УТВЕРЖДЕН
ТАСП.62.01.12.000.005 93 01-ЛУ

КОМПЛЕКС ПРОГРАММ
«ЗАЩИЩЕННАЯ ОПЕРАЦИОННАЯ СИСТЕМА «СИНТЕЗМ»
(КП «ЗОС «СинтезМ»)

Руководство системного программиста

ТАСП.62.01.12.000.005 32 01

Листов 408

2021

Литера___

Инв. №	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ является руководством системного программиста комплекса программ «Защищенная операционная система «СинтезМ» (далее по тексту – изделие или КП «ЗОС «СинтезМ») и содержит сведения о структуре изделия, правилах установки и настройки изделия.

Перечень терминов приведен в приложении А.

Перечень сокращений и обозначений, используемых в данном документе, приведен в приложении Б.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение программы

КП «ЗОС «СинтезМ» ТАСП.62.01.12.000.005 представляет собой комплекс программ (КП), и может быть использован для создания АСЗИ в части обеспечения функционирования серверных группировок и автоматизированных рабочих мест пользователей, а также обеспечения выполнения требований по защите информации, обрабатываемой в АСЗИ, от НСД и реализации защищенного вычислительного процесса.

КП «ЗОС «СинтезМ» может применяться для создания локальных либо территориально-распределенных автоматизированных и информационных систем (АС). Территориально-распределенные АС строимые с применением КП «ЗОС «СинтезМ» разворачиваются на базе комплексов средств автоматизации (КСА) различных уровней, имеющих иерархическую подчиненность.

1.2. Функции программы

КП «ЗОС «СинтезМ» обеспечивает следующие возможности в части использования в среде виртуализации (сервера виртуализации):

– создание отказоустойчивых кластеров серверов виртуализации;

– обеспечение живой миграции виртуальных машин между серверами виртуализации;

– подключение в качестве хранилищ образов виртуальных машин систем хранения данных по протоколам NFS, iSCSI, FC и Gluster;

– обеспечение работы сервера управления виртуальными машинами в виде высокодоступной виртуальной машины без необходимости выделения под нее отдельного физического сервера;

– предоставление веб-интерфейса администратора (портал администрирования средства управления средой виртуализации) для управления средой виртуализации;

– предоставление пользовательского веб-интерфейса для доступа пользователей к консолям виртуальных машин;

– выполнение централизованной авторизации в веб-интерфейс средства управления средой виртуализации посредством LDAP-каталогов FreeIPA, Active Directory;

– обеспечение запуска любых совместимых с архитектурой x86_64 гостевых операционных систем (Windows, Linux, BSD и прочие) в виртуальной машине;

– обеспечение возможности проброса в виртуальные машины PCI-устройств сервера виртуализации;

– обеспечение балансировки нагрузки на серверах виртуализации;

– создание сервера имен, централизованного хранилища учетных записей пользователей, LDAP-каталога и сервера авторизации с поддержкой протокола Kerberos;

– централизованное управление учетными записями пользователей, их идентификационными данными, атрибутами безопасности и групповыми характеристиками;

– выборку и представление записей о событиях на основе заданных критериев.

КП «ЗОС «СинтезМ» обеспечивает следующие возможности в части использования на рабочих станциях:

– поддержку функционирования автоматизированных рабочих мест (АРМ) пользователей на базе рабочих станций и ноутбуков в графическом режиме;

– использование в качестве гостевой операционной системы;

– обеспечение автоматизации деятельности пользователей за счет функциональных средств (WEB-браузер, проводник);

– обеспечение организации рабочих мест пользователей за счет поддержки технических средств (USB-устройств, PCI-устройств и оптических дисков).

КП «ЗОС «СинтезМ» реализует следующие функции безопасности:

– идентификация и аутентификация;

- управление доступом;
- регистрация событий безопасности;
- ограничение программной среды;
- изоляция процессов;
- защита памяти;
- контроль целостности;
- обеспечение надежного функционирования;
- фильтрация сетевого потока;
- среда виртуализации.

1.3. Функциональные ограничения на применение

Администраторам запрещается:

− включать автомонтирование образов дисков в формате ISO на АРМ непривилегированного пользователя;

− включать использование файловой системы UDF на АРМ пользователя;

− выполнять команду «pg_dumpall -g» с указанием директории, доступ на чтение к которой предоставлен пользователю;

− использовать ключ «-php-docroot» для uwsgi;

− использовать ключа «--protect-args» для rsync;

− запускать mod_wsgi в режиме демона;

− использовать файловые журналы для пакета mariadb-libs;

− устанавливать параметр max_message_unix_fds пакета dbus равным нечетному числу;

− настраивать пакет sssd на кэширование паролей;

− открывать на сервере порты для подключений по протоколу SMB1;

− включать проброс TCP посредством изменения значения параметра AllowTcpForwarding в файле /etc/ssh/sshd_config;

− выполнять SQL-команды формата "INSERT ... ON CONFLICT DO UPDATE".

Администраторам запрещается предоставлять непривилегированному пользователю следующие права:

- право на запуск службы Systemd;
- право на доступ к журналам и конфигурационным файлам СУБД из состава КП «ЗОС «СинтезМ», а также право на запуск серверных частей СУБД;
- право на изменение параметра max_message_unix_fds пакета dbus;
- право на изменение файла /etc/mailcap;
- право на использование утилиты sudo;
- привилегию CAP_NET_ADMIN;
- право на доступ к настройкам пакета ansible;
- право на доступ к файлу /dev/fuse;
- право на доступ к журналам Менеджера ВМ (ovirt-engine);
- право на доступ к каталогу хранения временных файлов sqlite;
- право на доступ к утилите pam_console_apply;
- право на доступ к файлу /dev/wcnss_wlan;
- права на запись в файлы httpd.conf и .htaccess;
- право на использование компиляторов из состава ОС;
- право на редактирование переменных среды;
- право на чтение файлов /proc/*/environ;
- право на запись в файлы /etc/passwd и /etc/shadow;
- право на запись в конфигурационный файл загрузчика grub;
- право на доступ к чтению записей аудита.

При эксплуатации ОС должно быть реализовано выполнение следующих ограничений:

- запрещается подключение bluetooth-устройств к хостам, функционирующим под управлением ОС;

− не должно быть возможности для передачи сетевых пакетов между хостами, функционирующими под управлением ОС, и FTP-серверами, к которым возможен доступ непривилегированных пользователей;

− должно быть исключено использование отчуждаемых носителей информации с содержимым, сформированным нарушителем;

− должны использоваться антивирусные средства;

− должно использоваться только лицензионное ПО фирм-производителей. В случае необходимости использования иного программного обеспечения, его применение должно быть санкционировано администратором безопасности. В любом случае стороннее ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПО СКЗИ;

− необходимо регулярно устанавливать пакеты обновления безопасности, обновлять антивирусные базы;

− при подключении к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов;

− должна быть установлена только одна операционная система, правом установки и настройки которой должен обладать только администратор;

− должна быть отключена возможность удаленного управления ОС;

− необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации), неиспользуемые протоколы, сервисы и службы рекомендуется отключить.

–

1.4. Требования к программным средствам

Для функционирования изделия на базе физических серверов, рабочих станций или ноутбуков (терминальных клиентов) не требуется наличие предустановленного программного обеспечения.

1.5. Требования к техническим средствам

Для функционирования сервера виртуализации необходимы технические средства со следующими минимальными характеристиками:

– процессор архитектуры x86_x64 с поддержкой аппаратной виртуализации и тактовой частотой не менее 2 ГГц;

– оперативная память не менее 16 ГБ;

– объем жесткого диска не менее 50 ГБ;

– сетевой контроллер с минимальной пропускной способностью 1000 Мбит;

Для функционирования рабочей станции или ноутбука необходимы технические средства со следующими минимальными характеристиками:

– процессор архитектуры x86_x64 с тактовой частотой не менее 2 ГГц;

– оперативная память не менее 4 ГБ;

– объем жесткого диска не менее 50 ГБ;

– сетевой контроллер с минимальной пропускной способностью 100 Мбит;

– монитор с разрешением 1024×768;

– клавиатура (рус./лат.);

– манипулятор «мышь».

Требования к конфигурации технических средств для сервера виртуализации могут меняться в зависимости от сложности архитектуры системы.

Расчет требований необходимо производить по следующим параметрам:

- количество ядер процессора;
- объем необходимого дискового пространства;
- объем оперативной памяти.

В общем случае расчет производится по формулам (1-3).

$$a_A = \frac{(0.5+x)N_B + N_C + \left\lceil \frac{N_D}{20} \right\rceil + 0.5N_E + X}{2} \quad (1);$$

$$b_A = (10 + (8+x)N_B + 110N_C + 20 + 2\left\lceil \frac{N_D}{20} \right\rceil + 5N_E + X \quad (2);$$

$$c_A = (2+x)N_B + 2N_C + 2\left\lceil \frac{N_D}{20} \right\rceil + 0.5N_E + X \quad (3),$$

где:

a_A – количество ядер, необходимое для функционирования сервера виртуализации;

b_A – объем дискового пространства, необходимый для функционирования сервера виртуализации;

c_A – объем оперативной памяти, необходимый для функционирования сервера виртуализации;

x – необходимое количество ресурса для обеспечения функционирования клиентских частей устанавливаемого ПО;

X – необходимое количество ресурса для обеспечения функционирования серверных частей устанавливаемого СПО;

N_B – количество пользовательских ВМ;

N_C – количество серверов для файлового хранилища;

N_D – количество терминальных серверов (АРМ);

N_E – количество серверов управления доступом.

Примечания:

1. Символ «⌈ ⌉» указывает на операцию округления получившегося числа к большему целому значению;

2. Для большинства АИС параметры Nc , N_D и N_E будут принимать значения, равные единице.

2. СТРУКТУРА ПРОГРАММЫ

2.1. Взаимодействие модулей программы

КП «ЗОС «СинтезМ» это высоко настраиваемая операционная система на базе Linux, предусматривающая возможность работы как на одном СВТ (АРМ, Сервер, ВМ), так и на разных СВТ объединенных в сеть.

КП «ЗОС «СинтезМ» реализуется в виде двух оцениваемых конфигурациях:

- операционная система (ОС), в двух вариантах установки:
  - серверная операционная система;
  - клиентская операционная система.
- среда виртуализации.

Конфигурациях ОС включает:

- базовая система (base) включающая в свой состав:
  - загрузчик ОС;
  - ядро ОС;
  - модули уровня ядра;
  - службы (демоны) ОС.
- графический клиент (x11);
- агент безопасности:
  - базовый (base-ab);
  - пользовательский (user-ab);
  - администратора (admin-ab).

Конфигурация Среда виртуализации включает:

- базовая система (base) включающая в свой состав:
  - загрузчик ОС;
  - ядро ОС;
  - модули уровня ядра;
  - службы (демоны) ОС.
- графический клиент (x11);
- агент безопасности:
  - базовый (base-ab);
  - пользовательский (user-ab);
  - администратора (admin-ab).

- гипервизор (virtualization-hypervisor);
- сервер безопасности (sb-server);
- средство управления доменными пользователями (server-ipa);
- средство управления средой виртуализации (manager-vm).

Описание компонентов представлено в таблице 2.1.

Таблица 2.1 - Описание компонентов

№	Наименование компонента	Описание
1.	Базовая система	компонент ОС, включающий в свой состав минимальный набор модулей необходимых для обеспечения функционирования операционной системы на серверах, АРМ и виртуальных машинах (ВМ). Базовая система работает на базе ядра Linux версии kernel-3.10.0-865.
2.	Графический клиент	компонент ОС, предназначенный для предоставления пользователям графического интерфейса, посредством которого осуществляется взаимодействие пользователя с ОС.
3.	Гипервизор	компонент КП «ЗОС «СинтезМ», предназначенный для обеспечения функционирования доверенной среды виртуализации, развертывания необходимого количества виртуальных машин и создания надежных, высокопроизводительных отказоустойчивых объектов с неограниченным числом пользователей.
4.	Сервер безопасности	компонент КП «ЗОС «СинтезМ», предназначенный для установки в ВМ Серверов безопасности предназначенный для сбора и хранения, отображения событий безопасности генерируемых агентами безопасности, обеспечения двухфакторной аутентификации пользователей.
5.	Агент безопасности	программное средство защиты информации (ПСЗИ), представляет собой компонент КП «ЗОС «СинтезМ», предназначенный для установки на физические сервера, виртуальные машины и рабочие станции для обеспечения реализации функций безопасности и взаимодействия с Сервером безопасности для обеспечения защиты информации от НСД. Агенты безопасности разделяются на три типа: базовый, пользовательский, администратора. Тип агента безопасности устанавливаемого на то или иное вычислительное средство определяется выбранной ролью КП «ЗОС «СинтезМ». Базовый Агент безопасности включает в свой состав минимальный набор модулей необходимых для реализации функций безопасности и устанавливается по умолчанию. Пользовательский агент безопасности и агент безопасности администратора содержат дополнительные модули и устанавливаются при развертывании КП «ЗОС «СинтезМ» на узлы предназначенные для обеспечения работы пользователей и администраторов.

№	Наименование компонента	Описание
6.	Средство управления доменными пользователями (сервер ИПА)	компонент КП «ЗОС «СинтезМ», предназначенный для установки в ВМ Серверов управления доступом. Сервер управления доступом включает в свой состав модули обеспечивающие доменную аутентификацию и идентификацию пользователей, а также графический интерфейс управления пользователями и группами пользователей.
7.	Средство управления средой виртуализации (Менеджер ВМ)	компонент КП «ЗОС «СинтезМ», предназначенный для предоставления администратору графического интерфейса для управления средой виртуализации.

КП «ЗОС «СинтезМ» в конфигурации ОС предназначена для предоставления пользователю многозадачной и многопользовательской операционной системы общего назначения, выступающей в качестве основы для исполнения приложений на серверах, АРМ, и гостевых ВМ.

КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» предназначен для обеспечения функционирования доверенной среды виртуализации, развертывания необходимого количества виртуальных машин и создания надежных, высокопроизводительных отказоустойчивых объектов в составе автоматизированной информационной системы с неограниченным числом пользователей.

Данная конфигурация предусматривает наличие, развернутых в рамках отдельных СВТ, ВМ (функционирующих в составе одной вычислительной сети), гипервизора, средства управления средой виртуализации (менеджер ВМ), средства управления доменными пользователями (сервер управления доступом), а также сервера безопасности.

КП «ЗОС «СинтезМ» выполняет следующие роли:

– серверная операционная система - предназначена для создания доверенной среды функционирования серверов и применения в качестве гостевой операционной системы для виртуальных машин;

– клиентская операционная система - предназначена для создания доверенной среды функционирования АРМ (рабочая станция), применения в

качестве гостевой операционной системы для виртуальных машин и предоставления пользователю графического интерфейса;

– сервер виртуализации (гипервизор) – предназначен для обеспечения функционирования среды виртуализации, в рамках которой выполняются виртуальные машины;

– сервер управления средой виртуализации (Менеджер ВМ) – предназначено для предоставления системному администратору графического интерфейса для управления средой виртуализации;

– сервер управления доменными пользователями (сервер ИПА) – предназначен для обеспечения доменной идентификации и аутентификации пользователей, а также хранения данных о пользователях и группах пользователей;

– сервер безопасности (СБ) – предназначен для сбора и хранения событий безопасности генерируемых агентами безопасности.

Роль задается на этапе установки КП «ЗОС «СинтезМ» и определяет набор устанавливаемых компонентов.

Сопоставление ролей и компонентов КП «ЗОС «СинтезМ» представлено в таблице 2.2.

Таблица 2.2 - Сопоставление ролей и компонентов

Роль КП «ЗОС «СинтезМ»	**Компоненты КП «ЗОС «СинтезМ»**
Серверная операционная система	– базовая система (base) – агент безопасности базовый (base-ab)
Клиентская операционная система	– базовая система (base) – графический клиент (x11) – агент безопасности базовый (base-ab) – агент безопасности базовый пользовательский/администратора (user-ab/admin-ab)
Сервер безопасности (СБ)	– базовая система (base) – агент безопасности базовый (base-ab) – сервер безопасности (sb-server)
Сервер управления доступом	– базовая система (base) – агент безопасности базовый (base-ab)

Роль КП «ЗОС «СинтезМ»	**Компоненты КП «ЗОС «СинтезМ»**
	– Средство управления доменными пользователями (сервер ИПА)
Сервер управления средой виртуализации	– базовая система (base) – агент безопасности базовый (base-ab) – менеджер ВМ (manager-vm)
Сервер виртуализации	– базовая система (base) – агент безопасности базовый (base-ab) – гипервизор (virtualization-hypervisor)

КП «ЗОС «СинтезМ» обеспечивает виртуальное окружение для обеспечения возможности запуска других ОС в программной среде. Каждая виртуальная машина (ВМ) представлена как процесс в ОС и является субъектом в соответствии со стандартом Linux касательно ограничения процессов.

Обработка каждой ВМ как обычного процесса ОС позволяет одновременное выполнение стандартных приложений в любое время. Средства администрирования реализованы как стандартные Linux приложения. Вычислительное окружение, обеспеченное ОС для пользователей, входящих в систему, не отличается от стандартов системы, в том числе, при работе ВМ. Стандартные приложения Linux и демоны могут выполняться одновременно с виртуальными машинами. Управление ВМ со стороны КП «ЗОС «СинтезМ» обеспечивается благодаря демону виртуальных машин libvirt.

Уникальные категории SELinux приписаны к каждой ВМ и её ресурсам. Политика SELinux предотвращает любой доступ с помощью виртуальной машины к её ресурсам, если категория SELinux не указана. В дополнение к этому, каждая ВМ выполняется без привилегий root (non-root UID), это гарантирует, что операции виртуальной машины не могут оказать влияние на политику системы, заданную и установленную на хост-системе.

Благодаря использованию механизма фильтрации пакетов хост-системы, сетевой трафик между ВМ и удалёнными объектами может контролироваться.

Учетные записи, используемые в КП «ЗОС «СинтезМ» разделяются на два типа:

- доменные;
- локальные (в том числе технологические).

Учетные записи пользователей КП «ЗОС «СинтезМ», хранящиеся в Средстве управления доменными пользователями, именуются доменными. Данные о таких пользователях распространяются Средством управления доменными пользователями на АРМ пользователей.

Доменные пользователи могут быть как служебными (данные субъекты осуществляют действия, выполняемые автоматически, без участия человека), так и сопоставленными лицу.

Учетные данные пользователей, хранящиеся локально на пользовательских АРМ, именуются локальными.

Локальные пользователи могут быть как служебными (данные субъекты осуществляют действия, выполняемые автоматически, без участия человека), так и сопоставленными лицу. В КП «ЗОС «СинтезМ» присутствуют служебные локальные пользователи. Данные субъекты действуют только в рамках одного компьютера или виртуальной машины, от имени данных пользователей функционируют системные сервисы защищенной операционной системы (ОС).

В КП «ЗОС «СинтезМ» выделены следующие роли:

- доменный администратор;
- локальный администратор;
- системный администратор;
- пользователь.

Примечание: далее по тексту при использовании терминов «доменный администратор», «локальный администратор», «системный администратор» для уточнения субъекта, которым выполняется действие, подразумевается пользователь которой обладает указанной ролью.

2.2. Структура программы

Структурная схема программного изделия КП «ЗОС «СинтезМ» приведена на рисунке 2.1

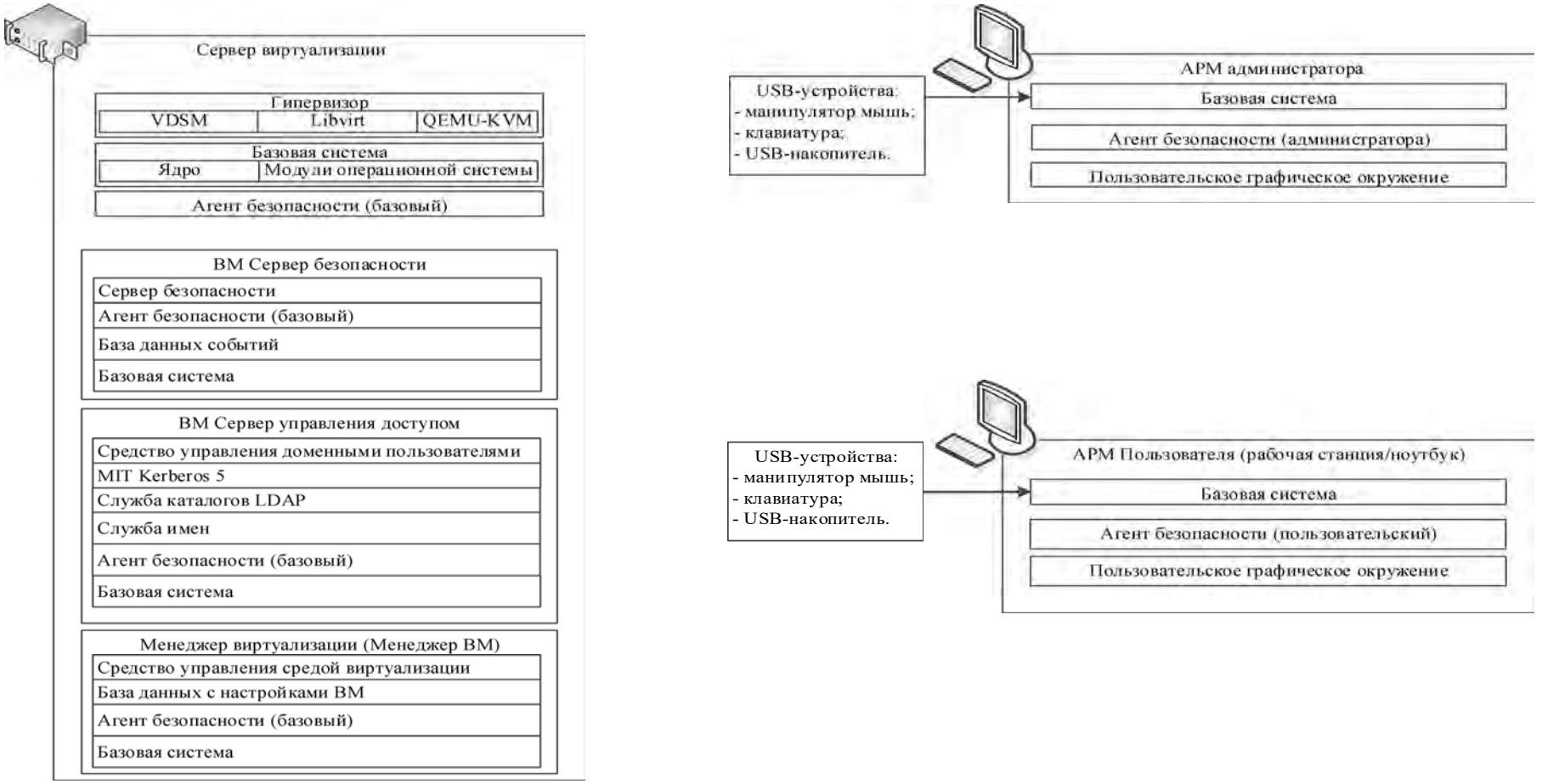


Рисунок 2.1– Структурная схема взаимодействия служб и модулей КП «ЗОС «СинтезМ»

2.2.1. Ядро (kernel)

Ядро это центральная часть ОС. Оно напрямую взаимодействует с аппаратным составляющим, реализует разделение ресурсов, предоставляет сервисы для программ, а также препятствует прямому доступу программ к аппаратно-зависимым функциям.

Сервисы предоставляемые ядром включают:

- контроль выполнения процессов путем их создания, прекращения или приостановки и связи. Это включает:

  - справедливое планирование процессов для выполнения на ЦП;
  - разделение процессов в ЦП в основе времени;
  - исполнение процесса в ЦП;
  - приостановка выполнения процесса при истечении времени выделенного на его обработку;
  - планирование другого процесса для выполнения;
  - планирование на исполнение приостановленного процесса;
  - управление метаданными процессов, связанными с безопасностью, такими как UID, GID, метки SELinux, возможности (capabilities).

- выделение памяти для исполняемого процесса. Это включает:

  - при определенных условиях ядро позволяет процессу выделять для совместного использования часть его адресного пространства, но обеспечивает защиту личного адресного пространства от воздействия извне.
  - взаимодействие с аппаратным оборудованием для установления адреса "виртуальный-в-физический", который сопоставляет генерируемые компилятором адреса (виртуальные) с их физическими адресами.

- управление жизненным циклом виртуальных машин. Это включает:

- установка ограничительных значений на ресурсы выделяемые виртуальной машине в соответствии с параметрами настроенными приложением эмуляции (QEMU-KVM);
- запуск виртуальной машины;
- обработка завершения работы виртуальных машин путем выполнения команды (инструкции) завершения или передачи команды завершения в приложении эмуляции.

– управление файловой системой. Это включает:

- структурирование файловой системы к хорошо понятному виду;
- защита файлов от несанкционированного доступа;
- посредничество в доступе между объектами и субъектами, позволяющее осуществлять контролируемый доступ на основе дискреционного разграничения доступа (DAC);
- разрешение контролируемого доступа к периферийным устройствам, таким как терминалы, ленточные накопители, дисководы и сетевые устройства.

Ядро КП «ЗОС «СинтезМ» является полностью выгружаемым (preemptible kernel). Это означает, что ядро позволяет выгружать выполняемую задачу в любой точке, если ядро находится в состоянии, в котором безопасно перепланировать задачу для ее выполнения через определенное время.

2.2.2. Кольца защиты

Кольца защиты – архитектура информационной безопасности и функциональной отказоустойчивости, реализующая аппаратное разделение системного и пользовательского уровней привилегий. Кольца защиты реализуются модулями Ядра ОС (kernel-3.10.0-865). Структура привилегий имеет вид нескольких концентрических кругов. В этом случае системный режим (режим супервизора или нулевое кольцо, так называемое «кольцо 0»), обеспечивающий максимальный доступ к ресурсам, является внутренним кругом, тогда как режим пользователя с ограниченным доступом — внешним. Семейство микропроцессоров x86

обеспечивает четыре кольца защиты (0-3) и виртуальное кольцо -1 в случае поддержки аппаратной виртуализации. При этом, в случае использования аппаратной виртуализации – на уровне кольца «-1» исполняются команды по управлению вспомогательными структурами гипервизора, а так же выполняются команды, позволяющие гипервизору переключать контекст исполнения с одной виртуальной машины на другую.

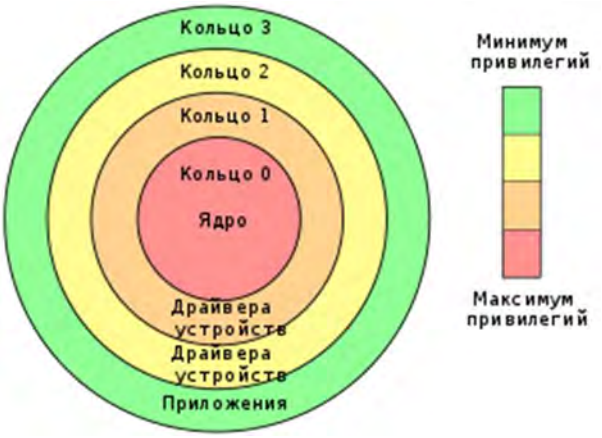


Рисунок 2.2 – Кольца защиты

Кольца защиты предназначены для разграничения доступа к:

1. Памяти;
2. Портам ввода-вывода;
3. Исполнению подмножества процессорных инструкций, а именно:
    а. LGDT - Load Global Descriptor Table;
    б. LLDT - Load Local Descriptor Table;
    в. LTR - Load Task Register;
    г. LIDT - Load Interrupt Descriptor Table Register;
    д. MOV - to and from control registers only;
    е. MOV - to and from debug registers only;
    ж. LMSW - Load Machine Status Word;
    з. CLTS - Clear Task Switched;
    и. INVD - Invalidate Cache;
    к. WBINVD - Write Back and Invalidate Cache;
    л. INVLPG - Invalidate TLB Entry;

м. HLT – Halt;

н. RDMSR - Read From Model Specific Register;

о. WRMSR - Write to Model Specific Register;

п. RDPMC - Read Performance Monitoring Counters;

р. RDTSC - Time Stamp Counter.

В любой отдельно взятый момент времени процессор семейства x86_64 «находится» в одном из колец, что определяет возможности исполняемого кода. Таким образом, когда процессор находится в 3м кольце, попытка исполнить одну из указанных выше процессорных инструкций проведет к general-protection exception. Ошибка схожа с исключением, которое генерируется КП «ЗОС «СинтезМ» при попытке доступа со стороны программы к некорректному виртуальному адресу. Такое же исключение генерируется при попытке доступа к защищенным областям памяти или портам ввода-вывода.

2.2.3. Логические компоненты ядра

Ядро состоит из логических подсистем, которые предоставляют разные функциональные возможности. Несмотря на то, что ядро является одной исполняемой программой, различные сервисы, которые она предоставляет, могут быть разбиты на логические компоненты. Эти компоненты взаимодействуют для обеспечения определенных функций.

Ядро состоит из следующих логических подсистем:

- подсистема ввода вывода;
- подсистема работы с процессами;
- подсистема работы с памятью;
- сетевая подсистема;
- подсистема IPC;
- подсистема модулей ядра;
- подсистема аудита;

- расширения безопасности;
- подсистема драйверов устройств;
- подсистема виртуализации.

2.2.3.1. Подсистема ввода вывода

Эта подсистема реализует функции, связанные с объектами файловой системы. Эти функции позволяют процессу создавать, поддерживать, взаимодействовать и удалять объекты файловой системы. Эти объекты включают обычные файлы, каталоги, символические ссылки, жесткие ссылки, специальные файлы устройств, именованные каналы (pipes) и сокеты.

2.2.3.2. Подсистема работы с процессами

Эта подсистема реализует функции, связанные с управлением процессами и управлением потоком. Эти функции позволяют создавать, планировать выполнение и удаление процесса, а также потоков.

В КП «ЗОС «СинтезМ» каждый процесс представлен в виде объекта типа struct task_struct – являющегося дескриптором процесса. Множество процессов в КП «ЗОС «СинтезМ» представлено как коллекция структур task_struct, доступ к которой осуществляется двумя способами – используя хэш-таблицу pidhash[] или же используя зацикленный список двойной связности, доступный из любого экземпляра task_struct при помощи указателей task->next_task и task->prev_task. Каждый дескриптор процесса содержит такие данные, как состояние выполнения, стек, набор флагов, указатель на дескриптор родительского процесса, поток выполнения (их может быть несколько), дескрипторы открытых процессом файлов и привязку к учетным данным пользователя.

Каждый дескриптор процесса связан с пользователем, от имени которого он исполняется при помощи двух указателей на объект типа struct cred– task->cred и task->real_cred. task->real_cred указывает на целевой контекст безопасности. task->cred указывает на субъективный (реальный на данный момент) контекст безопасности. Субъективный контекст определяет то, с какими привилегиями процесс будет

взаимодействовать с другими объектами в системе. Данный контекст может временно указывать на контекст, отличный от целевого.

2.2.3.3. Подсистема работы с памятью

Эта подсистема реализует функции, связанные с управлением ресурсами памяти системы. Реализованные функции включают те, которые создают и управляют виртуальной памятью, включая управление таблицами страниц и алгоритмами разбивки на страницы.

В КП «ЗОС «СинтезМ» процесс не работает с физической памятью напрямую – он работает с виртуальной памятью, которая представлена ему в виде неразрывного адресного пространства (или набором неразрывных сегментов). Виртуальная память – технология управления памятью, которая поддерживается как на уровне железа (MMU), так и на уровне ядра КП «ЗОС «СинтезМ».

Смысл виртуальной памяти – является задача отображения виртуальных адресов, вычисляемых в ходе работы исполняемого процесса – в физические адреса компьютерной памяти. Виртуальная память решает две задачи:

- адресная трансляция (перевод виртуального адреса в физический);
- управление виртуальными адресными пространствами.

2.2.3.4. Сетевая подсистема

Эта подсистема реализует сетевые сокеты, а также алгоритмы для планирования сетевых пакетов. Подсистема Netfilter является программно-аппаратной частью сетевой подсистемы (сетевой стек TCP/IP) и осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Подсистема состоит из модулей пространства ядра ip_tables, ebtables и утилит пространства пользователя с аналогичными названиями iptables, ebtables. Модули пространства ядра предоставляют таблице-ориентированную систему определения правил фильтрации и адресации сетевых пакетов. Перехват сетевого потока является основополагающим принципом, позволяющим подсистеме

выполнять свои задачи. Перехват осуществляется на двух уровнях сетевого стека: канальном и сетевом.

.

2.2.3.5. Подсистема IPC

Эта подсистема реализует функции, связанные с механизмами IPC. Реализованные функции включают тех, которые упрощают управляемый обмен информацией между процессами, позволяя им обменяться данными и синхронизировать их выполнение, чтобы взаимодействовать с общим ресурсом.

2.2.3.6. Подсистема модулей ядра

Эта подсистема реализует инфраструктуру для ядра, чтобы поддерживать различные механизмы ядра. Реализованные функции включают загрузку, инициализацию и выгрузку модулей ядра (подключаемые модули, исключение, аудит).

2.2.3.7. Подсистема Аудита

Подсистема аудита КП «ЗОС «СинтезМ» проводит аудит всех системных вызовов ядра системы, что позволяет проводить аудит приложений с привилегированными правами. Система аудита позволяет настраивать события, необходимые для аудита, из множества всех событий, которые могут быть обработаны. Настройка событий, необходимых для аудита, происходит в файле конфигурации. Далее происходит уведомление ядра, для создания внутренней структуры для проверяемых событий.

Подсистема аудита КП «ЗОС «СинтезМ» перехватывает все события ядра, анализирует данные события на основе правил аудита, и перенаправляет события аудита, которые запрашиваются для аудита, на демон аудита работающий в пользовательском пространстве.

События аудита генерируются в разных местах ядра КП «ЗОС «СинтезМ». Кроме того, приложения пользовательского пространства могут создавать записи аудита, которые загружаются в ядро для дальнейшей обработки.

Настройка аудита, расположенного в ядре КП «ЗОС «СинтезМ», производится приложениями пользовательского пространства. Обмен приложений с ядром происходит с использованием сетевого канала связи(netlink). Данный канал также используется приложениями, которые хотят отправить событие аудита в ядро.

2.2.3.8. Расширения безопасности

Расширения безопасности реализуют различные связанные с безопасностью аспекты включая платформу Модуля Безопасности (LSM).

В КП «ЗОС «СинтезМ» применяются расширения безопасности IMA и EVM.

2.2.3.8.1. Замкнутая программная среда (IMA/EVM)

Функцию безопасности по построению замкнутой программной среды обеспечивают модули Integrity Measurement Architecture (Архитектура Измерения Целостности, далее - IMA) и Extended Verification Module (Расширенный Модуль Проверки, далее – EVM). Архитектурно модули являются частью модуля безопасности системы и выполняет проверку целостности библиотек и исполняемых файлов, то есть гарантируют подлинность подписанных файлов с момента включения. Логически IMA и EVM являются двумя разными механизмами, выполняющими схожий функционал. IMA осуществляет проверку целостности содержимого файла, а EVM осуществляет проверку целостности атрибутов файла, тем самым предотвращая подмену атрибутов, необходимую в случае изменения содержимого файла.

Для управления подсистемой, в случае IMA, используются политики IMA, а в случае EVM – специальный флаг включения механизма. Определенный формат политик IMA позволяет задать категории файлов попадающих в область работы подсистемы. Например, исполняемый файл, файл открытый для записи или принадлежность файла к конкретной файловой системе. Файл политик хранится на машинах, использующих подсистему и загружается в нее во время запуска системы. Также при старте, специальным образом, загружаются ключи шифрования в хранилище ключей системы, и происходит включение модулей IMA и EVM.

При попытке запуска исполняемого файла, сперва EVM проводится оценка целостности расширенных атрибутов файла, а затем IMA оценка целостности содержимого файла. Не смотря на то, что сначала работает EVM, а после IMA, оценки значений атрибутов security.ima и security.evm осуществляет именно IMA. Таким образом, подсистему контроля целостности можно включить для работы с IMA или IMA/EVM. Возможность отдельного функционирования EVM не имеет.

2.2.3.9. Подсистема драйверов устройств

Эта подсистема реализует поддержку различных аппаратных и программных устройств через общий, независящий от устройств интерфейс.

2.2.3.10. Подсистема виртуализации

Эта подсистема реализует управление жизненным циклом виртуальной машины.

В КП «ЗОС «СинтезМ» за предоставление виртуализированных окружений отвечает подсистема виртуализации, основанная на двух компонентах – KVM (модуль ядра КП «ЗОС «СинтезМ») и QEMU (гипервизор).

2.2.3.10.1. KVM

Kernel-based Virtual Machine (далее - KVM) – инфраструктура виртуализации ядра КП «ЗОС «СинтезМ». KVM не осуществляет эмуляции – оно предоставляет интерфейс ядра /dev/kvm, который может быть использован userspace приложением для:

- развертывания адресного пространства гостевой ОС;
- загрузки инициализирующего образа для гостевой ОС (обычно, модифицированного BIOS);
- работы с вводом-выводом гостевой ОС;
- отображением видеодисплея гостевой ОС на физический дисплей.

Отдельно стоит отметить, что для использования технологии KVM – необходима поддержка виртуализации со стороны архитектуры центрального процессора (ЦП).

KVM вводит новый режим процессов в существующее ядро и пользовательские режимы. Новый режим называется guest и используется для выполнения кодов гостевой операционной системы. Пользовательский режим в ядре является непривилегированным и служит для выполнения кодов гостевой операционной системы.

Для выполнения операций ввода/вывода гостевой операционной системы предназначен QEMU – платформа, которая позволяет виртуализировать все оборудования (включая диски, графические адаптеры, сетевые устройства). Любые запросы ввода/вывода, которые делает гостевая операционная система, перехватываются и направляются в пользовательский режим для эмулирования с помощью процесса QEMU.

KVM обеспечивает виртуализацию памяти с помощью /dev/kvm. Каждая гостевая операционная система имеет свое собственное адресное пространство, которое устанавливается, когда создается гостевая система. Физическая память, которая назначается гостевой операционной системе, является в действительности виртуальной памятью процесса. Процессор также поддерживает процесс преобразования памяти, передавая управление гипервизору (базовому ядру).

KVM относится к модулям КП «ЗОС «СинтезМ» обеспечивающим выполнение требований безопасности.

2.2.3.10.2. QEMU

QEMU – гипервизор, осуществляющий виртуализацию аппаратной платформы. Он позволяет эмулировать ЦП через динамическую бинарную трансляцию и предоставляет различное эмулированное оборудование, для того чтобы гостевые ОС могли запускаться без модификации их исходного кода. QEMU используется совместно с KVM для того, чтобы гостевые ОС исполнялись со скоростью, близкой к скорости исполнения ОС на физической машине. В этом случае, QEMU используется

для эмуляции частей аппаратной платформы, но само исполнение гостевой ОС осуществляется при помощи KVM под управлением QEMU (только в случае наличия аппаратной поддержки виртуализации со стороны ЦП). В том случае, если аппаратной поддержки нет (отсутствует или отключены технологии VT-x или SVM) – QEMU осуществляет виртуализацию гостевой ОС без использования KVM, что существенно снижает вычислительную производительность виртуального окружения.

Виртуальные машины используют эмулятор аппаратной платформы QEMU для запуска гостевой операционной системы. Для работы с KVM был создан проект QEMU-KVM - форк кода QEMU для работы с KVM. QEMU отвечает за работу устройств ввода- вывода, управление виртуальной машиной. Виртуальная машина - обычный процесс в операционной системе.

2.2.4. Подсистема инициализации ОС (Менеджер системы и сервисов (systemd))

Подсистема инициализации ОС реализует возможность задания перечня компонентов программного обеспечения, разрешенных для автоматического запуска при загрузке операционной системы и запрещенных для автоматического запуска при загрузке ОС.

Программный модуль и комплекс утилит, отвечающих за подсистему инициализации ОС, называется “Менеджер системы и сервисов” (systemd). Менеджер предназначен для загрузки ОС после инициализации ядра и занимается запуском и распараллеливанием системных служб и компонентов программного обеспечения во время старта системы. Менеджер является родительским процессом для остальных процессов системы, загружается в системе самым первым и выгружается самым последним. Также менеджер осуществляет включение и выключение компонентов программного обеспечения во время работы ОС.

Менеджер оперирует специально оформленными файлами конфигурации – юнитами (unit). Каждый юнит отвечает за отдельно взятую службу, точку монтирования, подключаемое устройство, файл подкачки, виртуальную машину. Существуют специальные типы юнитов, которые не несут функциональной нагрузки,

но позволяют задействовать дополнительные возможности менеджера. К таким типам юнитов относятся: target, slice, automount. Менеджер поддерживает следующие типы юнитов:

- .target – позволяет группировать юниты, воплощая концепцию уровней запуска (runlevel);
- .service - отвечает за запуск сервисов (служб), также поддерживает вызов интерпретаторов для исполнения пользовательских скриптов;
- .mount – отвечает за монтирование файловых систем;
- .automount – позволяет отложить монтирование файловых систем до фактического обращения к точке монтирования;
- .swap – отвечает за подключение файла или устройства подкачки;
- .timer – позволяет запускать юниты по расписанию;
- .socket – предоставляет службам поддержку механизма сокет-активации;
- .slice – отвечает за создание контейнера cgroups;
- .device – позволяет реагировать на подключения устройств;
- .path – управляет иерархией файловой системы.

Юнит представляет собой текстовый файл, состоящий из секций. Секции содержат некоторый набор переменных и их значений. Простейший юнит обычно содержит секции Unit, Service, Install. Секция Unit содержит описание юнита и порядок его загрузки. Секция Service определяет как запускать юнит: способ и команды запуска. Секция Install содержит уровень запуска юнита. Пример юнита службы:

```
[Unit]
Description=NewUnit
After=nginx.service
Requires=nginx.service

[Service]
Type=forking
PIDFile=/www/newunit/pids/service.pid
WorkingDirectory=/www/newunit/current
User=newunit
```

```
Group=newunit
ExecStart=/usr/local/bin/somebin -c /www/newunit/service.conf
ExecStop=/usr/local/bin/somebin -s

[Install]
WantedBy=multi-user.target
```

2.2.4.1. Концепция уровней запуска

Уровни запуска реализовывают идею различных вариантов инициализации системы, в том числе ее перезагрузку или выключение. Существует семь уровней запуска пронумерованных от 0 до 6. Никакой последовательности выполнения уровней запуска нет, только один уровень выполняется при инициализации системы. Также один уровень запуска никогда не вызывает другой.

Уровень запуска определяет состояние системы после ее инициализации и означает:

- уровень 0 (Halt) – выключение системы;
- уровень 1 (Single-user mode) – режим для задач администрирования системы;
- уровень 2 (Multi-user mode) – многопользовательский режим без сетевых интерфейсов и сервисов;
- уровень 3 (Multi-user mode with networking) – нормальный запуск системы без графической оболочки;
- уровень 4 (Not used) – не используется;
- уровень 5 (Multi-user mode with GUI) – нормальный запуск системы с графической оболочкой;
- уровень 6 (Reboot) – перезагрузка системы.

Таргеты представляют собой юниты, группирующие другие юниты и контролирующие запуск системных служб и компонентов программного обеспечения. Таким образом таргеты определяют перечень компонентов, запускающихся во время инициализации системы. Соответствие уровней запуска

определенным таргетам, а также алиасы для соблюдения концепции инициализации системы представлены ниже:

- уровень 0 - “poweroff.target” (алиас “runlevel0.target”);
- уровень 1 - “rescue.target” (алиас “runlevel1.target”);
- уровень 2 - “multi-user.target” (алиас “runlevel2.target”);
- уровень 3 - “multi-user.target” (алиас “runlevel3.target”);
- уровень 4 - “multi-user.target” (алиас “runlevel4.target”);
- уровень 5 - “graphical.target” (алиас “runlevel5.target”);
- уровень 6 - “reboot.target” (алиас “runlevel6.target”).

2.2.4.2. Процесс инициализации ОС

Во время старта операционной системы происходит проверка наличия и работоспособности аппаратной части компьютера. Данную проверку проводит предварительно встроенное программное обеспечение – Базовая Система Ввода Вывода (BIOS, Basic Input Output System). Далее BIOS находит загрузочные секторы на всех подключенных загрузочных устройствах. Первый найденный сектор, с правильной загрузочной записью, загружается в ОЗУ и получает управление дальнейшим процессом запуска.

GRUB (Великий Унифицированный Загрузчик, GRAND Unified Bootloader) является загрузчиком, содержащимся в загрузочной записи и выполняющим следующий этап запуска системы. Для этого он совершает ряд действий, основное из которых найти и загрузить ядро в оперативную память и переключить управление компьютером на ядро.

После инициализации, ядро загружает менеджер системы и передает ему управление. Менеджер монтирует файловые системы, заданные в /etc/fstab, после чего получает доступ к своим конфигурационным файлам. Затем менеджер запускает юнит по умолчанию (default.target), принадлежащий типу цель и расположенный в /etc/systemd/system/default.target. Данная цель определяет состояние, в которое менеджер должен запустить систему. Цель default.target содержит уровень запуска

ОС и является символической ссылкой на настоящую цель, запускающую системные службы и сервисы. Обычно default.target соответствует уровню 5, то есть происходит исполнение цели graphical.target.

Выполнение целей, соответствующих уровням запуска, ведет к выполнению зависимых целей, что в конечном итоге приводит к многочисленным запускам различных системных служб и сервисов, результатом чего является рабочая ОС. Для более быстрой и эффективной загрузки ОС, старт системных служб и сервисов выполняется параллельно, однако не все компоненты могут быть запущены раньше других. Существует две контрольные точки, достижение которых определяет ряд служб, функционирующих к этому моменту. Первая точка представлена целью sysinit.target. По ее достижении компоненты, отвечающие за монтирование файловых систем, настройку файлов подкачки, запуск udev, установку генератора случайных чисел, запуск криптографических служб, при наличии зашифрованных файловых систем и другие низкоуровневые службы, необходимые для минимальной функциональности системы, находятся в рабочем состоянии. Вторая точка представлена целью basic.target. В этой точке запущенны компоненты, отвечающие за настройку коммуникационных сокетов, таймеров, путей к различным исполняемым каталогам.

