

МИНИСТЕРСТВО ПРИРОДНЫХ РЕСУРСОВ И ЭКОЛОГИИ РОССИЙСКОЙ
ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ГИДРОМЕТЕОРОЛОГИИ И МОНИТОРИНГУ
ОКРУЖАЮЩЕЙ СРЕДЫ

(Росгидромет)

Федеральное государственное бюджетное учреждение «Всероссийский научно-
исследовательский институт гидрометеорологической информации - Мировой центр
данных» (ФГБУ «ВНИИГМИ-МЦЦ»)

Автоматизированная система учета наблюдательных подразделений
(АСУНП) Росгидромета

Инструкция по эксплуатации АПК

Версия 2.1 от 7.06.18

Обнинск 2018

СОДЕРЖАНИЕ

Обозначения и сокращения	3
1 ОБЩИЕ СВЕДЕНИЯ	5
1.1 Цель документа	5
1.2 Назначение документа	5
1.3 Эксплуатационная документация	5
2 СОСТАВ И СПЕЦИФИКАЦИИ УЗЛА.....	6
2.1 Программное обеспечение	6
2.2 Техническое обеспечение	6
2.3 Схема распределения компонентов АПК в рамках оборудования	7
3 ЭКСПЛУАТАЦИЯ АПК УЗЛА.....	8
3.1 Общие положения	8
3.2 Обеспечение информационной безопасности	9
3.5 Эксплуатация аппаратно-программного комплекса	10
3.6 Эксплуатация телекоммуникационного оборудования	13
3.7 Резервирование и восстановление базы данных	13
4. ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	14
Лист изменений	15

Обозначения и сокращения

Сокращения	Расшифровка
АПК	Аппаратно-программный комплекс
АСУНП	Автоматизированная систем учета наблюдательных подразделений Росгидромета
ОПО	Общее программное обеспечение
СПО	Специальное программное обеспечение
ФГБУ	Федеральное бюджетное государственное учреждение
УГМС	Управление гидрометеорологической службы Росгидромета
НИУ	Научно-исследовательское учреждение
ВСС	Ведомственная сеть связи
АРМ	Автоматизированное рабочее место
МРС	Мониторинг ресурсов и сервисов

ВВЕДЕНИЕ

Документ содержит инструкцию по эксплуатации АПК АСУНП. Документ предназначен для администратора узла АСУНП во ВНИИГМИ-МЦД.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Цель документа

Документ содержит детальную инструкцию по эксплуатации АПК АСУНП. В документе представлен состав и спецификации узла, инструкции по поддержанию узла в рабочем состоянии. Также в документе представлен полный перечень прикладных компонентов узла с информацией по их проверке и тестированию.

1.2 Назначение документа

Документ предназначен для системного администратора АПК АСУНП в ФГБУ «ВНИИГМИ-МЦД», отвечающего за развертывание и сопровождение узла и компонентов в его составе.

1.3 Эксплуатационная документация

АСУНП (модернизированная версия) имеет следующий комплект документации:

- Инструкция по эксплуатации АПК (настоящий документ);
- Руководство администратора/оператора в УГМС/НИУ;
- Руководство администратора/оператора АСУНП ВНИИГМИ-МЦД;
- Руководство пользователя АСУНП;

2 СОСТАВ И СПЕЦИФИКАЦИИ УЗЛА

2.1 Программное обеспечение

Используемое программное обеспечение (установочное):

Перечень общего программного обеспечения (ОПО) АСУНП (модернизированная версия) и их характеристики приведены в таблице 1.

