Автоматизированная система управления видеонаблюдением

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

На 22 листах

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ

Термин / сокращение	Расшифровка
DNS	Распределённая система для получения информации о доменах
PHP	Скриптовый язык общего назначения, интенсивно применяемый для разработки веб-приложений
SSL	Криптографический протокол, который обеспечивает установление безопасного соединения между клиентом и сервером
АРМ	Автоматизированное рабочее место
ВК	Видеокамера
БД	База данных
Демон	Компьютерная программа в системах класса UNIX, запускаемая самой системой и работающая в фоновом режиме без прямого взаимодействия с пользователем.
Модуль	Функционально законченный фрагмент АСУ ВН, выполняющий ряд конкретных прикладных задач.
МСВ	Муниципальная Система видеонаблюдения
Объект	Зона наблюдения (территория, здание, помещение)
ОС	Операционная системы
ПО	Программное обеспечение
Портал (Веб-сервер)	Компонент Модуля получения и обработки видеопотоков уровня РЦВ. Сайт в компьютерной сети, предоставляющий различные сервисы пользователям АСУ ВН
ПЭВМ	Персональный компьютер
РЦВ	Региональный центр видеонаблюдения
СКОУ	Система контроля качества оказания услуг.

Термин / сокращение	**Расшифровка**
СУБД	Система управления базой данных - программное обеспечение, с помощью которого создается и поддерживается база данных, а также осуществляется к ней контролируемый доступ.

1 ОБЩИЕ СВЕДЕНИЯ

1.1. Вид оборудования, для которого составлено руководство

Настоящее руководство по эксплуатации разработано для Автоматизированной системы управления видеонаблюдением.

АСУ ВН обеспечивает процесс сбора и агрегации видеопотоков и иной информации, получаемой от ВК, с последующим нормированием, обработкой и хранением полученных данных для последующего анализа и предоставления (визуализации) информации. Кроме того, программный комплекс позволяет автоматизировать процесс согласования заявок на установку видеокамер, а также работу с обращениями пользователей и поддержку источников видеосигнала.

Комплект СПО включает в себя следующие компоненты:

- медиасервер уровня РЦВ
- сервер приложений
- база данных системы, построенная на СУБД PostgreSQL
- пользовательский портал на базе Httpd+PHP
- административный портал
- сервер балансировки нагрузки на базе Nginx
- модуль СКОУ
- система видеонаблюдения МСВ (Axxon Next 3.6.1)
- АРМ МСВ (клиент Axxon Next 3.6.1)
- Zabbix Agent
- Puppet

1.2. Функции системы

Перечень дорабатываемых функций АСУ ВН:

1.2.1. Функции «Модуля интеграции»

- Создание документа реестра ВК
- Получение данных из других Систем для формирования записей реестра ВК
- Подключение внешних поставщиков VSaaS услуг

1.2.2. Функции «Модуля обеспечения управления сервисами»

- Предоставление требуемых сервисов для обеспечения работоспособности создаваемых Модулей:
  - сервис чтения, обработки и записи данных в БД;
  - сервис маршрутизации запросов.

1.2.3. Функции портала администратора

- Вход в портал администратора
- Работа с областью главного меню
- Работа с областью фильтров
- Работа с областью действий
- Работа с пейджингом страниц

1.2.4. Функции «Модуля администрирования»

- Администрирование реестра ВК;
- Администрирование реестра типов ВК;
- Администрирование реестра пользователей;
- Администрирование реестра групп пользователей и их прав;
- Администрирование реестра муниципальных образований;
- Администрирование реестра серверов уровня МСВ;
- Администрирование реестра контрактов.

1.2.5. Функции «Модуля согласования мест установки ВК»

- Администрирование реестра заявок согласования мест установки ВК;

- Формирование рабочих групп пользователей муниципальных образований;
- Согласование места установки ВК рабочей группой;
- Рассылка уведомлений рабочей группе и пользователям группы «Исполнитель».