Далее, в случае уровня запуска 5, происходит выполнение цели multi-user.target. Она занимается запуском служб и сервисов пространства пользователя. После этого исполняется цель graphical.target, запускающая графическую оболочку.

2.2.4.3. Конфигурирование инициализации ОС

Конфигурирование инициализации ОС осуществляется посредством настройки менеджера системы и сервисов. Для управления менеджером используется утилита systemctl. Обладая обширным перечнем возможностей, утилита позволяет гибко управлять менеджером и компонентами программного обеспечения. Часть этих возможностей с их описанием и командами вызова перечислена ниже:

- запуск юнита – включение компонента: “systemctl start <юнит>”.
- остановка юнита – выключение компонента: “systemctl stop <юнит>”.

- перезапуск юнита – выключение и включение компонента: “systemctl restart <юнит>”.
- перезагрузка юнита – перезагрузка конфигураций компонента: “systemctl reload <юнит>”.
- статус юнита – показывает состояние компонента: “systemctl status <юнит>”.
- проверка автозапуска юнита – проверка будет ли выполнен автоматический запуск компонента во время инициализации ОС: “systemctl is-enabled <юнит>”.
- включение автозапуска юнита – добавление автоматического запуска компонента во время инициализации ОС: “systemctl enable <юнит>”.
- исключение автозапуска юнита – исключение автоматического запуска компонента во время инициализации ОС: “systemctl disable <юнит>”.
- маскирование юнита – делает невозможным запуск компонента: “systemctl mask <юнит>”.
- снятие маскировки юнита – снимает маскировку компонента: “systemctl unmask <юнит>”.
- справочное руководство юнита – показывает справочное руководство компонента: “systemctl help <юнит>”.

Также существует команда перезапуска менеджера для поиска новых или измененных юнитов: “systemctl daemon-reload”. Для получения списка текущих загруженных целей необходимо выполнить команду: “systemctl list-units –type=target”.

Таким образом возможность задания перечня компонентов программного обеспечения, разрешенного для автоматического запуска при загрузке ОС, реализуется добавлением необходимых юнитов к цели текущего уровня запуска. Соответственно запрещенными окажутся все компоненты неуказанные в цели текущего уровня запуска или ее зависимостях. Изменение цели по умолчанию (default.target) возможно выполнением следующей команды: “systemctl set-default -f

<new.target>”. Это приводит к изменению символической ссылки юнита /etc/systemd/system/default.target и последующих инициализаций ОС по новой логике, реализованной в новой цели (<new.target>). Новая цель может быть как уже существующей, например multi-user.target, так и созданной. Для создания цели необходимо правильно написать свой целевой юнит systemd в /etc/systemd/system/<собственная.цель>. Затем создать каталог /etc/systemd/system/<собственная.цель>.wants и поместить в него символические ссылки на необходимые базовые службы из /usr/lib/systemd/system и собственные службы. Данный способ предоставляет полный контроль загружаемых компонентов и детальнейшую конфигурацию инициализации ОС.

2.2.5. Служба единого времени chrony

Для поддержания единого времени используются два типа часов. Первые - аппаратные, также называемые Real Time Clock, сокращенно RTC (они же - часы BIOS или CMOS) имеющие точность хода до нескольких секунд в день. Точность времени RTC зависит от различных параметров, например, от колебаний температуры окружающей среды. Аппаратные часы используются для поддержания значения времени на машине, в то время как она находится в выключенном состоянии. Вторые часы — внутренние программные (системные) часы. Системные часы подвержены отклонениям, связанным с большой системной нагрузкой и задержкой прерываний. При этом пока КП «ЗОС «СинтезМ» находится в запущенном состоянии, в качестве значения времени используются именно значения системных часов.

Системные часы поддерживают нужное время используя множество различных источников. В качестве одного из таких источников выступает счетчик TSC (Time Stamp Counter). TSC это счетчик частоты процессора, вычисляющий количество циклов с последнего момента установки ему значения (перезагрузки системы). TSC работает очень быстро, имеет высокую точность и при этом работает без прерываний.

Это связано с тем, что множество мелких корректировок основано на измерении отклонений и дрифтов системных часов.

Ядро КП «ЗОС «СинтезМ» использует данные с аппаратных часов для выставления значения системных часов во время загрузки системы. При выключении же системы запускается набор команд, присваивающих значение системных часов аппаратным часам, что позволяет системным часам иметь правильное значение при следующей загрузке системы. Аппаратное время виртуальных машин выставляется на основе времени гипервизора.

Дата и время в КП «ЗОС «СинтезМ» устанавливаются при загрузке системы на основании значения аппаратных часов, а также настроек часового пояса. Настройки часового пояса берутся из файла “/etc/localtime”.

Калибровка системных часов начинается в течении всего нескольких миллисекунд после старта ОС, но для достижения приемлемой точности может потребоваться от нескольких секунд до нескольких часов, в зависимости от аппаратного состава системы (hardware) и изначального состояния ОС.

В процессе функционирования КП «ЗОС «СинтезМ», обмен данными между системными и аппаратными часами осуществляется через программу chrony (рисунок 2.3).

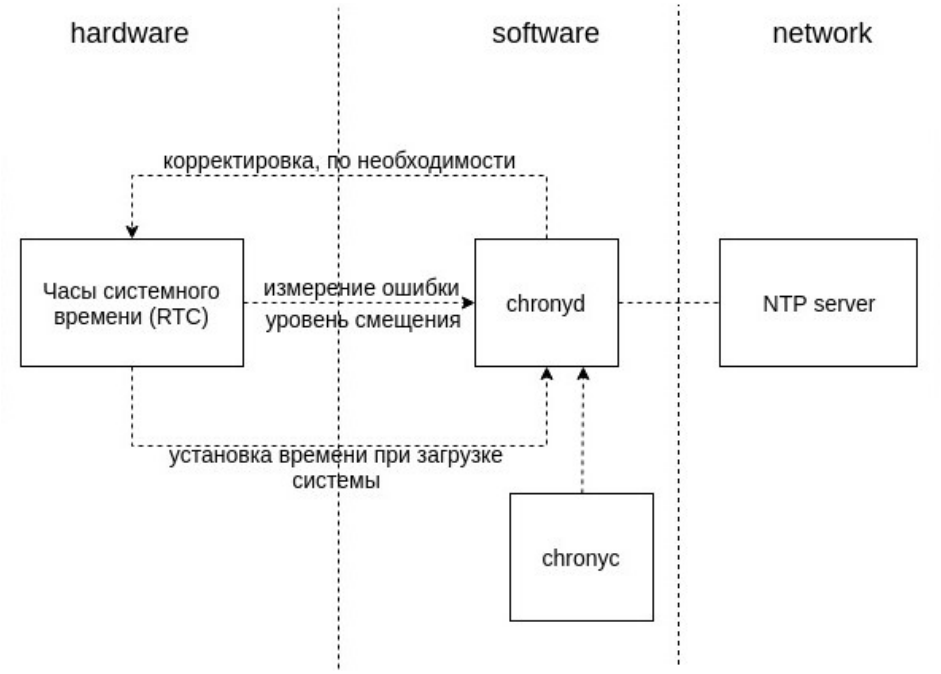


Рисунок 2.3 – Chrony

Программа chrony – это гибко настраиваемая реализация протокола NTP, позволяющая через сеть синхронизировать системное время с NTP серверами или же вручную, через консольный ввод. chrony используется на всех системах находящихся под управлением КП «ЗОС «СинтезМ»: ВМ, АРМ, физические сервера.

В КП «ЗОС «СинтезМ» используются следующие способы установки времени с помощью утилиты chrony:

– синхронизация системных часов с NTP серверами;

– синхронизация системных часов через ручной ввод (осуществляется локальным администратором).

Программа chrony состоит из двух модулей:

– chronyd – демон, работающий в фоновом режиме. Он получает информацию о разнице во времени между системными часами и часами внешнего источника времени (сервера времени), а также корректирует локальное время. Демон реализует протокол NTP и может выступать в качестве клиента или сервера. Его конфигурационный файл находится в директории: /etc/chrony/chrony.conf;

– chronyc – утилита командной строки для контроля и мониторинга работы chrony. Утилита используется для тонкой настройки различных параметров демона,

например, позволяет добавлять или удалять адреса NTP-серверов времени (при этом перезагрузка демона chronyd не требуется).

Демон chronyd вносит изменения в работу системных часов работающих в ядре КП «ЗОС «СинтезМ» через обращение к внешним источникам времени (используя протокол NTP). При отсутствии внешних источников синхронизации времени, chronyd будет использовать последнее высчитанное отклонение от реального времени (данная величина находится в файле /var/lib/chrony/drift). Например, для корректировки системных часов, отстающих на 1 секунду от реального времени, chronyd незначительно увеличивает величину, на которую системное время возрастает при каждом прерывании аппаратных часов (clock interrupt) до тех пор, пока ошибка, связанная с отставанием системного времени от реального времени, не будет исправлена. При необходимости корректирующие данные могут быть переданы chronyd также через chronyc.

Одной из главных задач chronyd является определение величины отклонения системных часов относительно реального времени – например в секундах, на которые системное время опережает или отстает от реального времени.

Отличительные характеристики программы chronyd:

– chronyd корректно функционирует и при условии отсутствия постоянного доступа к данным с внешних источников;

– chronyd выполняет синхронизацию часов быстро и с высокой точностью;

– chronyd быстро адаптируется к неожиданным изменениям в частоте хода аппаратных часов (например, связанным с изменением температуры кристалла);

– работа программ может быть связана с показаниями системных часов и, чтобы не нарушить ее, chronyd в своей базовой конфигурации никогда не вносит резких изменений в частоту хода часов;

– chronyd имеет возможность изменять частоту хода часов в широком диапазоне значений, что позволяет ему работать даже на системах с не работающими или не стабильно работающими часами (например, на виртуальных машинах);

– chronyd стабильно работает в изолированной сети, где единственный способ корректировки времени это ручной ввод (например, локальным администратором). chronyd определяет интенсивность, с которой системное время отклоняется от реального времени на основе уже учтенных корректировок разницы между системным и реальным временем; использует данные по интенсивности отклонения для настройки системного времени устройства;

– при необходимости корректировки системного времени chronyd меняет его постепенно. Для установки значения системных часов chronyd во время запуска КП «ЗОС «СинтезМ» использует данные с аппаратных часов, дополненные величиной отклонения системного времени от реального времени (данная величина хранится в файле /var/lib/chrony/drift).

Когда же вычислительное устройство под управлением КП «ЗОС «СинтезМ» подключено к ЛВС, демон chronyd имеет доступ к внешним NTP-серверам, от которых он и получает данные. На основе этих данных выполняется оценка ошибки системного времени текущего технического средства относительно реального времени и степень этой ошибки, т.е. величина отклонения системного времени данного вычислительного устройства относительно реального времени.

По умолчанию chronyd изменяет системное время постепенно замедляя или ускоряя скорость хода системных часов. Если значение системных часов сильно отстаёт от реального времени, синхронизация может занять много времени.

В КП «ЗОС «СинтезМ» для настройки системного времени с помощью chronyd в ее конфигурационном файле (/etc/chrony.conf) указывается директива “rtcsync”. При использовании этой директивы chronyd включает в ядре режим обновления RTC на основе системного времени каждые 11 минут (этот модуль ядра по умолчанию отключен). При этом, сам модуль chronyd напрямую с RTC не взаимодействует.

В зависимости от конфигурации демон chronyd может выступать как в качестве сервера точного времени, так и в качестве клиента. Настройка службы единого времени chrony представлена в п. 3.20.

2.2.6. Планировщик задач crond

Crond - программа-демон, предназначенная для выполнения заданий в определенное время, или через определенные промежутки времени. Для редактирования заданий используется утилита crontab.

Задание времени исполнения осуществляется в конфигурационном файле /etc/crontab и файлах расположенных в директории /etc/cron.d/. Задание времени осуществляется в следующем формате:

```
minute   hour   day   month   dayofweek   command
```

где:

- minute — любое целое число от 0 до 59;
- hour — любое целое от 0 до 23;
- day — любое целое от 1 до 31 (день должен быть корректным, если указан месяц);
- month — любое целое от 1 до 12 (или короткое название месяца, например: jan, feb и так далее);
- dayofweek — любое целое от 0 до 7, где 0 или 7 означает Воскресенье (или короткое название дня недели, например: sun, mon и так далее);
- command — команда, которая должны быть выполнена. Командой может быть как простая команда, например, ls /proc >> /tmp/proc, или команда запуска написанного вами специального сценария.

Для любых указанных выше параметров можно использовать звездочку (*), что означает все допустимые значения. Например, если поставить звёздочку в значении месяца, команда будет выполняться каждый месяц во время, указанное другими параметрами.

Дефис (-) между целыми числами обозначает диапазон чисел. Например, 1-4 означает целые числа 1, 2, 3 и 4.

Список значений, разделенных запятыми (,), обозначает перечень. Например, перечисление 3, 4, 6, 8 означает четыре указанных целых числа.

Косая черта (/) используется для определения шага значений. Целочисленное значение может быть пропущено в диапазоне, если после диапазона указать /<целое>. Например, значение минут 0-59/2, определяет, что будет пропущена каждая вторая минута. В качестве шага значений также может быть указана звёздочка. Например, значение месяца */3 определяет, что будет пропущен каждый третий месяц.

Любые строки, начинающиеся с символа решетки (#), являются комментариями, и не обрабатываются.

Если задачи cron должны выполняться по расписанию, но не ежечасно, ежедневно, еженедельно или ежемесячно, их можно добавить в каталог /etc/cron.d. Все файлы в этом каталоге имеют тот же синтаксис, что и /etc/crontab.

Демон cron каждую минуту ищет изменения в файле etc/crontab и каталогах /etc/cron.d/ и /var/spool/cron. Если какие-либо изменения будут найдены, они загружаются в память. Таким образом, демон не нуждается в перезапуске при изменении файла crontab.

Другие пользователи (не root) также могут настраивать задачи cron, используя программу crontab. Все созданные пользователями файлы crontab, хранятся в каталоге /var/spool/cron и выполняются, от имени создавшего их пользователя. Чтобы создать файл crontab для пользователя, войдите в систему под его именем и введите команду crontab -e, чтобы отредактировать crontab пользователя. Этот файл использует тот же формат, что и /etc/crontab. Когда изменения фала crontab будут сохранены, этот файл crontab будет записан в соответствии с именем пользователя, под названием /var/spool/cron/username.

Настройка расписания осуществляется в соответствии с пунктом 3.10.1 данной инструкции.

2.2.7. Загрузчик ОС

Загрузчик операционной системы необходим для обеспечения загрузки операционной системы непосредственно после включения компьютера.

Загрузчик ОС выполняет следующие задачи:

– загружает ядро операционной системы в оперативную память. Загрузка ядра операционной системы может происходить не только с жесткого диска, но и по сети;

– формирует входные параметры, передаваемые ядру операционной системы;

– передаёт управление ядру операционной системы.

Установщик GRUB прежде всего изменяет код MBR на свой собственный сектор MBR, в котором содержится главная загрузочная запись. Здесь содержится код основного загрузчика (446 байт), таблица разделов с описанием как основных, так и вторичных разделов жесткого диска (64 байта). Поскольку сектор MBR обладает малым объемом, запуск GRUB укладывается в два этапа. В секторе MBR размещена ссылка на конфигурационный файл, который может находиться на любом жестком диске. По ней будет определяться загрузка, которая начинается на втором этапе. Все настройки и данные для работы GRUB считываются из конфигурационного файла. Если же конфигурационный файл не был найден на втором этапе, то процесс загрузки будет прекращен. Описание работы с загрузчиком ОС представлено в п. 3.7.

2.2.8. Менеджер пакетов RPM

RPM – менеджер пакетов который может быть использован для создания, установки, проверки, обновления и удаления программного обеспечения. Структура пакета состоит из файлов и метаданных, используемых для установки и удаления архива файлов. Метаданные включают вспомогательные скрипты, атрибуты файлов и описательную информацию о пакете. Пакеты поставляются в двух вариантах: бинарные пакеты, используемые для инкапсулирования программного обеспечения для установки и исходные пакеты, содержащие исходный код и скрипты, необходимые для создания бинарных пакетов.

База данных RPM ведётся в каталоге /var/lib/rpm. Она состоит из одиночной базы данных (Packages), в которой хранится вся информация о пакетах, и множества маленьких баз (db.001, db.002 и т. д.), которые служат для индексации и содержат в себе сведения о том, какие файлы менялись и создавались при установке и удалении пакетов.

2.2.9. Менеджер пакетов YUM

yum – утилита для проверки, загрузки и установки RPM пакетов. Зависимости разрешаются и загружаются автоматически.

YUM расширяет возможности систем RPM, дополняя их функциями автоматического обновления и управления пакетами, включая управление зависимостями. YUM позволяет получать информацию об установленных в системе пакетах, работает с репозиториями, которые представляют собой коллекции пакетов, обычно доступных по сети.

2.2.10. Безопасная оболочка (ssh)

SSH (от англ. secure shell - безопасная оболочка) это набор программ, которые позволяют регистрироваться на компьютере по сети, удаленно выполнять на нем команды, а также копировать и перемещать файлы между компьютерами. SSH организует соединение поверх каналов связи. SSH предоставляет замены традиционным r-командам удаленного доступа.

В КП «ЗОС «СинтезМ» SSH применяется на этапе пуско-наладки в процессе развертывания менеджера ВМ, в процессе управления гипервизорами (добавление, удаление), а также для обеспечения отказоустойчивого кластера.

После проведения настройки ОС возможность удаленного входа по ssh на рабочие места для пользователей должна быть заблокирована. Настройка удаленного входа осуществляется в соответствии пунктом 3.7.5.

Возможность аутентификации от имени суперпользователя ограничена настройками демона SSHD, прописанными в базовом наборе конфигураций.

SSH обеспечивает:

- авторизацию на сервере (kerberos, pam);
- аутентификацию сервера (не позволяет выполнить подмену сервера);
- аутентификацию клиента;
- проверку целостности пакетов;

– ограниченную по времени аутентификацию.

В SSH-соединении участвуют две стороны: клиент и сервер. Сервер SSH реализован в виде программы ssh. Программа ssh предназначена для регистрации на удаленном хосте с использование протокола ssh и удаленного выполнения команд. Кроме того, ssh позволяет выполнять туннелирование любых TCP-соединений внутри ssh-канала (port forwarding). Стандартным портом, на котором ssh сервер ожидает соединение, является 22.

2.2.11. Модуль bash mail

В сессиях оболочек bash, после аутентификации пользователя, периодически выполняется проверка наличия новых сообщений в почтовой папке пользователя. Переменная среды MAIL указывает на почтовую директорию пользователя. Переменная среды MAILCHECK определяет периодичность опроса почтовой папки в секундах.

2.2.12. Модуль SSSD

SSSD - это системный демон с основной функцией обеспечения доступа к удаленному ресурсу идентификации и аутентификации через общую инфраструктуру, которая может обеспечить кэширование и автономную поддержку системы. Он предоставляет модули PAM и NSS. Он также обеспечивает базу данных для хранения локальных пользователей, а также расширенные пользовательские данные.

В КП «ЗОС «СинтезМ» SSSD настраивается на использование с LDAP и проверкой подлинности MIT Kerberos 5. Одним из основных преимуществ SSSD является автономная аутентификация. SSSD может кэшировать удаленные идентификаторы и аутентификационные данные. Это означает, что пользователь все еще может аутентифицироваться с этими удаленными идентификаторами, даже когда компьютер находится в автономном режиме. В системе SSSD пользователю нужно управлять только одной учетной записью. SSSD интегрируется с базой PAM и NSS и

поэтому может использоваться вместе с модулями PAM для локальных хранилищ учетных данных.

SSSD взаимодействует между собой через S-bus обертку над протоколом D-bus (код находится в директории src/sbus). SSSD находится между локальным клиентом и хранилищем (источником) данных (см. Рисунок 2.4) данные от источника процессу SSSD передаются через KDC.

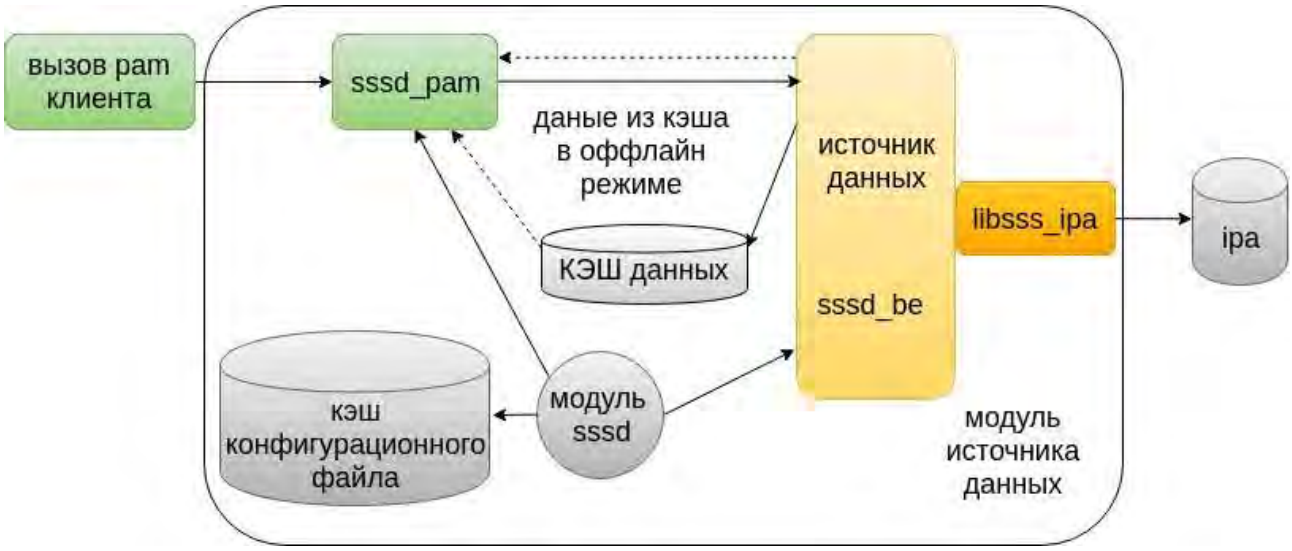


Рисунок 2.4 – Алгоритм работы SSSD

SSSD используется для хранения Kerberos билетов в SSSD кэше, что дает пользователю доступ в систему даже при отсутствии сетевого соединения. Таким образом, SSSD предоставляет возможность офлайн аутентификации через кэширование данных необходимых при логировании, за счет возможности SSSD осуществлять сопоставление локальных данных сервисов с кэшем. При этом кэш может храниться как локально, так и предоставляться непосредственно с удаленного клиента, например IPA.

SSSD настраивается через конфигурационный файл sssd.conf. Настройка SSSD осуществляется автоматически при добавления узла в сервер управления доступа (см. п 3.5).

2.2.13. Графическое окружение

Графическое окружение клиента состоит из:

– виртуальной видеокарты (QXL)+драйвер;

– X–сервера (Xorg);

– среды рабочего стола (MATE).

Виртуальная видеокарта QXL используется для предоставления удаленного доступа по сети по протоколу SPICE к экрану клиента под управлением X-сервера без использования эмуляции видеокарты гипервизором. Основными особенностями работы данной видеокарты являются:

- возможна удаленная работа на виртуальных машинах без сетевого подключения;
- обработка изображения происходит на стороне клиента;
- поддерживается сжатие изображения.

X – сервер Xorg является реализацией сервера X Window System, оконной системы, обеспечивающей стандартные инструменты и протоколы для построения графического интерфейса пользователя. Xorg реализует базовые функции графической среды: отрисовку и перемещение окон на экране, взаимодействие с устройствами ввода, такими как, например, мышь и клавиатура.

MATE – среда рабочего стола, являющаяся ответвлением от кодовой базы, не поддерживаемой в настоящее время среды GNOME 2. MATE представляет собой интуитивно понятный рабочий стол, использующий традиционную концепцию построения интерфейса. Разработчики MATE ориентируются на создании полностью свободной среды, доступной всем пользователям вне зависимости от их уровня технических навыков, физических ограничений и языка, на котором они говорят. MATE в своем составе содержит приложения для конечных пользователей. MATE построен на основе кроссплатформенной библиотеки элементов интерфейса GTK+. Составными частями библиотеки GTK+ являются GTK и GDK. GTK содержит набор шаблонных элементов интерфейса, GDK отвечает за вывод данных на экран с использованием Xorg.

2.2.14. Сервисные компоненты

Сервисные компоненты, обеспечивающие работу программного обеспечения:

– служба WEB-сервера Apache (httpd) – кроссплатформенный HHTP-сервер, обладающий модульной структурой. Apache имеет встроенный механизм виртуальных хостов. Он позволяет полноценно обслуживать на одном IP-адресе множество сайтов (доменных имён), отображая для каждого из них собственное содержимое. Для каждого виртуального хоста можно указать собственные настройки ядра и модулей, ограничивать доступ ко всему сайту или отдельным файлам. Некоторые MPM, например, Apache-ITK позволяют запускать процесс httpd для каждого виртуального хоста с отдельными идентификаторами uid и guid. Также, существуют модули, позволяющие учитывать и ограничивать ресурсы сервера (CPU, RAM, трафик) для каждого виртуального хоста;

– виртуальная машина JAVA (java-openjdk) – используется для запуска приложений и апплетов, написанных на языке Java. Java строго типизированный объектно-ориентированный язык программирования. Приложения Java обычно транслируются в специальный байт-код, выполняемый виртуальной машиной Java (JVM) – программой, обрабатывающей байтовый код и передающей инструкции оборудованию как интерпретатор. Достоинством подобного способа выполнения программ является полная независимость байт-кода от операционной системы и оборудования, что позволяет выполнять Java-приложения на любом устройстве, для которого существует соответствующая виртуальная машина;

– интерпретатор PHP – интерпретация скриптов, написанных на языке PHP. PHP – скриптовый язык общего назначения, интенсивно применяемый для разработки веб-приложений и автоматизации рутинных действий на сервере, также применяемый для написания кроссплатформенных графических приложений. Популярность в области построения веб-сайтов определяется наличием большого набора встроенных средств для разработки веб-приложений. Основные из них:

- автоматическое извлечение POST и GET-параметров, а также переменных окружения веб-сервера в предопределённые массивы;

- автоматизированная отправка HTTP-заголовков;
- работа с HTTP-авторизацией;
- работа с cookies и сессиями;
- работа с локальными и удалёнными файлами, сокетами;
- обработка файлов, загружаемых на сервер;
- работа с XForms;

– служба СУБД (PostgresSQL-server) – объектно-реляционная СУБД. PostgreSQL базируется на языке SQL и поддерживает многие из возможностей стандарта SQL:2011. PostgreSQL поддерживает одновременную модификацию БД несколькими пользователями с помощью механизма Multiversion Concurrency Control (MVCC). Благодаря этому соблюдаются требования ACID. Сильными сторонами PostgreSQL считаются:

- высокопроизводительные и надёжные механизмы транзакций и репликации;
- расширяемая система встроенных языков программирования: в стандартной поставке поддерживаются PL/pgSQL, PL/Perl, PL/Python и PL/Tcl; дополнительно можно использовать PL/Java, PL/PHP, PL/Py, PL/R, PL/Ruby, PL/Scheme, PL/sh и PL/V8, а также имеется поддержка загрузки C-совместимых модулей;
- наследование;
- легкая расширяемость;

– модуль сервера приложений (Mono) – набор библиотек и программного обеспечения для компиляции и исполнения приложений, написанных с использованием .NET Framework. Mono включает в себя компилятор языка C# – dmcs, среду исполнения .NET– mono (с поддержкой JIT) и mint (без поддержки JIT), отладчик, а также ряд библиотек, включая реализацию WinForms, ADO.NET и ASP.NET, а также компиляторы smcs (для создания приложений для Moonlight) и vbc (для приложений, написанных на VB.NET). Mono содержит альтернативу структуре WPF–приложений (XAML+C# или любой другой язык, который поддерживается в данной среде исполнения). Данный язык называется Glade, при помощи него можно

собирать GTK−приложения. Mono может исполнять модули, написанные на языках C#, F#, Visual Basic .NET, Java, Boo, Nemerle, Python, JavaScript, Erlang, SmallTalk, Lisp, PHP и Object Pascal;

– модуль работы с информацией о геолокации (geos) – используется в качестве библиотеки, реализующей набор функций и объектов для обработки геоданных;

– кроссплатформенная библиотека разработки ПО на языке программирования C++ (QT4.8, QT5.7), кроссплатформенный набор библиотек для разработки ПО на языке программирования C++. Позволяет запускать написанное с его помощью программное обеспечение в большинстве современных операционных системах путём простой компиляции программы для каждой операционной системы, без изменения исходного кода. Включает в себя все основные классы, которые могут потребоваться при разработке прикладного программного обеспечения, начиная от элементов графического интерфейса и заканчивая классами для работы с сетью, базами данных и XML. Qt является полностью объектно-ориентированным, легко расширяемым и поддерживающим технику компонентного программирования. Отличительная особенность Qt от других библиотек – использование Meta Object Compiler (MOC) – предварительной системы обработки исходного кода. MOC позволяет во много раз увеличить мощь библиотек, вводя такие понятия, как слоты и сигналы. Кроме того, это позволяет сделать код более лаконичным. Утилита MOC ищет в заголовочных файлах на C++ описания классов, содержащие макрос Q_OBJECT, и создаёт дополнительный исходный файл на C++, содержащий метаобъектный код.

2.2.15. Подключаемые модули аутентификации (PAM)

КП «ЗОС «СинтезМ» использует набор библиотек, называемых «Подключаемыми модулями аутентификации» (PAM), которые позволяют локальному администратору выбирать, как должны аутентифицировать пользователей приложения, использующие PAM. В данном пункте содержится краткое описание использования и конфигурирования PAM в ОО.

Pluggable Authentication Modules (PAM) является обобщённым API для служб, связанных с аутентификацией, которые позволяют локальному администратору добавлять новые методы аутентификации простой установкой новых модулей PAM, и изменять политику аутентификации посредством редактирования конфигурационных файлов. PAM отвечает за подсистему идентификации и аутентификации и обеспечивает централизованный механизм аутентификации всех сервисов. PAM допускает ограничения на доступ к приложениям и альтернативные настраиваемые методы проверки подлинности.

PAM состоит из набора разделяемых библиотечных модулей, которые предоставляют соответствующие услуги проверки подлинности и аудита для приложения.

Для управления режимами аутентификации используется сценарий sintez-pam-update, входящий в состав агента безопасности. Настройка режима аутентификации осуществляется локальным администратором в процессе установки и настройки ОС. В соответствии с применяемыми в КП «ЗОС «СинтезМ» схемами аутентификации выделяют следующие конфигурации PAM:

- локальная. Данная конфигурация настраивается за счет запуска сценария sintez-pam-update с параметром local.
- доменная. Данная конфигурация настраивается за счет запуска сценария sintez-pam-update с параметром domain.

Используемые в КП «ЗОС «СинтезМ» модули PAM представлены в таблице 2.3.

Таблица 2.3 – Модули PAM

Название библиотеки	Зависимости	Описание
pam_access.so	crond:6:account	Модуль управления доступом, основанным на именах пользователей, IP или именах хостов.
pam_cap.so	-	Модуль установки наследуемых прав

Название библиотеки	Зависимости	Описание
pam_console.so	gdm-smartcard:11:session xserver:3:auth gdm-autologin:10:session gdm-password:14:session login:11:session gdm-pin:15:session gdm-fingerprint:11:session	Модуль, определяющий пользователя, владеющего системной консолью
pam_deny.so	fingerprint-auth:6:auth fingerprint-auth:14:password system-auth-ac:9:auth system-auth-ac:20:password smartcard- ovirt-shutdown:3:auth ovirt-hibernate:3:auth system-auth:9:auth system-auth:20:password ovirt-container-list:3:auth smartcard-auth:11:auth smartcard-auth:23:password ovirt-flush-caches:3:auth password-auth-ac:9:auth password-auth-ac:20:password ovirt-locksession:3:auth other:2:auth other:3:account other:4:password other:5:session smartcard-auth-ac:6:auth password-auth:9:auth password-auth:20:password password- ovirt-logout:3:auth diskmapper:3:auth fingerprint-auth-ac:6:auth fingerprint-auth-ac:14:password	Блокирующий модуль
pam_env.so	fingerprint-auth:4:auth system-auth-ac:4:auth smartcard- system-auth:4:auth smartcard-auth:4:auth password-auth-ac:4:auth smartcard-auth-ac:4:auth gdm-autologin:2:auth password-auth:4:auth password- gdm-launch-environment:2:auth fingerprint-auth-ac:4:auth	Модуль загрузки переменных среды
pam_gnome_keyring.so	passwd:5:-password gdm-password:3:auth gdm-password:10:-password gdm-password:20:session	Модуль автоматической разблокировки Gnome Keyring

Название библиотеки	Зависимости	Описание
	mate-screensaver:6:auth mate-screensaver:16:#auth gdm-pin:4:auth gdm-pin:21:session	
pam_group.so	-	Модуль предоставления членства в группе
pam_keyinit.so	fingerprint-auth:16:session system-auth-ac:22:session remote:14:session smartcard- gdm-smartcard:14:session system-auth:22:session runuser-l:3:session smartcard-auth:25:session xserver:5:session password-auth-ac:22:session runuser:3:session sshd:16:session smartcard-auth-ac:16:session su-l:5:session gdm-autologin:13:session password-auth:22:session gdm-password:17:session login:15:session sudo:6:session gdm-launch-environment:7:session sudo-i:5:session gdm-pin:18:session gdm-fingerprint:14:session fingerprint-auth-ac:16:session	Модуль разграничения сессионного ключа и ключа пользователя
pam_krb5.so pam_krb5afs.so pam_krb5/ pam_krb5_cchelper	- ipa-client.rpm	Модуль аутентификации по Kerberos 5
pam_lastlog.so	postlogin:7:session postlogin:8:session postlogin-ac:7:session postlogin-ac:8:session	Модуль отображения даты последнего входа и выполнения блокировки активной учетной записи
pam_limits.so	password-auth:23:session runuser:4:session sudo-i:6:session system-auth-ac:23:session password-auth-ac:23:session fingerprint-auth-ac:17:session fingerprint-auth:17:session smartcard-auth-ac:17:session system-auth:24:session smartcard-auth:25:session	Модуль для ограничения ресурсов

Название библиотеки	Зависимости	Описание
pam_localuser.so	password-auth:5:auth password-auth:12:account system-auth-ac:5:auth system-auth-ac:12:account password-auth-ac:5:auth password-auth-ac:12:account fingerprint-auth-ac:9:account fingerprint-auth:9:account smartcard-auth-ac:9:account system-auth:5:auth system-auth:13:account smartcard-auth:14:#account	Модуль требует, чтобы пользователи были указаны в /etc/passwd
pam_loginuid.so	login:10:session remote:10:session crond:8:session gdm-autologin:9:session gdm-fingerprint:10:session gdm-password:13:session gdm-pin:14:session gdm-smartcard:10:session atd:8:session sshd:12:session	Модуль записывает пользовательский uid в атрибут процесса
pam_namespace.so	gdm-password:18:session sshd:15:session gdm-fingerprint:15:session gdm-pin:19:session login:14:session gdm-smartcard:15:session remote:13:session gdm-autologin:14:session	Модуль настройки окружения для сеанса
pam_nologin.so	gdm-password:6:account sshd:7:account gdm-fingerprint:4:account gdm-pin:7:account login:5:account gdm-smartcard:4:account remote:5:account samba:2:auth gdm-autologin:5:account ppp:3:account	Модуль запрета аутентификации пользователей без полномочий root
pam_oddjob_mkhomedir.so	password-auth:25:session system-auth-ac:25:session password-auth-ac:25:session fingerprint-auth-ac:19:session fingerprint-auth:19:session smartcard-auth-ac:19:session system-auth:26:session smartcard-auth:27:session	Модуль создания домашней директории пользователей через oddjob

Название библиотеки	Зависимости	Описание
pam_ovirt_cred.so	gdm-ovirtcred:2:auth	Модуль для получения учетных данных пользователя из службы guest agent
pam_permit.so	config-util:5:account config-util:6:session password-auth:15:account xserver:4:account diskmapper:4:account ovirt-container-list:4:account ovirt-flush-caches:4:account ovirt-hibernate:4:account ovirt-locksession:4:account ovirt-logout:4:account ovirt-shutdown:4:account gdm-autologin:3:auth gdm-launch-environment:3:auth vlock:3:account setup:4:account setup:5:session system-auth-ac:15:account password-auth-ac:15:account fingerprint-auth-ac:12:account fingerprint-auth:12:account smartcard-auth-ac:12:account system-auth:16:account smartcard-auth:17:account	Разрешающий модуль
pam_pkcs11.so	smartcard-auth-ac:5:auth smartcard-auth-ac:14:password smartcard-auth:5:auth smartcard-auth:19:#password	Модуль аутентификации для PKCS11 библиотек персональных идентификаторов
pam_postgresok.so	-	Проверка реального UID и соответствующего имени учетной записи
pam_pwquality.so	password-auth:17:password system-auth-ac:17:password password-auth-ac:17:password system-auth:18:password	Модуль проверки качества пароля
pam_rootok.so	config-util:2:#auth chfn:2:auth chsh:2:auth runuser:2:auth su:2:auth xserver:2:auth setup:2:auth	Модуль аутентифицирующий пользователя, только если UID равен 0
pam_securetty.so	login:2:auth remote:2:auth	Модуль ограничивающий вход для root на специальные устройства
pam_selinux.so	login:8:# login:9:session	Модуль установки контекста безопасности по умолчанию

Название библиотеки	Зависимости	Описание
	login:12:# login:13:session remote:8:# remote:9:session remote:11:# remote:12:session gdm-autologin:8:session gdm-autologin:12:session gdm-fingerprint:9:session gdm-fingerprint:13:session gdm-password:12:session gdm-password:16:session gdm-pin:13:session gdm-pin:17:session gdm-smartcard:9:session gdm-smartcard:13:session gdm-ovirtcred:6:session gdm-ovirtcred:7:session sshd:10:# sshd:11:session sshd:13:# sshd:14:session	
pam_sepermit.so pam_selinux_permit.so	sshd:2:auth gdm-password:1:auth gdm-pin:1:auth	Модуль разрешения/запрета входа в систему в зависимости от состояния SELinux окружения
pam_sss.so	password-auth:8:auth password-auth:14:account password-auth:19:password password-auth:28:session system-auth-ac:8:auth system-auth-ac:14:account system-auth-ac:19:password system-auth-ac:28:session password-auth-ac:8:auth password-auth-ac:14:account password-auth-ac:19:password password-auth-ac:28:session fingerprint-auth-ac:11:account fingerprint-auth-ac:22:session fingerprint-auth:11:account fingerprint-auth:22:session smartcard-auth-ac:11:account smartcard-auth-ac:22:session system-auth:8:auth system-auth:15:account system-auth:20:password system-auth:29:session smartcard-auth:7:auth smartcard-auth:16:account	Модуль для взаимодействия с демоном SSSD

Название библиотеки	Зависимости	Описание
	smartcard-auth:20:password smartcard-auth:30:session	
pam_succeed_if.so	password-auth:7:auth password-auth:13:account password-auth:26:session su:9:account diskmapper:2:auth ovirt-container-list:2:auth ovirt-flush-caches:2:auth ovirt-hibernate:2:auth ovirt-locksession:2:auth ovirt-logout:2:auth ovirt-shutdown:2:auth system-auth-ac:7:auth system-auth-ac:13:account system-auth-ac:26:session postlogin-ac:6:session postlogin:6:session password-auth-ac:7:auth password-auth-ac:13:account password-auth-ac:26:session fingerprint-auth-ac:10:account fingerprint-auth-ac:20:session fingerprint-auth:10:account fingerprint-auth:20:session smartcard-auth-ac:10:account smartcard-auth-ac:20:session system-auth:7:auth system-auth:14:account system-auth:27:session smartcard-auth:15:#account smartcard-auth:28:session	Модуль аутентификации на основе характеристик учётной записи пользователя
pam_systemd.so	password-auth:24:-session runuser-l:4:-session system-auth-ac:24:-session password-auth-ac:24:-session fingerprint-auth-ac:18:-session fingerprint-auth:18:-session smartcard-auth-ac:18:-session system-auth:25:-session smartcard-auth:26:-session	Модуль, регистрирующий пользовательскую сессию в диспетчере входа systemd
pam_sz_card_auth.so	smartcard-auth:6:auth smartcard-auth:21:password	Модуль аутентификации по персональному идентификатору
pam_sz_ldap_info.so	smartcard-auth:8:auth	Модуль аутентификации в LDAP
pam_sz_secr_serv.so	smartcard-auth:9:auth	Модуль аутентификации по случайной последовательности
pam_tally2.so	system-auth:10:auth	Модуль подсчёта количества входов пользователя

Название библиотеки	Зависимости	Описание
pam_time.so	config-util:3:#auth config-util:8:session smartcard-auth:13:account	Модуль аутентификации по времени
pam_timestamp.so	config-util:3:#auth config-util:8:session	Модуль аутентификации на основе успешных кэшированных попыток аутентификации
pam_unix.so pam_unix_acct.so pam_unix_auth.so pam_unix_passwd.so pam_unix_session.so	password-auth:6:auth password-auth:11:account password-auth:18:password password-auth:27:session runuser:5:session system-auth-ac:6:auth system-auth-ac:11:account system-auth-ac:18:password system-auth-ac:27:session password-auth-ac:6:auth password-auth-ac:11:account password-auth-ac:18:password password-auth-ac:27:session fingerprint-auth-ac:8:account fingerprint-auth-ac:21:session fingerprint-auth:8:account fingerprint-auth:21:session smartcard-auth-ac:8:account smartcard-auth-ac:21:session system-auth:6:auth system-auth:12:account system-auth:19:password system-auth:28:session smartcard-auth:12:#account smartcard-auth:29:session	Модуль аутентификации по паролю
pam_wheel.so	sudo:2:#auth sudo:3:auth su:4:#auth su:6:auth	Модуль, разрешающий доступ от root только пользователям из группы wheel
pam_xauth.so	config-util:7:session su:14:session	Модуль пересылки ключей xauth между пользователями
pam_mail.so		Проверка наличия непрочитанных сообщений при аутентификации пользователя

2.2.16. Модуль Rsyslog

Rsyslog – модуль КП «ЗОС «СинтезМ», отвечающий за:

- приём и обработку информационных и отладочных системных сообщений;
- формирование на их основе сообщений аудита;

– хранение и передачу сообщений аудита.

Данный модуль позволяет разделить приложения на:

– приложения, генерирующие системные сообщения;

– приложения, формирующие сообщения аудита;

– приложения, хранящие сообщения аудита;

– приложения, анализирующие сообщения аудита.

Взаимодействие модуля rsyslog с модулями системы представлено на рисунке 2.5.

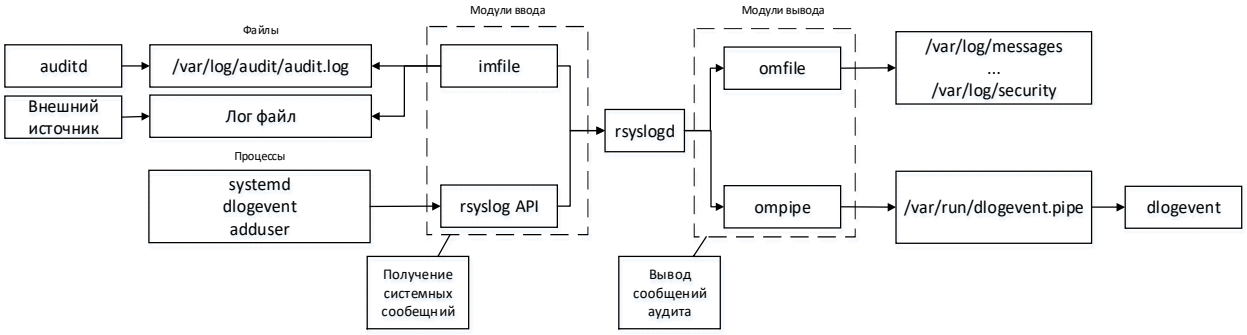


Рисунок 2.5 - Взаимодействие модулей системы с модулем rsyslog

Сообщение аудита представляет собой системное сообщение, расширенное дополнительными атрибутами модулем rsyslog. Перечень атрибутов сообщения аудита представлено в таблице 2.4.

Таблица 2.4 - Атрибуты сообщения аудита

Название	Описание
msg	Системное сообщение
rawmsg	Системное сообщение, полученное с сокета. Используется для отладки.
rawmsg-after-pri	Аналогична rawmsg, но без syslog PRI. Если PRI нет, rawmsgafter-pri идентичен rawmsg. Syslog PRI - поле заголовка, содержащее метку важности и метку объекта syslog. Он заключен в символы большего и меньшего размера(<191>). Данное поле необходимо для правильной классификации сообщения модулем rsyslog и его компонентами.
hostname	Имя хоста
source	Псевдоним для hostname
fromhost	Имя хоста системы, от которого было получено сообщение.
fromhost-ip	IP адрес хоста системы, от которого было получено сообщение.

syslogtag	Тэг
programname	Имя программы, сгенерировавшей системное сообщение
pri	Не кодированная PRI часть сообщения. Syslog PRI - поле заголовка, содержащее метку важности и метку объекта syslog. Он заключен в символы большего и меньшего размера(пример: <191>). Данное поле необходимо для правильной классификации сообщения модулем rsyslog и его компонентами.
pri-text	Декодированная PRI часть сообщения. (пример: local0.err)
syslogfacility	Метка объекта в цифровой форме
syslogfacility-text	Метка объекта в текстовой форме
syslogseverity	Метка важности в цифровой форме
syslogseverity-text	Метка важности в тестовой форме
syslogpriority	Аналогична syslogseverity
syslogpriority-text	Аналогична syslogseverity-text
timegenerated	Метка времени получения сообщения
timereported	Метка времени из сообщения.
timestamp	Аналогична timereported
inputname	Имя модуля ввода, сгенерировавшего сообщение (например, «imuxsock», «imudp»).