Таблица 1 - ОПО АСУНП (модернизированная версия)

Категория ПО	Наименование и характеристика ПО
Операционная система	Linux CentOS 6 x86_64
Средства виртуализации	ESXi 5.5
Среда разработки и функционирования	Sun JDK 1.7; JBoss Portal Platform 6.1;
ПО портала и безопасности	GateIn 3.6 SSO JOSSO 1.8.3
СУБД	PostgreSQL 9.3
клиент мониторинга ресурсов и сервисов	Zabbix

Перечень специального программного обеспечения (СПО) АСУНП (модернизированная версия) приведен в таблице 2

Таблица 2 - СПО АПК ЦСДП

Наименование компоненты	Назначение
Портал АСУНП и приложения	Среда функционирования портала и базовые настройки. Административная, информационная и презентационная службы. Ведение базы данных АСУНП посредством удаленного ввода данных; Отображение сведений по запросам, стандартизированной отчетности о состоянии сетей наблюдений; web-сервисы для программного доступа к базам данных системы; приложения обратной связи с пользователями; приложения оперативной отчетности о работе Системы
База данных АСУНП	Хранение, резервирование и восстановление информации о состоянии наземных, морских и космических сетей наблюдений, сведения о деятельности наблюдательных подразделений и их кадрово-финансовом обеспечении.

2.2 Техническое обеспечение

АПК АСУНП (модернизированная версия) имеет в составе средства вычислительной и телекоммуникационной техники.

Компоненты узла размещаются в составе оборудования, включающего:

- Монтажный напольный шкаф;
- Сетевой коммутатор;
- Сервер;
- Источник бесперебойного питания;
- KVM-консоль управления серверами;

Транспортная среда реализуется через выделенные ведомственные каналы связи (ВСС Росгидромета) и Интернет. Взаимодействие компонентов узла, между собой, с компонентами других центров и конечными пользователями осуществляется с использованием доменных имен. Поддержка доменных имен осуществляется на DNS серверах ФГБУ "ВНИИГМИ-МЦД" и ВСС.

Ниже дана спецификация сервера узла АСУНП:

- монтируемый в 19-дюймовую стойку, высота 2U;
- 2 шестиядерных 64-разрядных процессора, частота не ниже 2.8 ГГц;
- 12 модулей памяти объёмом по 8GB не ниже стандарта PC3-10600 CL9 ECC Registered DDR3;
- 4 сетевых интерфейса с пропускной способностью 1 Гбит/с;
- промышленный дисковый контроллер с поддержкой дисковых массивов RAID 6, имеющего аппаратный XOR процессор и 1Гб кэша основанного на флэш-памяти;
- 8 SAS жёстких дисков по 300GB с пропускной способностью интерфейса не менее 6 Гб/с, возможностью горячей замены, собранных в дисковый массив RAID 6;
- 2 блока питания с возможностью горячей замены;
- привод DVD-дисков;
- поддержка VMware ESXi 5;

2.3 Схема распределения компонентов АПК в рамках оборудования

Таблица 3 – Аппаратные ресурсы АСУНП (модернизированная версия)

№	Наименование компоненты	ОП, ГБ	ЖД, ГБ	ЦП, кол-во ядер
1	Портал АСУНП	16	47	8
2	База данных АСУНП	8	117	8

3 ЭКСПЛУАТАЦИЯ АПК УЗЛА

3.1 Общие положения

Эксплуатация узла осуществляется посредством

- мониторинга АПК и соответствующих информационных ресурсов, восстановления их работоспособности в случае нештатных ситуаций;
- выполнения профилактических работ.

Мониторинг АПК производится оператором и системным администратором узла.

Оператор узла выполняет:

- постоянную оценку работоспособности комплекса (телекоммуникационного оборудования и соединений, вычислительного оборудования и предоставляемых сервисов) с использованием АРМ МРС (<http://ms.meteo.ru>);
- информирование администратора узла о нештатных ситуациях, принятие мер по восстановлению работоспособности узла в случае сбоев самостоятельно или с привлечением администратора узла в оперативном порядке;
- ведение журнала эксплуатации узла в части АПК.

Восстановление работоспособности АПК и информационных ресурсов узла осуществляется в оперативном порядке посредством выполнения действия согласно разделам 3.2.-3.4. настоящего документа.