1.2.6. Функции «Модуля контроля качества оказания услуг»

- Получение и хранение сроком до 3-х лет данных о работоспособности:
  - СПД;
  - серверов видеонаблюдения уровня МСВ;
  - ВК;
  - АСУ ВН.
- Предоставление графического интерфейса визуализации текущего состояния контролируемых сегментов;
- Формирование отчета о работоспособности СПД, серверов видеонаблюдения уровня МСВ, работоспособности ВК за заданный произвольный период.

1.2.7. Функции «Модуля обработки обращений»

- администрирование реестра обращений;
- формирование отчета за заданный период;
- рассылка уведомлений;
- интеграция с существующей системой обработки обращений Заказчика.

1.2.8. Функции «Модуля журналирования»

- Получение отчета
- Экспорт отчета в файл формата CSV

1.2.9. Функции «Модуля балансировки нагрузки»

- Создание и поддержание работоспособности IP-адреса;
- Прием и обработка запросов к АСУ ВН.

1.2.10. Функции «Модуля получения, хранения обработки видеопотоков уровня РЦВ»

- Администрирование реестра блокировок ВК
- Просмотр/редактирование блокировки ВК
- Удаление блокировки ВК

1.2.11. Функции специальных пользователей АСУ ВН

- Возможность принудительного переключения любой из ВК системы на выделенный сегмент системы;
- Доступ к выделенному сегменту.

1.3. Режимы работы

Система поддерживает следующие режимы работы:

1. Нормальный режим работы - все устройства работают корректно в соответствии с правилами проверки функционирования.

2. Режим пуска/останова - особый режим работы, инициируемый ответственными за обслуживание Системы. Характеризуется большой вероятностью нарушения корректной работы Системы и соответствующими подготовительными мерами.

3. Аварийное отключение - режим внезапного выхода из строя программной или аппаратной составляющей Системы.

2 МЕРЫ БЕЗОПАСНОСТИ

Все работы по обслуживанию и эксплуатации комплекса технических средств Системы (монтажу, наладке, эксплуатации, обслуживании и ремонту технических средств) должны соответствовать действующим нормам и правилам техники безопасности, защите от воздействий электрических полей и электромагнитного излучения, пожарной безопасности, а также охраны окружающей среды согласно следующим документам:

- требования по безопасности используемых средств вычислительной техники в соответствии ГОСТ 25861-83;
  – требования по безопасности используемых электротехнических изделий в соответствии ГОСТ 12.2.007.0-75;
- нормы пожарной безопасности в соответствии с ГОСТ 12.1.004-91.

Для обеспечения надежного и безопасного функционирования КТС требуется соблюдение регламентных работ, предусмотренных для нормального режима функционирования.

3 ПОРЯДОК РАБОТЫ

3.1. Состав и квалификация персонала

К работе с АСУ ВН должны допускаться пользователи, которые обладают знаниями и навыками работы в качестве пользователя ПЭВМ в соответствии с Приложением к приказу Мининформсвязи России от 27.12.2005 г. № 147 «Об утверждении квалификационных требований к федеральным государственным гражданским служащим и государственным гражданским служащим субъектов Российской Федерации в области использования информационных технологий». В том числе пользователи должны:

- иметь опыт работы:
  - в среде Windows XP SP3 (и выше);
  - с веб-браузерами (Internet Explorer версии 8.0 или выше);
- знать эксплуатационную документацию на пользовательскую часть Системы;
- знать основы информационной безопасности.

3.1.1. Состав персонала

Персоналом Системы являются операторы, осуществляющие её эксплуатацию (Администраторы и Специалисты технической поддержки).

3.1.2. Квалификация персонала

Помимо наличия базовых навыков работы на ПЭВМ, к Специалистам технической поддержки и администраторам Системы предъявляются следующие требования:

- знание принципов построения систем управления базами данных;
- навыки работы с серверным и телекоммуникационным оборудованием;

- расширенные знания в области поддержки пользователей; основы информационной безопасности;
- знание требований по соблюдению правил электрической и противопожарной безопасности при проведении работ с техническими средствами Системы.