Типы меток важности модуля rsyslog представлены в таблице 2.5.

Таблица 2.5 - Типы меток важности модуля rsyslog

Цифровой формат	Текстовый формат	Описание
0	emerg	Сообщение о нестабильной системе
1	alert	Сообщение о необходимости немедленное действие
2	crit	Сообщение о критическом условии
3	error	Сообщение ошибки
4	warning	Сообщение предупреждения
5	notice	Информационное сообщение, но с значительным условием
6	info	Информационное сообщение
7	debug	Сообщение отладки

Типы меток объекта модуля rsyslog представлены в таблице 2.3.

Таблица 2.6 - Типы меток объекта модуля rsyslog

Цифровой формат	Текстовый формат	Описание
0	kern	Сообщения ядра
1	user	Сообщения пространства пользователя
2	mail	Сообщение почтовой службы
3	daemon	Сообщение системных демонов
4	auth	Сообщения защиты/аутентификации
5	syslog	Сообщения, генерируемые демоном syslogd
6	lpr	Сообщения системы печати

7	news	Сообщения интернет-новостной системы
8	uucp	Сообщения системы UUCP (передачи файлов между хостами)
9	cron	Сообщения демона периодического выполнения заданий
10	security	Сообщения защиты/аутентификации
11	ftp	Сообщения демона FTP
12	ntp	Сообщения NTP
13	logaudit	Сообщения аудита
14	logalert	Сообщения оповещения
15	clock	Сообщения демона времени
16	local0	Локальные сообщения тип 0
17	local1	Локальные сообщения тип 1
18	local2	Локальные сообщения тип 2
19	local3	Локальные сообщения тип 3
20	local4	Локальные сообщения тип 4
21	local5	Локальные сообщения тип 5
22	local6	Локальные сообщения тип 6
23	local7	Локальные сообщения тип 7

Хранение сообщений аудита осуществляется с помощью текстовых файлов – лог файлов. Лог файлы – файлы, содержащие сообщения аудита системы. Для каждого типа информации создаётся отдельный файл. В лог файл /var/log/messages, сохраняются сообщения аудита по умолчанию. В лог файл /var/log/security сохраняются сообщения аудита о безопасности системы и аутентификации. В лог файл /var/log/cron сохраняются сообщения аудита модуля cron – демона периодического выполнения заданий.

Список лог файлов, поддерживаемых rsyslogd, определён в файле конфигурации /etc/rsyslog.conf. Все лог файлы хранятся в директории /var/log/. Так же в каталоге /var/log/ находятся лог файлы других служб и архивы лог файлов (в названии файла присутствует метка времени, например, messages-20180408), созданные модулем logrotate.

Модуль rsyslog, помимо вывода сообщений аудита в файлы сообщении аудита, расположенные в /var/log/, основываясь на конфигурационном файле, описанном выше, так же выводит сообщения аудита в файл /var/run/dlogevent.pipe. Данный файл является однонаправленным именованным каналом меж процессного взаимодействия – pipe файл.

Принцип именованного канала заключается в том, что один процесс записывает данные в именованный канал, а второй процесс считывает данные. Процесс записи и считывания данных для процессов осуществляются стандартными методами чтения и записи данных из файла. При считывании данных, данные автоматически удаляются. Если считывающего процесса нет, данные хранятся в именованном канале и ожидают считывания.

2.2.17. Модуль Rsyslog-RELP

Rsyslog-RELP – модуль rsyslog, предоставляющий возможность получения (imrelp) и отправки (omrelp) сообщений аудита через протокол RELP. Модуль основан на библиотеке librelp.

Протокол RELP (Reliable Event Logging Protocol) - сетевой протокол для передачи сообщений аудита с обеспечением гарантированной доставки. Протокол использует клиент-серверную модель, где источник соединения называется клиентом, а слушающая часть - сервером. Для передачи сообщений аудита протокол использует TCP, что обеспечивает защиту от потери пакетов, но не гарантирует доставку. Для обеспечения гарантированной доставки используется обратный каналом, передающим информацию клиенту о сообщениях, полученных сервером. Обратный канал позволяет определить, какие сообщения были доставлены, даже в случае прерывания соединения.

RELP использует модель запрос-ответ. Клиент отправляет запросы серверу, на которые сервер отправляет клиенту ответ. Для обеспечения полнодуплексной связи, в определённый момент времени могут отправляться несколько запросов и несколько ответов. Сервер отвечает на запросы в любом порядке. Для экономии ресурсов количество запросов ограничено. Каждому запросу присваивается (относительный) уникальный, автоматически инкрементируемый идентификатор («номер транзакции», TXNR). Ответ имеет тот же идентификатор, что и исходящий запрос. Запрос и ответ называются транзакцией RELP. Как клиент, так и сервер могут завершить соединение TCP в любое время. В этом случае любые незавершённые запросы считаются невыполненными.

В случае ошибок соединения, узел (сервер или клиент), обнаруживший проблему, закрывает TCP соединение без ожидания ответа на подтверждения закрытия.

Отправка сообщения аудита является так же запросом RELP. Ответом на данный запрос является подтверждение получения сообщения.

2.2.18. Модуль Logrotate

Модуль logrotate предназначен для администрирования систем, позволяющий настроить автоматическую ротацию, сжатие, удаление, и пересылку журналов. Каждый файл журнала может обрабатываться ежедневно, еженедельно, ежемесячно или когда он становится слишком большим.

Модуль logrotate запускается ежедневно службой cron файлом /etc/cron.daily/logrotate. Модуль будет изменять журнал чаще раза в день, если критерий для этого журнала основывается на размере журнала и logrotate запускается чаще раза в день, или если используется опция -f или --force. Принцип работы модуля logrotate отображен на рисунке 2.6.

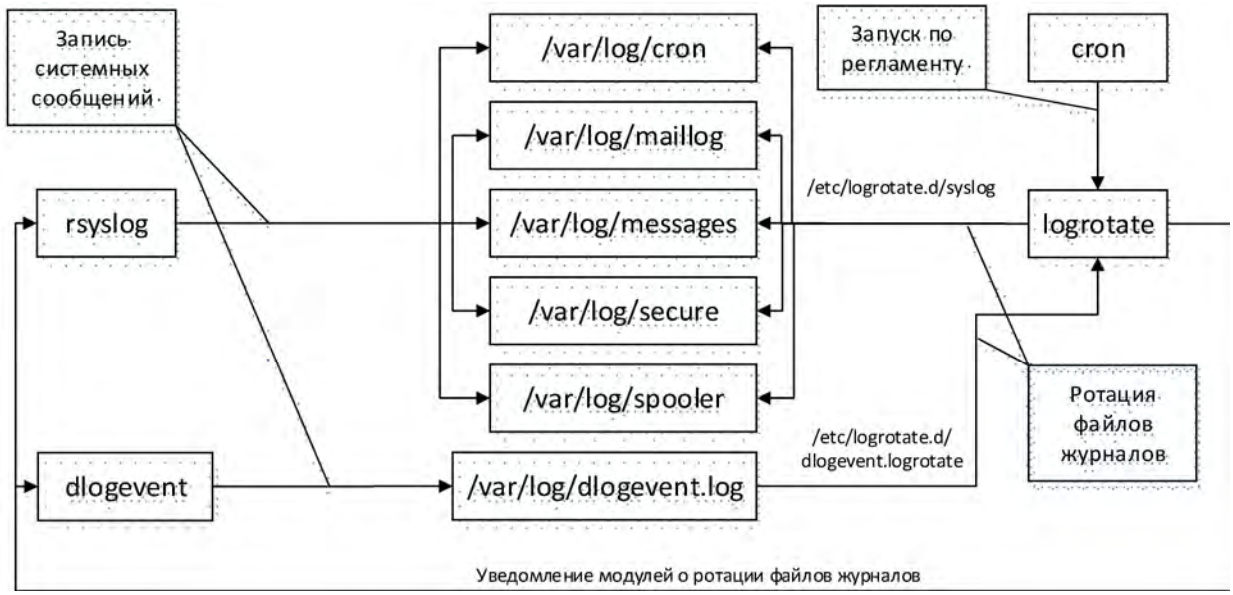


Рисунок 2.6 - Принцип работы модуля logrotate

При запуске модуля logrotate в командной строке может быть указано любое количество файлов конфигурации. Более поздний конфигурационный файл может отменять опции заданные более ранним. Поэтому порядок перечисления

конфигурационных файлов logrotate важен. По умолчанию используется один файл конфигурации, который включает в себя любые другие файлы конфигурации, которые необходимы, директивой include. Если в командной строке указан каталог, каждый файл в этом каталоге используется как конфигурационный файл.

Если в командной строке не указаны аргументы, logrotate напечатает версию и короткую справку по использованию. Если при ротации файлов журнала происходит ошибка, logrotate завершит работу с ненулевым статусом.

По умолчанию используется конфигурационный файл /etc/logrotate.conf и файл состояния /var/lib/logrotate.status. Файл состояния содержит перечень, состоящий из имени файла журнала и даты его последней ротации. Пример файла состояния:

```
logrotate state -- version 2
"/var/log/nginx/error.log" 2018-5-10-3:21:1
"/var/log/yum.log" 2018-3-16-3:0:0
"/var/log/maillog" 2018-5-6-3:48:1
"/var/log/secure" 2018-5-6-3:48:1
"/var/log/messages" 2018-5-6-3:48:1
"/var/account/pacct" 2018-3-16-3:0:0
"/var/log/cron" 2018-5-6-3:48:1
```

2.2.19. Модуль Keepalived

Доступность сервисов и информации при выходе из строя одного из технических средств (отказоустойчивый кластер) в конфигурации ОС достигается за счет применения модуля keepalived.

Keepalived - это программное обеспечение маршрутизации для балансировки нагрузки и высокой доступности.

В процессе функционирования «активный» (главный, «master») сервер информирует резервные («slave») сервера о своем состоянии с использованием протокола резервирования виртуального маршрутизатора (VRRP), который требует, чтобы главный сервер отправлял сообщения о статусе через регулярные промежутки времени. Если активный сервер перестает отправлять сообщения, в соответствии с конфигурацией, выбирается новый мастер, и он начинает принимать все новые соединения. Для реализации отказоустойчивости используется виртуальный IP-адрес

(Virtual IP address, VIP) который присваивается интерфейсу «активного» сервера, обеспечивая принятие соединений от клиентов.

Keepalived запускается в режиме демона на каждом сервере из состава кластера. Сервер с установленным и настроенным Keepalived называются узлы Keepalived. Сервер, которому в соответствии с конфигурационным файлом назначен наивысший приоритет, называется главным. После настройки и запуска различные узлы Keepalived постоянно передают свой статус в сеть и прослушивают друг друга. Если резервный узел не получает сообщение о статусе от мастера (узла с более высоким приоритетом, чем он сам), то будет выбран новый мастер. После того как выбран, новый мастер присваивает себе виртуальный IP-адрес и отправляет Address Resolution Protocol (ARP) сообщение. Любые соединения со старым главным узлом будут закрыты. Если предыдущий мастер узел восстановит свою работоспособность, то в зависимости от настроек, он может стать резервным либо заново стать мастером.

2.2.20. Модуль rsync

Программа rsync предназначена для синхронизации информации в виде файлов и каталогов файлов между двумя серверами с минимизированием трафика, используя кодировку данных при необходимости. Зеркалирование данных осуществляется одним потоком в каждом направлении (а не по одному или несколько потоков на каждый файл). rsync может копировать или отображать содержимое каталога и копировать файлы, опционально используя сжатие и рекурсию.

При передаче файлов на другой сервер через rsync пользователь должен аутентифицироваться с помощью учетных данных. Передача данных (по умолчанию) осуществляется по протоколу ssh (транспортный протокол).

Программа rsync относится к модулям КП «ЗОС «СинтезМ» обеспечивающим выполнение требований, позволяющих организовать доступ к информации при выходе из строя одного из технических средств (отказоустойчивый кластер). При этом информация синхронизируется между техническими средствами (серверами) кластера.

Rsync - консольная системная утилита, которая позволяет выполнять синхронизацию файлов и каталогов в двух местах с минимизированием трафика, используя кодировку данных при необходимости.

При копировании локальных файлов с помощью rsync на удаленный хост, используется программа удаленной оболочки в качестве транспорта (по умолчанию ssh).

2.2.21. Модуль inotify

Inotify - это модуль ядра КП «ЗОС «СинтезМ», который позволяет получать уведомления о событиях, связанных с файлами и каталогами файловой системы. Например, открытие файлов и каталогов для чтения или записи, изменения атрибутов, перемещение, удаление и т.п. С помощью подписки на события Inotify программным модулям необязательно периодически сканировать файловую систему для обнаружения изменений.

В уведомлениях о событиях inotify содержится маска типа события, которая является логическим 'ИЛИ' от следующих констант:

IN_ACCESS - К файлу было произведено обращение (чтение).

IN_ATTRIB - Были изменены метаданные (права доступа, временные метки, расширенные атрибуты и т.п.).

IN_CLOSE_WRITE - Файл, открывавшийся для записи, был закрыт.

IN_CLOSE_NOWRITE - Файл, открывавшийся не для записи, был закрыт.

IN_CREATE - Файл/каталог был создан в наблюдаемом каталоге.

IN_DELETE - Файл/каталог был удален в наблюдаемом каталоге.

IN_DELETE_SELF - Наблюдаемый файл/каталог был удален.

IN_MODIFY - Файл был изменён.

IN_MOVE_SELF - Наблюдаемый файл/каталог был перемещён.

IN_MOVED_FROM - Файл/каталог был перемещён из наблюдаемого каталога.

IN_MOVED_TO - Файл/каталог был перемещён в наблюдаемый каталог.

IN_OPEN - Файл/каталог был открыт.

2.2.22. KVM

ОО обеспечивает среду виртуализации на основе технологии KVM. КП «ЗОС «СинтезМ» реализует среду для функционирования виртуальных машин, а так же обеспечивает управление виртуальными машинами. Кроме того, КП «ЗОС «СинтезМ» предоставляет графический интерфейс управления (средство управления средой виртуализацией) для администрирования виртуальных машин, а также аудита операций пользователей и администраторов.

Когда ОО используется как хост-система для виртуализации KVM, в дополнение к привилегированному (режим ядра/kernel) и не привилегированному (прикладной/пользовательский/user) режиму добавляется третий привилегированный режим: гостевой режим (guest mode). Гостевой режим основан на использовании аппаратной поддержки предоставляемой процессором.

В гостевом режиме доступны регистры процессора, которые недоступны через два других режима. Используя эти регистры, реализуется другой уровень преобразования адресов памяти. Ядро КП «ЗОС «СинтезМ» использует этот режим при активации виртуализации KVM. В этом случае все ядро КП «ЗОС «СинтезМ» работает в режиме гипервизора.

Технология KVM отделяет среду выполнения виртуальных машин друг от друга. Ядро КП «ЗОС «СинтезМ» работает как гипервизор для виртуальных машин, а также обеспечивает вычислительную среду для системного администрата. Ядро поддерживает одновременное выполнение виртуальных машин и обычных приложений. КП «ЗОС «СинтезМ» использует поддержку аппаратной виртуализации процессоров, чтобы гарантировать, что виртуальные машины выполняются в среде виртуализации без значительной потери производительности по сравнению с выполнением на аппаратной платформе.

KVM реализован как часть ядра КП «ЗОС «СинтезМ», взаимодействующий с кодом из пользовательского пространства. Он состоит из двух основных компонентов, реализующих функциональность диспетчера виртуальных машин (гипервизора): модуль ядра KVM (драйвер KVM) и QEMU для аппаратной эмуляции.

Использование QEMU подразумевает, что KVM обеспечивает полную виртуализацию для гостевой машины и, поэтому, может выполнять гостевые операционные системы.

Модуль ядра KVM реализует функциональные возможности управления памятью и виртуальной машиной. Это расширение ядра делает ядро КП «ЗОС «СинтезМ» гипервизором. Виртуальные машины обрабатываются ядром КП «ЗОС «СинтезМ» как обычные приложения. Ядро планирует выполнение процессов виртуальных машин так же как и для обычных приложений. Процессы виртуальных машин можно обрабатывать, так же как и обычные приложения. Таким образом, процесс, реализующий виртуальную машину, можно увидеть в списках процессов, и ему могут быть отправлены регулярные сигналы, такие как SIGTERM.

На рисунке 2.7 показано, что с точки зрения ядра виртуальная машина - это еще один процесс. Однако процесс виртуальной машины имеет специальный уровень. Как показано на рисунке, процесс виртуальной машины визуально разделен на две части. Первая часть содержит обычную логику приложения, выполняемую в пользовательском пространстве (белая часть на рисунке), которая применяется для поддержки виртуализации ввода-вывода QEMU и некоторого другого небольшого программного обеспечения, связанного с KVM. Вторая часть содержит образ гостевого кода, обычно это операционная система (серая часть), которая выполняется в гостевом пространстве. Вся память, используемая для гостевой операционной системы, выделяется приложением QEMU. Ядро отслеживает, какие части приложения принадлежат гостевой операционной системе, а какие - к обычным приложениям.

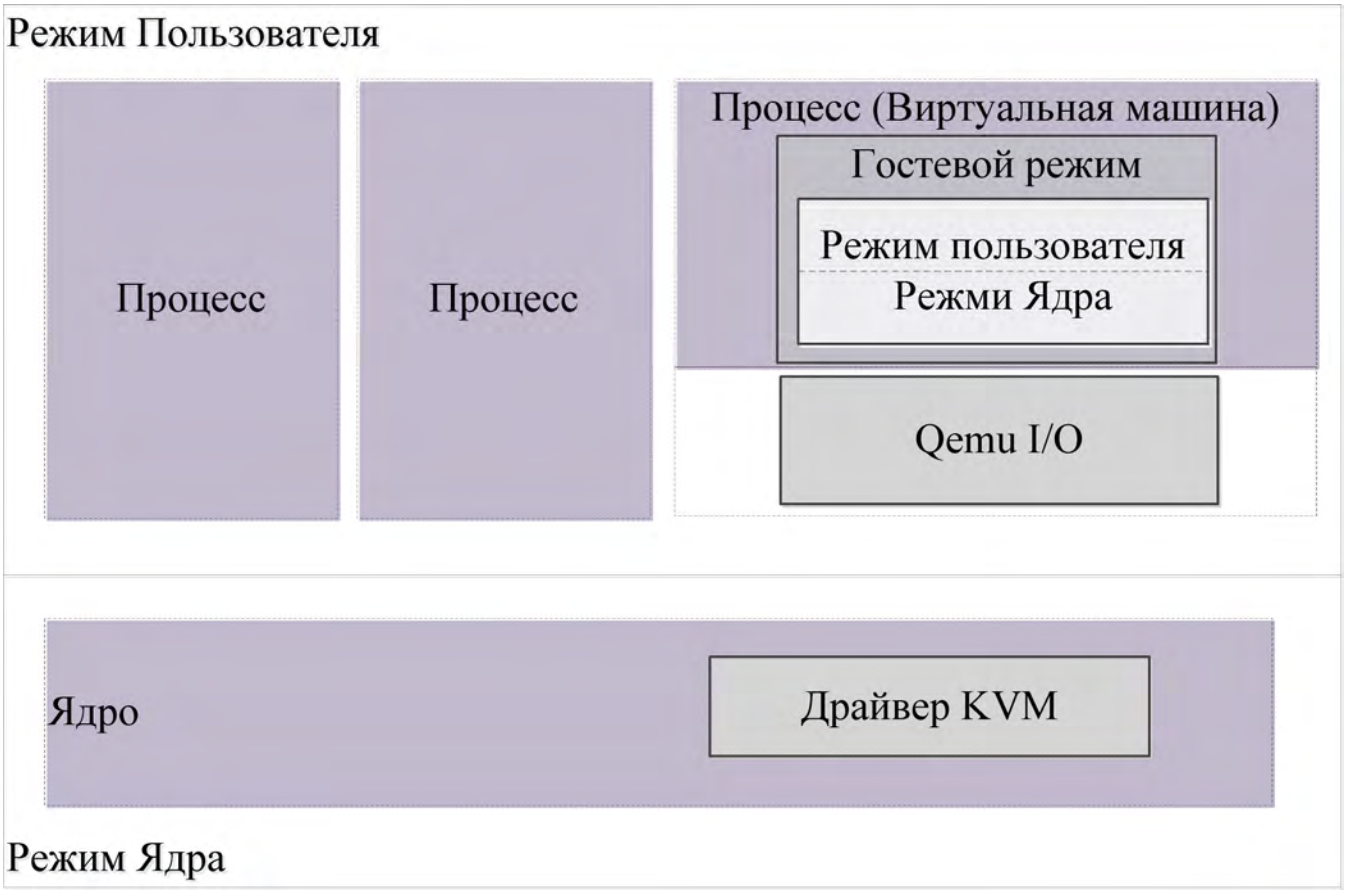


Рисунок 2.7 - Виртуализация

Демон управления libvirt устанавливает виртуальные машины и контролирует ресурсы, назначенные виртуальным машинам. Для поддержки изоляции виртуальных машин libvirt использует следующие механизмы:

- каждый процесс виртуальной машины запускается с нормальным, непривилегированным идентификатором пользователя «qemu» и идентификатором группы «qemu». Это означает, что эти процессы не обладают привилегией root.
- в процессе запуска виртуальной машины Libvirt для каждой виртуальной машины и ее ресурсов генерирует и назначает уникальные метки.
- каждый процесс виртуальной машины будет помещен в выделенную группу. Cgroup - это механизм ядра КП «ЗОС «СинтезМ» для обозначения процессов и назначения определенных свойств этим процессам - каждый процесс, порожденный уже отмеченным процессом, снова будет иметь тот же идентификатор.

При изоляция виртуальных машин в КП «ЗОС «СинтезМ» применяются механизмы изоляция процессов и защиты памяти описанные в пунктах 6 и 7 настоящего документа.

Управление процессами виртуальных машин осуществляется через демон libvirtd. Этот демон ограничен для пользователей, принадлежащих к группе libvirt. Все аспекты управления виртуальными машинами, включая создание виртуальных машин, назначение ресурсов, запуск, остановку и уничтожение виртуальных машин, осуществляется через libvirtd.

Управление средой виртуализации в КП «ЗОС «СинтезМ» осуществляется через средство управления средой виртуализацией (Менеджер ВМ) которое предоставляет системному администратору графический веб-интерфейс и обеспечивает взаимодействие с серверами виртуализации (демоном VDSM).

Серверная часть системы виртуализации состоит из следующих компонентов:

1. средство управления средой виртуализации;
2. VDSM – набор демонов для управления виртуализацией со стороны менеджера
1. libvirt – демон, предоставляет API для получения информации о работающих на гипервизоре виртуальных машинах, и действий над ними;
2. kvm – набор подключаемых модулей ядра, который предоставляет возможности виртуализации с использованием технологий intel-vt. Модуль KVM работает в пространстве ядра, гостевые ОС работают как отдельные процессы в пользовательском пространстве, KVM предоставляет возможность виртуальным машинам использовать физические устройства гипервизора;
3. qemu – эмулятор физических устройств, используется для эмуляции физических устройств для гостевых ОС.

2.2.23. Средство управления средой виртуализации (oVirt)

В состав КП «ЗОС «СинтезМ» входит средство управления средой виртуализации (далее - менеджер ВМ, oVirt, ovirt-engine) предоставляющее системному администратору веб-интерфейс:

- управления серверами виртуализации (гипервизорами KVM);
- управления жизненным циклом виртуальными машин (ВМ);
- управления виртуальными сетями;
- управления хранилищами;
- мониторинга состояния серверов виртуализации, хранилищ, виртуальных машин.

Интерфейс средства управления средой виртуализации состоит из:

- портал администрирования;
- портал управления ВМ.

Портал управления виртуальными машинами предназначен для управления состоянием виртуальных машин: запуск, остановка, перезагрузка, приостановка. Доступ к функциям управления ВМ возможен только аутентифицированным пользователям и только в соответствии с перечнем ВМ назначенных этим пользователям.

Портал администрирования предназначен для предоставления системному администратору графического интерфейса к функциям управления средой виртуализации, а также назначения правил разграничения доступа к этим функциям на основе ролей. Доступ к функциям портала администрирования возможен только аутентифицированным пользователям. Права пользователей на выполнение функции определяются в процессе аутентификации пользователя в соответствии с ролью, пользователя в средстве управления средой виртуализации, назначенной системным администратором.

oVirt позволяет управлять виртуальными машинами через веб-интерфейс, используя для администрирования библиотеку libvirt. oVirt позволяет работать как с образами расположенными на жестком диске машины хоста, так и с образами хранящимися на сетевом хранилище и доступными через интерфейсы NFS или iSCSI. Выполнение виртуальных машин может происходить на бездисковых серверах, ОС для которых (ovirt-node) загружается с управляющего узла. Управляющий узел с

ovirt-server предоставляет веб-интерфейс и управляет процессом расстановки виртуальных машин с указанными образами по доступным узлам. Возможно совмещение всех функций на единственном сервере.

2.2.24. Модуль VDSM

В КП «ЗОС «СинтезМ» используются следующие системные сервисы vdsm:

- демон mom-vdsm.service;
- демон supervdsmd.service;
- демон vdsmd.service;
- vdsm-network-init.service;
- vdsm-network.service.

Демон mom-vdsm.service используется для управления загруженностью гипервизоров. Собирает данные о активных виртуальных машинах на хосте с использованием VDSM api и libvirt, сверяет с политиками перегрузки. Используется для контроля и поддержки механизма распределения оперативной памяти гипервизора между виртуальными машинами. Демон стартует при загрузке гипервизора, инициатором запуска выступает systemd (см. пункте 2.2.4). Запуск осуществляется следующей командой:

```
/usr/sbin/momd -c /etc/vdsm/mom.conf
```

Демон supervdsmd используется для выполнения операции требующих прав суперпользователя, слушает сокет созданный vdsmd. Демон стартует при загрузке гипервизора, инициатором запуска выступает systemd. Запуск осуществляется следующей командой:

```
/usr/share/vdsm/daemonAdapter "/usr/share/vdsm/supervdsmServer" --sockfile "/var/run/vdsm/svdsm.sock".
```

Демон vdsmd обеспечивает взаимодействие с менеджером ВМ для управления гипервизорами и виртуальными машинами (Рисунок 2.8). VDSM получает данные о состоянии гипервизора и виртуальных машин; управляет: памятью гипервизора, сетевыми интерфейсами, хранилищем виртуальных машин, производит логирование и сбор статистики. vdsmd основной скрипт управляющий гипервизором. VDSMD

принимает xmlrpc и jsonrpc запросы через порты 54321/54322 для безопасного обмена данными используется протокол SSLv23. Демон стартует при загрузке гипервизора, инициатором запуска выступает systemd. Запуск осуществляется следующей командой:

```
/usr/share/vdsm/daemonAdapter -0 /dev/null -1 /dev/null -2 /dev/null
"/usr/share/vdsm/vdsm"
```

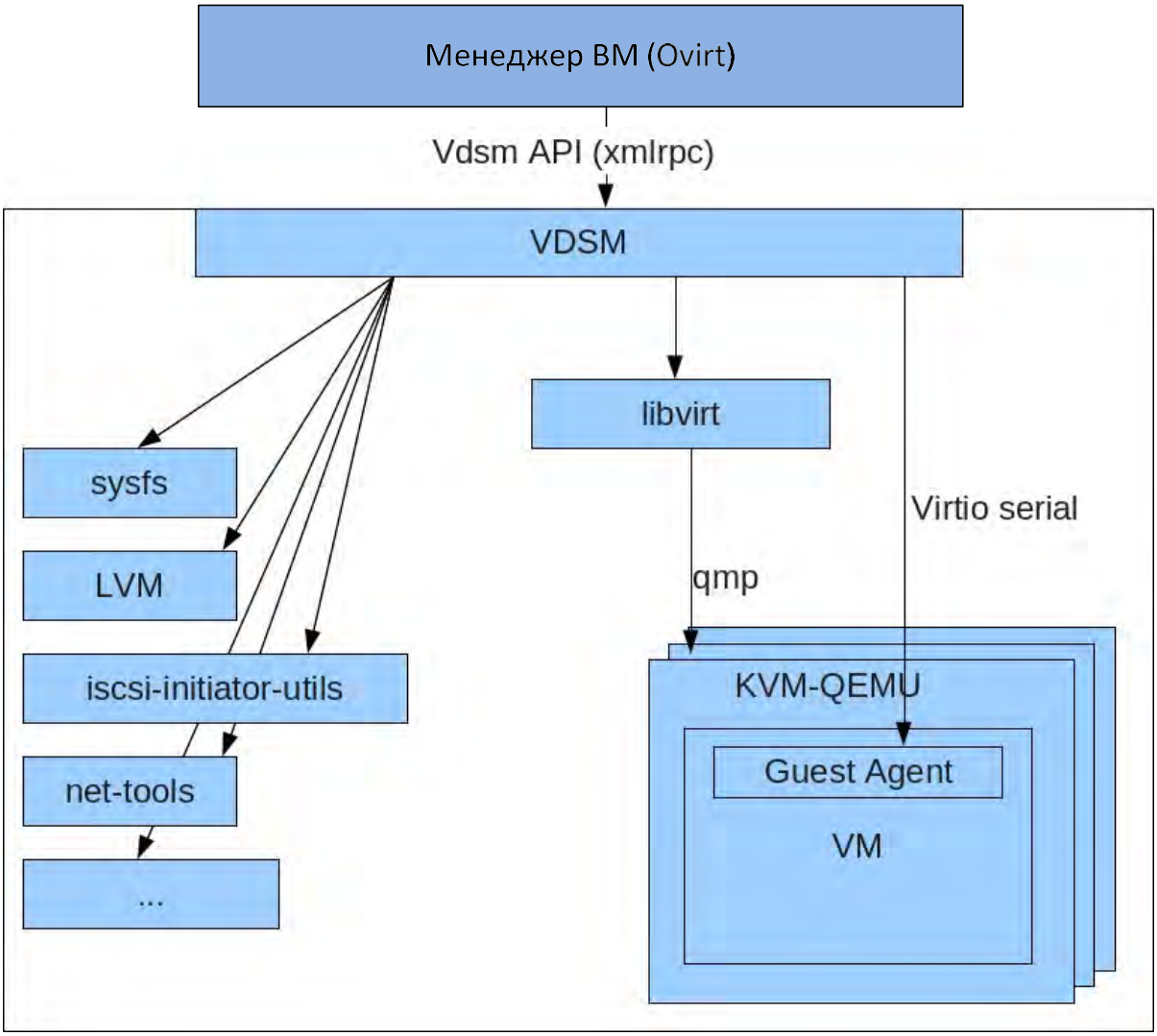


Рисунок 2.8 - VDSM

Сервис vdsm-network-init применяется для восстановления сетевой конфигурации OVS (Open Virtual Switch) при старте гипервизора. Сервис стартует при загрузке гипервизора, инициатором запуска выступает systemd. Восстановление сетевой конфигурации осуществляется следующей командой:

```
/usr/bin/vdsm-tool restore-nets-init
```

Сервис vdsm-network.service применяется для восстановления сетевых настроек гипервизора, при старте гипервизора, к последнему состоянию установленному сервисом vdsm. Сервис стартует при загрузке гипервизора, инициатором запуска выступает systemd. Восстановление сетевой конфигурации осуществляется следующей командой:

```
/usr/bin/vdsm-tool restore-nets
```

2.2.25. Модуль Libvirt

Библиотека libvirt – совокупность открытого API, демона и набора инструментов для управления виртуализацией. Позволяет управлять гипервизорами KVM и QEMU, входящими в состав КП «ЗОС «СинтезМ», предоставляет возможность контролировать виртуальные машины по сети, расположенные на других компьютерах. Libvirt предоставляет обобщенное API для управления гостевыми ОС, запущенными на хосте. На рисунках 2.9, 2.10 представлена общая архитектура КП «ЗОС «СинтезМ» и место libvirt в ней.

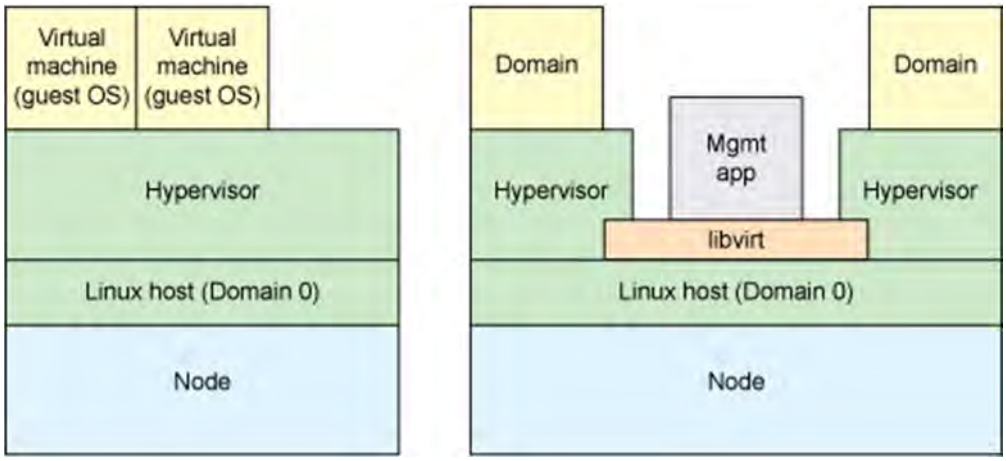


Рисунок 2.9 - libvirt

В терминологии libvirt физический хост называется «узлом» (node), гостевая ОС называется «доменом» (domain). При этом считается, что libvirt и ее приложения работают в домене на хосте в КП «ЗОС «СинтезМ» – domain 0.

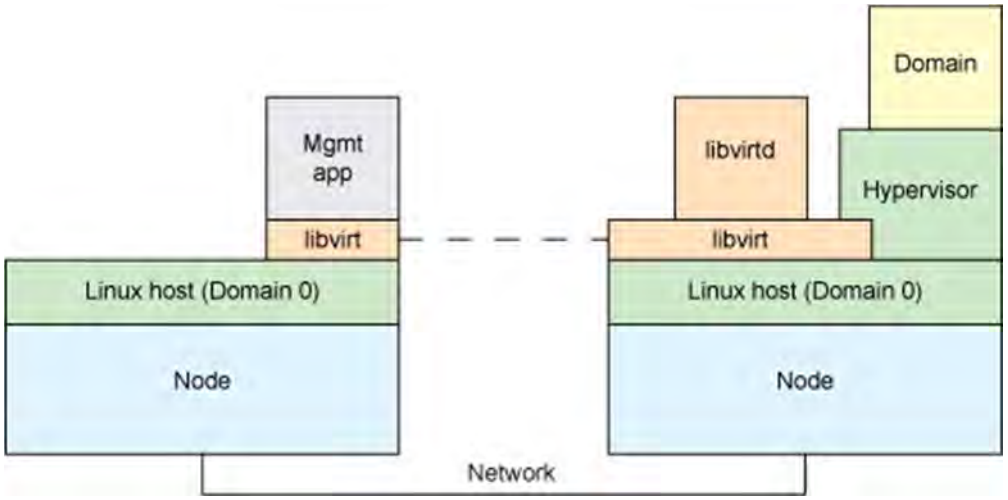


Рисунок 2.10 - Взаимодействие libvirt

Libvirt интегрируется с гипервизорами различных типов при помощи driver-based архитектуры, которая позволяет реализовать API для управления всеми типами гипервизоров в КП «ЗОС «СинтезМ» (QEMU, KVM).

Задачи, выполняемые libvirt:

- создание домена;
- изменение домена;
- запуск домена;
- остановка или перезагрузка домена;
- приостановка домена;
- создание снимки домена;
- получение списка снимков домена;
- восстановление состояния домена из снимка;
- удаление снимка.

Демон Libvirtd – серверный компонент системы виртуализации. Демон стартует при загрузке гипервизора, инициатором запуска выступает systemd. Запуск осуществляется следующей командой:

```
/usr/sbin/libvirtd --listen
```

Демон запускается на всех гипервизорах и выполняет задачи, поступающие от vdsm, такие как запуск, остановка, миграция ВМ, управление сетью и хранилищем гостевых ВМ.

Для управления виртуализации демон Vdsm подключается к демону libvirt чтобы передать задачи и собрать информацию о ресурсах гипервизора и данные о гостевых ВМ. Демон libvirt прослушивает порт 16514, к которому подключается vdsmd.

Перезапуск демона libvirtd не влияет на работающие гостевые ВМ, информация о работающих ВМ будет получена заново из xml файлов, хранящихся в /var/run/libvirt/qemu/.

Гостевые операционные системы описываются с использованием формата XML. XML использован как формат файлов для хранения всех данных в libvirt, включая домены, сетевые настройки, данных о СХД. XML позволяет провести лёгкую интеграцию с другими технологиями и средствами управления.

Libvirt различает два типа доменов временные и постоянные:

- данные о временном домене хранятся на гипервизоре до тех пор пока временный домен не будет отключен или не будет перезагружен гипервизор;
- данные о постоянных доменах не удаляются после перезагрузки гипервизора или отключение домена.

После создания домена (независимо от типа) его состояние может быть сохранено в файл. Домен можно восстановить в исходное состояние из файла.

Домен может находиться в следующих состояниях:

- неопределённо – базовое состояние. Libvirt не имеет никакой информации о домене, потому что домен не был определён или создан;
- определён или Остановлен – домен был определён, но не запущен, только постоянные домены могут находиться в этом состоянии;
- работающий – домен был создан и запущен (временный или постоянный). В этом состоянии домен работает на гипервизоре виртуализации;

– приостановлен – работа домена на гипервизоре была приостановлена, его состояние сохраняется до тех пор пока домен не будет возобновлён. Домен не получает информации о том был он приостановлен или нет;
– сохранён – аналогично состоянию “приостановлен”, но в данном случае данные домена сохраняются на хранилище ВМ.

На приведённой ниже диаграмме (Рисунок 2.11) показано как состояния доменов могут изменяться в зависимости от текущего состояния:

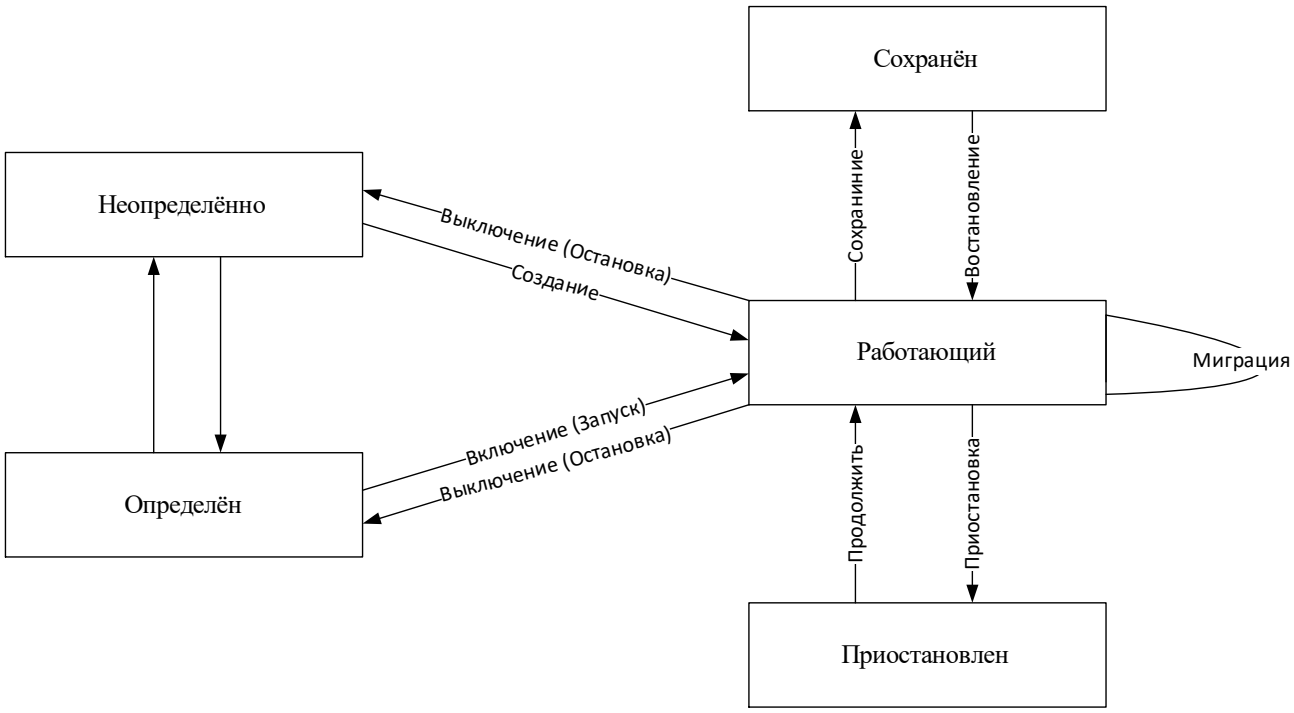


Рисунок 2.11 – Переход между состояниями Домена

2.2.26. Сервис печати CUPS

Сервис печати CUPS представляет собой сервис печати для UNIX-подобных операционных систем, который принимает задания на печать сформированные пользовательскими средствами работы с текстовыми и графическими документами, обрабатывает их и отправляет на соответствующий принтер. Сервис печати (CUPS) функционирует на TCP-порту 631 и принимает задания на печать сформированные пользовательскими средствами работы с текстовыми и графическими документами. Кроме того CUPS предоставляет веб интерфейс для управления и отображения устройств печати и управления заданиями на печать.

2.2.27. Агент безопасности

Агент безопасности представляет собой компонент КП «ЗОС «СинтезМ», предназначенный для установки на физические сервера, виртуальные машины и рабочие станции для обеспечения реализации функций безопасности и взаимодействия с Сервером безопасности для обеспечения защиты информации от НСД. Агенты безопасности разделяются на три типа: базовый, пользовательский, администратора. Тип агента безопасности устанавливаемого на то или иное вычислительное средство определяется выбранной ролью КП «ЗОС «СинтезМ». Базовый Агент безопасности включает в свой состав минимальный набор модулей необходимых для реализации функций безопасности и устанавливается по умолчанию. Пользовательский агент безопасности и агент безопасности администратора содержат дополнительные модули и устанавливаются при развертывании КП «ЗОС «СинтезМ» на узлы предназначенные для обеспечения работы пользователей и администраторов.

Агент безопасности включает в свой состав следующие компоненты:

- утилита расчета контрольных сумм;
- модуль dlogevent;
- модули аутентификации;
- модуль самотестирования;
- утилита удаления файлов Shred;
- модуль Mail Notification
- базовый набор конфигураций и модуль sz-user-policy.

2.2.27.1. Утилита расчета контрольных сумм

AIDE – утилита для расчета контрольных сумм объектов файловой системы, используется в системе контроля целостности (КЦ) файловой системы ОС. Утилита расчета контрольных сумм в КП «ЗОС «СинтезМ» управляется скриптом counthash. Целостность системы проверяется посредством сравнения хеш-сумм рассчитанных с помощью алгоритма ГОСТ 28147-89 в режиме выработки имитовставки.

В процессе своего функционирования AIDE формирует базу данных на основе рассчитанных хеш-сумм файлов перечисленных в ее конфигурационном файле: aide.conf. Базы данных AIDE хранят множество атрибутов файлов включая: тип файла, права доступа, номер инода файла, пользователя, группу, размер файла, mtime, ctime и atime, параметры изменения размера файла, число ссылок на файл и имена ссылок. AIDE рассчитывает хеш-сумму каждого из файлов используя алгоритм ГОСТ 28147-89. Дополнительно может быть выбрано использование модулей: acl, xattr, selinux и e2fsattrs.

Реализованный в КП «ЗОС «СинтезМ» контроль целостности можно разделить на следующие виды:

- КЦ при загрузке ОС;
- периодический КЦ в соответствии с заданным локальным администратором расписанием;
- КЦ по требованию локального администратора.

Для осуществления контроля целостности в процессе развертывания и настройки ОС, для объектов, перечисленных в конфигурационных файлах AIDE, должны быть рассчитаны хеш-суммы, на основе которых будет создана эталонная база данных. Эта эталонная база данных содержит информацию об объектах ОС и используется для выявления несанкционированных изменений в контролируемых файлах внесенных в процессе эксплуатации ОС. База данных содержит информацию о ключевых бинарных файлах системы, библиотеках, заголовочных файлах и всех файлах, которые должны оставаться в неизменном состоянии в течении всего времени работы системы. Данная база не должна включать часто изменяемые файлы, такие как лог-файлы, mail spools, proc-файловые системы, пользовательские директории и директории содержащие временные файлы. Базы данных, создаваемые AIDE и используемые для контроля целостности, сохраняются в архивах с расширениями «.db.gz» и «.db.new.gz.»

Архивы aide.startup.db.new.gz (используется при загрузке) и aide.db.new.gz (используется для периодического контроля целостности и контроля целостности по

требованию локального администратора) содержащие значения контрольных сумм файлов и директорий формируются программой AIDE в процессе подсчета контрольных сумм.

Контроль целостности объектов файловой системы осуществляется за счет сравнения средствами AIDE, текущих значений контрольных сумм файлов (из архива с расширением “.db.new.gz”) с эталонными значениями контрольных сумм файлов (из архива с расширением “.db.gz”).

2.2.27.2.Модуль dlogevent

За обработку сообщений аудита и формирование на их основе событий безопасности отвечает модуль dlogevent. При запуске модуль dlogevent переходит в контекст демона. Демон – процесс, работающий в фоновом режиме без прямого взаимодействия с пользователем.

Модуль dlogevent запускается при старте системы модулем инициализации системны init.d. Модуль init.d запускает модуль dlogevent согласно файлу /etc/init.d/dlogevent. Запуск производится после загрузки семейства модулей файловой системы, семейства модулей syslog, семейства модулей network. Параметры запуска приведены в таблице 3.16.

Таблица 2.7 - Параметры запуска модуля dlogevent

Параметр	Пояснение
-s	Старт dlogevent
-t	Остановка dlogevent
-d	Подробный вывод действий при работе модуля
-h	Вывод информации о параметрах запуска dlogevent

Подробный вывод при работе модуля осуществляется в лог файл /var/log/dlogevent.log. Лог-файл - файл с записями о работе модуля в хронологическом порядке, обеспечивающий регистрацию событий.