В случае выхода из строя вычислительного и телекоммуникационного оборудования восстановление работоспособности производится в порядке и на условиях гарантийного обслуживания оборудования, а также согласно порядку, принятому в организации, для послегарантийного периода.

Обеспечивается выполнение комплекса профилактических мер по поддержке АПК и информационных ресурсов узла в работоспособном состоянии:

- 1) по телекоммуникационному оборудованию:
 - создание резервных копий настроек оборудования (по мере внесения изменений в конфигурацию оборудования);
 - аудит событий на основе анализа системного журнала оборудования (еженедельно);
 - изменение парольной защиты (ежемесячно).
- 2) по вычислительному оборудованию и программному обеспечению:
 - визуальный осмотр и проверка работоспособности аппаратной части (еженедельно);

- аудит системных журналов событий ОС и программного обеспечения (еженедельно);

- создание резервных копий конфигурационных файлов ПО;

3.2 Обеспечение информационной безопасности

ФГБУ «ВНИИГМИ-МЦД» (далее, Центр) обеспечивает защиту информации от несанкционированного доступа (НСД) по направлениям: сетевое взаимодействие, программное обеспечение и информационные ресурсы узла.

3.2.1 Защита сетевого взаимодействия выполняется посредством:

- разграничения доступа (физического и сетевого) к сетевому оборудованию, а так же в сегмент локальной сети узла, контроля состояния межсетевых экранов и криптографических устройств и нарушений правил их работы на основе анализа системных журналов и встроенных систем мониторинга (еженедельно); Для ограничения доступа необходимо на АПК

- оценки эффективности и обновления средств защиты, в т.ч. сопровождение парольной защиты (один раз в три месяца);

- создание резервных копий настроек сетевого оборудования (по необходимости, в случае внесения изменений в настройки).

3.2.2 Защита программного обеспечения включает действия:

- контроль правил разграничения доступа к ПО на основе анализа системных журналов (еженедельно) с изменением правил при необходимости;

- создание резервных копий образов виртуальных машин (после приемочных испытаний Центра).

- Создание резервных копий рабочих каталогов компонент.

- оценка эффективности и обновление средств защиты, в т.ч. сопровождение парольной защиты (один раз в три месяца);

3.2.3 При возникновении НСД Центр принимает меры по восстановлению работоспособности узла, включающие в себя:

- ограничение доступа (при необходимости полная изоляция АПК) к компонентам АПК узла на момент восстановительных работ;

- восстановление компонентов узла и оценка их работоспособности.

3.2.4 При кадровых изменениях в составе персонала Центра принимаются меры по изменению правил доступа к компонентам узла по необходимости. В обязательном порядке производится изменение парольной защиты не зависимо от даты последних изменений.

Каждое вышеописанное действие фиксируется в журнале эксплуатации узла.

3.5 Эксплуатация аппаратно-программного комплекса

Проверка работоспособности АПК комплекса осуществляется средствами VMware vSphere Client. В качестве примера используется среда виртуализации узла ФГБУ «ВНИИГМИ-МЦД».

- Запуск VMware vSphere Client 5.5
- Введите имя пользователя и пароль в окно входа VMware vSphere Client показанное на рис.1.



Рисунок 1 - Окно входа VMware vSphere Client

- Если не настроены сетевые сертификаты безопасности на сервере VMware ESXi и клиенте VMware vSphere Client, то возможно отобразиться окно предупреждения показанное на рис. 2. В таком случае необходимо нажать кнопку «Ignore» и соединение с сервером продолжится.