От Администраторов Системы дополнительно требуется:

- высокий уровень квалификации и практический опыт выполнения работ по установке, настройке и администрированию ПО, применяемого в Системе;

3.2. Порядок проверки знаний персонала и допуска его к работе

Порядок подготовки и проверки знаний персонала должен включать в себя:

1. Освоение персоналом учебных материалов, содержащие сведения о порядке и способах использования всех функций АСУ ВН в соответствии с ролями пользователей.

3.3. Описание работ и последовательность их выполнения

3.3.1. Установка

3.3.1.1. *Установка СУБД*

АСУ ВН использует СУБД PostgreSQL версии 9.2. Установка на целевой машине производится следующим образом:

```
#yum install postgresql92-server postgresql95-contrib
#service postgresql-9.2 initdb
#chkconfig postgresql-9.2 on service postgresql-9.2 start
```

3.3.1.2. Веб-сервер пользовательского портала

Веб-сервер пользовательского портала по сути – веб-приложение, работающее под управлением httpd (Apache) web-сервера и PHP-расширения.

3.3.1.3. Установка Apache

С учетом наличия сервера балансировки нагрузки, первым шагом настраиваем брандмауэр:

```
# systemctl stop firewalld && systemctl disable firewalld
```

Следующим идет непосредственно установка с SSL:

```
# yum -y install httpd mod_ssl
```

После чего необходимо отредактировать конфигурационный файл /e**tc/httpd/conf/httpd.conf** таким образом, чтобы ServerName параметр отражал ip-адрес или имя сервера, а строка

```
IncludeOptional conf.d/*.conf
```

оказалась бы в самом конце конфигурационного файла.

Далее добавляется главный виртуальный хост на порт 80 с параметрами папки веб-приложения в DocumentRoot.

Прописываем Apache в автозапуск:

```
# systemctl enable httpd.service
```

После чего демон стартуется командой:

```
# systemctl start httpd.service
```

3.3.1.4. Установка PHP

Устанавливаем пакеты PHP:

```
# yum install php-common php-gd php-mcrypt php-pear php-pecl-memcache php-
mysql php-xml php
```

Перезагрузка Apache:

```
# service httpd restart
```

3.3.1.5. Установка Zabbix Agent

Zabbix агенты разворачиваются на наблюдаемых целях для активного мониторинга за локальными ресурсами и приложениями (статистика жестких диски, памяти, процессоров и т.д.).

На компонентах АСУ ВН устанавливается Zabbix Agent версии 3.0. Причем это происходит как на Linux-машинах, так и Windows-ориентированных аппаратных комплексах МСВ. Соответственно, для установки используются немного разные способы.

3.3.1.6. Установка Zabbix Agent на целевые комплексы под ОС Windows

Установка очень проста и включает в себя 3 шага:

1. Создание файла конфигурации. Типично это C:\zabbix_agent.conf (он имеет синтаксис с файлом конфигурации UNIX агента). Пример конфигурационного файла есть в поставке дистрибутива (в conf/zabbix_agentd.win.conf).
2. Установить агент как сервис Windows.

```
zabbix_agentd.exe --install
```

Внимание! Для 64-битной версии ОС потребуется и 64-битная версия дистрибутива Zabbix для всех проверок, связанных с запущенными 64-битными процессами, для корректной работы.

При желании можно использовать клиентскую конфигурацию, отличную от пути по умолчанию (C:\zabbix_agent.conf):

```
zabbix_agentd.exe --config <ваш_файл_конфигурации> --install
```

3. Запустите агента.

Теперь можно использовать Панель управления для запуска агента как сервиса или выполнить из командной строки следующую строку:

```
zabbix_agentd.exe --start
```

3.3.1.7. Установка Zabbix Agent на целевые комплексы под семейство ОС Linux

В данном случае агент будет работать как автономный демон на наблюдаемом узле сети.