После проверки, что работающего dlogevent в операционной системе нет, происходит старт демона.

2.2.27.2.1. Шаблоны сообщений аудита

Шаблоны сообщений аудита основаны на регулярных выражениях.

Регулярное выражение (regular expressions) – формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов. Для поиска используется шаблон строки (строка-образец), состоящая из символов и метасимволов и задающая правило поиска.

Пример шаблона сообщения аудита запуска контроля целостности:

```
«.*type=start suffix={suffix} result={result}»
```

Пример сообщения системы о запуске контроля целостности:

```
«type=start suffix= result=success»
```

Метасимвол «.*» означает любое количество любых символов или их отсутствие.

В результате наложения шаблона на сообщение системы будут выделены следующие полезные данные:

Ключ полезного данного	Значение полезного данного
«suffix»	«»
«result»	«success»

На основе полученных полезных данных формируется событие безопасности. Пример события безопасности для запуска контроля целостности:

```
«[{UUID}] Запуск контроля целостности. Тип {suffix}. Результат: {result}»
```

Поскольку у данного шаблона сообщения аудита нет шаблонов сообщений аудита, от которого данный шаблон зависит и которые необходимы для формирования события безопасности, полезные данные берутся только из данного шаблона. В случае, если такие шаблоны сообщений аудита есть, полезная информация составляется из данного сообщения аудита и от зависимых сообщений аудита.

В результате подстановки полезных данных в событие безопасности получается следующее:

```
«[{UUID}] Запуск контроля целостности. Тип. Результат: success»
```

Значение полезного данного UUID берётся из инициализирующей базы init.sqlite. В результате получается сформированное сообщение события безопасности:

```
«[ab0ed56a-a47f-44a3-8378-b9b558dd1013] Запуск контроля целостности. Тип. Результат: success»
```

В таблице 2.8 представлено соответствие идентификаторов событий безопасности произошедшим действиям в системе.

Таблица 2.8 – Типы событий.

Источник	Тип события	Действие	Идентификатор
Агент Безопасности	Аутентификация	Извлечение ТК/ПИ	4ede7c4b-a6b8-4fc6-a4b7-9caaf8df31da
		Аутентификация по ТК/ПИ	75d846d4-6db7-4fc7-a202-e74bf71319d0
		Смена пароля на ТК/ПИ	467def27-4732-43ce-b676-f9f356ab1009
		Вход на ВМ через spice-сессию	a5ab13a4-d888-4a94-a178-1a631607bbab
		Вход на хост	22485898-4849-4fad-ba63-22f1ce789222
		SU. Успех	37b1cb9b-64d7-4b1f-a1c5-9b5bfc494d48
		SU. Ошибка	c9ee4e23-b461-4189-b5c1-a396a879146a
		SSH. Успех	19a558f1-eeda-4798-9ca2-2d4b2a3384f2
		SSH. Ошибка	3d66817a-21b3-442c-9805-1048795bc294
		GDM. Успех	29867b5f-528b-4fe6-a3d1-a2d440cbacc8
		GDM. Ошибка	7698f81a-e186-48b2-a783-5cc0dadc5b70
		Общая аутентификация. Успех	a286c682-7d91-4cc1-98fc-101baa92a964
		Общая аутентификация. Ошибка	94eeda59-e70c-4777-9274-342d8cc544f3
		Запуск сеанса	af6f9dd4-eb46-468d-b72e-3f68059825f8
		Остановка сеанса	477235ed-a0ce-4c5c-8908-cd8cf476d56e
	Локальные пользователи	Добавление	169cfde6-c726-4091-a61e-7b7a86c656b1

Источник	Тип события	Действие	Идентификатор
			70b7c8d8-5d72-470a-8de9-2223418f99ea
			c206ea3f-44e0-49ed-afc8-a90ea1f81bbf
		Создание домашней директории	1508924a-87a5-4048-9ea5-412214fa8338
		Блокировка	46eabe55-7b7d-4600-9567-9621d76fc65c
		Разблокировка	b7ea9c8b-e787-44f0-a6ce-e38a8570ea4b
		Удаление	ad7753ab-b8ae-462a-a363-c457e8a9ca10
			73a1ca86-6110-4d55-a2fa-7893611088da
		Сброс пароля	0e555053-bd79-47da-bb47-c8826f71f861
		Истёкший пароль	aa48074f-b46d-49b8-b697-025b7970126c
			97378202-ad4d-4653-9528-d3ac4ebcbf4c
			947e96f6-b576-401d-9aac-111dc7060b08
		Истёкший пользователь	dce7fb07-83c6-4af6-8214-7701c3bd01b3
			82cf895f-92dc-47a7-aa8d-c164c359c074
			7a8e27fb-8fad-4e49-8f50-b0d983664bdd
		Модификация пароля	659d760c-03bb-43ed-b924-b3cae27d775b
		Модификация администраторов	0912b335-9f08-4c29-a88d-d171da05dd7c
		Модификация пользователя	6643aa15-2179-43fb-86e7-2770b088f6fd
		Модификация файла паролей	d5913e2c-06c1-4165-b9f8-e5a8f2433a5a
	Локальные группы	Удаление	913d49e1-21b3-4acc-bd45-200e07f6f3c8
		Добавление	aad87513-6ed9-4fb3-a6a0-d8633ce4c04f
		Модификация	9492ddc3-d034-49ac-bd6d-84b896268013
		Модификация файла групп	04f6e99d-d8d7-4637-8b8d-750ff7f507d3
	Локальные/доменные пользователи	Смена пароля	1822a0a3-2e0d-4399-9739-6c6cb1ab188c

Источник	Тип события	Действие	Идентификатор
		Достигнут предел неудачных попыток входа	be681734-bc1a-4c29-bea2-ceabab559b6f
		Блокировка пользователя	0019fb58-ebb7-431e-a2b9-0e4adb17de76
	АВЗ	Старт	07030486-05ce-4e87-be2f-07901217bb6c
		Повторный запуск	5c16612e-ad12-4272-8bdf-64a844c329f3
		Обновление	078a4c1a-47c6-4250-80cc-28de1a02ccca
			5149355c-f58e-423f-94cc-5d0f89ecf147
		Завершение	ebfee86c-f474-408d-8185-5e7887d54cd9
		Сканирование	cf966881-e024-455e-ba1c-2b2e452faa14
	КЦ	Запуск	ab0ed56a-a47f-44a3-8378-b9b558dd1013
		Проверка	085747d7-bb7e-452f-8891-fd32ed68ecb0
		Обновление	24694f33-8860-475e-893c-62cf64f2605d
	Файловая система	НСД	435f062e-be18-4665-b412-0355e0f663d9
			4345a12f-a8ff-4a1a-9636-5b3fdd5fe657
	Модификация конфигураций	audit	d5aea4d3-4ff5-47b2-b810-654cc68f0a1f
		rsyslog	6c21b9f7-d7ea-4033-95b6-700f8e3954a5
		dlogevent	fff33c10-db7e-4972-b23e-f4c09b2a1e2d
		pszi-shred	3bd4259c-4cac-42a5-98e1-63b5f0f82f20
		Аутентификационная информация	a4a40ea7-a254-4f37-8329-83c1216c00ef
		PAM модули	d3857ba1-06c7-496d-8c90-4aa95cccd85c
	Управляющие утилиты	audit	d2f1f07f-8ec4-457d-8307-bd7a9932c74a
		rsyslog	0385e54f-d8d4-412e-93ec-d1ca159082f2
		dlogevent	902a1db7-0127-4f70-96d3-f72a6fa7e445
	Процессы	Запуск	d47cec25-1d4e-453e-b604-2a7553dfb31b
			24aeeec0-6767-4c9d-b171-39ed3bfa9682

Источник	Тип события	Действие	Идентификатор
		Остановка	38dc1c30-52f6-43ab-b924-08f3ad590493
			a9b7da81-25b0-4d61-bb9a-d721515c95fc
			a2336565-414e-49d3-961f-4dc87851ec40
	USB устройства	Подключение	0d1e0b59-d5b8-413f-a74c-8258f812dcdd
		Монтирование	a8647673-d95b-4a63-9c64-2eaed388e9f3
		Размонтирование	74d9560e-ed6f-4d56-9935-4d65e0c0ec75
		Отключение	68f4e12d-c7f6-42ab-96ba-eed82e47aa7d
	Хост	Загрузка	07fa117f-ceba-485f-b124-6acae4116e2e
		Остановка	1050f919-8229-45c1-a1c6-f93660a8a6e4
Аутентификация на ТК	(Служебные сообщения)		1158acdc-b835-427a-8203-429425e9dab8
			6a0e394c-5be8-432a-8a25-203dc224ebed
	Ошибка	Смена пароля	bf9a7069-5c42-4703-bfc1-1f8c9153b7fb
		Ввод пароля	3cc5cd37-91fc-4ea8-8af4-ec588d6fab71
		Получение серийного номера	de7505e7-1dd7-44cf-ade4-70e32e15e1c9
		Получение адреса менеджера	7517642f-a0ad-487c-8aaf-efde22d6a392
		Получение адреса сервера безопасности	54d1b4cc-2d40-49c6-8aea-44ed25a65103
		Получение открытого ключа и случайной последовательности	fa4b91fd-a61e-41bd-8d4c-528fee251171
		Проверка открытого ключа	c6632c10-b5e3-44ab-b757-ad27ea654603
		Некорректный пароль	a6c78e1b-9331-4ca9-89f8-babc97ca52b7
		Некорректные символы	b8069c4f-f570-4ace-b6c6-0cc206f2004c
		Некорректная длинна	517d08e3-192f-40b3-a9d9-5998ee40e494
		Заблокирован	906e2341-b167-49be-8224-8c3b46e4dae5

Источник	Тип события	Действие	Идентификатор
		Ошибка аутентификации	b7f8f4a1-2dea-4342-b36e-6e51b2d5ce0e
		Получение сертификатов менеджера	4fd379d9-12fd-45c4-b349-446f2d3f3f9c
	Успешное		abcf1e49-e571-4d03-854a-90714ddc950f
Сервер безопасности	Группы	Добавление	76287bab-22eb-48c7-bdac-a5c71a0e1a73
			c1ff3bf9-478c-4651-8dbd-f11584a7a3d3
			3c10b3d5-943b-49f0-b9d9-addf120ecccb
			1823f1b7-fd27-4a4c-bd59-38839cd40b15
		Редактирование	18fdce20-68ed-4279-8553-470148d8de36
			c053a2b1-08fd-4a26-a45e-1850c6870bb8
			adbba09d-dd0d-4d17-a47b-94e6c078d39a
		Удаление	61fa9f82-6396-45eb-9bad-75d6cb37eee5
			0781f9bc-e3d6-413d-accd-b9f7e280c0be
			b55a48d0-c43e-4d6a-a2e5-bda68c4d820e
			e68d4868-3513-406b-bfbb-2c542617a51f
			d2d7d8d9-b370-448b-baa9-45550700c554
		Блокирование	68e8a44f-57c0-4e09-b03c-52b50a293451
			b781eaba-dc33-4dc0-ac74-c7b794aee0c7
	Пользователи	Добавление	bd168a77-8b56-45ee-8559-ea980487755b
			0c3f9616-9161-4893-a0bc-ace0447def88
			55c0e4a9-d273-44b9-ba33-dc50e2914feb
		Обновление	cfefc05a-d52b-4c16-bd8c-3cf7045c2fb4
			7c760f8a-8af1-42e6-8ccf-fed41335abbd
		Удаление	933786a5-1583-4904-bd78-444a1e7a8e54
			8f044442-273b-40fd-ac77-4cca9172231c

Источник	Тип события	Действие	Идентификатор
		Блокирование	867fed7a-2246-486c-ad21-71a3040e6f34
			d941717b-fe24-4698-a33b-cbf4e1fae6f2
		Сброс	06a15e52-a4d2-4824-b800-0b14c516623a
	Расписание	Доведение	4d67ea65-7da6-4b1e-8010-d0ae6b23709d
			684391a6-46d0-41fe-88c2-7441892d6ecd
	СФХ	Добавление директории.	2e9571f4-fe21-44a3-b18b-38344a2ecdf9
			eefc1145-b411-4ce2-a8ff-1a8dc2bed6aa
		Обновление настроек директории	d054968d-33db-4290-bdf7-aab990ad0784
			7d449aef-868f-40d4-89ad-8c3b798bff25
		Удаление директории	987656e6-32e5-4fc4-b638-32cf7b63a32c
			4dd3bacc-7767-4e92-9c87-397fa7bac7b1
		Разграничение доступа к директории	004d7254-5709-4dfa-acf6-daccbfe95123
			05d3b0f6-0ece-40a9-990d-c053959c42c7
		Обновление разграничения доступа к директории	e9ead998-a867-4d2c-b7a1-e2b2e153fceb
			1750ab3d-729a-4922-872c-980519162a03
		Удаление разграничения доступа к директории.	7397b707-4ca1-42fb-b547-386d7143e8b0
			42c1f9b6-9061-40ff-9a94-a99b148cbdd1
			b9a4cf6f-5c26-4c5b-a220-ba4c0c982d43
		Доведение	be03a88d-55b8-490e-8287-36707abdca73
			ff706ee2-df6b-4ced-b3b8-a38250b4f783
	ВМ	Создание	eb9c95eb-20eb-4aac-9e0d-6a436c82c647
			0985aef4-dcb3-402a-98be-4d7179c63697
			7b8ac0e9-3ca7-4c5b-8e4b-aa138a0d61e6
			36ca254e-102e-4145-9b83-3aa52fcc6aa3

Источник	Тип события	Действие	Идентификатор
			4f32a595-8dd4-4d02-9a9d-68d3dfb871f3
	События безопасности	Очистка	2cd259e7-81dd-4e29-b1dc-7e105a01c0d4
		Выгрузка	5dc4ee00-0f9b-4a7f-a850-cf17c75392fe
		Скачивание	50c9b5ba-203a-4a05-8322-583c3f95c644
	Политика паролей	Доведение	
Генерация и аудит	События безопасности	Обработка сообщений по умолчанию	9c7d1704-07a9-4d11-9a13-e81be76206f0
	dlogevent	Запуск	afc6b326-60f1-4ef8-b697-6ce34d6e79ff
		Завершение	5cbef62d-abcb-41ca-bd45-c52d807d0e6a
	auditd	Запуск	08f43f26-32a6-442e-88a7-45bf66d2c746
		Завершение	1b82f5b8-cf45-475f-b02a-a834c5840cc6
	rsyslog	Запуск	8210acc4-5c1b-4e88-a435-8266430a5fef
		Завершение	07859615-8c0d-4038-a587-ce2be496968e
Тестирование	Генерация и аудит		c7432bb8-c09f-43c3-a099-67b336c83ff3
			2ae9b387-0a58-4be3-9c37-6ab30075af3a
			5f32f71e-254c-4425-b244-c903e80f9911
			ae5b2bea-4092-4439-a5b6-bb7eb7ef880c
			2f6c9975-d4d1-4afe-b546-04e17a006ce6
			b537cfef-1d75-4e5e-a6ab-299fc0bb4927
	КЦ		f65788dc-d4e0-4eb6-b9b2-d3b31061b8a9
			fa4381a7-e5ea-42c6-a87e-2f44084d7621
Печать	pszi-printing-server	Разрешена	c927f5b2-c23f-400a-b85a-62ab82da4b43
		Запрещена	e322cb6e-facb-4c48-86b1-4e054d9baeed
Виртуализация	Пользователи	Добавление	ffb5d411-5136-49e1-85da-f2af5846d97b
		Удаление	41d72605-2779-400d-8d98-55d580689064

Источник	Тип события	Действие	Идентификатор
		Вход	f94ac67d-ac80-4b5d-ba22-391d42721a10
		Выход	56ce8f3e-9873-4eeb-bf48-e11991681063
	Виртуальные машины	Инициализация подключения	a0afddc6-e625-4d32-94ab-5be5f3c47657
		Вход пользователя	7f0cfb76-6d30-4562-a7b6-abbb55baa3bc
		Выход пользователя	5e00d7cf-7016-4daf-8e41-84e064b805f7
		Запуск	37b6e601-c3d2-4764-80ed-1ea46a59a7f7
		Остановка	b5f9fa54-78b4-488e-a924-7c9446eed4dc
		Заморозка	cc55a125-daf8-471a-8963-9de705a77bce
		Запуск миграции	906518e7-b3eb-4414-9a50-f0d054da4893
		Миграция завершена	de3eb006-7315-4540-9589-13223024d726
		Создание	3516bc6f-e580-49f6-8e20-0038dcf8c9b9
		Удаление	1f5cea88-7fcf-4e1b-b0e3-ba171c4692e1
		Изменение статуса	eb98e628-2fd1-4943-9aa9-ff9f96162e45
		Экспорт старт	596ef3f7-d800-4325-9c1b-b01ec27f93e0
		Экспорт стоп	ac2d3385-bd9c-4bca-b741-486f74640b5c
		Импорт старт	dd3e92b0-92b6-4e8c-99c7-d9156430e74c
		Импорт стоп	1c705d9f-70c8-4686-8184-9af7c27988e1
		Изменение конфигурации	b81b2fe4-13b0-45e6-936c-a449884bc9f0
	Менеджер	Превышение CPU	87b4d9ad-3453-46ae-8585-924cc9af6dda
	Разграничение доступа на ВМ	Добавление	c3db6860-ee70-4013-a413-3339a5e947fa
		Удаление	6422f933-d6cb-42c3-b58d-35b436af6044
	Разграничение доступа на менеджер	Добавление	4d885c11-8aed-4037-b6e8-486f4d2831ad
		Удаление	9fa35549-a737-4c1f-9fea-e167fa9acdf8
	Доменные пользователи	Блокировка	5d186df0-65cf-4ae5-8f7d-819a4f6f185f

Источник	Тип события	Действие	Идентификатор
Сервер управления доступом		Ошибка аутентификации	8130950a-c193-4fee-8cfe-8483a7b7558b
		Аутентификация заблокированного пользователя	f245c912-335a-4256-a7fa-de466cfd6561
		Истекший пароль	ef1a2cf9-1aa0-48d2-91d8-39f2d22f7c77
		Истекший билет	3d6fc116-c33d-4c24-abc3-70d9a7bfb989
		Истекший пользователь	1d146dd9-8737-417e-a9c7-5da976f47b22
		Разблокировка	9b114b17-0238-411f-a891-88f75c5c77a9
		Блокировка	a9608c13-baaf-4842-8677-d036c46289b6
		Смена пароля	970933df-a0ce-446a-a02e-17cbe4c98144
		Сброс пароля	15eaba5c-7925-4b11-af37-c9688ff2112f
		Создание	a0b625f0-410f-44c8-b40a-0a749dd36eb3
			13e0a71f-0580-4188-bd8a-b5c4442a62ce
		Удаление	fdfa256c-7e2a-4588-b865-10b938961e19
			34c1c8ff-9602-49cb-83f6-7f63e54d0e21
	Парольные политики	Создание	9bc61b0e-9fef-42f4-8f91-27791cfbb554
		Изменение	791cbb32-6269-4a23-a4c0-df8781457056
		Удаление	75c3fc88-a445-44b2-bee2-d5982714bf4e

2.2.27.1. Модуль самотестирования

В состав агента безопасности КП «ЗОС «СинтезМ» входит модуль самотестирования обеспечивающий демонстрацию правильного выполнения: подсистемы регистрации событий безопасности, контроля целостности, фильтрации сетевого потока.

Запуск самотестирования осуществляется при запуске ОС, периодически в процессе нормального функционирования, по требованию локального администратора.

Запуск самотестирования при старте обеспечивается средствами systemd. Скрипт запуска security_self_test_startup находится в /etc/init.d/.

Запуск самотестирования по расписанию обеспечивается демоном CRON в соответствии с расписание указанным в файле /etc/cron.d/security_self_test_timetable.

По умолчанию в КП «ЗОС «СинтезМ» тесты находятся в директории: /etc/sintez/tests/. Управление перечнем запускаемых тестов обеспечивается за счет добавления/удаления полного пути до файла с тестами в конфигурационный файл /etc/sintez/self_test.conf.

Самотестирование выполняется непосредственно на узлах функционирующих под управлением КП «ЗОС «СинтезМ», результат самотестирования отправляется на сервер безопасности. Общая схема модуля самотестирования показана на рисунке 2.12.

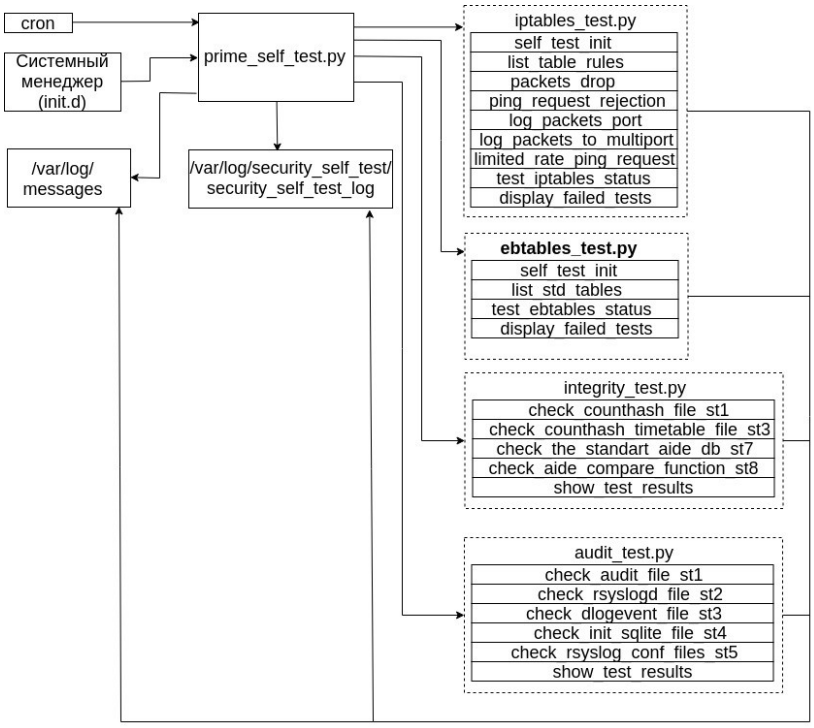


Рисунок 2.12 - Общая схема модуля самотестирования

2.2.27.2.Утилита удаления файлов Shred

Недоступность любого предыдущего информационного содержания в КП «ЗОС «СинтезМ» достигается за счет применения утилиты Shred. Данная утилита

обеспечивает возможность удаления объектов файловой системы путем многократной перезаписи уничтожаемых (стираемых) объектов файловой системы специальными битовыми последовательностями.

Утилита вызывается пользователем из пользовательского пространства при необходимости удаления файла или каталога. Для запуска скрипта удаления через окружение mate, используется конфигурация в которой описано поведение оболочки при выборе контекстного меню.

Утилита /usr/bin/shred выполняет удаление файлов путём повторяющейся перезаписи информации о них и последующим заполнением блоков памяти нулями.

Описание работы с данной утилитой приведено в разделе 3.2.6 руководства оператора ТАСП.62.01.12.000.005 34 01.

2.2.27.3.Модуль Mail Notification

Модуль Mail Notification выполняет мониторинг почтовой папки пользователя на наличие непрочитанных сообщений. Когда приходит новая почта, модуль Mail Notification уведомляет пользователя, отображая значок в области уведомлений.

2.2.27.4.Модуль sz-user-policy

Модуль /usr/bin/sz-user-policy входящий в состав пакета pszi-arm-config-1.4-0.el7.sz.noarch отвечает за настройку базовых конфигураций КП «ЗОС «СинтезМ» в зависимости от роли средства на котором функционирует КП «ЗОС «СинтезМ».

В зависимости от переданных параметров модуль sz-user-policy обеспечивает:

- настройку модуля Mail Notification;
- настройку параметров автоматического завершения сеанса при бездействии;
- ограничения количества активных сессий для пользователей;
- настройку параметров аутентификации (локальная, доменная, использование персонального идентификатора) в том числе за счет вызова скриптов pszi-auth-conf-setup и pszi-auth-pam-setup;
- ограничение ролей на менеджере ВМ;

- создание учетных записей для администраторов (локального и доменного);
- установку пароля на загрузчик ОС GRUB;
- включение подсистемы самотестирования;
- запрет подключения пользователя root по протоколу ssh к ВМ, АРМ;
- ограничение на использование утилит /bin/su и /bin/sudo;
- удаление не используемых pam-модулей;
- ограничение виртуальных консолей управления.

2.2.28. Сервер Безопасности (СБ)

Модуль Сервер Безопасности, участвует в процессе доменной двухфакторной аутентификации с применением ПИ пользователя. При доменной двухфакторной аутентификации, на основе серийного номера ПИ и имени пользователя, модуль Сервер Безопасности по запросу агента безопасности возвращает случайную последовательность, генерируемую по алгоритму ГОСТ 34.11-2012, а также открытый ключ пользователя, хранимый в базе данных сервера безопасности. Случайная последовательность генерируется модулем dstreebog, функционально входящим в состав СБ.

Открытый и закрытый ключи парно генерируются на ПИ пользователя в процессе инициализации персонального идентификатора. Закрытый ключ является не извлекаемым и храниться в памяти персонального идентификатора, в отличие от парного открытого, передаваемого для хранения на сервер безопасности.

Кроме того, сервер безопасности, отвечает за сбор событий безопасности и представление их на портале сервера безопасности. Портал сервера безопасности – это веб-интерфейс, доступный доменному администратору и предоставляющий средство просмотра событий безопасности в удобном, для последующего анализа, формате.

2.2.28.1. Модуль Dstreebog

Модуль dstreebog устанавливается на сервере безопасности (СБ) и предназначен для формирования случайной последовательности по алгоритму ГОСТ Р 34.11-2012 (размер хеша — 256 бит). Формирование случайной последовательности реализуется библиотекой libgosts.so (из состава пакета pszi-libgosts), разработанной на базе реализации данного алгоритма из openssl. В качестве исходных параметров взяты параметры из openssl.

Инициализации программного датчика осуществляется при старте СБ. Процесс отвечающий за генерацию случайной последовательности запускается при старте ОС и работает в режиме демона. При запуске процесса, для инициализации, случайным образом выбирается один из файлов содержащих инициирующую последовательность. Для данной последовательности по алгоритму ГОСТ Р 34.11-2012 рассчитывается значение хэш-функции, которое сохраняется в оперативной память и используется в последующем для расчета следующих значений хэш-функций. При этом файл содержащий использованную инициирующие последовательность удаляется из ФС СБ.

В качестве случайной последовательности, выдаваемой по запросу, используется значение, полученное как результат нескольких (случайное число 1-10) раундов расчета хэш-функции, рассчитываемой по алгоритму ГОСТ Р 34.11-2012 от значения хэш-функции полученной в предыдущем раунде. Хранение предыдущего (последнего) значения случайной последовательности осуществляется в оперативной памяти сервера безопасности и используется в качестве исходного данных для расчета следующей случайной последовательности.

2.2.29. Сервер управления доступом

Сервер управления доступом представляет собой компонент КП «ЗОС «СинтезМ», предназначенный для установки в ВМ Серверов управления доступом. Сервер управления доступом включает в свой состав модули, обеспечивающие

доменную аутентификацию и идентификацию пользователей, а также графический интерфейс управления пользователями и группами пользователей.

Сервер управления доступом является комплексным решением для идентификации, аутентификации и контроля информации безопасности. Он представляет собой централизованную систему по управлению идентификацией пользователей, задания политик доступа и аудита для сетей. Сервер предоставляет возможность аутентификации, авторизации и получения информации об аккаунте, храня данные о пользователях, группах, хостах и других объектах, необходимых для управления безопасностью в компьютерных сетях.

Сервер управления доступом состоит из:

- средство управления доменными пользователями (Free Identity Policy and Audit, FreeIPA) (далее - сервер ИПА, ИПА, IPA) - Apache и Python для Web интерфейса управления системой;
- DNS (BIND) для получения доменных имен;
- сервера LDAP (389 Directory Server) – служба каталогов для хранения данных;
- MIT Kerberos 5 для аутентификации и единой точки входа; ntpd для управления синхронизацией времени.

Аутентификацию пользователя обеспечивает клиент-серверное взаимодействие компонентов программного обеспечения на компьютере пользователя и сервере управления доступом. Реализацию данного взаимодействия на машинах пользователей предоставляет служба безопасности системы (System Security Services Daemon, SSSD), на сервере Средство управления доменными пользователями.

2.2.29.1. Средство управления доменными пользователями (IPA)

Компонент IPA необходим для взаимодействия с программным обеспечением IPA, например реализациями механизма аутентификации (Kerberos) или службы

каталогов (LDAP). IPA включает в себя следующие основные модули: ipalib, ipaclient, ipaserver, ipapython. Модули написаны на языке программирования Python.

Модуль ipalib является ядром компонента; предоставляет различный функционал остальным модулям, например интерфейс командной строки (Command Line Interface, CLI), набор констант, шаблоны сообщений для логирования работы. Модуль обеспечивает реализацию клиент-серверного взаимодействия подмодулей IPA. Модуль ipapython реализует внутренний функционал компонента. Также необходим для выполнения задач установки и настройки IPA. Модуль ipaclient содержит подмодули с клиентской частью основного функционала компонента, например управление пользователями и группами пользователей, настройка правил ACI и HBAC. Для взаимодействия с серверной частью, использует протокол вызова удаленных процедур XML-RPC.

Модуль ipaserver содержит подмодули с серверной частью основного функционала компонента. Модуль реализует основной функционал и отвечает за взаимодействие с системой и внешними механизмами.

2.2.29.2. DNS (BIND)

Domain Name System (система доменных имен) является распределенной системой наименования компьютеров, сервисов и других ресурсов в компьютерных сетях. Система используется для получения информации о доменном имени, например IP адреса по имени хоста. BIND представляет собой реализацию DNS сервера и обеспечивает преобразования доменных имен в IP адреса и наоборот. Служба BIND находится в /usr/sbin/named.

2.2.29.3. Служба каталогов LDAP (389 Directory Server)

LDAP является протоколом прикладного уровня сетевого стека TCP/IP и предоставляет доступ и управление распределенной службой каталогов. Протокол позволяет проводить операции аутентификации, поиска, сравнения, а также операции добавления, изменения и удаления записей в службе каталогов. 389 Directory Server –

это служба каталогов, реализующая протокол LDAP и предназначенная для централизованного управления доступом к ресурсам на множестве сетевых серверов.

В качестве хранилища данных, служба использует базу данных, а именно Berkeley DB. Для представления данных применяется модель ацикличного орграфа, называемая ориентированным деревом. Хранилище данных использует определенную реализацию ориентированного дерева – B-tree. По умолчанию создается дерево, содержащее вершину (корневой суффикс) и несколько поддеревьев. Поддерево config содержит информацию о внутренних настройках службы каталогов. Поддерево NetscapeRoot содержит записи с конфигурационной информацией о других службах каталогов и серверах администрирования. Поддерево userRoot содержит записи с пользовательской информацией. Суффикс userRoot может быть изменен при развертывании службы, например на example.ru.

Поддеревья NetscapeRoot и userRoot являются базами данных. Файлы баз данных находятся в /var/lib/dirsrv/slapd-instance_name/db/, где instance_name название отдельного экземпляра службы. Имя можно указать во время установки службы, по умолчанию используется имя хоста. Например, если полное доменное имя server.example.com, то instance_name будет server.

Среди файлов БД содержатся файлы вида db.00x (x – любая цифра от 0 до 9) для внутреннего использование базой данных; файлы log.xxxxxxxxxx – хранят лог транзакций для каждой БД; файл DBVERSION – хранит версию БД; директория NetscapeRoot, хранящая БД поддерева NetscapeRoot и директория userRoot, хранящая БД поддерева userRoot.

Пользовательская информация представлена в виде определенной структуры, называемой деревом информационных каталогов (Directory Information Tree, DIT). Каждый объект, например пользователь, представлен в виде записи, состоящей из атрибутов. Атрибут определяет уникальную характеристику объекта, например пользовательский пароль. Структура записи, то есть какие именно атрибуты должны содержаться в записи, определяется значениями атрибутов класс объектов (objectclass). Определение самих атрибутов и классов объектов содержится в схемах.

2.2.29.3.1. Дерево информационных каталогов

Поддерево userRoot представляет собой иерархию каталогов, включающих в себя записи с пользовательской информацией. Эта информация включает в себя авторизационные и личные данные пользователей, важные сведения о группах, сервисах, хостах. Для получения любого объекта необходимо указать путь до его записи. Путь выглядит как выражение, состоящее из ряда равенств, где каждое равенство, кроме первого, представляет собой каталог, например “uid=user1,cn=users,cn=accounts,dc=example,dc=ru”. Первое равенство является самой записью, а читать выражение следует справа налево: внутри ru, внутри example (корневой суффикс поддерева), в каталоге accounts, в каталоге users, находится запись user1.

Таким образом, дерево информационных каталогов содержит всю необходимую информацию для обеспечения безопасности пользователей и сервисов в сети. Сама информация также должна быть надежно защищена, что реализовано внутренними механизмами службы каталогов, например шифрование, контроль доступа.

2.2.29.3.2. Схемы

Для описания структуры самих записей используется понятие схем. Схемы реализованы в виде тексто-ориентированного формата LDAP Data Interchange Format (LDIF), позволяющие создавать структурированные записи и поддерживать целостность хранимых данных. Для этого схема строго определяет размер, диапазон и формат значений, содержащихся в записях. Также схема определяет тип записи, содержащийся в каталоге, например сотрудник, устройство, организация. Стандартные схемы находятся в /etc/dirsrv/scheme/ и обеспечивают определение множества классов объектов и атрибутов, необходимых службе каталогов и пользователям этой службы. При необходимости, возможно добавление собственных схем.

Класс объектов является атрибутом, содержащим значение с названием класса. Этот класс определяет набор дополнительных атрибутов, содержащихся в записи. Запись может обладать несколькими классами объектов, что определяет ее полный перечень атрибутов. В LDIF файле схемы содержится информация описывающая классы объектов и атрибуты. Например атрибут общего имени (common name) описывается особым идентификатором (object identfier, OID); именем атрибута; именем класса объекта, содержащего атрибут; названием спецификации, определяющей этот атрибут и именем, запрещенным к использованию. Описание атрибута в схеме выглядит так:

```
attributeTypes: ( 2.5.4.3 NAME ( 'cn' 'commonName' )
  SUP name
  X-ORIGIN 'RFC 4519'
  X-DEPRECATED 'commonName' )
```

2.2.29.3.3. Записи

Записи содержат всю необходимую информацию об объекте, например пользователе. Запись состоит из набора строк атрибут-значение. Каждая запись обязательно содержит атрибут DN (distinguished name, отличительное имя), значение которого уникально и состоит из суффикса поддерева userRoot и иерархии каталогов до самой записи. Например, для пользователя Алексей из отдела разработки и доменного имени example.ru DN будет вида “dn:uid=Алексей,cn=users,ou=development,dc=example,dc=ru”. Суффиксом поддерева является “dc=example, dc=ru” где dc (domain component) – компонент доменного имени, а иерархия катологов выглядит так: внутри “ou=development” (organizational unit) – департамент организации, среди “cn=users” (common name) – общее имя, сотрудник Алексей “uid=Алексей” (user identifier) – идентификатор пользователя.

Каждая запись содержит атрибуты класс объекта (objectclass), определяющие вид объекта и набор дополнительных атрибутов записи. Также существуют атрибуты, которые закрыты от стандартных способов поиска и просмотра записей, например userPassword, содержащий зашифрованный пароль пользователя.

2.2.29.3.4. Атрибуты

Информация об объекте определяется в виде атрибута и его значения. Каждый атрибут определяет конкретную характеристику записи. К примеру, запись может содержать класс объекта сотрудникОрганизации, определяющий пользователя внутри компании. Этот класс будет поддерживать атрибуты имяСотрудника и номерТелефона. Значение этих атрибутов задает имя и номер телефона пользователя соответственно. Также существуют атрибуты только для чтения, значения которых вычисляется службой каталогов. Они называются операционными атрибутами и могут указываться доменным администратором для обеспечения контроля доступа.

Стандартные атрибуты представляют собой простую пару атрибут-значение. Некоторые из таких атрибутов могут встречаться в записи множество раз и содержать уникальные значения. Для управления взаимосвязями между записями существует несколько механизмов. Эти механизмы представлены специальными управляемыми атрибутами: уникальные атрибуты, классы службы, управляемые записи, связные атрибуты, распределенные числовые присвоения.

Уникальные атрибуты требуют, чтобы каждый экземпляр атрибута внутри поддерева имел уникальное значение. Классы службы используют одну запись в качестве шаблона, и когда значение атрибута в шаблоне меняется, тогда все остальные записи, определенные внутри записи класса службы, автоматически получают тоже значение атрибута. Механизм управляемых записей используется для создания записи, соответствующей определенному шаблону, в момент, когда в обозначенной области создана другая запись. Связные атрибуты просматривают значение атрибута DN в одной записи и автоматически добавляют в указанную запись предопределенные атрибуты, содержащие значения, указанные в оригинальной записи. Распределенные числовые присвоения автоматически добавляют записям уникальные идентификационные номера, например для атрибутов GID и UID.

2.2.29.3.5. Функция безопасности LDAP

Для обеспечения функции безопасности и предоставления разрешенного доступа к ресурсам служба каталогов использует определенную иерархию каталогов и использует следующие механизмы:

- аутентификация – позволяет установить личность пользователя, осуществляющего запрос на выполнение какой-либо операции.
- политики паролей – определяют критерии, которым должны удовлетворять пароли.
- шифрование – позволяет защитить личные данные посредством их преобразования.
- контроль доступа – позволяет назначать различные права доступа разным пользователям.
- блокировка аккаунтов – позволяет выключать аккаунты пользователей, группы аккаунтов или целиком домен, в следствии чего запросы аутентификации будут автоматически отклоняться.
- безопасные соединения – позволяют поддерживать целостность информации путем шифрования соединений через TLS, Start TLS или SASL. Принимаемая сторона может определить изменялась ли зашифрованная информация во время передачи.
- аудит – позволяет определить была ли служба каталогов скомпрометирована.

2.2.29.3.5.1. Аутентификация в LDAP

Служба каталогов предоставляет следующие методы аутентификации:

- простое и безопасное связывания;
- аутентификация на основе сертификата;
- прокси-аутентификация.

Простое связывание происходит, когда клиент запрашивает DN и указывает аутентифицирующие данные, например пароль. Служба находит запрашиваемую

запись и проверяет совпадает ли значение пароля указанное клиентом со значением указанным в записи. Если совпадение успешно, то клиент аутентифицирован, иначе клиент получает сообщение об ошибке. Безопасное связывание происходит, когда между службой и клиентским приложением установлено безопасное соединение, например TLS или Start TLS. После этого выполняется простое связывание, но передаваемые данные уже защищены внутри соединения.

Аутентификация на основе сертификата использует во время процесса связывания цифровой сертификат. При первом доступе к службе, она запрашивает у пользователя пароль. Однако вместо сопоставления паролей, служба использует пароль для открытия базы данных сертификата пользователя. При указании правильного пароля, клиентское приложение получает аутентифицирующую информацию из базы данных сертификата. Затем клиентское приложение и служба используют эту информацию для идентификации пользователя путем сопоставления сертификата пользователя с DN каталога. Служба разрешает или запрещает доступ на основе DN каталога, идентифицированного во время этого процесса аутентификации.

Во время прокси-аутентификация пользователь, запрашивая доступ к каталогу, связывается не со своим DN, а с прокси DN. Прокси DN является записью, которая имеет соответствующие права для выполнения операции, запрашиваемых пользователем. Когда прокси права назначаются пользователю или приложению, им предоставляется право указывать любой DN в качестве прокси DN, за исключением DN Менеджера Каталогов (Directory Manager). Одним из основных преимуществ прокси прав является то, что приложения LDAP могут использовать один поток для одного связывания, обслуживая при этом нескольких пользователей, осуществляющих запросы к службе. Вместо того, чтобы связывать и аутентифицировать каждого пользователя, клиентское приложение связывается со службой, используя прокси DN.

2.2.29.3.5.2. **Политики паролей**

Политики паролей позволяют производить гибкую настройку паролей пользователей и обеспечивают безопасность личных данных. Изменение

пользователем пароля проверяется несколькими политиками, при условии, что они включены:

- минимальный возраст пароля – если установленное время действия пароля не достигнуто, то изменение пароля будет отклонено;
- история паролей – если устанавливаемый пароль присутствует в списке использованных паролей, то изменение пароля будет отклонено;
- минимальная длина пароля – если количество символов устанавливаемого пароля меньше этого значения, то изменение пароля будет отклонено;
- синтаксис пароля – если устанавливаемый пароль совпадает с названием существующих атрибутов, то изменение пароля будет отклонено.

Помимо этих проверок пароля, существуют также проверки на минимальное количество символов, минимальное количество цифр, минимальное количество букв, минимальное количество букв в верхнем регистре, минимальное количество букв в нижнем регистре, минимальное количество специальных знаков, минимальное количество 8-битных знаков, максимальное количество повторяющихся подряд одинаковых знаков, минимальное количество применяемых к паролю категорий (знаки верхнего или нижнего регистра, цифры и т.д.).

Существует возможность установить для пароля количество неверных попыток ввода. В случае неверного ввода пароля, счетчик инкрементируется и при достижении установленного количества, аккаунт пользователя блокируется. Разблокировка аккаунта выполняется либо доменным администратором, либо автоматически, после истечении специально установленного времени.

Также у паролей существует время, через которое они считаются устаревшими и должны быть обязательно изменены. Обычно политика устаревания пароля устанавливается от 30 до 90 дней. Для предупреждения пользователя о необходимости изменения пароля используется специальный атрибут. Значение атрибута показывает за сколько дней до устаревания пароля необходимо

предупредить пользователя. Срок действия пароля никогда не закончится раньше, чем было выслано предупреждение.

Логин и пароль хранятся в записи пользователя в атрибутах uid и userPassword. Пароль хранится в зашифрованном виде. Служба каталогов поддерживает несколько вариантов шифрования: Salted Secure Hash Algorithm (SSHA, SSHA-256, SSHA-384, SSHA-512) – наиболее безопасная схема шифрования; CLEAR – отсутствие шифрования, необходимое для установки безопасного соединения, например SASL Digest-MD5; Secure Hash Algorithm (SHA, SHA-256, SHA-384, SHA-512) – менее безопасный вид шифрования чем SSHA; UNIX CRYPT – алгоритм поддерживающий совместимость с UNIX паролями; MD5 – менее безопасный чем SSHA, используется для совместимости с устаревшими приложениями; Salted MD5 – более безопасный чем MD5, но менее чем SSHA.

По умолчанию политики проверки синтаксиса и устаревания паролей отключены, а используемый метод шифрования SSHA.

2.2.29.3.5.3. **Шифрование**

Шифрование базы данных позволяет хранить значение некоторых атрибутов в зашифрованном виде. В соответствии с конфигурацией, каждый экземпляр конкретного атрибута, даже индекс, зашифровывается и может быть доступен только с использованием безопасного соединения, например TLS.

2.2.29.3.5.4. **Контроль доступа**

Контроль доступа позволяет назначать пользователям права доступа к различной информации. Контроль доступа определяется использованием одного или более списков контроля доступа (Access Control List, ACL). Каталог с ACL содержит одно или более выражений об информации контроля доступа (Access Control Information, ACI). Эти выражения позволяют разрешать или запрещать права доступа (чтение, запись, поиск и т.д.) к записям и их атрибутам. Списки могут быть установлены на любой уровень дерева информационных каталогов: служба каталогов целиком, поддерево службы каталогов, определенная запись каталога, определенный набор атрибутов записи, любая запись, соответствующая фильтру поиска.

В дополнение, права доступа могут быть установлены для определенного пользователя, для всех пользователей определенной группы или для всех пользователей службы каталогов, а также доступ может быть определен для сетевого местоположения: IP адрес или имя DNS. Это становится возможным благодаря модели ролей. Роль представляет собой привилегию или группу привилегий, которые состоят из набора выражений ACI. Назначение такой роли пользователю или группе пользователей автоматически определяет их права доступа. То есть объект несущий определенную роль попадает под определенные ролью правила доступа.

Выражении ACI состоит из цели, операции и правила связывания. Цель определяет элемент службы каталогов на который действует ACI. Целью может быть только одна запись, множество атрибутов или фильтр поиска. Операции определяют разрешен или запрещен определенный тип доступа к выбранной цели. Правило связывания определяет DN или сетевое местоположение к которому применяется операция. Таким образом выражение ACI определено как: “Для цели службы каталогов, разрешить или запретить операцию, если правило связывания успешно выполнено”. Операция и правило связывания устанавливаются как пара, что позволяет присваивать одной цели множество таких пар. Операции подразделяются на следующие:

- чтение – указывает, что данные каталога могут быть прочитаны.
- запись – указывает, что данные каталога могут быть созданы или изменены. Данные также могут быть удалены, но не сама запись целиком. Для этого пользователь должен обладать правом удаления.
- поиск – указывает, можно ли искать данные каталога. Отличие от чтения в том, что чтение позволяет просматривать данные каталога, если они возвращены как часть операции поиска.
- сравнение – указывает, что данные могут использоваться в операциях сравнения. используется операция поиска, но возвращаемое значение является булевым и идентифицирует совпадение. Операция применяется для сопоставления значений пароля во время аутентификации.

- само-запись – используется только для управления группами. Операция позволяет пользователю добавлять и удалять себя из группы.
- добавление – указывает, что дочерняя запись может быть создана.
- удаление – указывает, что запись может быть удалена.
- проксирование – указывает, что пользователь может использовать для доступа любой DN с правами этого DN, кроме Менеджера Каталогов.

Обычно правило связывания указывает, что DN связан с операцией доступа. Правило может указывать на такие атрибуты как время дня или IP адрес. Правила связывания обозначают некоторые ситуации в которых могут быть применимы ACI:

- если операция связывания запрашивается с определенного IP адреса или имени хоста DNS. В основном используется для принудительного обновления службы с заданного компьютера или сетевого домена;
- если пользователь связывается анонимно. Установка операций для анонимного связывания разрешает эти операции всем, кто связывается с каталогом;
- для любого, кто успешно связывается с каталогом. Это обеспечивает общий доступ, предотвращая анонимный доступ;
- если клиент связан как непосредственный родитель записи;
- если запись, с которой связан пользователь, соответствует определенным критериям поиска.