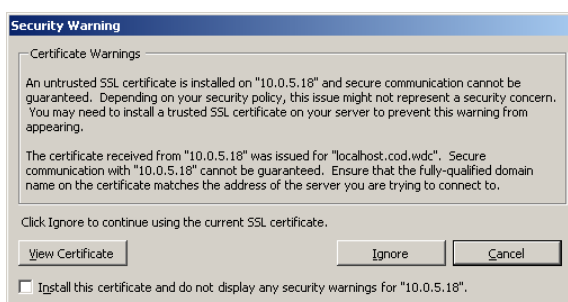


Рисунок 2 - Окно предупреждения непроверенных сертификатов безопасности

- В случае правильно введённых данных учётной записи пользователя появиться окно подключения, показанное на рис.3 с индикатором в левом нижнем углу. Процесс подключения может занять значительное время.



Рисунок 3 - Окно процесса подключения

- Далее необходимо открыть свойства сервера ESXi, нажав имя или IP-адрес сервера в левой панели структуры сервера, как показано на рис. 4.

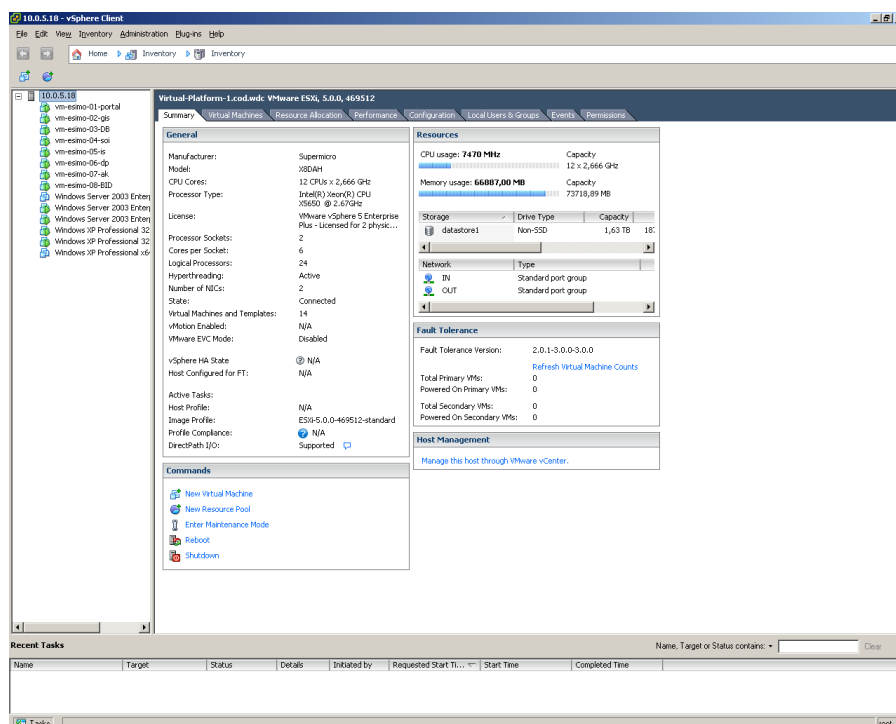


Рисунок 4 - Отображение структуры сервера

- Перейдите на вкладку «Производительность» и выберите необходимый параметр мониторинга, как показано на рис. 5, и просмотрите отображаемую информацию. Точно такая же вкладка доступна в каждой виртуальной машине, где есть возможность осуществить мониторинг индивидуально по каждой виртуальной машине. Примечание: состав раздела «Производительность» будет сильно зависеть от возможностей используемого аппаратного обеспечения и значительно отличаться на серверах различного типа.