Установите пакет конфигурации репозитория. Этот пакет содержит файлы конфигурации yum.

```
# rpm -ivh http://repo.zabbix.com/zabbix/3.0/rhel/7/x86_64/zabbix-release-3.0-1.el7.noarch.rpm
```

Далее установить сам агент:

```
# yum install zabbix-agent
```

Пример установки только пакета агента:

```
# apt-get install zabbix-agent
```

Для запуска агента (единичного экземпляра) выполните:

```
shell> cd sbin

shell> ./zabbix_agentd
```

Так же, как и в Window-версии, можно указать путь к конфигурации, отличный от стандартного (/usr/local/etc/zabbix_agentd.conf).

Zabbix агент спроектирован для запуска от непривилегированного пользователя (non-root). Он будет работать от любого непривилегированного пользователя, от которого был запущен. Таким образом, можно запускать агент от имени любого непривилегированного пользователя без каких-либо последствий. При попытке запустить агента от 'root', он сразу переключится на пользователя 'zabbix', который должен присутствовать в вашей системе.

Единственный способ запустить агента от пользователя 'root' - соответствующим образом отредактировать параметр 'AllowRoot' в файле конфигурации агента.

3.3.1.8. Установка Puppet-клиента

Puppet – система централизованного управления конфигурацией. И именно в этом качестве клиентская часть ее устанавливается на видеосерверы МСВ для обновления агентов СКОУ.

Установочный пакет puppet-клиента представляет из себя стандартный .msi установщик, который разворачивает в системе всю необходимую инфраструктуру. Пакеты названы по следующей схеме: puppet-agent-<version>-<x64/x86>.msi.

Для того, чтобы puppet нормально функционировал, необходимо соблюдение следующих условий:

- у клиента должна быть возможность соединиться с мастером по IP-адресу и имени компьютера (последнее особенно важно, так как SSL сертификаты подписываются с учётом указанного имени). Для этого может потребоваться у клиента в файле /etc/hosts прописать строку с IP-адресом и именем host, или корректная настройка dns-сервера;
- должны быть открыты исходящие соединения для Puppet на порту 8140 для работы и 8139 для передачи обратных отчётов (или фаервол полностью отключен);
- должны быть синхронизированы часы (из практических соображений, так как часть команд может задаваться с привязкой ко времени и используемое SSL шифрование тоже имеет привязку к времени существования сертификатов).

3.3.1.9. Установка NGINX-сервера балансировки нагрузки

Для настройки репозитория yum для RHEL/CentOS необходимо создать файл с именем /etc/yum.repos.d/nginx.repo и таким содержимым:

```
[nginx]

name=nginx repo

baseurl=http://nginx.org/packages/RHEL/7/$basearch/

gpgcheck=0

enabled=1
```

Для проверки подписи пакетов используется ключ, который необходимо установить командой:

```
sudo rpm --import nginx_signing.key
```

3.3.2. НАСТРОЙКА

3.3.2.1. Настройка СУБД

Настройка СУБД заключается в создании базы посредством выполнения скрипта, приложенного в поставку АСУ ВН.

3.3.2.2. Настройка веб-сервера

Настройка веб-сервера заключается в копировании веб-приложения из поставки и подстановки соответствующего conf-файла, с образованием виртуального узла.

3.3.2.3. Настройка Zabbix Agent

Конфигурирование Zabbix Agent достигается подстановкой в стандартный zabbix_agent.conf, находящийся в поставке ПО, некоторых специфических параметров.

Таблица 1 – параметры при настройке Zabbix Agent

Параметр	**Описание**
Hostname	Уникальное, регистрозависимое имя хоста. Требуется для активных проверок и должно совпадать с именем узла сети указанном на сервере. Допустимые символы: буквенно-цифровые, '.', ' ', '_' и '-'. Максимальная длина: 64
ListenPort	Агент будет слушать этот порт для подключений с сервера. По умолчанию 10050.
Server	Список IP адресов (или имен хостов) Zabbix серверов, разделенных запятыми. Пробелы недопустимы. Входящие соединения будут приниматься только с хостов указанных в этом списке. Обратите внимание, что имена хостов должны резолвиться имя хоста→IP-адрес и IP-адрес→имя хоста. Если включена поддержка IPv6, тогда '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' обрабатываются одинаково.