Служба каталогов предоставляет несколько ключевых слов для более простого выражения таких типов доступа:

- Parent – если связанный DN является непосредственной родительской записью, то правило выполняется. То есть определенные операции могут быть разрешены для ветви каталога, что позволяет управлять дочерними записями;

- Self – если связанный DN тот же, что и запрашиваемый для доступа, то правило выполняется. Некоторые операции могут быть индивидуально разрешены пользователям для обновления их собственных записей;
- All – правило связывания выполняется для любого, кто успешно связался с каталогом;
- Any – правило связывания выполняется для всех. Используется для разрешения и запрета анонимного доступа.

По умолчанию любой доступ запрещен для всех, кроме Менеджера Каталогов. Поэтому, чтобы появилась возможность доступа к каталогам, некоторые ACI должны быть применены к каталогам и пользователям. Во время попытки доступа к записи, для определения прав доступа, служба каталогов пользуется правилом приоритета. Правило определяет, что в случае, когда существует две конфликтующие операции приоритетным считается операция, запрещающая доступ.

2.2.29.3.5.5. **Блокировка аккаунтов**

Блокировка аккаунтов позволяет предотвратить доступ к пользовательской информации скомпрометированным аккаунтам. После того как аккаунт заблокирован или отключен, запросы аутентификации с такого аккаунты будут отклонены. Блокировку можно выполнить в ручную или автоматически. Разблокировать аккаунт может доменный администратор или если установлено специальное время, то после его истечении. Для автоматической блокировки необходимо настроить специальные политики:

- блокировка после достижении количества неверных попыток ввода пароля;
- блокировка после истечении отведенного количества времени действия аккаунта;
- в случае долгого отсутствия пользователя в системе, блокировка после истечении времени с последней аутентификации.

2.2.29.4. MIT Kerberos 5

Kerberos – сетевой протокол аутентификации, позволяющий аутентифицировать клиентов в незащищенных сетях. В качестве клиентов выступают пользовательские машины и машины сервисов. Также протокол обеспечивает взаимную аутентификацию и безопасный обмен данными между пользователем и сервисом. Для реализации этих задач необходимо наличие третьей доверенной стороны и применение системы билетов.

В процессе взаимной аутентификации пользователь и сервис должны обмениваться важной информацией, которая может быть перехвачена злоумышленниками. Чтобы этого избежать, сообщения надо передавать в зашифрованном виде, что означает необходимость использования системы билетов. Билеты содержат ключи шифрования и аутентифицирующую информацию. Для того, чтобы ключи шифрования не оказались скомпрометированы, билеты также должны быть зашифрованы, что делает обязательным наличие третьей доверенной стороны. При условии, что все клиенты доверяют третьей стороне, а сама она является гарантом безопасности, становится возможным обеспечить безопасный обмен данными в незащищенных сетях.

Этой доверенной стороной выступает Центр распределения ключей (Key Distribution Center, KDC). Центр аутентифицирует на своей стороне всех клиентов, после чего распределяет между ними билеты, необходимые для подтверждения клиентами своей сущности. В случае пользовательских машин, эти билеты необходимы для дальнейших запросов на получение билетов к сервисам. В качестве хранилища данных сетевой инфраструктуры применяется сервер LDAP (389 Directory Server).

В настоящее время используется пятая версия протокола, реализующая алгоритм шифрования AES и спецификацию GSS-API Version 2. Конфигурационная информация протокола находится в /etc/krb5.conf.

2.2.29.4.1. Центр распределения ключей (KDC)

Центр распределения ключей предназначен для аутентификации клиентов в незащищенной сети и распределения им билетов. Также центр выполняет функцию единой точки входа для клиентов сети. Центр состоит из модуля KDC, разделенного на два логических подмодуля: сервер аутентификации (Authentication Server, AS) и сервер выдачи билетов (Ticket Granting Server, TGS). Подмодули выдают разные типы билетов: билет для получения билетов (Ticket-granting Ticket, TGT), выдающийся сервером аутентификации и клиент-серверный билет (Client-to-server Ticket, CST), выдающийся сервером выдачи билетов.

Центр предоставляет возможность хранения информации о существующих объектах сетевой инфраструктуры в локальной базе данных. Группа KDC, расположенных на разных машинах, но использующих одно хранилище данных, объединяется в один реалм. В архитектуре мастер-мастер, KDC используют собственные хранилища данных, но из-за репликации, поддерживающей однородность и достоверность информации в обоих хранилищах, оперирование происходит с одними и теми же объектами сетевой инфраструктуры. Таким образом такие KDC также образуют один реалм. Названия реалма обычно записывается в верхнем регистре и использует имя домена, то есть для домена example.com, имя реалма будет EXAMPLE.COM.

В момент аутентификации клиента в KDC, происходит обмен зашифрованными сообщениями. Для их шифрования используются секретные ключи клиентов. KDC получает секретные ключи во время создания клиентов, например пользователя или сервиса. Для пользователя секретным ключом будет результат применения хэш-функции к паролю, а для сервиса хэш, сгенерированный во время создания сервиса. Клиенты получают секретные ключи, во время логина по паролю, в случае пользователя или в keytab файле, в случае сервиса. Keytab файл содержит список имен объектов, доступных для получения TGT. Также, для каждого объекта, в файле содержится аутентифицирующая информация (хэш), позволяющая получить TGT без ввода пароля.

В целях более удобного и подробного хранения данных об объектах, используется служба каталогов 389 Directory Server. Имена объектов в службе и в локальном хранилище KDC соотносятся один к одному, а для получения различной информации об объектах (пользовательский пароль, описание сервиса) KDC отправляет службе соответствующие запросы. Файл конфигурации KDC находится в /etc/sysconfig/krb5kdc, а сам центр расположен в /usr/sbin/krb5kdc.

2.2.29.4.2. Билет для получения билетов

TGT выдается клиенту в процессе его аутентификации в KDC и используется для дальнейшего получения клиент-серверных билетов к доступным ему сервисам. Билет включает в себя: идентификатор пользователя, сетевой адреса клиента, время действия билета и сессионный ключ TGS. Также билет зашифрован секретным ключом TGS и не может быть расшифрован на пользовательской машине.

После получения TGT, клиенту больше нет необходимости предъявлять свои аутентификационные данные для обращения в KDC или к существующим сервисам. На основании билета, до истечения его времени действия, пользователь может получать клиент-серверные билеты, необходимые для доступа к сервисам. После того, как TGT стал просрочен, пользователь обязан снова пройти процедуру аутентификации в KDC. Время действия билета задается настройками KDC.

2.2.29.4.3. Клиент-серверный билет

Клиент-серверный билет может быть получен после запроса в TGS, перед непосредственным обращением клиента к определенному сервису. Билет включает в себя: идентификатор клиента, сетевой адрес клиента, время действия билета и сессионный ключ сервера. Билет зашифрован секретным ключом сервиса и не может быть расшифрован на пользовательской машине.

Билет выдается после предъявления пользователем своего TGT и прохождения некоторых проверок. После получения клиент-сервисного билета пользователь получает возможность пройти взаимную аутентификацию с запрашиваемым сервисом. В результате предъявления билета сервису и обмена некотором

количеством сообщений, процедура прохождения обоюдной аутентификации завершена и установлен безопасный обмен данными.

Таким образом выдача билета контролирует наличие у пользователя доступа к сервису, а время действия билета – продолжительность этого доступа. Время действия билета задается настройками KDC.

2.2.29.4.4. Сервер аутентификации (AS)

Сервер аутентификации отвечает за выдачу клиентам TGT. После получения от клиента запроса аутентификации, сервер проверяет существование клиента в хранилище данных. Также проверяется метка времени, которая должна быть близка к локальному времени KDC. Если проверки пройдены, то клиенту отправляется зашифрованный TGT, иначе сообщение об ошибке.

2.2.29.4.5. Сервер выдачи билетов (TGS)

Сервер выдачи билетов отвечает за выдачу клиентам клиент-серверного билета, позволяющего пройти клиенту и сервису взаимную аутентификацию. После приема запроса на получение клиент-серверного билета, сервер проводит ряд проверок и формирует сессионный ключ сервера. Затем TGS отправляет клиенту сообщение, содержащее этот ключ, зашифрованный клиент-серверный билет, идентификатор сервиса и время действия билета.

2.2.29.5. Взаимодействие KDC и LDAP

Для выполнения своих функций KDC необходимо иметь доступ к хранилищу данных, содержащему информацию о пользователях, сервисах и других объектов сетевой инфраструктуры. В качестве такого хранилища выступает LDAP сервер – 389 Directory Server. Сервер хранит информацию в виде, соответствующем протоколу LDAP. KDC отправляет запрос на сервер и получает необходимые данные в ответе.

KDC и LDAP находятся на одной машине, а обмен данными происходит посредством технологии межпроцессного взаимодействия (Inter-process Communication, IPC). Для этого используются Unix-сокеты, что позволяет обеспечить

высокую скорость и безопасность передаваемых данных. Настройки способа взаимодействия с LDAP находятся в /etc/ipa/default.conf. Настройки запуска сервера LDAP, например путь к его ccache и keytab файлам, находятся в /etc/sysconfig/dirsrv и /etc/sysconfig/dirsrv-instance_name, где instance_name название отдельного экземпляра сервера.

3. УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

КП «ЗОС «СинтезМ» это высоко настраиваемая операционная система на базе Linux, предусматривающая возможность работы как на одном СВТ (АРМ, Сервер, ВМ), так и на разных СВТ объединенных в сеть.

КП «ЗОС «СинтезМ» реализуется в виде двух конфигураций:

– операционная система (ОС), в двух вариантах установки:

- серверная операционная система;
- клиентская операционная система.

– среда виртуализации.

КП «ЗОС «СинтезМ» в конфигурации ОС предназначена для предоставления пользователю многозадачной и многопользовательской операционной системы общего назначения, выступающей в качестве основы для исполнения приложений на серверах, АРМ, и гостевых ВМ.

КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» предназначен для обеспечения функционирования доверенной среды виртуализации, развертывания необходимого количества виртуальных машин и создания надежных, высокопроизводительных отказоустойчивых объектов в составе автоматизированной информационной системы с неограниченным числом пользователей.

Данное программное обеспечение может быть установлено на:

– физический сервер;

– автоматизированное рабочее место (АРМ);

– виртуальную машину (ВМ).

Роль задается на этапе установки КП «ЗОС «СинтезМ» и определяет набор устанавливаемых компонентов.

Сопоставление конфигураций, ролей и компонентов КП «ЗОС «СинтезМ» представлено в таблице 3.6.

В рамках данной инструкции в качестве параметров, задаваемых при установке будут использоваться значения, приведенные в таблицах 3.1-3.5

Таблица 3.1– Параметры установки

№	Наименование машины	Имя хоста	IP-адрес
1.	АРМ Администратора	sintezm-adm1.fintech.ru	10.10.10.100
2.	Гипервизор	sintezm-h.fintech.ru	10.10.10.2
3.	Менеджер ВМ	sintezm-m.fintech.ru	10.10.10.125
4.	Сервер управления доступом	sintezm-ipa.fintech.ru	10.10.10.73
5.	Сервер Безопасности	sintezm-sb.fintech.ru	10.10.10.50
6.	А	sintezm-arm1.fintech.ru	10.10.10.83
7.	Виртуальная машина 1	s	
8.	Виртуальная машина 2	s	

Таблица 3.2 – Параметры сервера виртуализации

№	Наименование параметра	Значение	Примечание
«Параметры IPv4»			
1.	Имя узла		
2.	Адрес		
3.	Маска		
4.	Шлюз		
Выбор NTP сервера			
5.	Сервер NTP		
Пароль root			
6.	Пароль root		
Параметры /etc/resolv.conf			
7.			
8.	nameserver	10.10.10.73	<IP-адрес IPA>
Параметры /etc/hosts			
9.			Структура: <IP-адрес> <hostname>
10.			
11.			

Таблица 3.3 – Параметры ВМ Сервера управления доступом

№	Наименование параметра	Значение	Примечание
Параметры ВМ			
1.	Операционная система	Red Hat Enterprise Linux 7.x x64	Вкладка «Общее»
2.	Оптимизировано для		Вкладка «Общее»
3.	Имя		Вкладка «Общее»
4.	Размер (GB)		Вкладка «Общее»
5.	Политика выделения	Размеченный	Вкладка «Общее»
6.	Размер памяти		Вкладка «Система»

№	Наименование параметра	Значение	Примечание
7.	Размер памяти		Вкладка «Система»
Параметры IPv4			
8.	Имя узла		
9.	Адрес		
10.	Маска		
11.	Шлюз		
Выбор NTP сервера			
12.	Сервер NTP		
Пароль root			
13.	Пароль root		
Параметры /etc/resolv.conf			
14.			
15.			
Параметры /etc/hosts			
16.	10.10.10.2	sintezm-h.fintech.ru	Структура: <IP-адрес>
17.	10.10.10.125	sintezm-m.fintech.ru	Структура: <IP-адрес> <hostname>
18.	10.10.10.73	sintezm-ipa.fintech.ru	Структура: <IP-адрес> <hostname>

Таблица 3.4 – Параметры ВМ Сервера безопасности

№	Наименование параметра	Значение	Примечание
Параметры ВМ			
1.	Операционная система	Red Hat Enterprise Linux 7.x x64	Вкладка «Общее»
2.	Оптимизировано для		Вкладка «Общее»
3.	Имя	s	Вкладка «Общее»
4.	Размер (GB)		Вкладка «Общее»
5.	Политика выделения		Вкладка «Общее»
6.	Размер памяти		Вкладка «Система»
7.	Размер памяти		Вкладка «Система»
Параметры IPv4			
8.	Имя узла	s	
9.	Адрес		
10.	Маска		
11.	Шлюз		
Выбор NTP сервера			
12.	Сервер NTP		
Пароль root			
13.	Пароль root		
Параметры /etc/resolv.conf			
14.			
15.			
Параметры /etc/hosts			

№	Наименование параметра	Значение	Примечание
16.	10.10.10.50	sintezm-sb.fintech.ru	Структура: <IP-адрес>
17.	10.10.10.73	sintezm-ipa.fintech.ru	Структура: <IP-адрес> <hostname>

Таблица 3.5 – Параметры АРМ ОБИ

№	Наименование параметра	Значение	Примечание
«Параметры IPv4»			
1.	Имя узла		
2.	Адрес		
3.	Маска		
4.	Шлюз		
Выбор NTP сервера			
5.	Сервер NTP		
Пароль root			
6.	Пароль root		
Параметры /etc/resolv.conf			
7.			
8.			
Параметры /etc/hosts			
9.	10.10.10.50	sintezm-sb.fintech.ru	Структура: <IP-адрес> <hostname>
10.	10.10.10.73	sintezm-ipa.fintech.ru	

3.1. Загрузка с внешнего носителя и выбор варианта установки

Установка КП «ЗОС «СинтезМ» может проводиться на сервера, АРМ и ВМ.

Для установки комплекса программ на сервер или автоматизированное рабочее место, необходимо вставить оптический диск с дистрибутивом изделия в устройство для чтения дисков и дождаться его загрузки.

После завершения загрузки оптического диска, в зависимости от режима загрузки технического средства (legacy, EFI) отобразится меню загрузки изделия.

При загрузке в режиме legacy (рисунок 3.1), для установки изделия необходимо выбрать пункт меню «Установка КП ОС СинтезМ-К» и нажать на клавишу [Enter].

Помимо установки программного комплекса администратору доступны следующие действия:

– протестировать носитель и установить КП;

– восстановить систему;

– загрузка с жесткого диска.

Если ни одна клавиша не была нажата в течение 60 секунд, то по умолчанию запустится установка ОС. Для переключения типа действий использовать кнопки навигации.

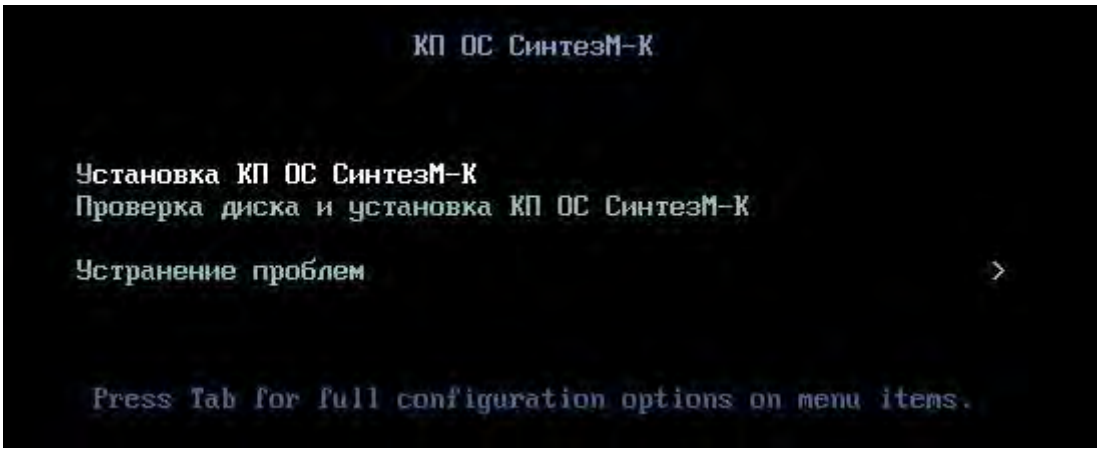


Рисунок 3.1 – Выбор устанавливаемой версии программного изделия (legacy)

При загрузке в режиме EFI (Рисунок 3.2) для установки изделия необходимо выбрать пункт меню «Install KP OS SintezM-K 7» и нажать на клавишу [Enter].

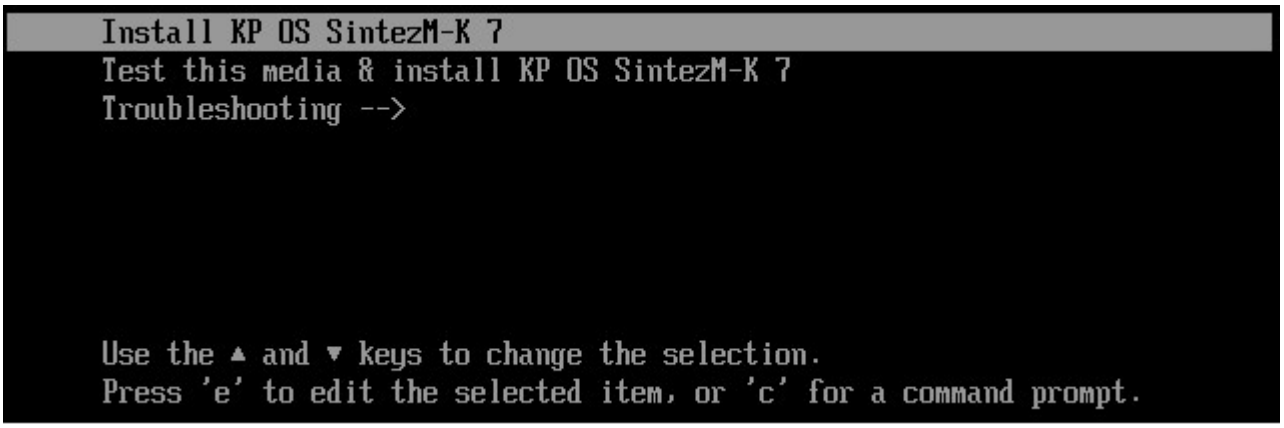


Рисунок 3.2 - Выбор устанавливаемой версии программного изделия (EFI)

После выбора типа действия «Установка» (пункты «Установка КП ОС СинтезМ-К» или «Install KP OS SintezM-K 7») откроется окно выбора языка установки (рисунок 3.3). Для выбора языка необходимо выделить его в списке или ввести в окне поиска и нажать кнопку «Продолжить».

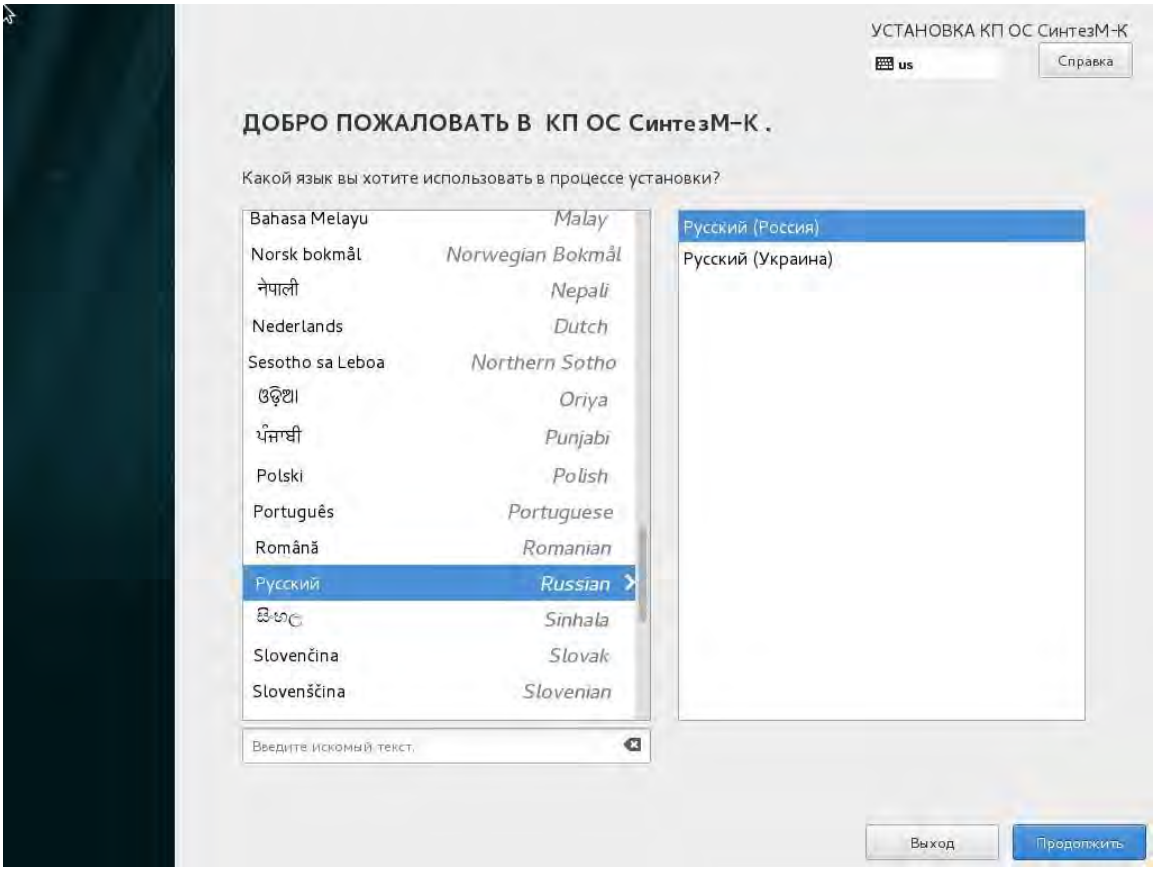


Рисунок 3.3 – Окно выбора языка установки

После выбора языка, откроется меню настройки программного изделия (рисунок 3.4).

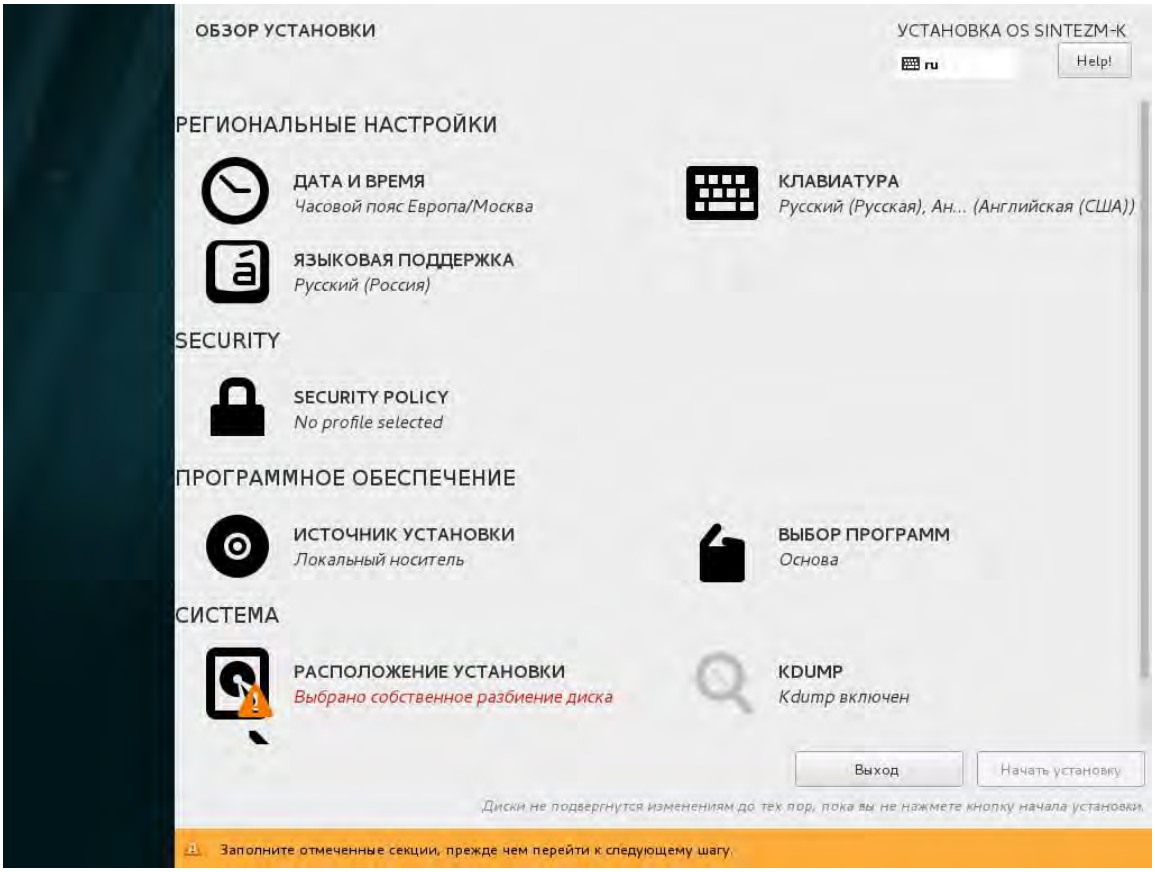


Рисунок 3.4 – Окно «Обзор установки»

В данной форме оператору необходимо:

1. Выбрать программное обеспечение;
2. Настроить место установки (расположение установки);
3. Настроить сеть и имя узла;
4. Назначить региональные настройки.

Выбор конфигурации и варианта установки осуществляется в интерфейсе программы установки за счет выбора соответствующего базового и дополнительного окружения.

Для настройки базового окружения и назначения дополнений для выбранного окружения (рисунок 3.4) необходимо нажать на кнопку «Выбор программ».

Оператору доступно следующее базовое окружение:

– базовая система (Основа);
– графический клиент (Графический-клиент);
– сервер виртуализации (Гипервизор);

– сервер управления виртуальными машинами (Менеджер-ВМ);
– сервер управления доступом (Сервер-ИПА);
– сервер безопасности (Сервер-СБ).

Таблица 3.6 - Сопоставление конфигураций, ролей и компонентов КП «ЗОС «СинтезМ»

Конфигурация КП «ЗОС «СинтезМ»	**Роль КП «ЗОС «СинтезМ»**	**Компоненты КП «ЗОС «СинтезМ»**
Операционная система	Серверная операционная система	– базовая система (base) – агент безопасности базовый (base-ab)
	Клиентская операционная система	– базовая система (base) – графический клиент (x11) – агент безопасности базовый (base-ab) – агент безопасности базовый пользовательский/администратора (user-ab/admin-ab)
Среда виртуализации	Сервер безопасности (СБ)	– базовая система (base) – агент безопасности базовый (base-ab) – сервер безопасности (sb-server)
	Сервер управления доступом	– базовая система (base) – агент безопасности базовый (base-ab) – Средство управления доменными пользователями (сервер ИПА)
	Сервер управления средой виртуализации	– базовая система (base) – агент безопасности базовый (base-ab) – менеджер ВМ (manager-vm)
	Сервер виртуализации	– базовая система (base) – агент безопасности базовый (base-ab) – гипервизор (virtualization-hypervisor)

Для выбора базового окружения и дополнений для выбранного окружения напротив соответствующих позиций (Рисунок 3.5) необходимо установить флаг выбора.

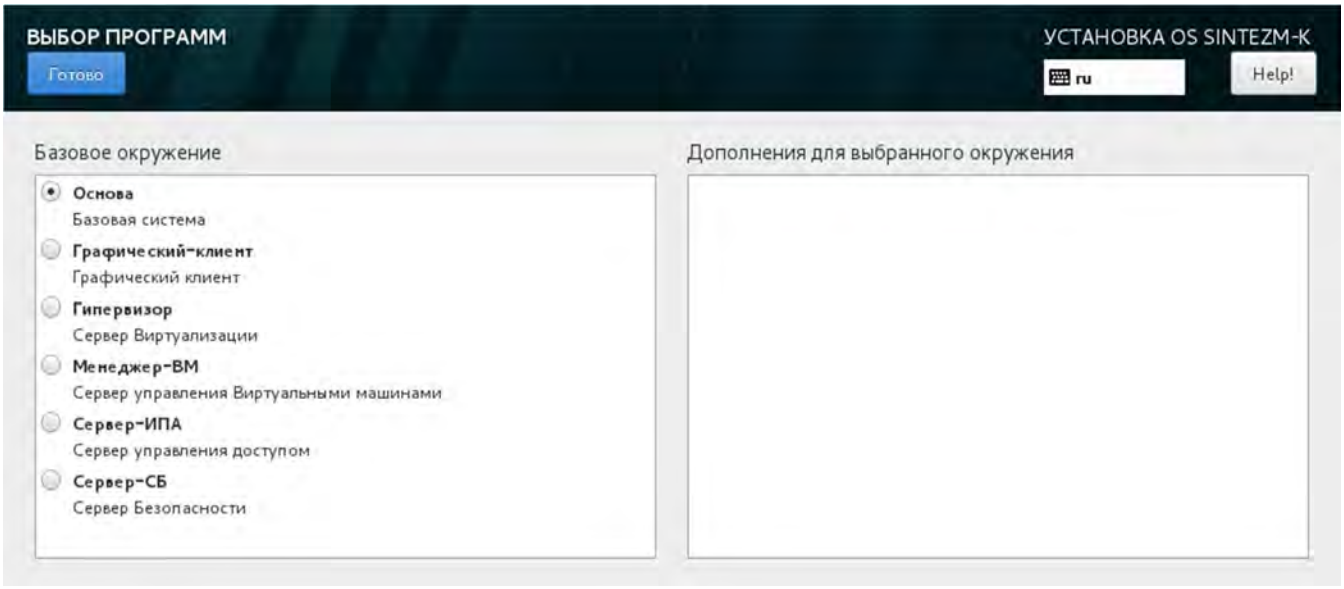


Рисунок 3.5 – Окно «Выбор программ»

3.2. Установка в конфигурации «Операционная система»

Установка КП «ЗОС «СинтезМ» в конфигурации «Операционная система» может производиться на сервера, АРМ и ВМ.

3.2.1. Установка Серверной операционной системы

Для установки Серверной операционной системы необходимо произвести действия описанные в пункте 3.1 данной инструкции, после чего в окне «Выбор программ» в качестве базового окружения выбрать позицию «Основа» (Рисунок 3.5).

Примечание. Для функционирования КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» необходимо помимо действий описанных ниже произвести предварительные настройки, описанные в п. 3.4.1.4 «Предварительная настройка ОС»

3.2.1.1. Настройка места установки для серверной ОС

Установка изделия может производиться на локальный, в этом случае необходимо выбрать соответствующее устройство в поле «Локальные диски», или на сетевой диск. Выбор дисков и разделов производится после нажатия на пиктограмму «Расположение установки» (в окне «Обзор установки» см. Рисунок 3.4). В открывшемся окне (Рисунок 3.6) необходимо выбрать диск, на который будет

производиться установка ОС. Далее в нижней части окна выбрать параметр «Я настрою разделы», и нажать на

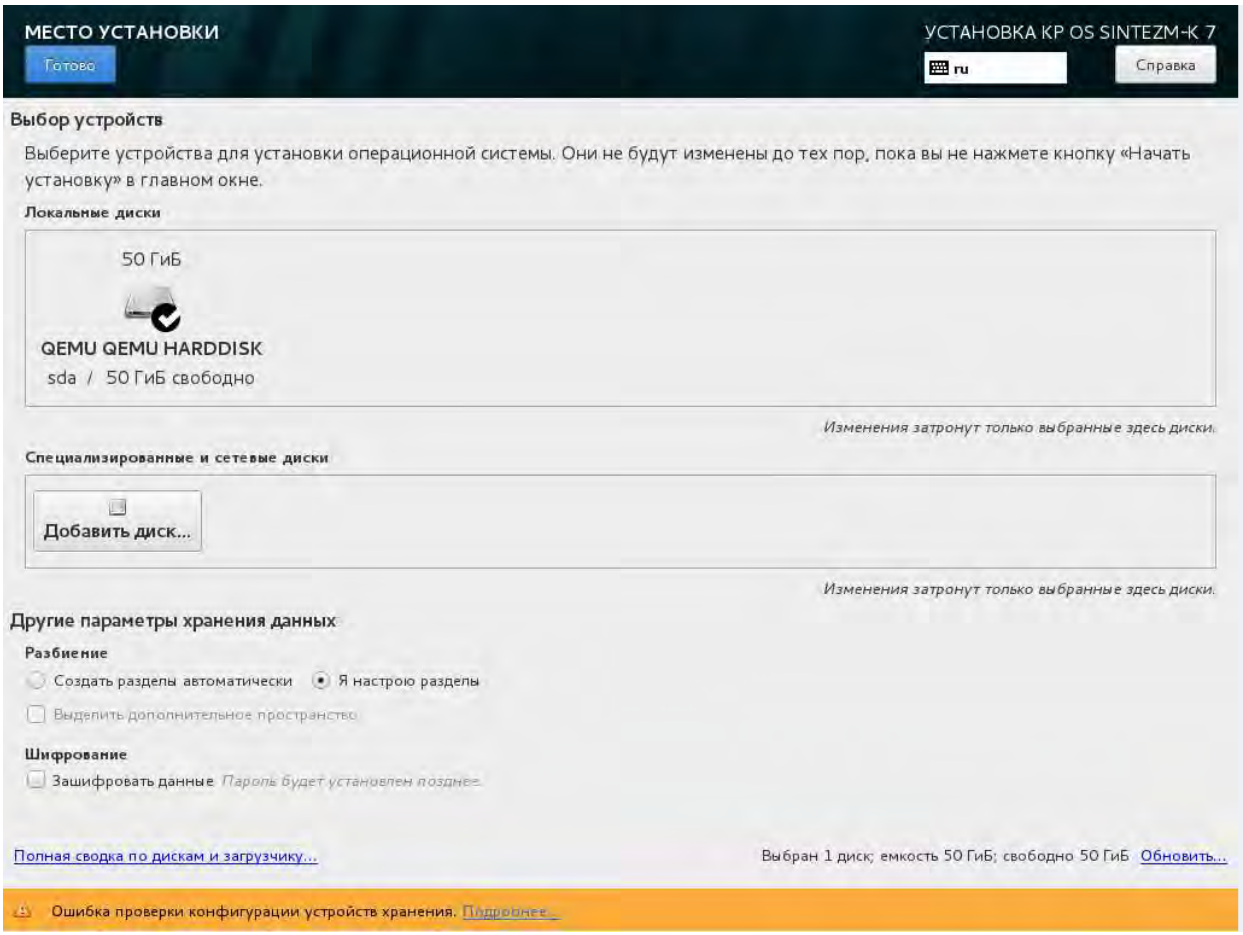


Рисунок 3.6 - Окно выбора создания разделов серверной ОС

Следующим шагом необходимо произвести настройку разделов изменить структуру логических томов (Рисунок 3.7). Для этого необходимо раскрыть выпадающий список «Новая установка OS SINTEZM-K» и выбрать «Создать их автоматически».

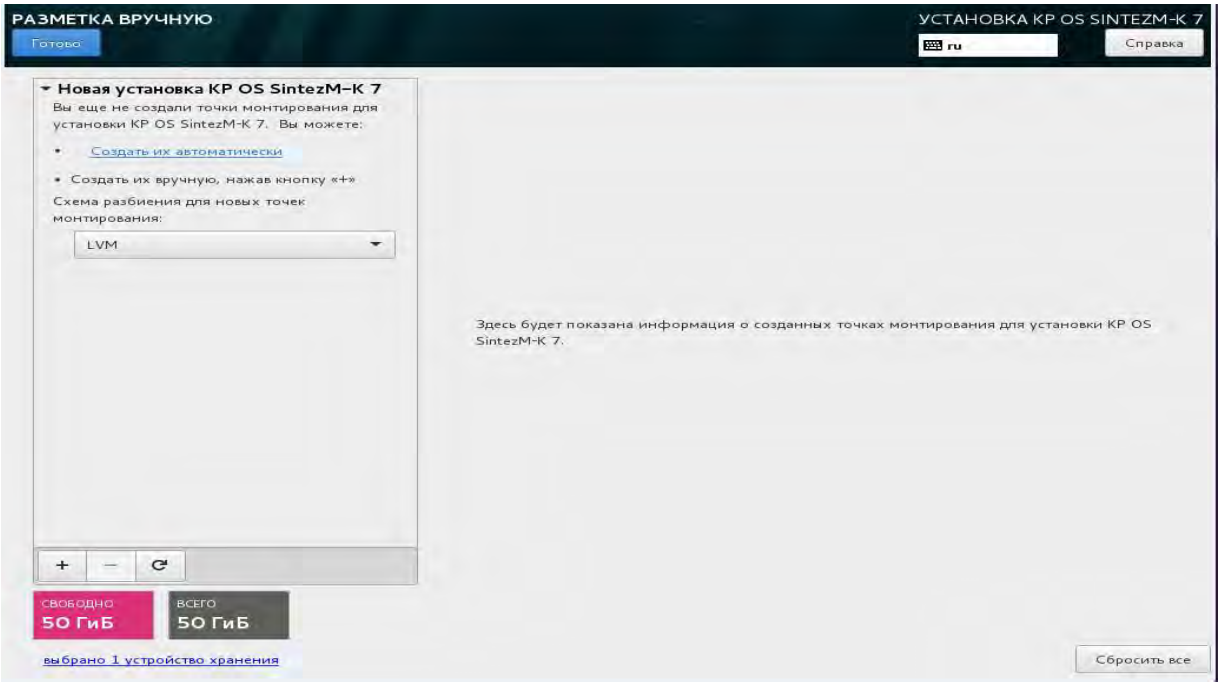


Рисунок 3.7 – Настройка разделов

По умолчанию программа создает логические тома: «swap», «/home», «/», boot», которые необходимо отредактировать. Для этого, необходимо:

– выбрать том «/home», после чего нажать на кнопку  **«Удалить»**;

– выбрать том «/swap», после чего нажать на кнопку  **«Удалить»**.

Оставшееся место на диске необходимо распределить в директорию root. Для этого необходимо:

– выбрать раздел «/»;

– задать в поле "Требуемый размер" максимально доступное значение (таким образом, необходимо стремиться к тому, чтобы значение свободного неиспользуемого пространства, отображаемое в нижнем левом углу, было как можно меньше);

– нажать на кнопку «**Применить**»;

– нажать на кнопку «**Готово**».

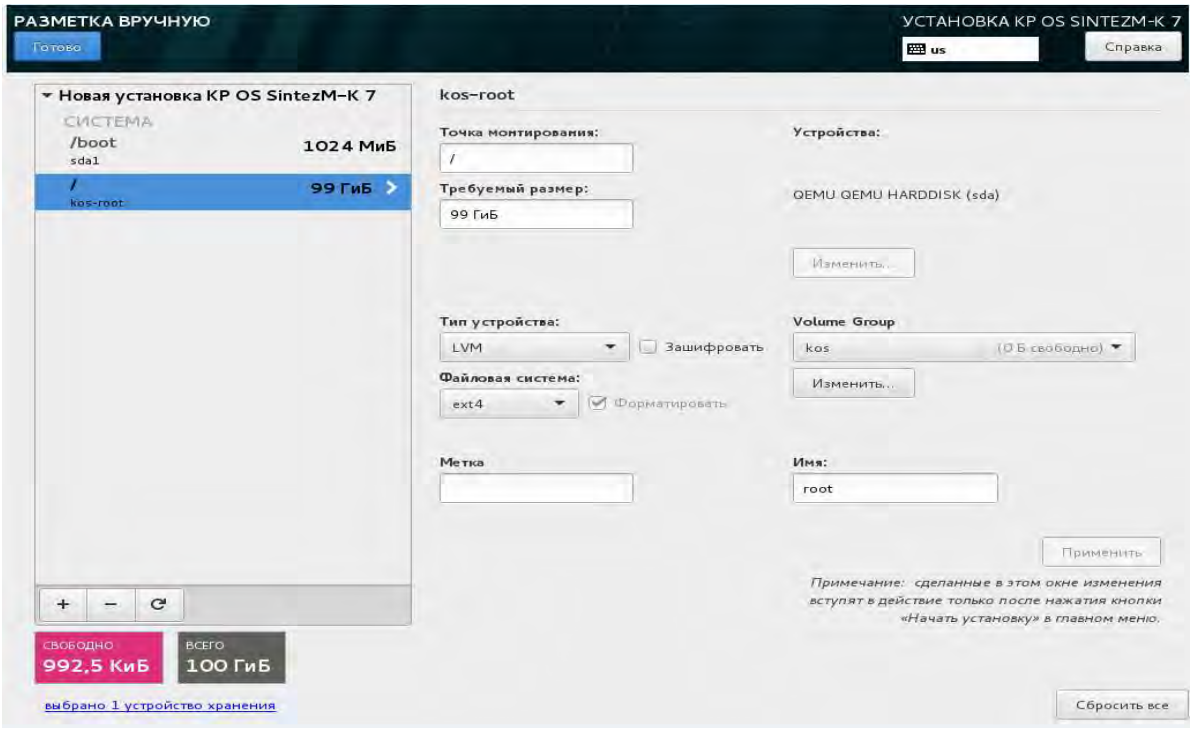


Рисунок 3.32 – Окно создания разделов вручную

В открывшемся окне «Обзор изменений» (Рисунок 3.8) необходимо нажать на кнопку **«Принять изменения»**.

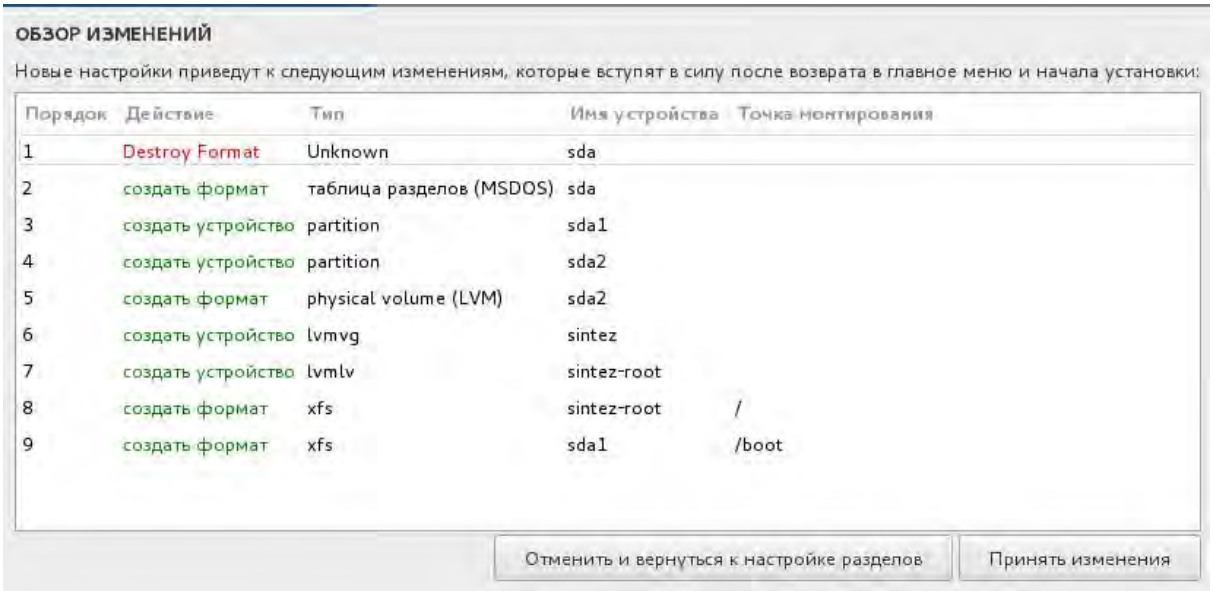


Рисунок 3.8 - Окно «Обзор изменений»

3.2.1.2. Конфигурирование сети и имени узла

Конфигурирование сети и имени узла производится после нажатия на пиктограмму «Сеть и имя узла» (Рисунок 3.9).

Рисунок 3.9 – Окно «Обзор установки»

Откроется окно «Сеть и имя узла» (Рисунок 3.10).