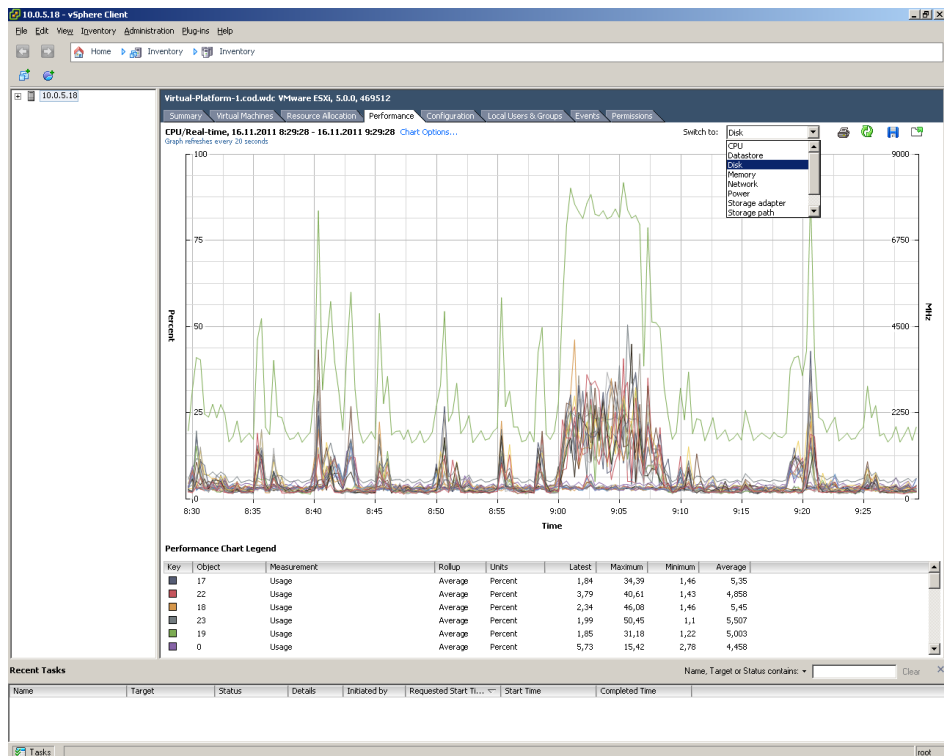


Рисунок 5 - Мониторинг сервера ESXi

- Перейдите на вкладку «Конфигурация». По умолчанию откроется раздел «Состояние здоровья», если нет, то выберите его в левой панели, как показано на рис. 6. В этом разделе отображается информация о состоянии аппаратного обеспечения сервера. С его помощью можно спрогнозировать или определить аппаратный отказ. Примечание: состав раздела «Состояние здоровья» будет сильно зависеть от возможностей используемого аппаратного обеспечения и значительно отличаться на серверах различного типа.