Стандартный конфигурационный файл с уже проставленными параметрами включен в поставку необходимого ПО АСУ ВН и в большинстве случаев изменение параметров после копирования этого файла на целевые машины не требуется.

3.3.2.4. Настройка Puppet

Для того, чтобы клиенту знать, где искать мастера, необходимо в файле **puppet.conf** добавить строку:

```
[agent]

server = puppet-master.domain

node_name = cert

certname = workstation
```

Таким образом клиент при аутентификации на мастере всегда будет представляться как **workstation**. Данная настройка упрощает управление, позволяя задавать имена, соответствующие определённой целевой группе клиентов.

Запрос сертификата у сервера и тестовый запуск puppet (без активации службы), но при этом происходит подключение к серверу и применение всех доступных конфигураций можно выполнить как:

```
puppet agent --test
```

В первой попытке соединиться с мастером клиенту будет отказано по причине отсутствия подписанного SSL-сертификата, поэтому, получив отказ, клиент оставит запрос на его получение. Посмотреть список запросов можно с помощью команды:

```
puppet cert --list
```

Подписать сертификат и, соответственно, разрешить доступ клиенту можно командой:

```
puppet cert sign puppet-client.domain
```

где «puppet-client.domain» — имя клиента. Удалить сертификат с сервера:

```
puppet cert clean puppet-client.domain
```

4. ПРОВЕРКА ПРАВИЛЬНОСТИ ФУНКЦИОНИРОВАНИЯ

Для выполнения проверки работоспособности АСУ ВН осуществляется ведение журнала мониторинга работоспособности Системы.

Кроме того, несколько раз в неделю Специалистом технической поддержки проводится диагностика работы системы путем проведения тестовых испытаний и осуществляется контроль полученных результатов.

5. УКАЗАНИЯ О ДЕЙСТВИЯХ В РАЗНЫХ РЕЖИМАХ

5.1. Нормальный режим

В нормальном режиме функционирования Системы проводятся следующие работы:

- ежедневный мониторинг серверной части Системы;
- работы по обслуживанию БД;
- профилактические работы по поддержанию работоспособности АРМ пользователя (проводятся по мере необходимости).

5.2. Аварийное отключение оборудования

Работы по восстановлению работоспособности Системы проводятся в оперативном режиме и могут включать в себя следующие мероприятия:

- восстановление сбоев аппаратной части (замена жестких дисков, оперативной памяти и т.д.);
- восстановление операционной системы;
- восстановление серверной части Системы;
- восстановление базы данных Системы.

Точный список мероприятий определяется в конкретной ситуации в зависимости от характера аварии.

5.3. Пуск/остановка Системы

Плановые работы по внесению изменений в серверную часть Системы проводятся в часы отсутствия активности пользователей в Системе с обязательным предварительным уведомлением о времени и продолжительности проведения работ.

Порядок проведения работ:

- Отключение общего доступа пользователей к серверной части Системы (выполняется средствами операционной системы).
- Резервное копирование базы данных на отдельный носитель (выполняется в соответствии с инструкцией по обслуживанию БД).
- При необходимости резервное копирование системных файлов Системы и другой критически важной информации (выполняется средствами операционной системы и/или ПО резервного копирования).
- Отключение серверной части Системы при необходимости внесения изменений в аппаратную часть.
- Проведение плановых работ (изменение программной или аппаратной части).
- Проверка правильности функционирования серверной части Системы.
- Запуск Системы и проверка основных режимов работы Системы.
- Подключение пользователей к работе с Системой (выполняется средствами операционной системы).