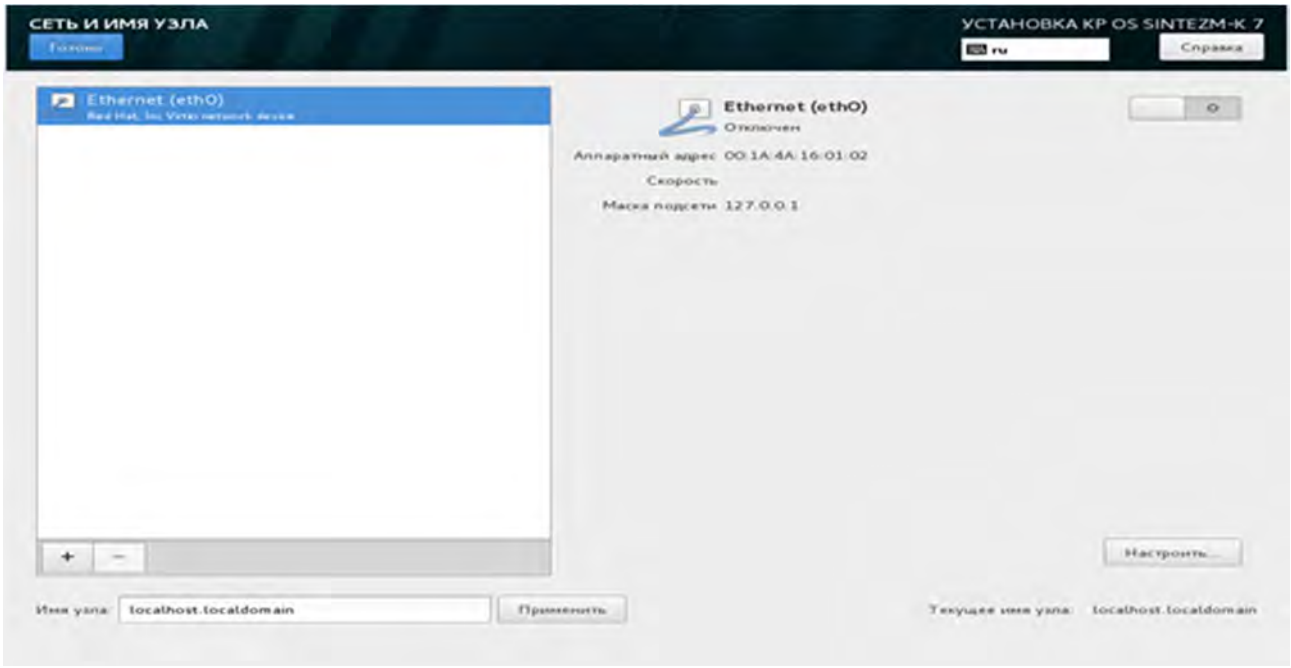


Рисунок 3.10 - Окно «Сеть и имя узла»

Локально доступные сетевые интерфейсы автоматически распознаются программой установки и не могут быть добавлены или удалены вручную. Обнаруженные сетевые интерфейсы перечислены в левой панели.

Для – переместить переключатель в верхнем правом углу экрана настройки в положение «I»;

– ввести «имя узла» для этого компьютера в левой нижней части экрана.

Примечание: в данной установке будут использоваться параметры, указанные в таблице 3.1. Так же, в имени хоста должен содержаться домен второго уровня.

Для того, чтобы вручную настроить сетевое подключение, необходимо нажать на кнопку **«Настроить»**, расположенную в правом нижнем углу окна. Откроется диалоговое окно (Рисунок 3.11), предназначенное для настройки выбранного соединения.

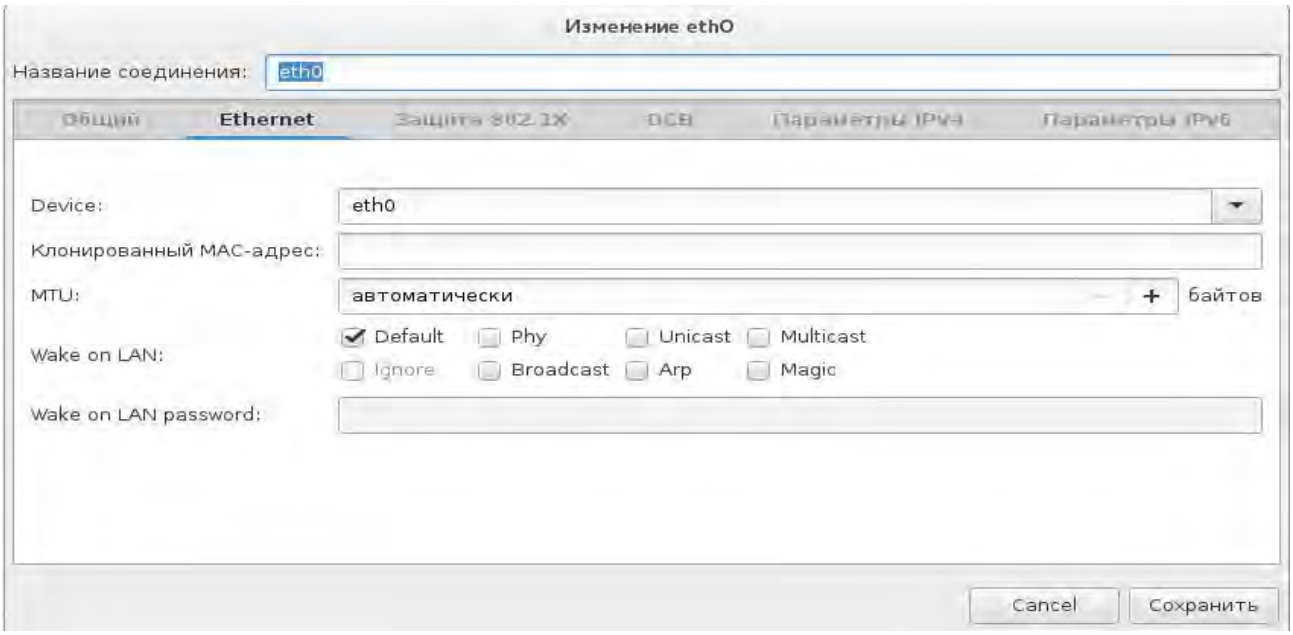


Рисунок 3.11 - Окно параметров Ethernet

Далее необходимо перейти во вкладку «Параметры IPv4» и выбрать в поле «Способ настройки» из ниспадающего списка значение «Вручную». Для добавления адреса необходимо нажать на кнопку **«Добавить»** и ввести IP-адрес, маску сети и

шлюз. В строке DNS необходимо прописать адрес сервера управление доступом

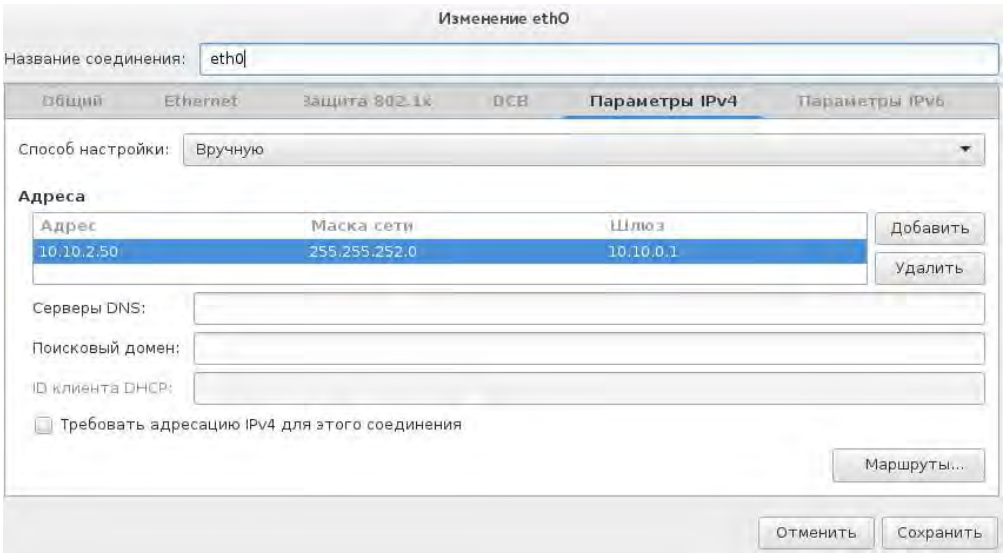


Рисунок 3.12 - Окно «Изменение соединения». Вкладка «Параметры IPv4»

Далее необходимо перейти во вкладку «Параметры IPv6» (Рисунок 3.13) и выбрать в поле «Способ настройки» из ниспадающего списка значение «Игнорировать».

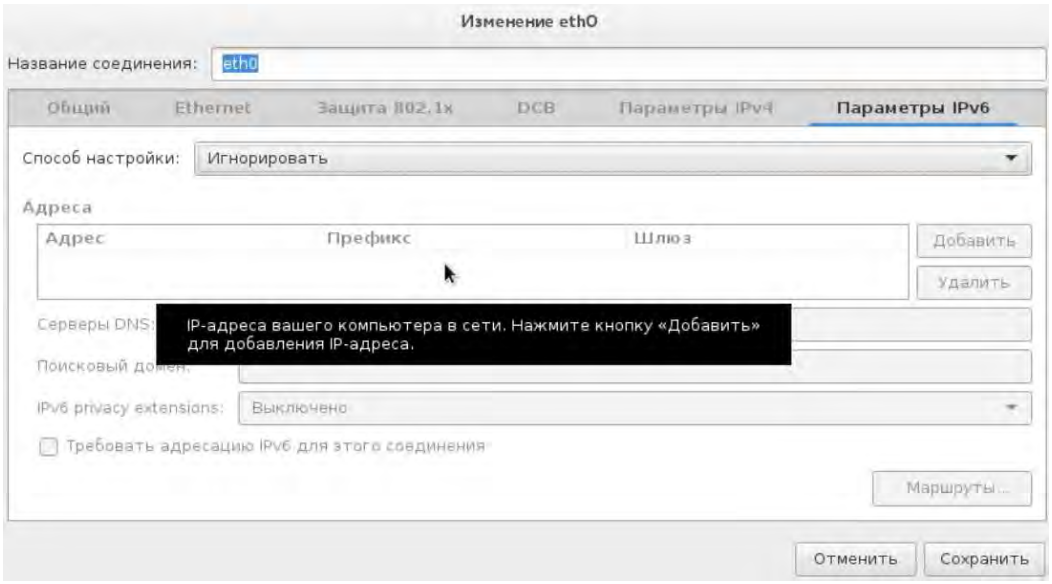


Рисунок 3.13 – Окно «Изменение соединения». Вкладка «Параметры IPv6»

Далее необходимо перейти во вкладку «Общий» (Рисунок 3.14) и выставить маркер «Автоматически подключаться к этой сети, когда она доступна» и нажать на кнопку «**Сохранить**».

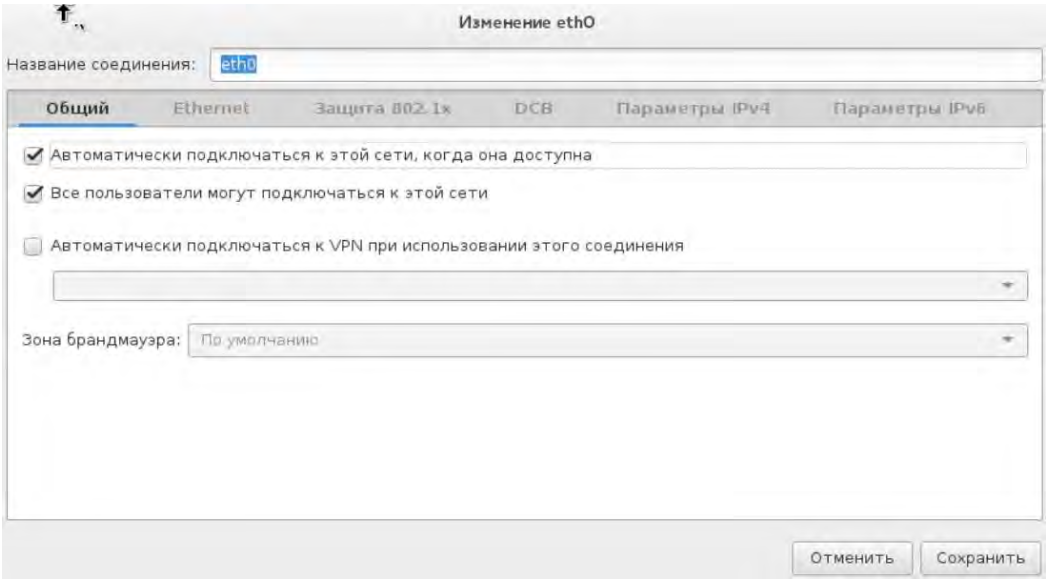


Рисунок 3.14 – Окно «Изменение соединения». Вкладка «Общий»

Примечание: если проводилась перенастройка устройства, которое было уже активно во время установки, то его необходимо перезагрузить, используя переключатель в верхнем правом углу экрана настройки (ВКЛ/ВЫКЛ).

В поле «Имя узла», расположенном в левом нижнем углу окна «Сети и имя узла» необходимо указать полное имя узла согласно таблице 3.1. При этом флаг выбора должен быть активирован .

После окончания всех сетевых настроек нажать на кнопку «Готово», р

а

с

П

о

л

о

ж

е

н

н

у

ю

3.2.1.3. Назначение региональных настроек

Настройка даты и времени производится после нажатия на пиктограмму «Дата и время» (в окне «Обзор установки» см. Рисунок 3.4). Откроется окно выбора часового пояса (Рисунок 3.15).

Для выбора часового пояса необходимо выполнить одно из следующих действий:

– с помощью мыши нажать на интерактивную карту, чтобы выбрать конкретный город;

– пролистать регионы и города в раскрывающихся меню в верхней части окна.

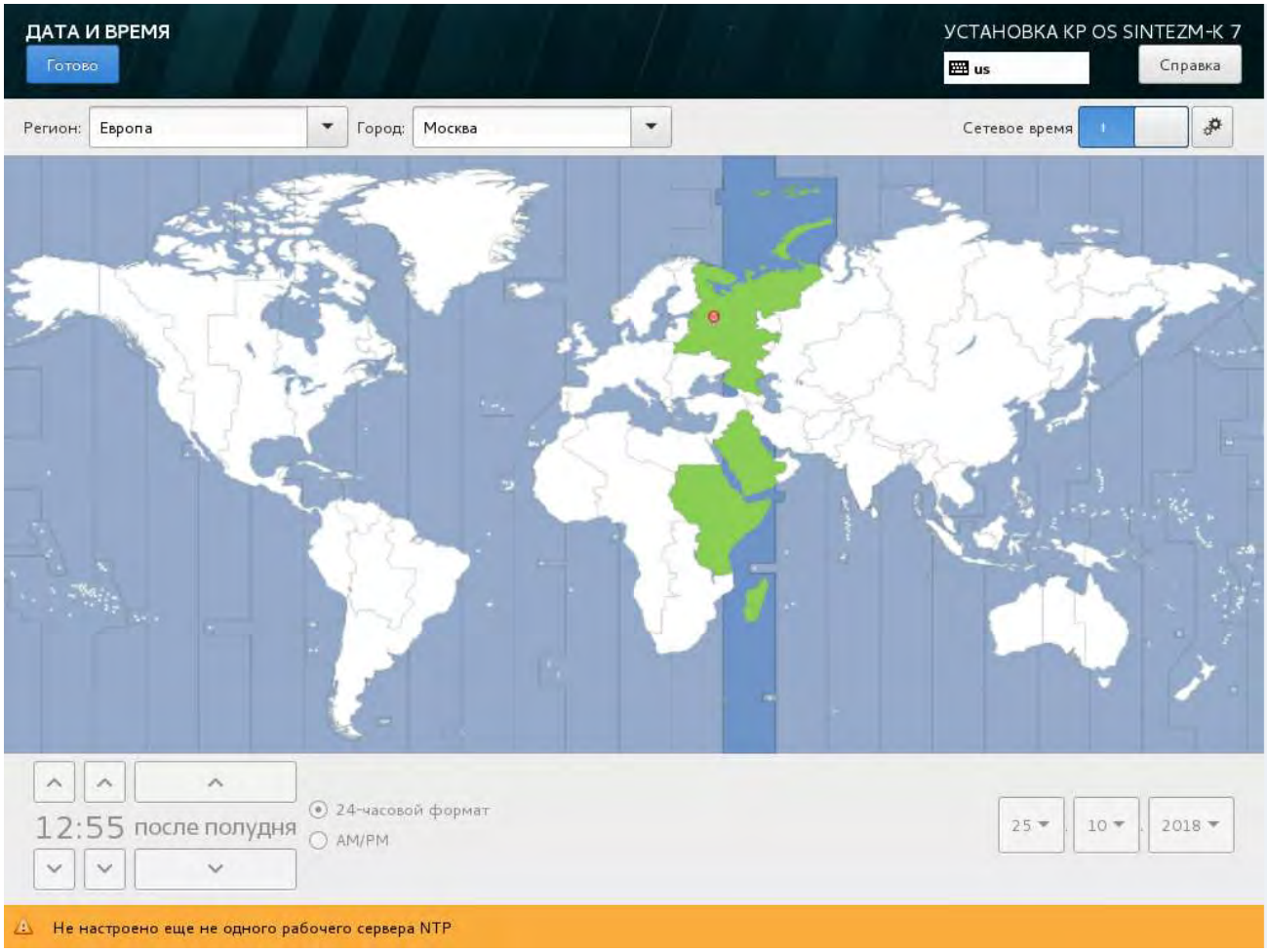


Рисунок 3.15 – Окно «Дата и время»

Примечание: если необходимый город отсутствует на карте или в выпадающем меню, необходимо выбрать ближайший крупный город в том же часовом поясе.

После проведения настройки необходимо нажать на кнопку **«Готово»**, расположенную в верхнем левом углу окна.

Если в системе используется удаленный сервер времени, необходимо ввести данные о нем. Для этого необходимо нажать на кнопку, содержащую изображение шестеренок, расположенную в верхней правой части окна. В появившемся окне серверов времени и добавить необходимые данные сервера: IP-адрес или доменное имя.

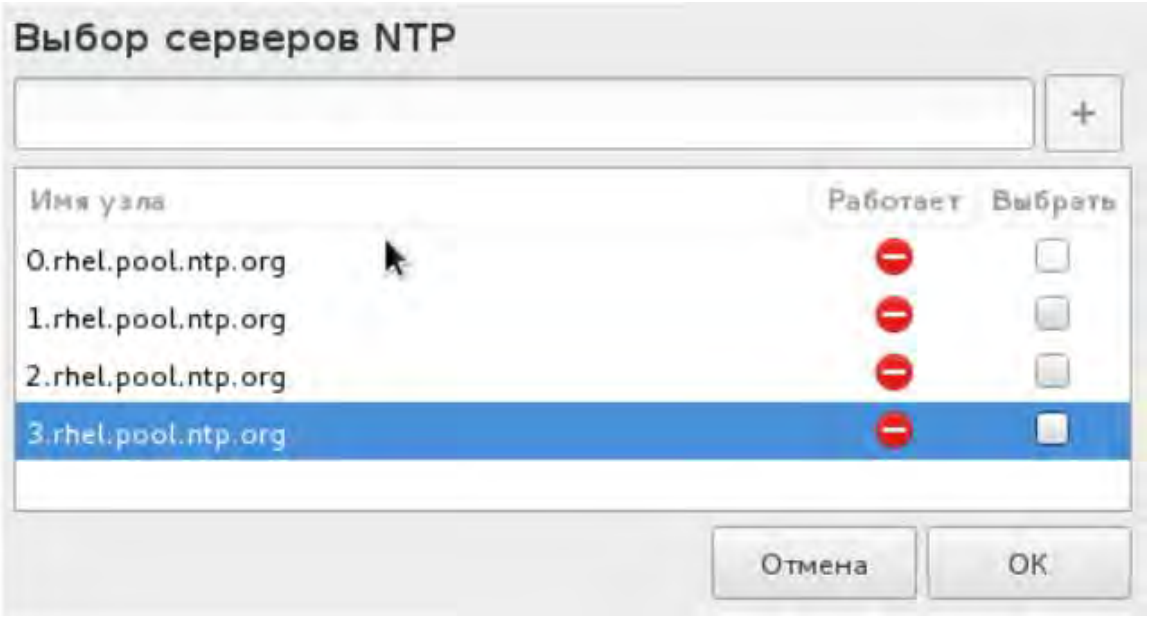


Рисунок 3.16 – Окно «Выбор серверов NTP»

Для добавления сервера необходимо в поле ввода ввести IP-адрес соответствующего сервера и нажать на кнопку «+», расположенную в правой верхней части окна.

Также можно не добавлять новые сервера времени, а изменить стандартные. Возможность изменения, предоставляется путем двойного нажатия на имя соответствующего узла.

После выбора всех необходимых серверов времени необходимо нажать на кнопку «**ОК**».

После завершения настройки даты и времени необходимо нажать на кнопку

3.2.1.4. Запуск установки ОС

После проведения всех указанных настроек необходимо нажать на кнопку **Начать установку**» (Рисунок 3.17).

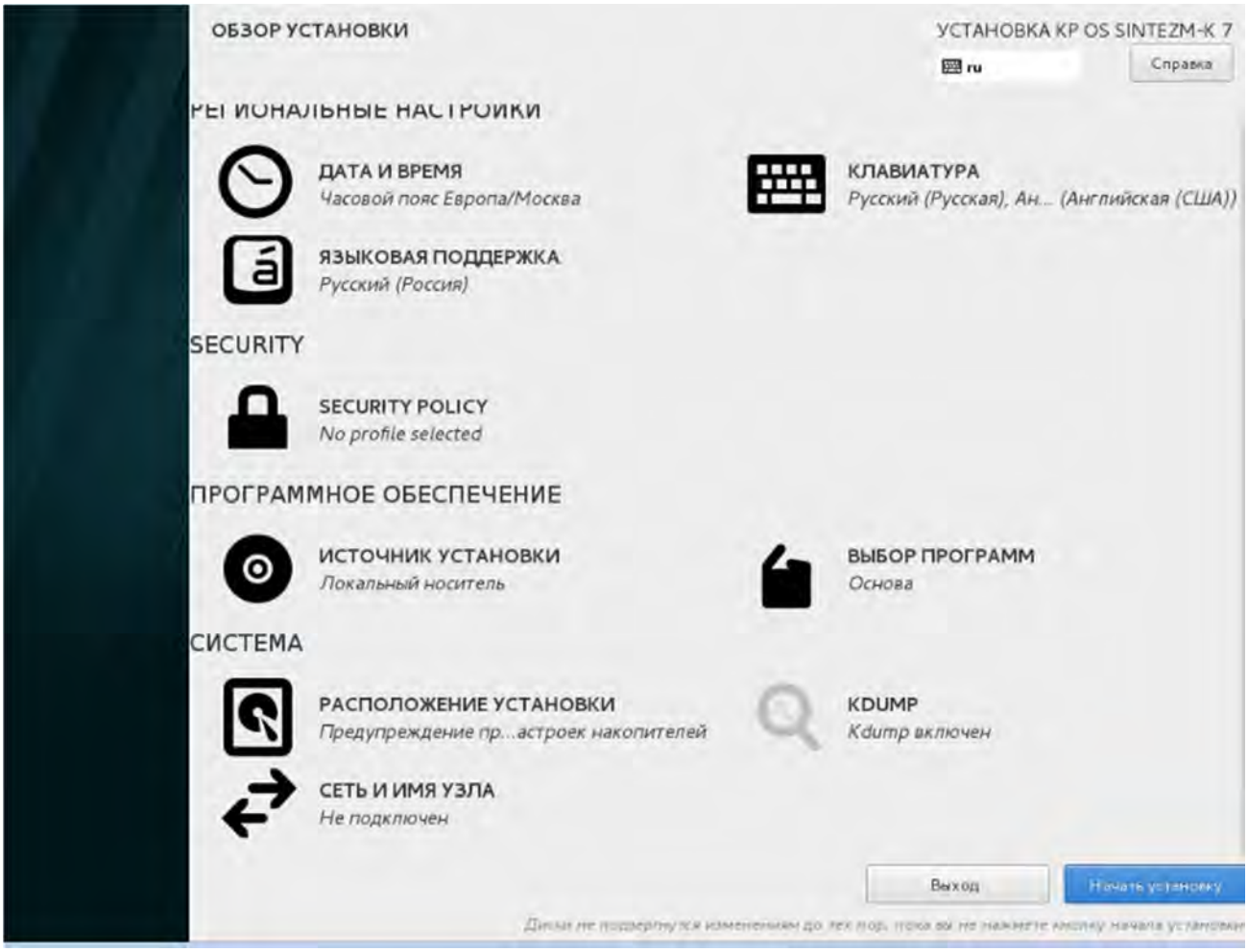


Рисунок 3.17 – Окно «Обзор установки»

Откроется окно, содержащее сведения о процессе установки системы (Рисунок

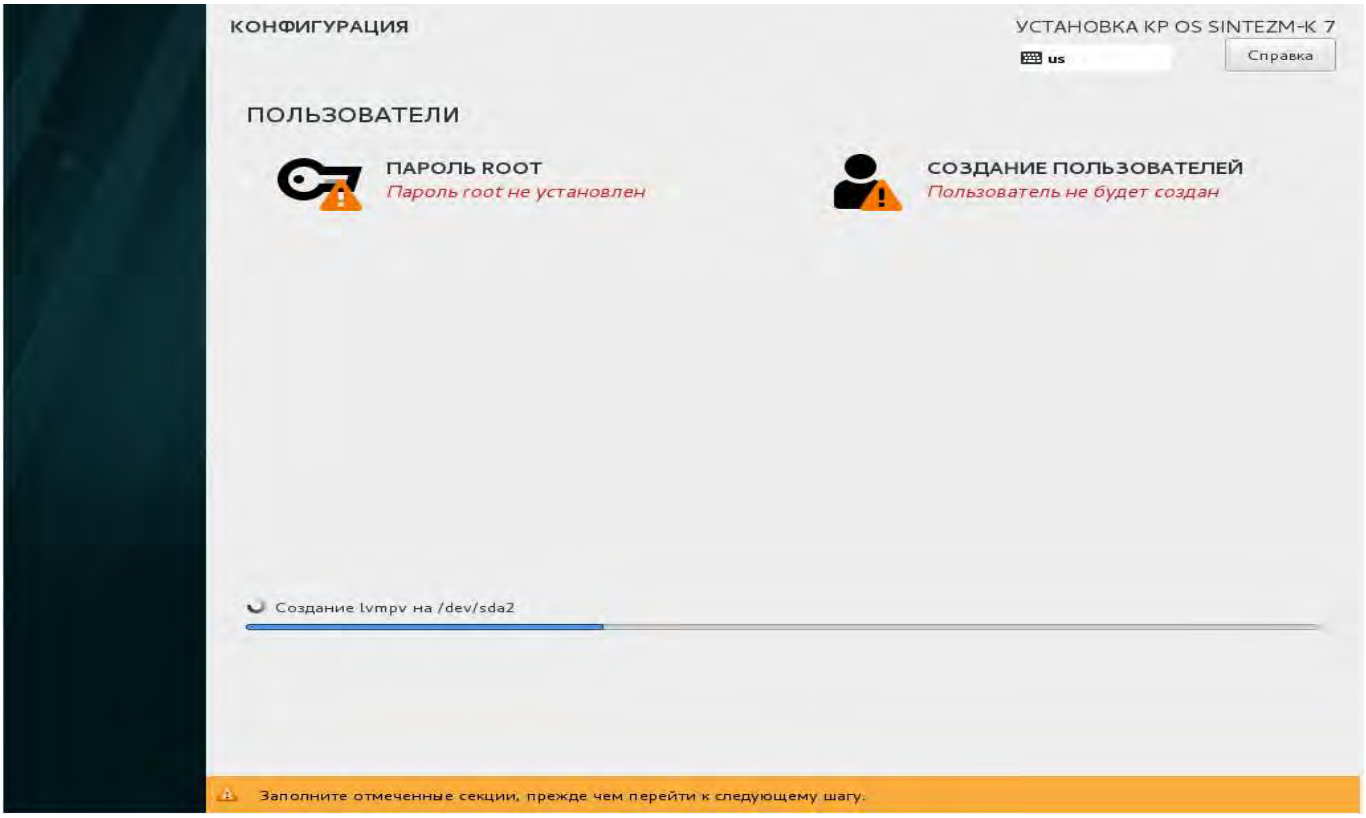


Рисунок 3.18 - Окно «Конфигурация»

Во время процесса установки пакетов необходимо установить пароль системного пользователя root. Для этого, необходимо нажать на кнопку «Пароль root». Пароль системного пользователя root должен быть не короче 8 символов с применением символов верхнего и нижнего регистров и цифр, при этом вводимые символы не отображаются на экране (Рисунок 3.19). Необходимо ввести его дважды, если пароли не совпадают, программа установки запросит повторный ввод пароля.

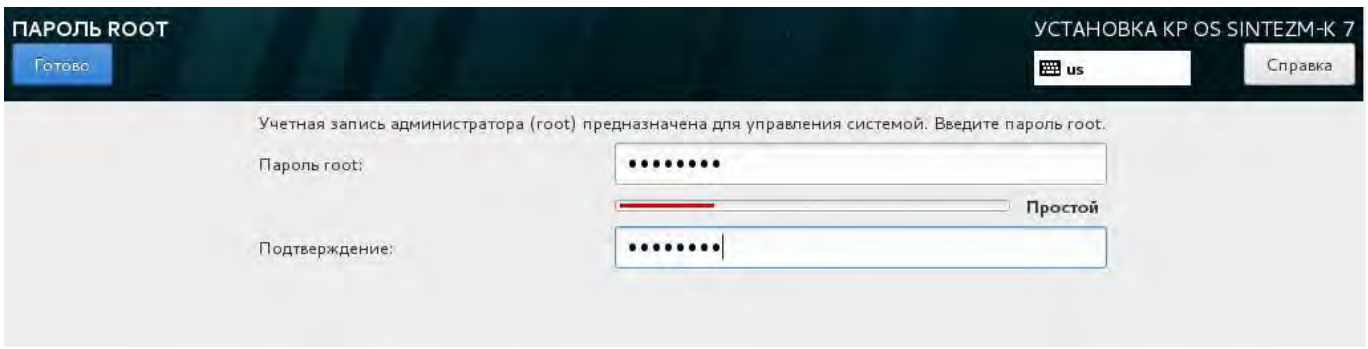


Рисунок 3.19– Окно настройки пароля root

В случае несоответствия пароля root необходимым требованиям, предъявляемым к стойкости пароля, будет отображено сообщение:

«Слабый пароль! Пароль не прошел проверку орфографии. Слишком простой. Для подтверждения дважды нажмите «Готово».

После завершения установки необходимо перезагрузить систему, для этого необходимо нажать на кнопку «Перезагрузка».

3.2.1.5. Настройка базовой конфигурации

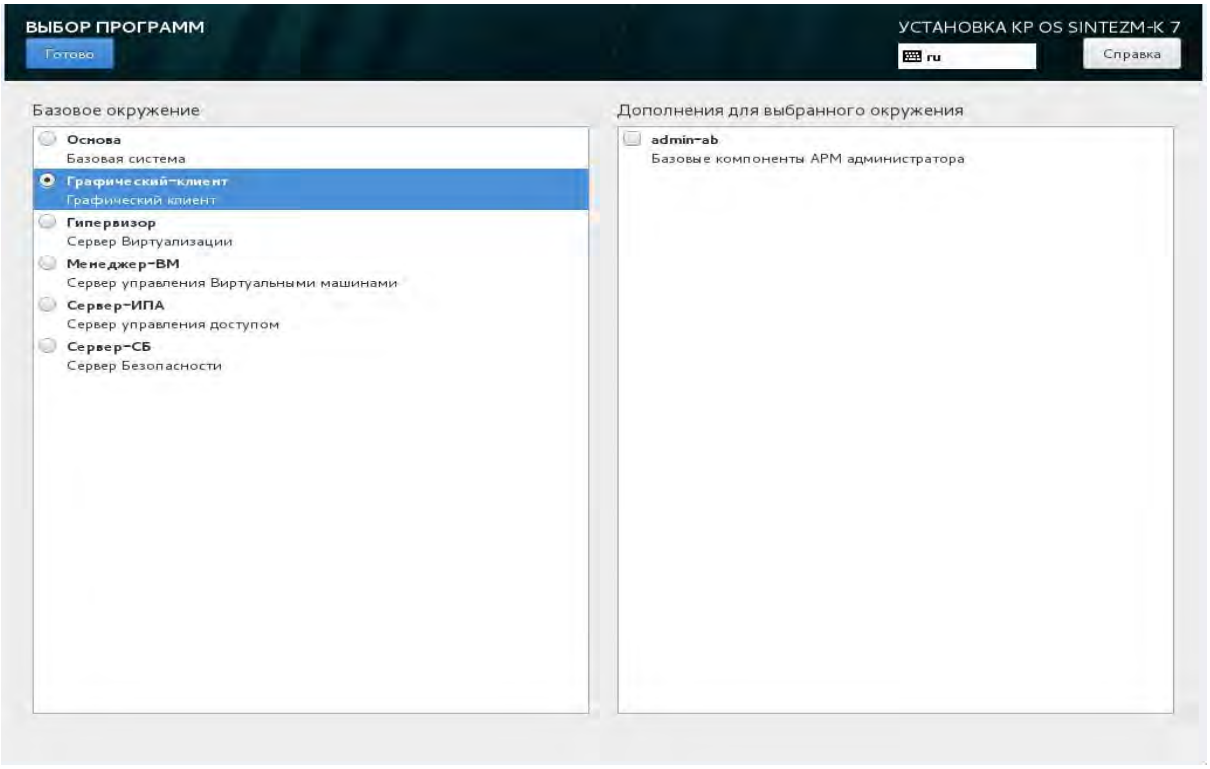
Настройка базовой конфигурации осуществляется в соответствии с используемой конфигурацией КП «ЗОС «СинтезМ» согласно п. 3.7 «Применение

При использовании КП «ЗОС «СинтезМ» в конфигурации «Операционная система» настройка базовой конфигурации осуществляется в соответствии с ролью технического средства согласно п. 3.7.1 «Применение базового набора конфигураций

При использовании КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» настройка базовой конфигурации осуществляется в соответствии с ролью технического средства согласно п. 3.7.2 «Применение базового набора

3.2.2. Установка Клиентской операционной системы

Для установки Клиентской операционной системы необходимо произвести действия описанные в пункте 3.1 данной инструкции, после чего в окне «Выбор Программ» в качестве базового окружения выбрать позицию «Графический-клиент» (Рисунок 3.20).



Примечание. Для установки Клиентской ОС для администратора (для конфигурации «Среды виртуализации») необходимо дополнительно выбрать дополнение «admin-ab» в панели «Дополнения для выбранного окружения».

Примечание. Для функционирования КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» необходимо помимо действий описанных ниже произвести предварительные настройки, описанные в п. 3.4.1.4 «Предварительная настройка ОС»

3.2.2.1. Настройка места установки для клиентской ОС

Установка изделия может производиться на локальный, в этом случае необходимо выбрать соответствующее устройство в поле «Локальные диски», или на сетевой диск. Выбор дисков и разделов производится после нажатия на пиктограмму «Расположение установки» (в окне «Обзор установки» см. Рисунок 3.4). В открывшемся окне (Рисунок 3.21) необходимо выбрать диск, на который будет производиться установка ОС. Далее в нижней части окна выбрать параметр «Я настрою разделы» и нажать на кнопку **«Готово»**.

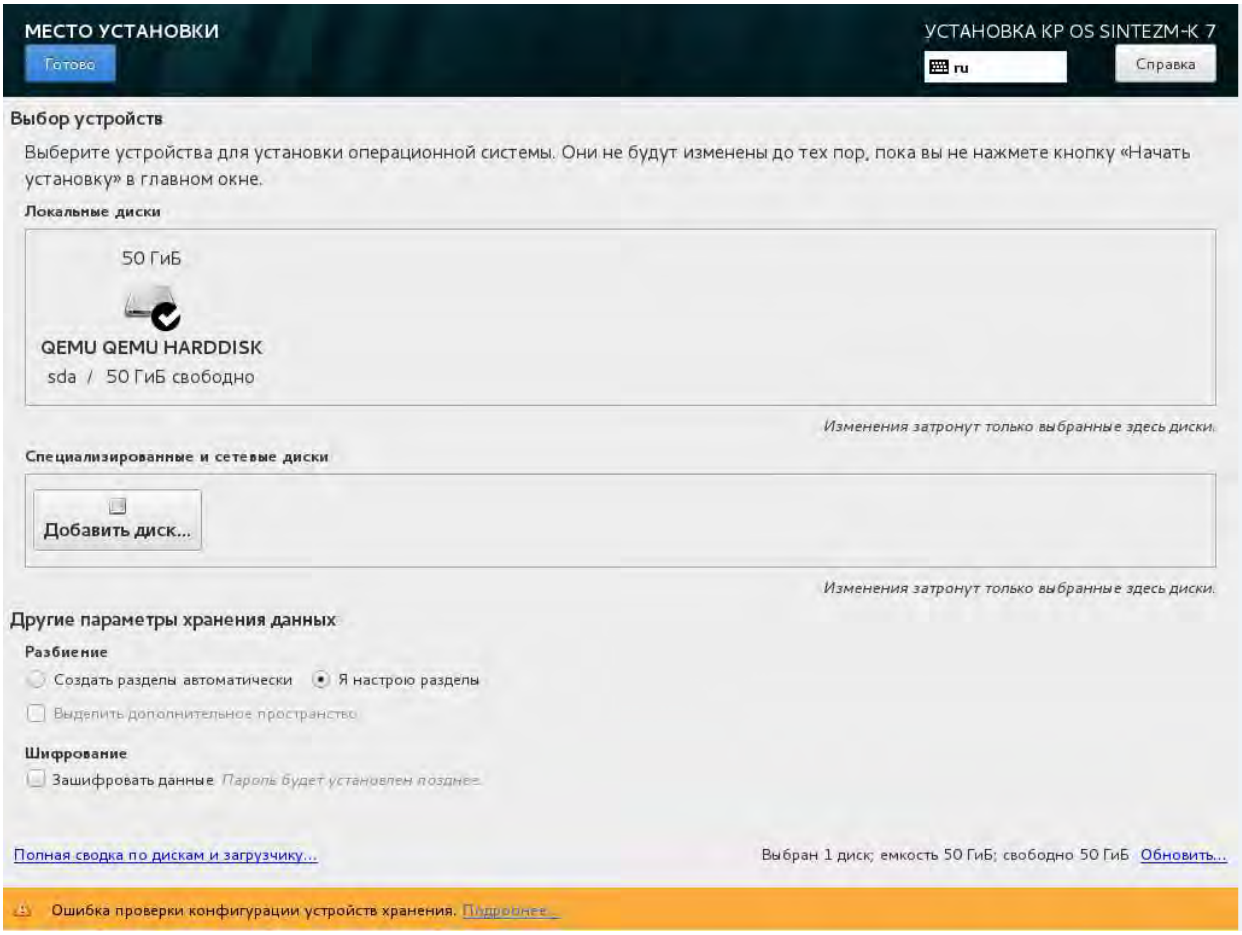


Рисунок 3.21 - Окно выбора создания разделов клиентской ОС

Следующим шагом необходимо произвести настройку разделов изменить структуру логических томов (Рисунок 3.22). Для этого необходимо раскрыть выпадающий список «Новая установка OS SINTEZM-K» и выбрать «Создать их автоматически».

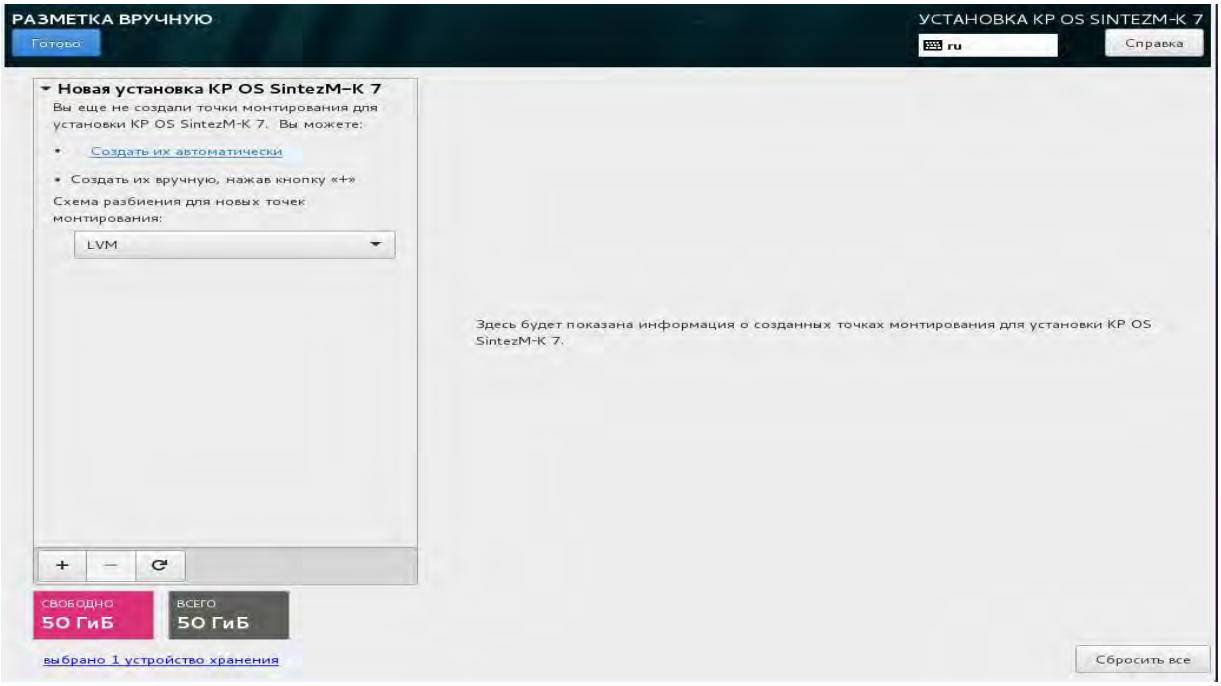


Рисунок 3.22 – Настройка разделов

По умолчанию программа создает логические тома: «swap», «/home», «/», boot», которые необходимо отредактировать. Для этого, необходимо:

– выбрать том «/home», после чего нажать на кнопку [–] **«Удалить»**;

– выбрать том «/swap», после чего нажать на кнопку [–] **«Удалить»**.

Далее необходимо изменить размер тома «/» для этого, необходимо:

– выбрать том «/», в правой части окна;

– в поле «Требуемый размер» задать необходимый для установки размер тома (рекомендуется задать размер тома «/» не менее 10Гб);

– нажать кнопку «Применить».

Оставшееся место на диске необходимо распределить в директорию «/home». Для этого необходимо:

– нажать кнопку [+] «Добавить»;

– в открывшемся окне «Создание точки монтирования» (Рисунок 3.23), в выпадающем списке «Точка монтирования» необходимо выбрать «/home»;

– поле «Размер» можно оставить пустым, в результате чего всё свободное место будет выделено данному разделу;

– нажать на кнопку «Добавить».

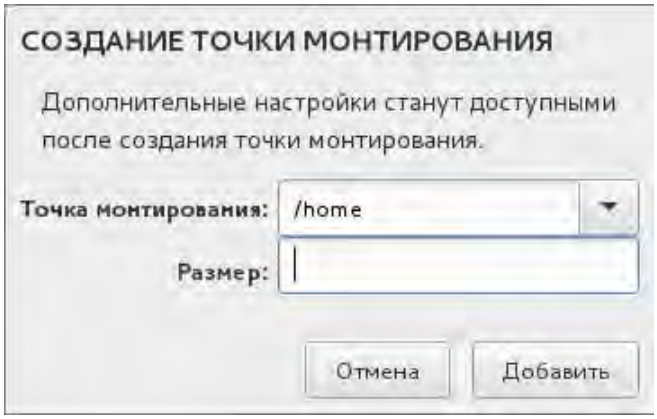


Рисунок 3.23 - Окно «Создание точки монтирования»

В результате проделанных действий разметка диска должна быть аналогична представленной на рисунке 3.24.

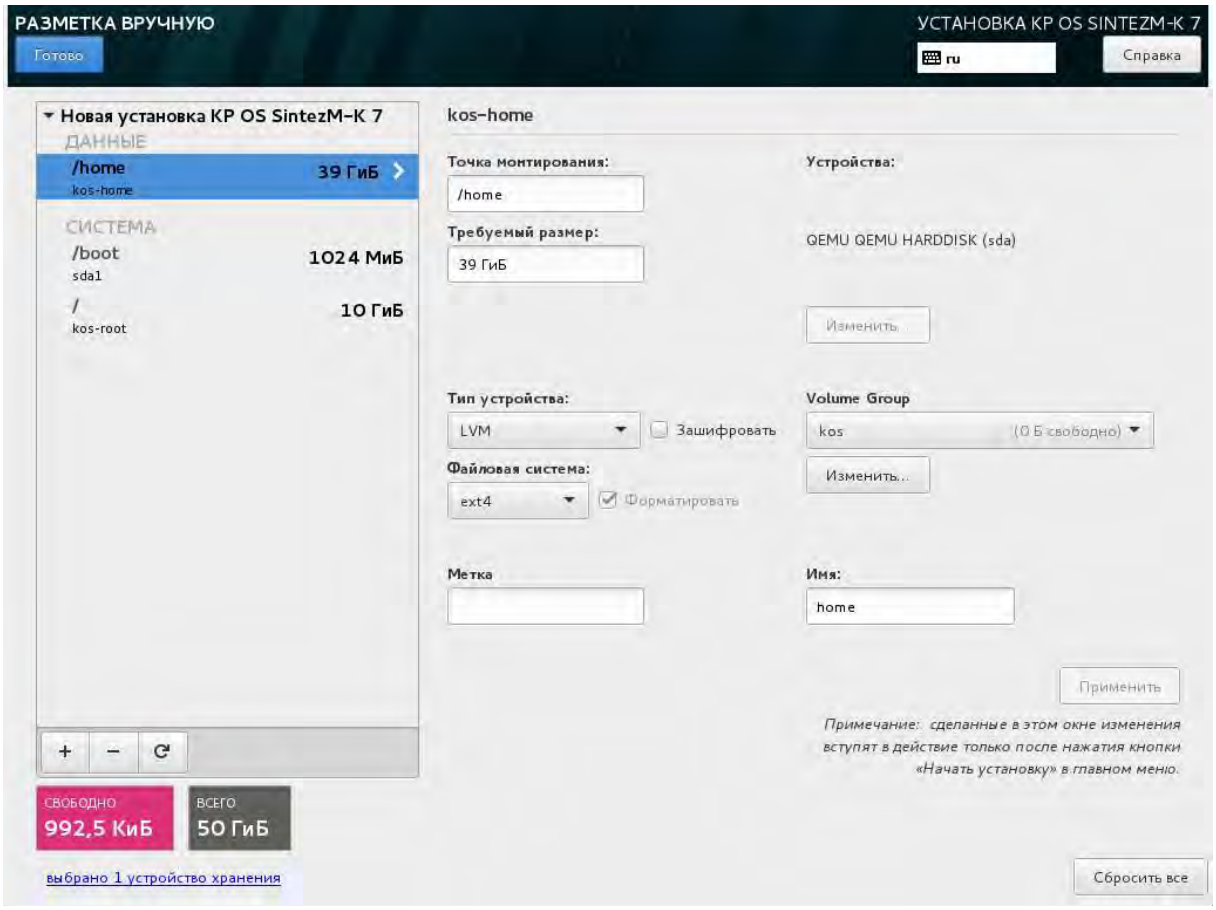


Рисунок 3.24 – Окно «Разметка вручную»

Для завершения разметки диска необходимо нажать на кнопку «**Готово**», после чего, в открывшемся окне «Обзор изменений» (Рисунок 3.25) необходимо нажать на кнопку «Принять изменения».

