатур	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Обнаружено нештатное сетевое устройство	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Объект инфицирован	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Подключение устройства	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Пользователь ввел неверный идентификатор в СДЗ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Пользователь ввел неверный логин в ОС	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Пользователь ввел неверный пароль в ОС	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Пользователь ввел неверный пароль в СДЗ	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Попытка запуска неподписанного файла в режиме ЭПС	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Попытка несанкционированной печати	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Попытка регистрации в неразрешенное время суток	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Попытка регистрации в неразрешенный день недели	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Сохранить Отмена

2

Консоль управле...

20:50 ПН, 7 ОКТ



- 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.