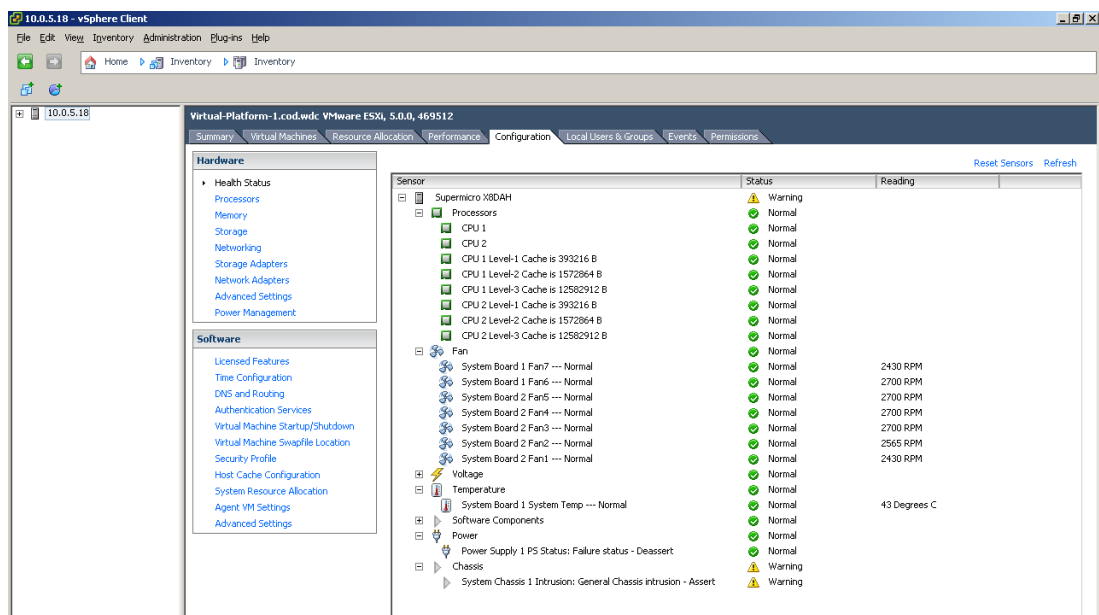


Рисунок 6 - Мониторинг сервера ESXi

Проверка системных журналов на наличие ошибок или несанкционированного доступа осуществляется стандартными средствами. Для проверки системных журналов используйте команду «`cat /var/log/messages | more`». Для проверки системного журнала от несанкционированного доступа используйте команду «`cat /var/log/secure | more`».

Для уменьшения вероятности от несанкционированного доступа необходимо ежемесячно производить смену паролей к ОС пользователей root и специализированного пользователя jboss.

Для проверки работы кластера, необходимо

- Произвести подключение к кластеру;
- Осуществить просмотр раздела работы сервисов и раздела управления дисками синхронизации.

Требования к паролям пользователей ОС:

- Пароль должен содержать латинские символы от a-z в верхнем и нижнем регистре;
- Спец символы !»№~%?*()@#\$\$%^&;
- Длина пароля должна быть не меньше 8 символов.

3.6 Эксплуатация телекоммуникационного оборудования

Эксплуатация, контроль работоспособности, управление телекоммуникационным оборудованием узла осуществляется согласно принятым правилам, регламентам и/или другим распорядительным документам, принятым в ФГБУ «ВНИИГМИ-МЦД».

3.7 Резервирование и восстановление базы данных

Предусмотрен механизм автоматического регулируемого создания резервных копий в случае возникновения сбоев и отказов. Механизм представляет собой скрипт, запускаемый по расписанию и создающий уникальную резервную копию все БД АСУНП (схемы asunp и asunp_new), например, asunp_new_20180602. Восстановление информации осуществляется администратором вручную с использование утилиты pg_restore. Изменение режима (времени и периодичности запуска) осуществляется через команду «`crontab -e`» в ОС в компоненте БД АСУНП.

4. ОБНОВЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Администратор узла осуществляет обновление версий программного обеспечения узла по компонентам, к ним относятся:

- прикладное программное обеспечение сервера;
- ОС (ядро операционной системы);
- среда функционирования (JDK, сервер приложений, библиотеки программ).

Администратор узла при получении информации о выпуске новой версии программного обеспечения по электронной почте самостоятельно применяет выпущенные обновления в пятидневный срок согласно инструкции в сообщении. Применение обновления включает выполнение следующих работ:

1) Загрузка обновления и обновленной эксплуатационной документации согласно инструкции по обновлению программного обеспечения, представляемой в сообщении электронной почты;

2) Создание резервной копии текущей версии обновляемого компонента узла;

3) В случае возникновения исключительных ситуаций при тестировании обновления осуществить разрешение проблемы с использованием технической документации на компонент или с привлечением разработчиков компоненты.

Обновление ОС и базового программного обеспечения производится администратором узла запуском стандартного менеджера установки пакетов ОС **yum**. Для произведения обновления необходимо выполнить команду **yum update -y** после завершения обновления необходимо перезапустить ОС командой **shutdown -r now**.

Примечание! Обновление ОС и базового программного обеспечения производится, в случае обнаружения уязвимости в работе ОС или базового программного обеспечения. В любых других случаях обновление ОС и базового программного обеспечения не производится.

ЛИСТ ИЗМЕНЕНИЙ

№ п/п	Дата внесения изменений	Номер раздела, пункта	Содержание внесенного изменения	Версия документа после внесения изменений	Должность, Ф.И.О.
1	6.062.18	1-4	Уточнение текста в связи с выкладыванием новой версии ПО	2.1	Белов К