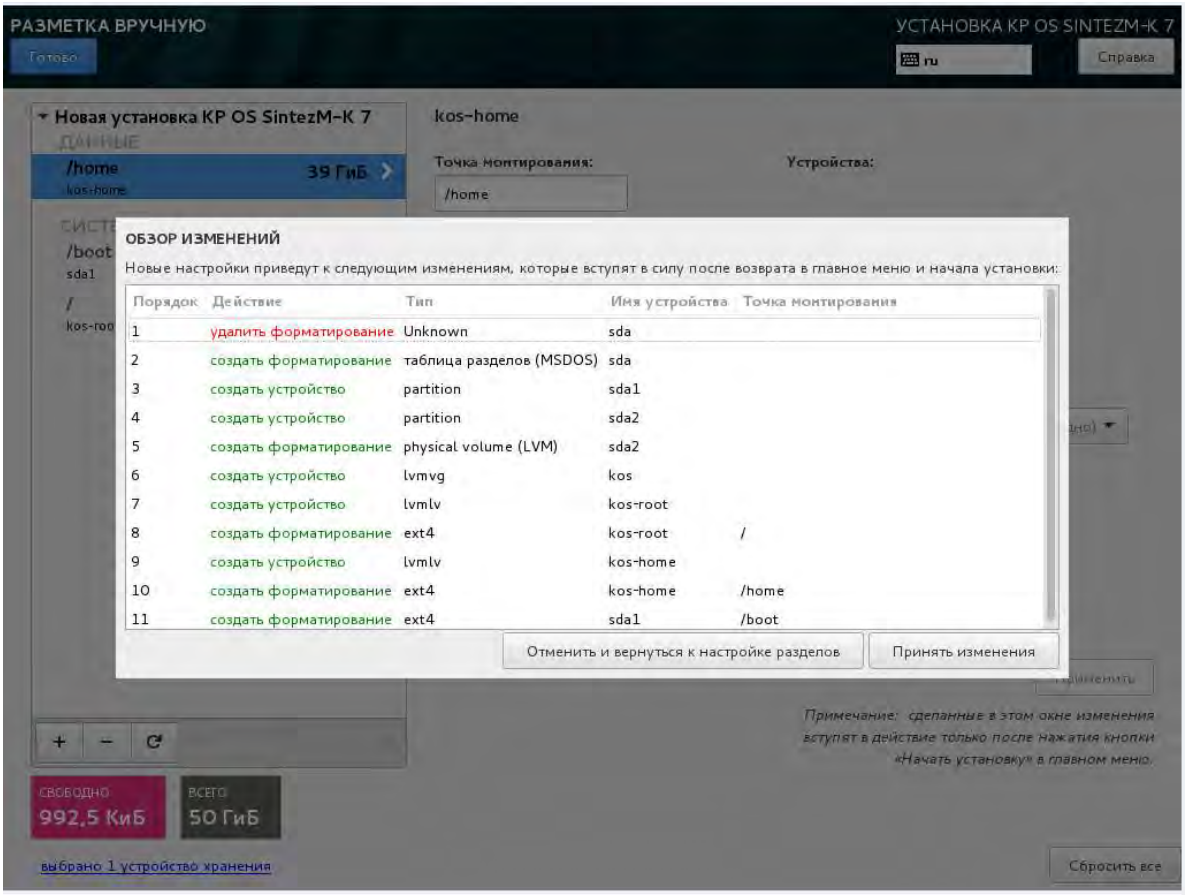


Рисунок 3.25 - Окно «Обзор изменений»

3.2.2.2. Конфигурирование сети и имени узла

Конфигурирование сети и имени узла при установке клиентской ОС производится аналогично порядку, описанному в пункте 3.2.1.2.

3.2.2.3. Назначение региональных настроек

Настройка даты и времени при установке клиентской ОС производится аналогично порядку, описанному в пункте 3.2.1.3.

3.2.2.4. Запуск установки ОС

Запуск установки ОС при установке клиентской ОС производится аналогично порядку, описанному в пункте 3.2.1.4.

3.2.2.5. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с используемой конфигурацией КП «ЗОС «СинтезМ» согласно п. 3.7 «Применение

н

а

б

о

При использовании КП «ЗОС «СинтезМ» в конфигурации «Операционная система» настройка базовой конфигурации осуществляется в соответствии с ролью технического средства согласно п. 3.7.1 «Применение базового набора конфигураций

При использовании КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» настройка базовой конфигурации осуществляется в соответствии с ролью технического средства согласно п. 3.7.2 «Применение базового набора

3.3. Установка АРМ Администратора

АРМ Администратора – это роль КП «ЗОС «СинтезМ», обеспечивающая управление атрибутами безопасности пользователя. Установка АРМ Администратора может осуществляться как на рабочую станцию, так и на ВМ.

В рамках данной инструкции при развёртывании АРМ Администратора будут использованы параметры, представленные в Таблица 3.5.

Установка и настройка АРМ Администратора осуществляется аналогично установке клиентской ОС описанной в п. 3.2.2.

При этом необходимо помнить, что для установки Клиентской ОС для администратора необходимо выбрать дополнение «admin-ab» в панели «Дополнения для выбранного окружения».

3.3.1. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с используемой конфигурацией КП «ЗОС «СинтезМ» согласно п. 3.7 «Применение

При использовании КП «ЗОС «СинтезМ» в конфигурации «Операционная система» настройка базовой конфигурации осуществляется в соответствии с ролью технического средства согласно п. 3.7.1 «Применение базового набора конфигураций

При использовании КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» настройка базовой конфигурации осуществляется в соответствии с

ролью технического средства согласно п. 3.7.2 «Применение базового набора конфигурации «Среда виртуализации» в соответствии с пунктом 3.13.7 данной инструкции.

3.3.2. Настройка централизованного аудита

Настройка централизованного аудита осуществляется при использовании

3.4. Установка среды виртуализации

Установка КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» может производиться на сервера, АРМ и ВМ (за исключением сервера виртуализации).

3.4.1. Установка и настройка сервера виртуализации

Сервер виртуализации (гипервизор) — это роль КП «ЗОС «СинтезМ», обеспечивающая функционирование среды виртуализации. Установка сервера виртуализации осуществляется на физический сервер с поддержкой аппаратной виртуализации.

Для установки Сервера виртуализации необходимо произвести действия описанные в пункте 3.1 данной инструкции, после чего в окне «Выбор программ» в качестве базового окружения выбрать позицию «Гипервизор» (Рисунок 3.26).

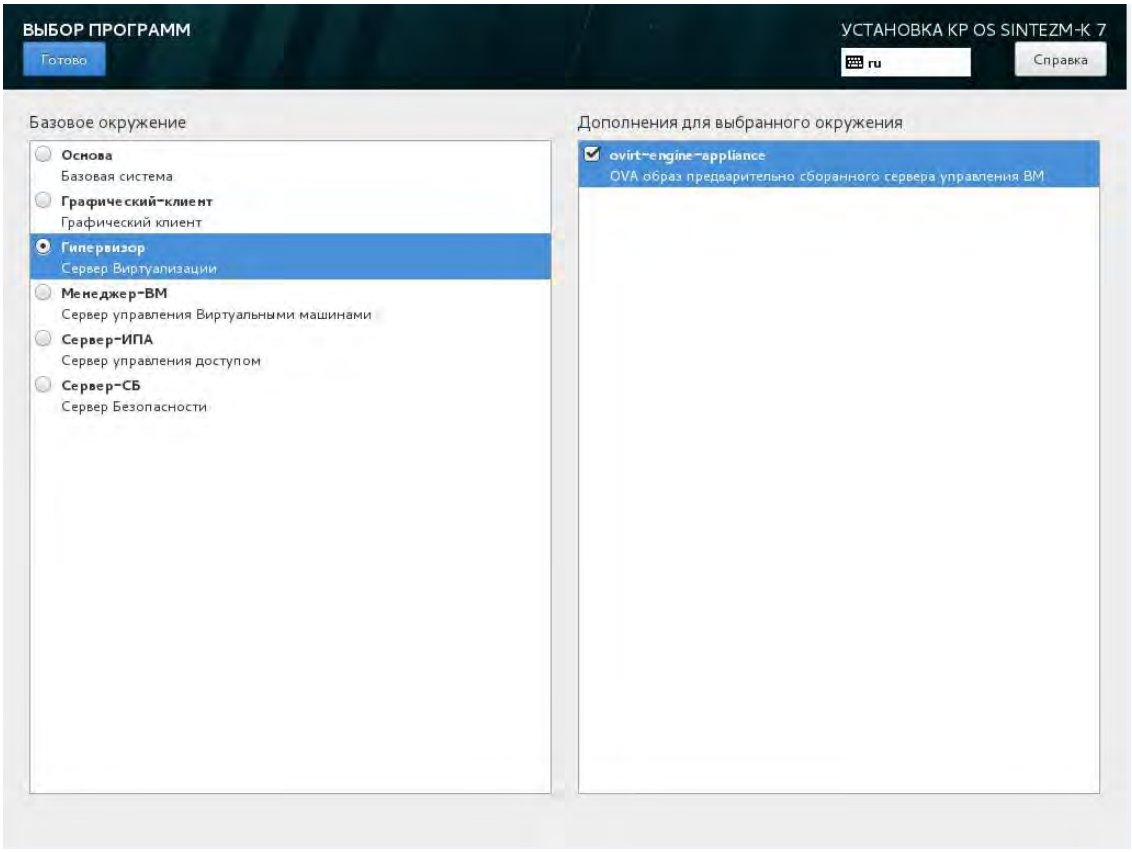


Рисунок 3.26 – Установка сервера виртуализации

Примечание. Для последующего развертывания Менеджера ВМ в среде виртуализации работающего по технологии self-hosted engine необходимо на любом из серверов виртуализации из состава кластера дополнительно установить флаг выбора напротив позиции «ovirt-engine-appliance».

3.4.1.1. Настройка места установки для сервера виртуализации

Настройка места установки при установке сервера виртуализации производится аналогично порядку, описанному в пункте 3.2.1.1.

3.4.1.2. Конфигурирование сети и имени узла

Конфигурирование сети и имени узла при установке сервера виртуализации производится аналогично порядку, описанному в пункте 3.2.1.2.

3.4.1.3. Назначение региональных настроек

Настройка даты и времени при установке сервера виртуализации производится аналогично порядку, описанному в пункте 3.2.1.3.

3.4.1.4. Предварительная настройка ОС

Для функционирования КП «ЗОС «СинтезМ» в конфигурации «Среда виртуализации» необходимо осуществить предварительную настройку. Для настройки ОС необходимо авторизоваться пользователем root локально или по протоколу ssh.

Параметры для конфигурационных файлов представлены в «Таблица 3.2».

Сперва необходимо добавить узлы Сервера управления доступом и самого СВТ в файл /etc/hosts, выполнив следующую команду «vim /etc/host». В конце файла добавить соответствующие адреса, указанные в таблице 3.1.

Примечание. Предварительная настройка ОС осуществляется с использованием «Краткой инструкции по использованию редактора vim».

Пример формата записи в файле /etc/host:

```
10.10.10.83 sintezm-arm1.fintech.ru
10.10.10.73 sintezm-ipa.fintech.ru
```

Затем необходимо добавить IP-адрес Сервера управления доступом в файл /etc/resolv.conf, параметру **nameserver**. Для это выполняется команда:

```
vim /etc/resolv.conf
```

Данный файл приводится к виду:

```
generated by /usr/sbin/dhclient-script
nameserver 10.10.10.73
search fintech.ru
```

Необходимо настроить на гипервизоре дату и время (если это не сделали при установке ОС). Для того чтобы настроить дату и время необходимо открыть консоль сервера.

Примечание:

1. Консолью может служить монитор, подключенный к серверной стойке, или KVM-консоль. При наличии ноутбука возможно произвести настройку удаленно подключившись к серверу по протоколу ssh.

2. Все настройки сервера необходимо производить в режиме командной строки (консоли) с использованием стандартного текстового редактора vim.

Также следует убедиться, что расхождение во времени между Сервером управления доступом и СВТ должно быть не более 60 с. Для проведения настройки необходимо в консоли ввести следующую команду для проверки времени:

```
# date
```

Пример:

В результате выполнения команды отобразятся сведения следующего формата:

```
Thu Dec 22 00:00:00 EST 2016
```

Значение EST показывает часовую зону расположение сервера. В приведенном примере значение EST обозначает европейское стандартное время.

Для указания часового пояса по месту расположения сервера необходимо ввести следующую команду:

```
timedatectl set-timezone Регион/Город
```

Пример:

Указание московского часового пояса:

```
timedatectl set-timezone Europe/Moscow
```

Для указания даты и времени необходимо выполнить следующую команду:

```
date ММДДччмм,
```

где ММ – месяц, ДД – день, чч – час, мм – минуты.

Пример:

```
date 05241200
```

Для синхронизации аппаратного времени (время сервера т.е. BIOS) необходимо выполнить следующую команду:

```
hwclock -w
```

Для настройки данного сервиса необходимо открыть файл настроек с использованием стандартного текстового редактора vim, выполнив команду:

```
vim /etc/chrony.conf
```

В открывшемся файле необходимо найти следующие строки:

```
#allow 192.168/16
#local stratum 10
```

В указанных строка необходимо убрать комментарий изменить данные подсети и маски на соответствующие адреса.

Пример:

```
allow 10.10.10.0/24
local stratum 10
```

Далее изменить строку:

`server 127.127.1.0 iburst` на следующие значения:

```
server 127.127.1.0 minpoll 1 maxpoll 1 iburst prefer
```

Далее изменить строку:

`makestep 10 3` на следующие значения:

```
makestep 0.1 -1
```

После чего перезапустить сервис chronyd:

```
systemctl restart chronyd.service
```

3.4.1.5. Настройка сервера виртуализации

После окончания предварительной настройки ОС и перезагрузки сервера необходимо провести настройку сервера виртуализации.

Выключение протокола IPv6

Для выключения протокола IPv6 необходимо изменить параметры файла /etc/sysctl.conf путем редактирования. Установить:

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

После изменения конфигурации файла выполнить команду:

```
sysctl -p
```

Настройка сервера времени

В данной конфигурации сервер виртуализации выступает в качестве внешнего источника времени для АРМ и ВМ. Его настройка осуществляется через редактирование файла /etc/chrony.conf, которое описано в п 3.20.1 «Настройка Службы единого времени chrony в качестве сервера точного времени» данной инструкции. В данной конфигурации стенда используется сервер синхронизации времени (NTP). В результате файл /etc/chrony.conf должен выглядеть следующим образом:

```
# These servers were defined in the installation:
server 127.127.1.0 iburst
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
# Ignore stratum in source selection.
stratumweight 0
# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
# Enable kernel RTC synchronization.
rtcsync
# In first three updates step the system clock instead of slew
# if the adjustment is larger than 10 seconds.
makestep 10 3
# Allow NTP client access from local network.
allow 10.10.10.0/24
# Listen for commands only on localhost.
bindcmdaddress 127.0.0.1
bindcmdaddress ::1
# Serve time even if not synchronized to any NTP server.
local stratum 10
keyfile /etc/chrony.keys
# Specify the key used as password for chronyc.
commandkey 1
# Generate command key if missing. Generatecommandkey
# Disable logging of client accesses. noclientlog
# Send a message to syslog if a clock adjustment is larger than 0.5
seconds.
logchange 0.5
logdir /var/log/chrony
#log measurements statistics tracking
```

Так как на данном стенде гипервизор выступает в качестве сервера времени как для АРМ, так и для ВМ, то необходимо в правила сервиса firewalld добавить правило для разрешения доступа к NTP-серверу. Это осуществляется двумя командами:

```
firewall-cmd --zone=public --add-service=ntp --permanent
firewall-cmd --reload
```

Добавление узла в сервер управления доступом

Примечание. Выполнение данного пункта необходимо осуществить после установки и настройки Сервера управления доступом (см п.3.4.4).

После установки сервера управления доступом узел гипервизора необходимо добавить в сервер управления доступом. Данная операция осуществляется согласно п. 3.5 «Добавление узла в Сервер управления доступом» Руководство системного программиста» (ТАСП.62.01.12.000.005 32). Непосредственно для гипервизора команда добавления узла в сервер управления доступом выглядит следующим образом:

```
ipa-client-install --enable-dns-updates --all-ip-addresses --mkhomedir
-N      --server=sintezm-ipa.fintech.ru      --domain=fintech.ru      --
principal=admin --password=12345678 –unattended --no-ssh
```

3.4.1.6. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с выбранной схемой аутентификации согласно п. 3.7 «Применение набора базовой конфигурации».

3.4.1.7. Настройка централизованного аудита

Примечание: выполнение данного пункта необходимо осуществить после установки и настройки Сервера безопасности (см п. 3.4.5).

Настройка централизованного аудита осуществляется в соответствии с пунктом данной инструкции 3.13.7.

3.4.2. Установка и настройка Менеджера ВМ

Для установки Менеджера ВМ в среде виртуализации работающего по технологии self-hosted engine необходимо при установке сервера виртуализации

установить флаг выбора напротив позиции «ovirt-engine-appliance» и осуществить установку и настройку сервера виртуализации в соответствии с пунктом 3.4.1.

3.4.2.1. Первоначальная настройка

Первоначально необходимо настроить на гипервизоре дату и время (если это не сделали при установке ОС).

Примечания:

1. Консолью может служить монитор, подключенный к серверной стойке, или KVM-консоль. При наличии технической возможности произвести настройку можно удаленно подключившись к серверу по протоколу ssh.

2. Все настройки сервера необходимо производить в режиме командной строки (консоли) с использованием стандартного текстового редактора vim.

Далее необходимо добавить узел гипервизора и менеджера ВМ в файл /etc/hosts, выполнив следующую команду:

```
vim /etc/hosts
```

В рамках данной инструкции в качестве параметров, задаваемых при установке, будет использоваться значения, указанные в таблице 3.1.

Пример формата записи в файле /etc/host:

```
10.10.10.2 sintezm-h.fintech.ru
10.10.10.125 sintezm-m.fintech.ru
```

Визуальное представление описанных действий по редактированию файла hosts представлено на рисунке 3.27.

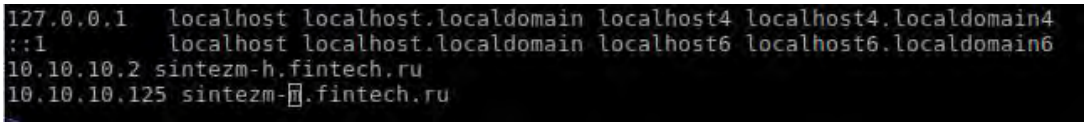


Рисунок 3.27 - Редактирование файла hosts

Для успешной установки Менеджера ВМ необходимо, чтобы в системе была установлена локаль **en_US.UTF8**. Чтобы убедиться в этом, необходимо выполнить команду:

```
locale
```

Если вывод команды показывает другое значение установленного языка, то необходимо выполнить команду:

```
export LANG=en_US.UTF8
```

3.4.2.2. Настройка хранения данных

Для локального хранения данных нужно создать директорию /ovirt командой:

```
mkdir /ovirt
```

Для настройки прав доступа на директорию /ovirt необходимо на гипервизоре ввести следующие команды:

```
chmod 755 /ovirt
chown 36:36 /ovirt
```

Далее необходимо добавить в файл «exports» запись о хранилище – директории, где будут храниться данные, выполнив следующую команду:

```
vim /etc/exports
```

В файле конфигурации /etc/exports необходимо указывать сети или конкретные хосты, которым эти директории доступны, для работы среды виртуализации необходимо чтобы под правило монтирования попадали все гипервизоры и ВМ средства управления средой виртуализации:

Пример формата записи в файле /etc/exports:

```
/ovirt 10.10.10.2(rw)
```

или

```
/
```

или

```
ovirt 10.10.10.0/24(rw,sync)
```

Далее необходимо перезапустить службу nfs, выполнив команду:

```
systemctl restart nfs.service
```

Включить службу в автозагрузку, выполнив команду:

```
systemctl enable nfs.service
```

Визуальное представление описанных действий по перезапуску службы nfs представлено на рисунке 3.28.

Рисунок 3.28 – Перезапуск службы nfs

3.4.2.3. Установка и настройка ВМ менеджера

Менеджер ВМ устанавливается по технологии self-hosted engine, которая обеспечивает работу виртуальной машины в режиме высокой доступности.

Установка виртуальной машины выполняется после первоначальной настройки системы хранения данных и гипервизора (см пп 3.4.2.1, 3.4.2.2).

Для запуска установки необходимо выполнить следующую команду:

```
hosted-engine --deploy
```

Установка осуществляется в режиме “вопрос-ответ”

[INFO] Stage: Initializing

[INFO] Stage: Environment setup

During customization use CTRL-D to abort.

Continuing will configure this host for serving as hypervisor and create a local VM with a running engine.

The locally running engine will be used to configure a storage domain and create a VM there.

At the end the disk of the local VM will be moved to the shared storage.

A

r При появлении данного сообщения необходимо ввести «Yes»

e It has been detected that this program is executed through an SSH connection without using screen.

Continuing with the installation may lead to broken installation if the network connection fails.

y It is highly recommended to abort the installation and run it inside a screen session using command o"screen".

u Do you want to continue anyway? (Yes, No)[No]: **Yes**

При появлении данного сообщения необходимо ввести «Yes»

s Configuration files: []

u Log file: /var/log/ovirt-hosted-engine-setup/ovirt-hosted-engine-setup-20180503114141-

r i1cpv4.log

e Version: otopi-1.7.7 (otopi-1.7.7-1.el7.centos)

y

o

[INFO] Stage: Environment packages setup

[INFO] Stage: Programs detection

[INFO] Stage: Environment setup

[INFO] Stage: Environment customization

--== STORAGE CONFIGURATION ==--

--== HOST NETWORK CONFIGURATION ==--

Please indicate a pingable gateway IP address [10.10.10.2]: **10.10.10.2**

В данном сообщении программой установки запрашивается IP-адрес используемого шлюза. В данной установке необходимо ввести значение «**10.10.10.2**»

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Detecting interface on existing management bridge]

[INFO] skipping: [localhost]

[INFO] TASK [Get all active network interfaces]

[INFO] TASK [Filter bonds with bad naming]

[INFO] TASK [Generate output list]

[INFO] ok: [localhost]

Please indicate a nic to set ovirtmgmt bridge on: (eno2) [eno2]: **eno2**

В данном сообщении программой установки запрашивается физический сетевой интерфейс, который будет использован для создания интерфейса сетевого моста ovirtmgmt. В данной установке используется сетевой интерфейс «**eno2**»

--== VM CONFIGURATION ==--

If you want to deploy with a custom engine appliance image,

please specify the path to the OVA archive you would like to use

(leave it empty to skip, the setup will use ovirt-engine-appliance rpm installing it if missing):

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

[INFO] Detecting host timezone.

Please provide the FQDN you would like to use for the engine appliance.

Note: This will be the FQDN of the engine VM you are now going to launch,

it should not point to the base host or to any other existing machine.

Engine VM FQDN: []: **sintezm-m.fintech.ru**

В данном сообщении программой установки запрашивается полное доменное имя для ВМ менеджера. Для данной установки будет использоваться «**sintezm-m.fintech.ru**»

Please provide the domain name you would like to use for the engine appliance.

Engine VM domain: [fintech.ru]

В данном сообщении программой установки запрашивается домен, в котором будет находиться ВМ менеджера. Для данной установки будет использоваться значение «fintech.ru» предлагаемое в качестве значения по умолчанию (значение по умолчанию рассчитывается на основе полного доменного имени заданного ранее).

Enter root password that will be used for the engine appliance: **12345678**

Confirm appliance root password: **12345678**

В двух вышеуказанных сообщениях запрашивается и подтверждается пароль для доступа пользователю root на ВМ менеджера. Для данной установки будет использоваться пароль: **12345678**

Enter ssh public key for the root user that will be used for the engine appliance (leave it empty to skip):

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

[WARNING] Skipping appliance root ssh public key

Do you want to enable ssh access for the root user (yes, no, without-password) [yes]:

В данном сообщении программой установки запрашивается информация о разрешении доступа пользователю root по ssh на ВМ менеджера. Для данной установки будет использоваться значение по умолчанию «**yes**»

Please specify the number of virtual CPUs for the VM (Defaults to appliance OVF value): [4]:

В данном сообщении программой установки запрашивается информация о количестве виртуальных CPU, которые будут выделены для ВМ менеджера. Для данной установки будет использоваться значение по умолчанию (**4**).

Please specify the memory size of the VM in MB (Defaults to appliance OVF value): [16384]:

В данном сообщении программой установки запрашивается информация о размере ОЗУ, в мегабайтах, которое будет выделено для ВМ менеджера. Для данной установки будет использоваться значение **16384**.

You may specify a unicast MAC address for the VM or accept a randomly generated default [00:16:3e:6b:40:ab]:

В данном сообщении программой установки запрашивается MAC-адрес, который будет выдан ВМ менеджера. В данной установке можно использовать значение по умолчанию (**00:16:3e:6b:40:ab**)

How should the engine VM network be configured (DHCP, Static)[DHCP]: **Static**

В данном сообщении программой установки запрашивается информация о том, как должна быть сконфигурирована сеть внутри ВМ менеджера. В данной установке используется статическая настройка сети. Для этого, необходимо ввести значение **Static**

Please enter the IP address to be used for the engine VM [10.128.150.1]: **10.10.10.125**

В данном сообщении программой установки запрашивается информация о IP-адресе ВМ менеджера. Для данной установки будет использоваться «**10.10.10.125»**

[INFO] The engine VM will be configured to use 10.10.10.125/24

Please provide a comma-separated list (max 3) of IP addresses of domain name servers for the engine VM

Engine VM DNS (leave it empty to skip) []:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

Add lines for the appliance itself and for this host to /etc/hosts on the engine VM?

Note: ensuring that this host could resolve the engine VM hostname is still up to you

(Yes, No)[No] **Yes**

В данном сообщении программой установки запрашивается информация о необходимости прописать в файле /etc/hosts запись о хосте ВМ менеджера. В данной установке необходимо ввести значение «**Yes**».

--== HOSTED ENGINE CONFIGURATION ==--

Please provide the name of the SMTP server through which we will send notifications [localhost]:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу **Enter**

Please provide the TCP port number of the SMTP server [25]:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу **Enter**

Please provide the email address from which notifications will be sent [root@localhost]:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

Please provide a comma-separated list of email addresses which will get notifications [root@localhost]:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

Enter engine admin password: **12345678**

Confirm engine admin password: **12345678**

В двух вышеуказанных сообщениях запрашивается и подтверждается пароль для доступа пользователю admin на web-интерфейс Менеджера ВМ. Для данной установки будет использоваться пароль: **12345678**

[INFO] Stage: Setup validation

[WARNING] Failed to resolve sintezm-h.fintech.ru using DNS, it can be resolved only locally

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

[INFO] Cleaning previous attempts

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Stop libvirt service]

[INFO] changed: [localhost]

[INFO] TASK [Drop vdsm config statements]

[INFO] TASK [Restore initial abrt config files]

[INFO] TASK [Restart abrtd service]

[INFO] changed: [localhost]

[INFO] TASK [Drop libvirt sasl2 configuration by vdsm]

[INFO] changed: [localhost]

[INFO] TASK [Stop and disable services]

[INFO] TASK [Start libvirt]

[INFO] changed: [localhost]

[INFO] TASK [Check for leftover local Hosted Engine VM]

[INFO] changed: [localhost]

[INFO] TASK [Destroy leftover local Hosted Engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Check for leftover defined local Hosted Engine VM]

[INFO] changed: [localhost]

[INFO] TASK [Undefine leftover local engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Remove eventually entries for the local VM from known_hosts file]

[INFO] ok: [localhost]

[INFO] Starting local VM

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Start libvirt]

[INFO] ok: [localhost]

[INFO] TASK [Activate default libvirt network]

[INFO] ok: [localhost]

[INFO] TASK [Get libvirt interfaces]

[INFO] ok: [localhost]

[INFO] TASK [Get routing rules]

[INFO] changed: [localhost]

[INFO] TASK [Save bridge name]

[INFO] ok: [localhost]

[INFO] TASK [Wait for the bridge to appear on the host]

[INFO] changed: [localhost]

[INFO] TASK [Refresh network facts]

[INFO] skipping: [localhost]

[INFO] TASK [Prepare CIDR for virbr0]

[INFO] ok: [localhost]

[INFO] TASK [Add outbound route rules]

[INFO] changed: [localhost]

[INFO] TASK [Add inbound route rules]

[INFO] changed: [localhost]

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Register the engine FQDN as a host]

[INFO] changed: [localhost]

[INFO] TASK [Create directory for local VM]

[INFO] changed: [localhost]

[INFO] TASK [Set local vm dir path]

[INFO] ok: [localhost]

[INFO] TASK [Fix local VM directory permission]

[INFO] changed: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Install ovirt-engine-appliance rpm]

[INFO] ok: [localhost]

[INFO] TASK [Parse appliance configuration for path]

[INFO] changed: [localhost]

[INFO] TASK [Parse appliance configuration for sha1sum]

[INFO] changed: [localhost]

[INFO] TASK [Get OVA path]

[INFO] ok: [localhost]

[INFO] TASK [Compute sha1sum]

[INFO] ok: [localhost]

[INFO] TASK [Compare sha1sum]

[INFO] skipping: [localhost]

[INFO] TASK [Register appliance PATH]

[INFO] skipping: [localhost]

[INFO] TASK [Extract appliance to local VM directory]

[INFO] changed: [localhost]

[INFO] TASK [Find the appliance image]

[INFO] ok: [localhost]

[INFO] TASK [Get appliance disk size]

[INFO] changed: [localhost]

[INFO] TASK [Parse qemu-img output]

[INFO] ok: [localhost]

[INFO] TASK [Create cloud init user-data and meta-data files]

[INFO] TASK [Create ISO disk]

[INFO] changed: [localhost]

[INFO] TASK [Create local VM]

[INFO] changed: [localhost]

[INFO] TASK [Get local VM IP]

[INFO] changed: [localhost]

[INFO] TASK [Remove eventually entries for the local VM from /etc/hosts]

[INFO] changed: [localhost]

[INFO] TASK [Create an entry in /etc/hosts for the local VM]

[INFO] changed: [localhost]

[INFO] TASK [Wait for SSH to restart on the local VM]

[INFO] ok: [localhost -> localhost]

[INFO] TASK [Gathering Facts]

[INFO] ok: [sintezm-m.fintech.ru]

[INFO] TASK [Wait for the local VM]

[INFO] ok: [sintezm-m.fintech.ru]

[INFO] TASK [Add an entry for this host on /etc/hosts on the local VM]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Set FQDN]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Force the local VM FQDN to resolve on 127.0.0.1]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Restore sshd reverse DNS lookups]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Generate an answer file for engine-setup]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Include before engine-setup custom tasks files for the engine VM]

[INFO] TASK [Execute engine-setup]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Include after engine-setup custom tasks files for the engine VM]

[INFO] TASK [Configure LibgfApi support]

[INFO] skipping: [sintezm-m.fintech.ru]

[INFO] TASK [Restart ovirt-engine service for LibgfApi support]

[INFO] skipping: [sintezm-m.fintech.ru]

[INFO] TASK [Mask cloud-init services to speed up future boot]

[INFO] TASK [Clean up bootstrap answer file]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Wait for ovirt-engine service to start]

[INFO] ok: [localhost]

[INFO] TASK [Detect VLAN ID]

[INFO] changed: [localhost]

[INFO] TASK [Set Engine public key as authorized key without validating the TLS/SSL certificates]

[INFO] changed: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Obtain SSO token using username/password credentials]

[INFO] ok: [localhost]

[INFO] TASK [Enable GlusterFS at cluster level]

[INFO] skipping: [localhost]

[INFO] TASK [Set VLAN ID at datacenter level]

[INFO] skipping: [localhost]

[INFO] TASK [Force host-deploy in offline mode]

[INFO] changed: [localhost]

[INFO] TASK [Add host]

[INFO] changed: [localhost]

[INFO] TASK [Wait for the host to be up]

[INFO] ok: [localhost]

[INFO] TASK [Check host status]

[INFO] skipping: [localhost]

[INFO] TASK [Remove host-deploy configuration file]

[INFO] changed: [localhost]

На этапе, когда установщик ВМ Менеджера запросит информацию по хранилищу для хранения виртуальной машины менеджера, необходимо провести дополнительную настройку ВМ менеджера. На этом этапе ВМ менеджера уже работает и информация доступна по IP-адресу вида 192.168.122.XXX, где последний октет выделяется динамически. Информацию об актуальном IP-адресе ВМ менеджера можно посмотреть в файле /etc/hosts на гипервизоре. После чего, следует открыть новое консольное окно и зайти по ssh на ВМ менеджера.

Отключить SELinux командой:

```
setenforce 0
```

И так же поменять локаль на en_US.UTF8 командами:

```
export LANG=en_US.UTF8
```

После этого возвращаемся в гипервизор и продолжаем установку менеджера ВМ.

Please specify the storage you would like to use (glusterfs, iscsi, fc, nfs)[nfs]:

В данном сообщении программой установки запрашивается информация о протоколе сетевого доступа к хранилищу виртуальной машины. В данной установке используется протокол nfs, поэтому можно использовать значение по умолчанию.

Please specify the nfs version you would like to use (auto, v3, v4, v4_1)[auto]:

При появлении данного сообщения необходимо ввести параметр: **auto**

Please specify the full shared storage connection path to use (example: host:/path): **sintezm-h.fintech.ru:/ovirt**

В данном сообщении программой установки запрашивается полный путь к сетевому хранилищу, где будет храниться ВМ менеджера. Путь к сетевому хранилищу должен быть записан в виде **host:/path**. Для данной установки будет использоваться

If needed, specify additional mount options for the connection to the hosted-engine storagedomain []:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу **Enter**

[INFO] Creating Storage Domain

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Check local VM dir stat]

[INFO] ok: [localhost]

[INFO] TASK [Enforce local VM dir existence]

[INFO] skipping: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Obtain SSO token using username/password credentials]

[INFO] ok: [localhost]

[INFO] TASK [Fetch host facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch cluster ID]

[INFO] ok: [localhost]

[INFO] TASK [Fetch cluster facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter ID]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter name]

[INFO] ok: [localhost]

[INFO] TASK [Add NFS storage domain]

[INFO] changed: [localhost]

[INFO] TASK [Add glusterfs storage domain]

[INFO] skipping: [localhost]

[INFO] TASK [Add iSCSI storage domain]

[INFO] skipping: [localhost]

[INFO] TASK [Add Fibre Channel storage domain]

[INFO] skipping: [localhost]

[INFO] TASK [Get storage domain details]

[INFO] ok: [localhost]

[INFO] TASK [Find the appliance OVF]

[INFO] ok: [localhost]

[INFO] TASK [Parse OVF]

[INFO] ok: [localhost]

[INFO] TASK [Get required size]

[INFO] ok: [localhost]

[INFO] TASK [Check storage domain free space]

[INFO] skipping: [localhost]

Please specify the size of the VM disk in GB: [50]: **100**

В данном сообщении программой установки запрашивается информация о размере диска ВМ менеджера в ГБ. В данной установке необходимо ввести значение

[INFO] Creating Target VM

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Register the engine FQDN as a host]

[INFO] changed: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Obtain SSO token using username/password credentials]

[INFO] ok: [localhost]

[INFO] TASK [Get local VM IP]

[INFO] changed: [localhost]

[INFO] TASK [Fetch host facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Cluster ID]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Cluster facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter facts]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Cluster name]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter ID]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Datacenter name]

[INFO] ok: [localhost]

[INFO] TASK [Get Cluster CPU model]

[INFO] ok: [localhost]

[INFO] TASK [Get storage domain details]

[INFO] ok: [localhost]

[INFO] TASK [Add HE disks]

[INFO] TASK [Register disk details]

[INFO] ok: [localhost]

[INFO] TASK [Add VM]

[INFO] changed: [localhost]

[INFO] TASK [Register external local VM uuid]

[INFO] changed: [localhost]

[INFO] TASK [Gathering Facts]

[INFO] ok: [sintezm-m.fintech.ru]

[INFO] TASK [Find configuration file for SCL PostgreSQL]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Check SCL PostgreSQL value]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Update target VM details at DB level]

[INFO] TASK [Insert Hosted Engine configuration disk uuid into Engine database]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Disable IPv6]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Reload sysctl]

[INFO] changed: [sintezm-m.fintech.ru]

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [Trigger hosted engine OVF update]

[INFO] changed: [localhost]

[INFO] TASK [Wait until OVF update finishes]

[INFO] ok: [localhost]

[INFO] TASK [Parse OVF_STORE disk list]

[INFO] ok: [localhost]

[INFO] TASK [Check OVF_STORE volume status]

[INFO] TASK [Prepare images]

[INFO] TASK [Fetch Hosted Engine configuration disk path]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Hosted Engine virtio disk path]

[INFO] ok: [localhost]

[INFO] TASK [Fetch Hosted Engine virtio metadata path]

[INFO] ok: [localhost]

[INFO] TASK [Shutdown local VM]

[INFO] changed: [localhost]

[INFO] TASK [Wait for local VM shutdown]

[INFO] changed: [localhost]

[INFO] TASK [Undefine local VM]

[INFO] ok: [localhost]

[INFO] TASK [Detect spmId]

[INFO] changed: [localhost]

[INFO] TASK [Parse spmId]

[INFO] ok: [localhost]

[INFO] TASK [Detect ovirt-hosted-engine-ha version]

[INFO] changed: [localhost]

[INFO] TASK [Set ha_version]

[INFO] ok: [localhost]

[INFO] TASK [Create configuration templates]

[INFO] TASK [Create configuration archive]

[INFO] changed: [localhost]

[INFO] TASK [Create ovirt-hosted-engine-ha run directory]

[INFO] changed: [localhost]

[INFO] TASK [Copy configuration files to the right location on host]

[INFO] TASK [Copy configuration archive to storage]

[INFO] changed: [localhost]

[INFO] TASK [Initialize metadata volume]

[INFO] changed: [localhost]

[INFO] TASK [Find the local appliance image]

[INFO] ok: [localhost]

[INFO] TASK [Generate DHCP network configuration for the engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Generate static network configuration for the engine VM]

[INFO] changed: [localhost]

[INFO] TASK [Inject network configuration with guestfish]

[INFO] changed: [localhost]

[INFO] TASK [Extract /etc/hosts from the Hosted Engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Clean /etc/hosts for the Hosted Engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Copy /etc/hosts back to the Hosted Engine VM]

[INFO] skipping: [localhost]

[INFO] TASK [Copy local VM disk to shared storage]

[INFO] changed: [localhost]

[INFO] TASK [Clean /etc/hosts on the host]

[INFO] changed: [localhost]

[INFO] TASK [Add an entry in /etc/hosts for the target VM]

[INFO] changed: [localhost]

[INFO] TASK [Start ovirt-ha-broker service on the host]

[INFO] changed: [localhost]

[INFO] TASK [Initialize lockspace volume]

[INFO] changed: [localhost]

[INFO] TASK [Start ovirt-ha-agent service on the host]

[INFO] changed: [localhost]

[INFO] TASK [Wait for the engine to come up on the target VM]

[INFO] changed: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Obtain SSO token using username/password credentials]

[INFO] ok: [localhost]

[INFO] TASK [Check for the local bootstrap VM]

[INFO] ok: [localhost]

[INFO] TASK [Make the engine aware that the external VM is stopped]

[INFO] TASK [Wait for the local bootstrap VM to be down at engine eyes]

[INFO] ok: [localhost]

[INFO] TASK [Remove bootstrap external VM from the engine]

[INFO] changed: [localhost]

[INFO] TASK [Include custom tasks for after setup customization]

[INFO] Stage: Clean up

[INFO] Cleaning temporary resources

[INFO] TASK [Gathering Facts]

[INFO] ok: [localhost]

[INFO] TASK [include_tasks]

[INFO] ok: [localhost]

[INFO] TASK [Remove local vm dir]

[INFO] changed: [localhost]

[INFO] Generating answer file '/var/lib/ovirt-hosted-engine-setup/answers/answers-20180503154151.conf'

[INFO] Generating answer file '/etc/ovirt-hosted-engine/answers.conf'

[INFO] Stage: Pre-termination

[INFO] Stage: Termination

[INFO] Hosted Engine successfully deployed

Если в конце установки появляется сообщение «[INFO] Hosted Engine successfully deployed», то Менеджер ВМ установлен и настроен. Для того, чтобы зайти в менеджер ВМ, необходимо открыть браузер, ввести доменное имя менеджера или IP адрес ВМ, подтвердить в браузере конфиденциальность страницы, выбрать портал администрирования, авторизоваться пользователем admin и ранее заданным паролем для этого пользователя, домен «internal». В открывшейся странице находится интерфейс управления ВМ.

Для настройки подключения к порталу средства управления виртуализации необходимо в конфигурационном файле /etc/nginx/nginx.conf привести опции в соответствие для секции http:

В файле /etc/httpd/conf.modules.d/00-lua.conf закомментировать строку:

```
LoadModule lua_module modules/mod_lua.so
```

, а так же переопределить или добавить глобальную опцию в файле /etc/httpd/conf/httpd.conf :

```
TraceEnable off
```

В файлах /etc/httpd/conf.d/*.conf привести опции в соответствие для всех секций VirtualHost где используется шифрование через SSL engine:

```
SSLProtocol         all -SSLv3
SSLHonorCipherOrder on SSLCipherSuite "EECDH+ECDSA+AESGCM
EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA
RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS +RC4 RC4"
```

Примечание:

Изначально на web-интерфейс менеджера ВМ можно зайти только, используя доменное имя. Для разрешения доступа по IP необходимо внести изменения в файл /etc/ovirt-engine/engine.conf.d/11-setup-sso.conf. В переменной SSO_ALTERNATE_ENGINE_FQDNS="" необходимо вписать IP менеджера ВМ и перезапустить сервис ovirt-engine.service командой:

```
systemctl restart ovirt-engine.service
```

3.4.2.4. Добавление и настройка хранилищ в Менеджер ВМ

Для продолжения работы необходимо добавить хранилище в систему виртуализации. Подключение может быть реализовано как к локальному хранилищу (на гипервизоре), так и к внешней СХД.

Для создания локального хранилища (на гипервизоре) необходимо перейти на сервер виртуализации в консольном режиме выполнить:

– создание папки для хранения данных командой:

```
mkdir /storage
```

– включить поддержку nfs v4.2;

Для включения поддержки nfs версии 4.2 нужно в файле /etc/sysconfig/nfs выставить параметр: `RPCNFSDARGS="-V 4.2"`

– включить проброс меток;

Для `/storage *(rw,security_label)`

– назначение метки ресурса по умолчанию;

Для назначения метки ресурса по умолчанию выполнить команды:

```
semanage fcontext -a -t virt_var_lib_t '/storage(/.*)?'
restorecon -RFv /storage
```

, где `/storage` – директория с nfs ресурсом.

– задать папке права доступа:

```
chmod 755 /storage/
chown 36:36 /storage
```

– перезапустить службу экспортирования:

```
systemctl restart nfs-config.service
systemctl restart nfs-server.service
systemctl restart nfs.service
```

Примечание. Удостовериться, что в /proc/fs/nfsd/versions представлена следующая последовательность: `-2 +3 +4 +4.1 +4.2`

Далее необходимо перейти в веб-интерфейс портала администрирования и авторизоваться. В боковом меню навигации, в пункте «Хранилище», выбрать раздел Домены». В открывшейся странице нажать кнопку «Новый домен». В появившемся окне (рисунок 3.29) выбрать соответствующий дата центр (Default (V4), функцию домена хранение (Данные), тип подключаемого домена (NFS), имя (Storage), путь экспорта (на котором будет задействован домен и путь к каталогу хранения (Export

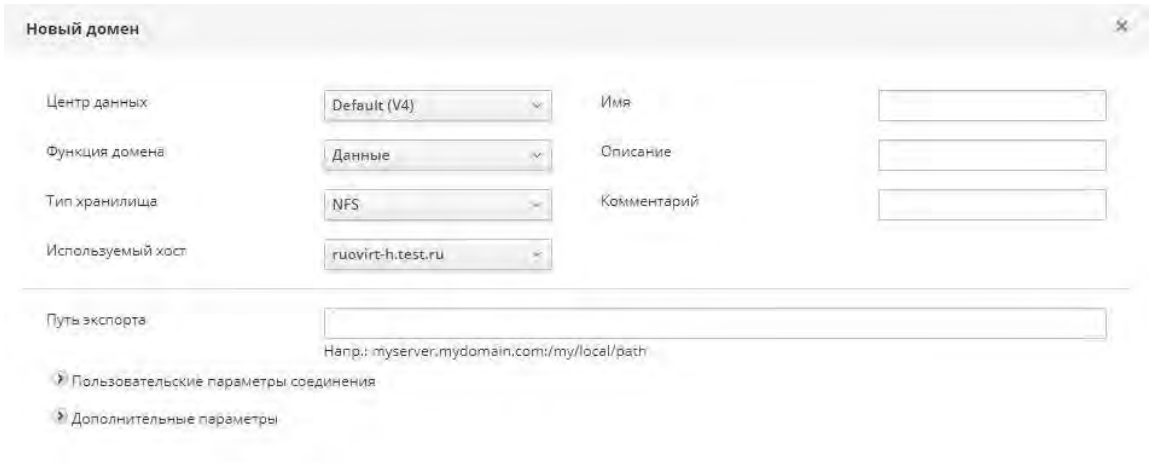


Рисунок 3.29 – Окно «Новый домен» подключение системы хранения данных NFS

Путь экспорта задаётся в формате **myserver.mydomain.com:/my/local/path**, где:
– полное доменное имя хоста, где запущен NFS-сервер, на котором будут храниться виртуальные машины. В данной установке в качестве такого NFS-сервера используется гипервизор;
– полный путь до директории NFS-сервера, в которой будут храниться ВМ. В данной установке используется ранее созданная директория /storage.

После внесения общих данных по домену, необходим добавить запись в «Пользовательские параметры соединения» (Рисунок 3.30).

Рисунок 3.30 – Пользовательские параметры соединения

В поле «Версия NFS» выставить значение: **V4.2**

В поле «Дополнительные параметры монтирования»: **v4.2**

Далее необходимо нажать на кнопку «**ОК**» и дождаться инициализации хранилища.

Примечание. После инициализации хранилища удостовериться в версии nfs (**vers=4.2**), а также проверить что на точке монтирования прокинулись selinux-метки.

Для проверки версии nfs, зайти по протоколу ssh на сервер виртуализации, выполнить команду: `mount`.

Пример вывода:

```
10.10.10.2:/storage on /rhev/data-center/mnt/10.10.10.2:_storage type nfs4 (rw,relatime,seclabel,vers=4.2,…)
```

Для проверок меток на сервере виртуализации, выполнить команду:

```
ls -Z /rhev/data-center/mnt/10.10.10.2\:_storage/
```

Пример вывода:

drwxr-xr-x. vdsm kvm system_u:object_r:**virt_var_lib_t**:s0 ae0deacf-f69a-4e9e-a39c-98dbb3f73c70

Затем, следует в ручном режиме создать и активировать ISO_DOMAIN. Для этого необходимо зайти по ssh на Менеджер ВМ. Создать директорию /var/lib/exports/iso командой:

```
mkdir -p /var/lib/exports/iso
```

Задать необходимые права:

```
chmod 777 /var/lib/exports/iso/
chown vdsm.kvm /var/lib/exports/iso/
```

После создания директории необходимо отредактировать файл «exports» и вписать в него информацию о директории. Затем запустить службу nfs.

Процедура добавления ISO_DOMAIN аналогична процедуре добавления хранилища. При этом стоит учитывать одно отличие: в качестве функции домена хранения необходимо выбрать ISO.

Для последующей загрузки образов необходимо использовать команду scp на АРМ-установщике. Все файлы образов хранятся в директории images/11111111-1111-1111-1111-111111111111/, где

<GUID> - автоматически задаётся при подключении ISO_DOMAIN

П р и м е р :

На АРМ-установщике ввести команду:

```
scp /path/to/sintezm-client_base-x86_64.iso
root@10.10.10.125:/var/lib/exports/iso/<GUID>/images/11111111-1111-1111-1111-111111111111/
```

После окончания копирования файла образа в директорию хранения образов iso-файлу необходимо задать требуемые права командой:

```
chown vdsm.kvm sintezm-7-x86_64.iso
```

Установка и настройка системы виртуализации изделия закончена. Система настроена, можно приступать к дальнейшей её эксплуатации, созданию ВМ, добавлению новых узлов и т.д.

3.4.2.5. Процедура добавления Менеджера ВМ в Сервер управления доступом

Для обеспечения возможности аутентификации доменными пользователями в портале Менеджера ВМ необходимо осуществить процедуру добавления Менеджера ВМ в Сервер управления доступом.

Примечание. Выполнение данного пункта необходимо осуществить после установки и настройки Сервера управления доступом (см п. 3.4.4).

Перед добавлением Менеджера ВМ в Сервер управления доступом необходимо произвести предварительную настройку ОС в соответствии с п 3.4.1.4, а также процедуру добавления узла в Сервер управления доступом в соответствии с п. 3.5 Добавление узла в Сервер управления доступом» Руководство системного программиста» (ТАСП.62.01.12.000.005 32).

Для добавления Менеджера ВМ в Сервер управления доступом необходимо в Менеджере ВМ подключить внешний источник для авторизации доменных пользователей, в качестве которого будет выступать Сервер управления доступом. Для этого необходимо выполнить команду:

```
ovirt-engine-extension-aaa-ldap-setup
```

Процедура осуществляется в режиме «вопрос-ответ»

```
[INFO] Stage: Initializing
[INFO] Stage: Environment setup
    Configuration files: ['/etc/ovirt-engine-extension-aaa-ldap-setup.conf.d/10-packaging.conf']
    Log file: /tmp/ovirt-engine-extension-aaa-ldap-setup-20180511112218-0jqjpe.log
    Version: otopi-1.7.7 (otopi-1.7.7-1.el7.centos)
```

[INFO] Stage: Environment packages setup

[INFO] Stage: Programs detection

[INFO] Stage: Environment customization

Welcome to LDAP extension configuration program

Available LDAP implementations:

1 - 389ds

2 - 389ds RFC-2307 Schema

3 - Active Directory

4 - IBM Security Directory Server

5 - IBM Security Directory Server RFC-2307 Schema

6 - IPA

7 - Novell eDirectory RFC-2307 Schema

8 - OpenLDAP RFC-2307 Schema

9 - OpenLDAP Standard Schema

10 - Oracle Unified Directory RFC-2307 Schema

11 - RFC-2307 Schema (Generic)

12 - RHDS

13 - RHDS RFC-2307 Schema

14 - iPlanet

Please select: **6**

В данном сообщении программой установки запрашивается тип LDAP-сервера. В нашей установке используется IPA-сервер, поэтому необходимо ввести **6.**

NOTE:

It is highly recommended to use DNS resolution for LDAP server.

If for some reason you intend to use hosts or plain address disable DNS usage.

Use DNS (Yes, No) [Yes]: **Yes**

В данном сообщении программой установки запрашивается информация о том, будет ли использоваться DNS-сервер. В данной установке используется. Поэтому, надо вводить **Yes.**

Available policy method:

1 - Single server

2 - DNS domain LDAP SRV record

3 - Round-robin between multiple hosts

4 - Failover between multiple hosts

Please select: **1**

В данном сообщении программой установки запрашивается информация о типе DNS-сервера. В данной установке используется только один DNS-сервер, поэтому необходимо выбрать пункт **1.**

Please enter host address: **sintezm-ipa.fintech.ru**

В данном сообщении программой установки запрашивается адрес сервера управления доступом.

В данной установке необходимо ввести значение **sintezm-ipa.fintech.ru.**

[INFO] Trying to resolve host 'sintezm-ipa.fintech.ru'

NOTE:

It is highly recommended to use secure protocol to access the LDAP server.

Protocol startTLS is the standard recommended method to do so.

Only in cases in which the startTLS is not supported, fallback to non standard ldaps protocol.

Use plain for test environments only.

Please select protocol to use (startTLS, ldaps, plain) [startTLS]: **plain**

В данном сообщении программой установки запрашивается информация о методе подключения Менеджера ВМ к LDAP-серверу. В данной установке используется метод **plain.**

[INFO] Connecting to LDAP using 'ldap://sintezm-ipa.fintech.ru:389'

[INFO] Connection succeeded

Enter search user DN (for example uid=username,dc=example,dc=com or leave empty for anonymous):

В данном сообщении программой установки запрашивается информация о пользовательском DN. В данной установке для доступа используется пользователь ymous, поэтому необходимо нажать на клавиатуре клавишу <**Enter**>

Enter search user password:

При появлении данного сообщения необходимо нажать на клавиатуре клавишу

[INFO] Attempting to bind using '[Anonymous]'

Please enter base DN (dc=fintech,dc=ru) [dc=fintech,dc=ru]:

Are you going to use Single Sign-On for Virtual Machines (Yes, No) [Yes]: No

В данном сообщении программой установки запрашивается информация об использовании SSO-авторизация для доступа к ВМ в менеджере. В данной установке SSO не используется, поэтому необходимо ввести **No**

Please specify profile name that will be visible to users [sintezm7-ipa.fintech.ru]: **fintech.ru**

В данном сообщении программой установки запрашивается информация о том, как будет отображаться информация о домене в поле “Profile”, в web-интерфейсе Менеджера ВМ. В данной установке используется имя профиля fintech.ru

[INFO] Stage: Setup validation

NOTE:

It is highly recommended to test drive the configuration before applying it into engine.

Login sequence is executed automatically, but it is recommended to also execute Search sequence manually after successful Login sequence.

Please provide credentials to test login flow:

Enter user name: **admin**

В данном сообщении программой установки запрашивается имя пользователя для тестового доступа. В данной установке используется пользователь **admin**

Enter user password: **12345678**

В данном сообщении программой установки запрашивается пароль для тестового пользователя, который был указан в предыдущем сообщении. В данной установке для данного пользователя задан пароль **12345678.**

[INFO] Executing login sequence...

Login output:

2018-05-30 14:27:52,107+03 INFO ==========

2018-05-30 14:27:52,135+03 INFO ========== Initialization ==========

2018-05-30 14:27:52,136+03 INFO

==========

2018-05-30 14:27:52,177+03 INFO Loading extension 'fintech.ru-authn'

2018-05-30 14:27:52,252+03 INFO Extension 'fintech.ru-authn' loaded

2018-05-30 14:27:52,257+03 INFO Loading extension 'fintech.ru-authz'

2018-05-30 14:27:52,272+03 INFO Extension 'fintech.ru-authz' loaded

2018-05-30 14:27:52,272+03 INFO Initializing extension 'fintech.ru-authn'

2018-05-30 14:27:52,273+03 INFO [ovirt-engine-extension-aaa-ldap.authn::fintech.ru-authn] Creating LDAP pool 'authz'

2018-05-30 14:27:52,556+03 INFO [ovirt-engine-extension-aaa-ldap.authn::fintech.ru-authn] LDAP pool 'authz' information: vendor='389 Project' version='389-Directory/1.3.5.10 B2018.116.040'

2018-05-30 14:27:52,558+03 INFO [ovirt-engine-extension-aaa-ldap.authn::fintech.ru-authn] Creating LDAP pool 'authn'

2018-05-30 14:27:52,586+03 INFO [ovirt-engine-extension-aaa-ldap.authn::fintech.ru-authn] LDAP pool 'authn' information: vendor='389 Project' version='389-Directory/1.3.5.10 B2018.116.040'

2018-05-30 14:27:52,587+03 INFO Extension 'fintech.ru-authn' initialized

2018-05-30 14:27:52,588+03 INFO Initializing extension 'fintech.ru-authz'

2018-05-30 14:27:52,589+03 INFO [ovirt-engine-extension-aaa-ldap.authz::fintech.ru-authz] Creating LDAP pool 'authz'

2018-05-30 14:27:52,602+03 INFO [ovirt-engine-extension-aaa-ldap.authz::fintech.ru-authz] LDAP pool 'authz' information: vendor='389 Project' version='389-Directory/1.3.5.10 B2018.116.040'

2018-05-30 14:27:52,603+03 INFO [ovirt-engine-extension-aaa-ldap.authz::fintech.ru-authz] Available Namespaces: [dc=fintech,dc=ru]

2018-05-30 14:27:52,603+03 INFO Extension 'fintech.ru-authz' initialized

2018-05-30 14:27:52,604+03 INFO Start of enabled extensions list

2018-05-30 14:27:52,604+03 INFO Instance name: 'fintech.ru-authn', Extension name: 'ovirt-engine-extension-aaa-ldap.authn', Version: '1.3.7', Notes: 'Display name: ovirt-engine-extension-aaa-ldap-1.3.7-1.el7', License: 'ASL 2.0', Home: 'http://www.ovirt.org', Author 'The oVirt Project', Build interface Version: '0', File: '/tmp/tmp1vMuug/extensions.d/fintech.ru-authn.properties', Initialized: 'true'

2018-05-30 14:27:52,605+03 INFO Instance name: 'fintech.ru-authz', Extension name: 'ovirt-engine-extension-aaa-ldap.authz', Version: '1.3.7', Notes: 'Display name: ovirt-engine-extension-aaa-ldap-1.3.7-1.el7', License: 'ASL 2.0', Home: 'http://www.ovirt.org', Author 'The oVirt Project', Build interface Version: '0', File: '/tmp/tmp1vMuug/extensions.d/fintech.ru-authz.properties', Initialized: 'true'

2018-05-30 14:27:52,605+03 INFO End of enabled extensions list

2018-05-30 14:27:52,605+03 INFO
==========

2018-05-30 14:27:52,605+03 INFO ========== Execution
==========

2018-05-30 14:27:52,606+03 INFO
==========

2018-05-30 14:27:52,606+03 INFO Iteration: 0

2018-05-30 14:27:52,607+03 INFO Profile='fintech.ru' authn='fintech.ru-authn' authz='fintech.ru-authz' mapping='null'

2018-05-30 14:27:52,607+03 INFO API: ->Authn.InvokeCommands.AUTHENTICATE_CREDENTIALS profile='fintech.ru' user='admin'

2018-05-30 14:27:52,640+03 INFO API: <-- Authn.InvokeCommands.AUTHENTICATE_CREDENTIALS profile='fintech.ru' result=SUCCESS

2018-05-30 14:27:52,644+03 INFO --- Begin AuthRecord ---

2018-05-30 14:27:52,644+03 INFO AAA_AUTHN_AUTH_RECORD_PRINCIPAL: admin

2018-05-30 14:27:52,645+03 INFO --- End AuthRecord ---

2018-05-30 14:27:52,645+03 INFO API: ->Authz.InvokeCommands.FETCH_PRINCIPAL_RECORD principal='admin'

2018-05-30 14:27:52,657+03 INFO API: <-- Authz.InvokeCommands.FETCH_PRINCIPAL_RECORD status=SUCCESS

2018-05-30 14:27:52,657+03 INFO --- Begin PrincipalRecord ---

2018-05-30 14:27:52,658+03 INFO AAA_AUTHZ_PRINCIPAL_PRINCIPAL: admin

2018-05-30 14:27:52,658+03 INFO AAA_AUTHZ_PRINCIPAL_LAST_NAME: Administrator

2018-05-30 14:27:52,658+03 INFO AAA_LDAP_UNBOUNDID_DN: uid=admin,cn=users,cn=accounts,dc=fintech,dc=ru

2018-05-30 14:27:52,659+03 INFO AAA_AUTHZ_PRINCIPAL_NAMESPACE: dc=fintech,dc=ru

2018-05-30 14:27:52,659+03 INFO AAA_AUTHZ_PRINCIPAL_ID: 8735e7fa-63f9-11e8-97d2-001a4a160100

2018-05-30 14:27:52,659+03 INFO AAA_AUTHZ_PRINCIPAL_NAME: admin

2018-05-30 14:27:52,660+03 INFO --- End PrincipalRecord ---

[INFO] Login sequence executed successfully

Please make sure that user details are correct and group membership meets expectations (search for PrincipalRecord and GroupRecord titles).

Abort if output is incorrect.

Select test sequence to execute (Done, Abort, Login, Search) [Done]: **Done**

Если перед этим сообщением появляется строка «[INFO] Login sequence executed successfully», то необходимо ввести Done

[INFO] Stage: Transaction setup

[INFO] Stage: Misc configuration

[INFO] Stage: Package installation

[INFO] Stage: Misc configuration

[INFO] Stage: Transaction commit

[INFO] Stage: Closing up

CONFIGURATION SUMMARY

Profile name is: fintech.ru

The following files were created:

/etc/ovirt-engine/aaa/fintech.ru.properties

/etc/ovirt-engine/extensions.d/fintech.ru-authz.properties

/etc/ovirt-engine/extensions.d/fintech.ru-authn.properties

[INFO] Stage: Clean up

Log file is available at /tmp/ovirt-engine-extension-aaa-ldap-setup-20180530142502-r4068d.log:

[INFO] Stage: Pre-termination

[INFO] Stage: Termination

Данная команда должна выполниться без ошибок.

Далее необходимо перезапустить сервис ovirt-engine.service командой:

```
systemctl restart ovirt-engine.service
```

После этого на странице авторизации, в выпадающем списке «Profile» появится домен, который был введён в процессе настройки.

3.4.2.6. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с выбранной схемой аутентификации согласно п. 3.7.2.

3.4.2.7. Настройка централизованного аудита

Для функционирования централизованного аудита на менеджере ВМ (сообщения транслируются на сервер безопасности) необходимо привести файл /etc/rsyslog.d/rsyslog-send.conf к следующему виду:

```
module(load="omrelp")
if ( $programname == "dlogevent" ) then {
    action(
        type="omrelp"
        Target="[ip-адрес сервера безопасности]"
        Port="2514"
        queue.type="LinkedList"
        queue.size="10000"
        queue.filename="q_sendRule"
        queue.highwatermark="9000"
        queue.lowwatermark="50"
        queue.maxdiskspace="1g"
        queue.saveonshutdown="on"
        action.resumeRetryCount="-1"
        action.resumeInterval="3"
    )
}
```

, где `[ip-адрес сервера безопасности]` – адрес сервера безопасности на который будут пересылаться события безопасности.

А также привести файл /etc/rsyslog.d/rsyslog-ovirt.conf к следующему виду:

```
$ModLoad imfile
$InputFileName /var/log/ovirt-engine/engine.log
$InputFileTag ovirt-engine:
$InputFileStateFile ovirt-engine.state
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
```

После внесений изменений в файл перезагрузить сервисы rsyslog и dlogevent:

```
service rsyslog restart
service dlogevent restart
```

3.4.3. Создание виртуальной машины

Для создания виртуальной машины необходимо зайти на портал администрирования Менеджера ВМ. Для этого необходимо запустить браузер, в адресной строке ввести адрес Менеджера ВМ, выбрать «Портал администрирования» (

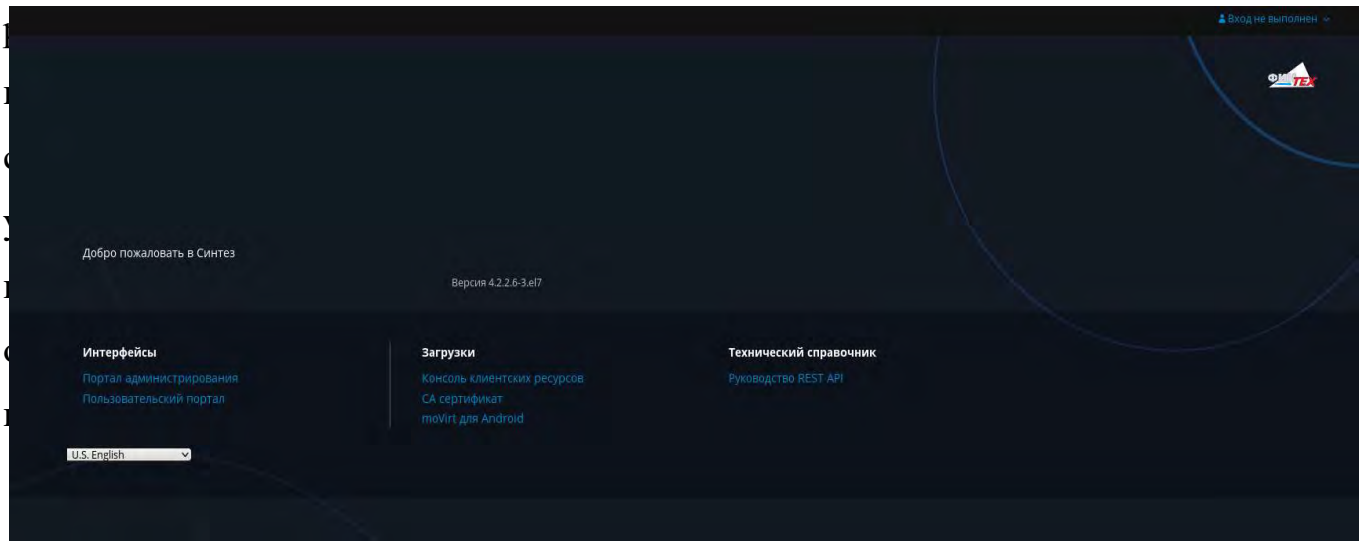


Рисунок 3.31 – Окно страницы доступа к порталу

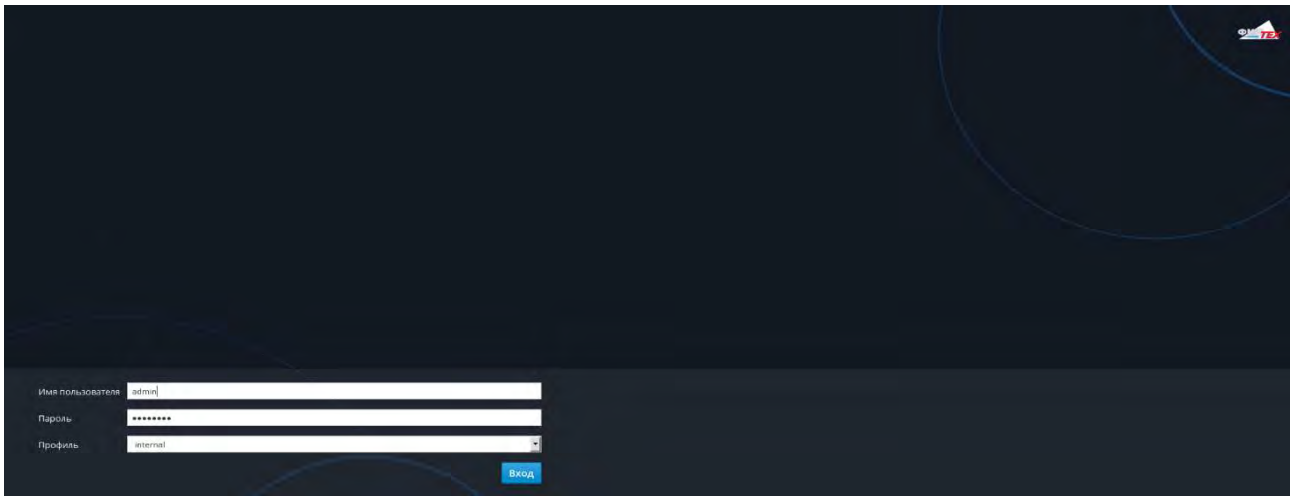


Рисунок 3.32 – Окно авторизации менеджера

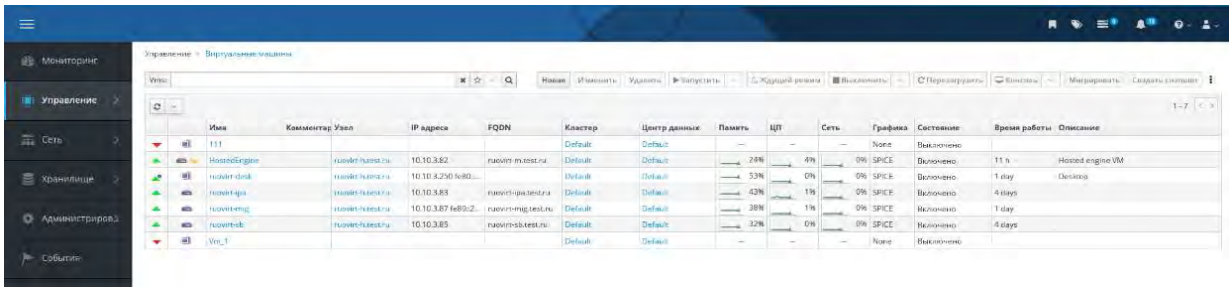


Рисунок 3.33 – Окно управления ВМ

После успешной авторизации перейти на вкладку «Виртуальные машины» и нажать на кнопку «Новая» (рисунок 3.33).

В открывшемся окне настройки параметров виртуальной машины необходимо перейти во вкладку «General» и нажать на кнопку «**Показать расширенные**

Д

а – «Кластер» – выбрать Центр данных, на котором будет функционировать ВМ (к«Default»);

е – «Шаблон» – оставить без изменений;

е – «Операционная система» – выбрать из ниспадающего списка устанавливаемую ОС и нажать на кнопку «ОК» («Red Hat Enterprise Linux 7.x x64»);

– «Тип экземпляра» – необходимо выбрать «Пользовательский» для настройки параметров вручную (выбор данного параметра из выпадающего списка автоматически задает параметры ВМ (оперативная память, количество и распределение процессоров, и т.д.) в зависимости от выбранного типа);

б – «Оптимизировано для» – указывает оптимизацию под серверное решение или рабочую станцию. Соответственно если выполняется установка виртуального сервера выбрать оптимизацию «Сервер», если рабочей станции – то «Рабочий стол»;

д – «Имя» – указывается имя виртуальной машины;

и – «Код ВМ» – указывается индикационный номер виртуальной машины в базе данных. По умолчанию данный параметр можно не задавать и оставить его пустым;

о – «Описание» – в данном поле указывается описание для данной ВМ, можно оставить поле пустым или для удобства пометить, к примеру «Начальник отдела»;

н

а

– «Комментарий» – аналогичен параметру «Description».

– позиции «Без запоминания состояния», «Запустить в режиме приостановки» и «Защита от удаления» необходимо оставить неактивными.

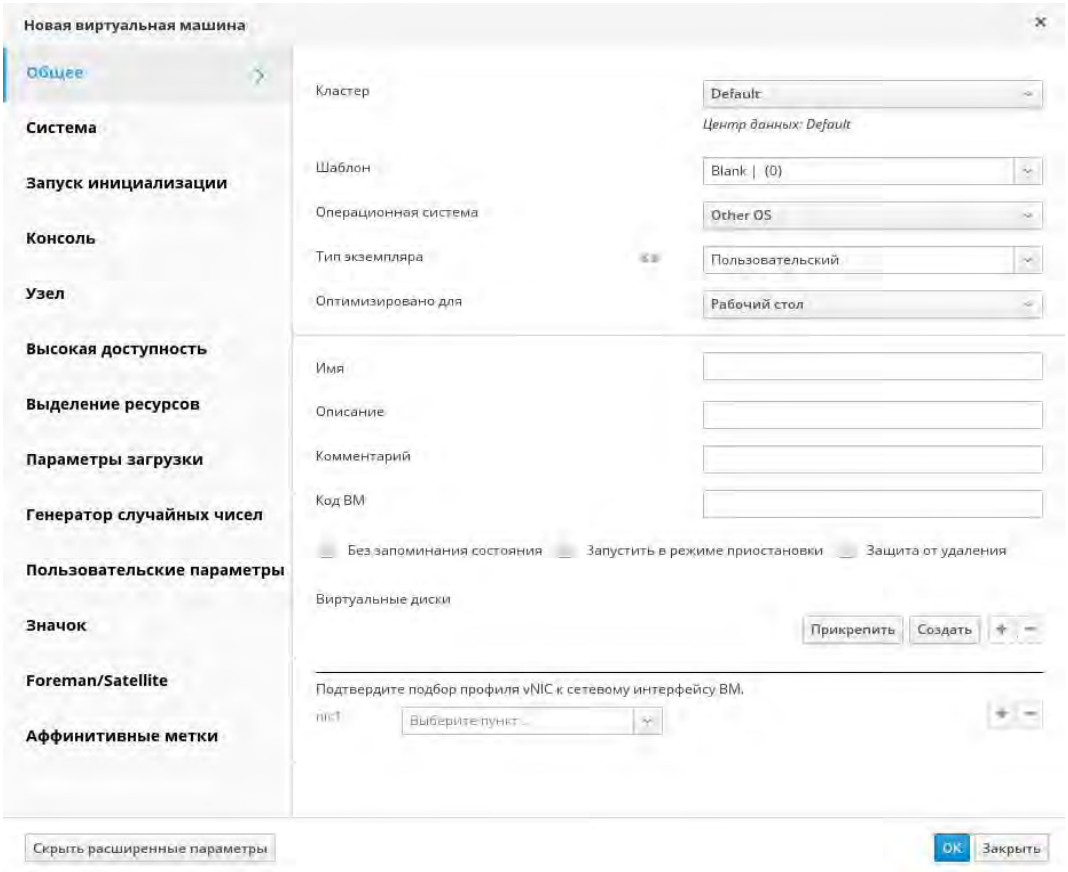


Рисунок 3.34 – Настройка параметров виртуальной машины

Параметр «Виртуальные диски» позволяет прикреплять уже имеющиеся или создавать новые виртуальный жесткий диск. Для этого необходимо нажать на кнопку жесткого диска – размер, место хранения и другие параметры:

– размер (GB) – размер жесткого диска;

– псевдоним– название диска (оставить по умолчанию);

– описание– примечание (оставить по умолчанию);

– интерфейс– интерфейс жесткого диска (оставить по умолчанию);

– домен хранения– домен хранения виртуальных образов (указать, где будут храниться ВМ);

– политика выделения – политика разбиения жесткого диска (Примечание: для низко производительных доменов хранения, например, подключаемых по NFS дисках гипервизоров, необходимо устанавливать параметр «Размеченный» ;

– профиль диска– профиль диска (оставить по умолчанию);

– очистить после удаления– очистить место после удаления (оставить по умолчанию);

– загрузочный– диск будет загрузочным (оставить по умолчанию);

– может быть общим– сделать общим доступным (оставить по умолчанию);

– только для чтения– сделать диск только для чтения (оставить по умолчанию).

После настройки параметров жесткого диска необходимо нажать на кнопку

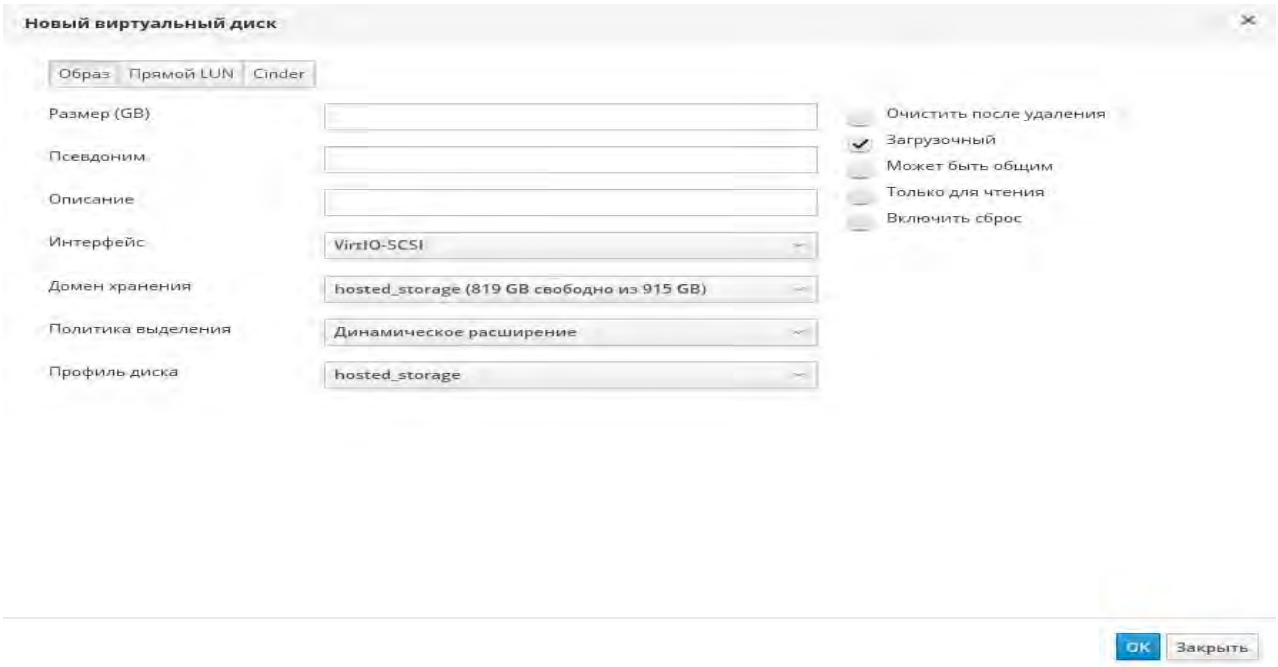


Рисунок 3.35 – Создание нового виртуального диска

Параметр «Подтвердите подбор профиля vNIC к сетевому интерфейсу ВМ.» позволяет выбрать виртуальную сеть к которой будет подключен интерфейс для данной ВМ – Для данной конфигурации из ниспадающего списка необходимо выбрать подключение «ovirtmgmt» (рисунок 3.36).

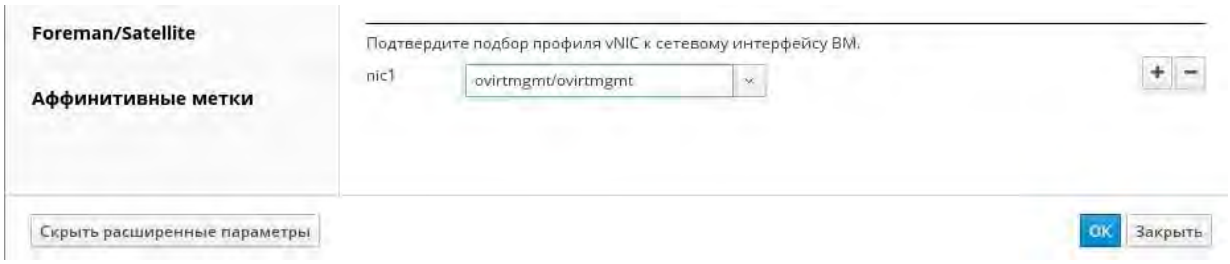


Рисунок 3.36 – Выбор сетевого подключения

Примечание. Для изменения настройки сети, необходимо перейти во вкладку «Виртуальные машины», выбрать ВМ, далее во вкладках данной ВМ выбрать «Сетевые интерфейсы», выбрать подключение и нажать на кнопку «**Изменить**».

Далее необходимо перейти во вкладку «Система» (см. рисунок 3.33) и в открывшемся окне указать следующие параметры (рисунок 3.37):

– «Размер памяти» – объем выделяемой памяти для ВМ;

– «Всего виртуальных ЦП» – количество выделяемых процессоров.

Примечания:

1. в дополнительных параметрах CPU, указывается число виртуальных сокетов, число ядер на узле, тип процессора;

2. «Смещение аппаратных часов» – указывает смещение времени (то есть часовой пояс), указать пояс места нахождения сервера.

Остальные параметры необходимо оставить без изменений.

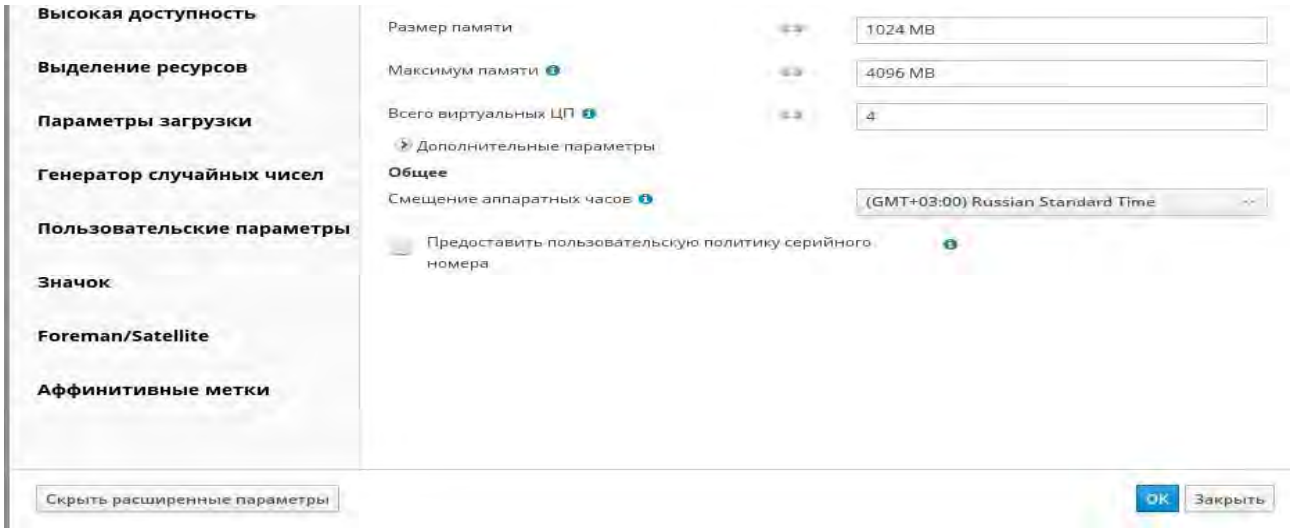


Рисунок 3.37 – Вкладка «Система»

Далее, необходимо перейти во вкладку «Консоль» (см. рисунок 3.33) и в открывшемся окне указать следующие параметры (рисунок 3.38):

– «Тип видео-адаптера» – выбрать режим «QXL»;

– «Графический протокол» – выбрать «Spice». Данный параметр выбирает графический протокол передачи данных;

– «Поддержка USB» – оставить в выключенном положении. Данный параметр включает или выключает поддержку usb накопителей для ВМ;

– «Действие отключения консоли» – указать параметр lock screen. Данный параметр указывает действия ВМ при отключении пользователя;

– «Наблюдатели» – указать количество мониторов у данной ВМ;

– «Смарт карты включены» – оставить не активным, а параметр Метод единого входа выбрать «Использовать гостевого агента»;

– в «Дополнительных параметрах» – ничего не менять;

– «Выключить строгую проверку пользователей» – отключение блокировки spice сессии при работе администратора (при необходимости).

– «Звуковая карта включена» – включение звуковой карты для данной ВМ (при необходимости).

Остальные параметры необходимо оставить без изменений.

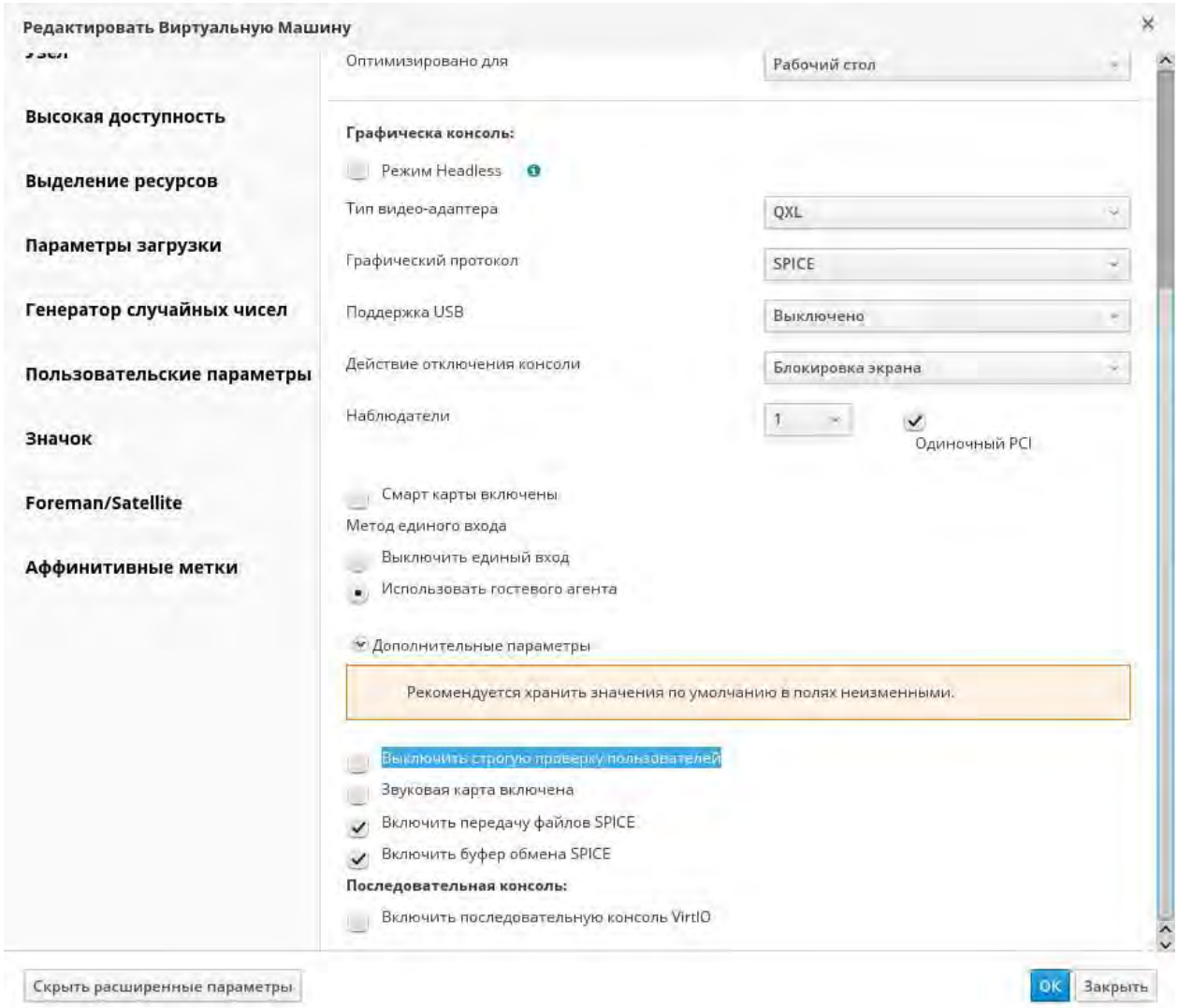


Рисунок 3.38 – Вкладка «Консоль»

Далее, необходимо перейти во вкладку «Узел» (см. рисунок 3.33). Все настройки оставить без изменений (рисунок 3.39):

– «Запускается на» – настраивает запуск ВМ на определенном узле или на любом доступном;

– «Параметра миграции» – настраивает дополнительные параметры при миграции виртуальной машины на другие узлы.

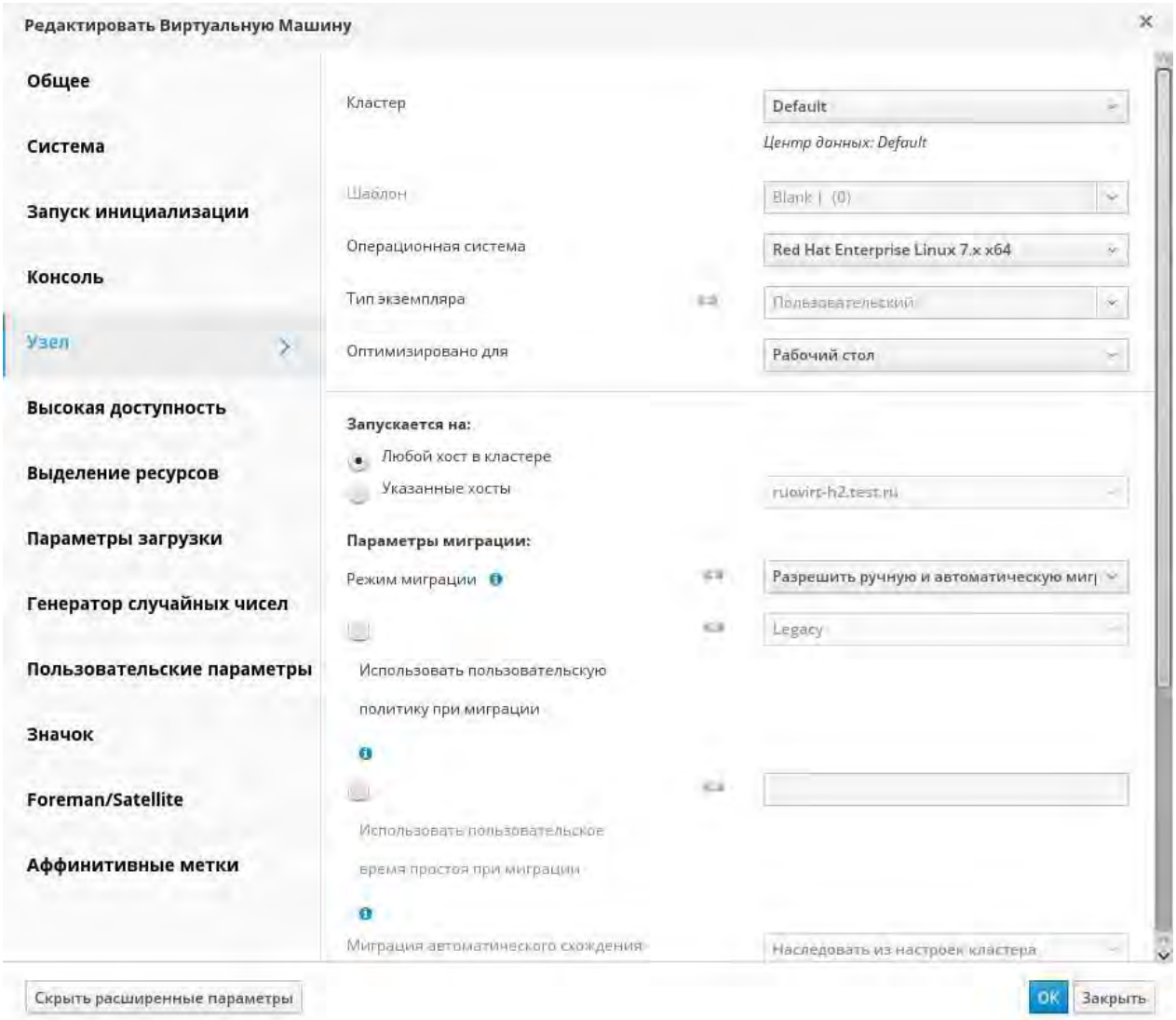


Рисунок SEQ Рисунок * ARABIC \s 1 39 – Вкладка «Узел»

Далее, необходимо перейти во вкладку «Высокая доступность» (рисунок 3.40) затем выполнить следующие действия:

– активировать радиокнопку «Высокая доступность»;

– в выпадающем списке «Целевой домен для хранения аренды виртуальной машины» выбрать домен, который будет использоваться для аренды ВМ;

– в выпадающем списке «Возобновление поведения», установить значение «KILL»;

– в разделе «Приоритет очереди запуска/миграции», в выпадающем списке «Приоритет» выбрать значение «Высокий».

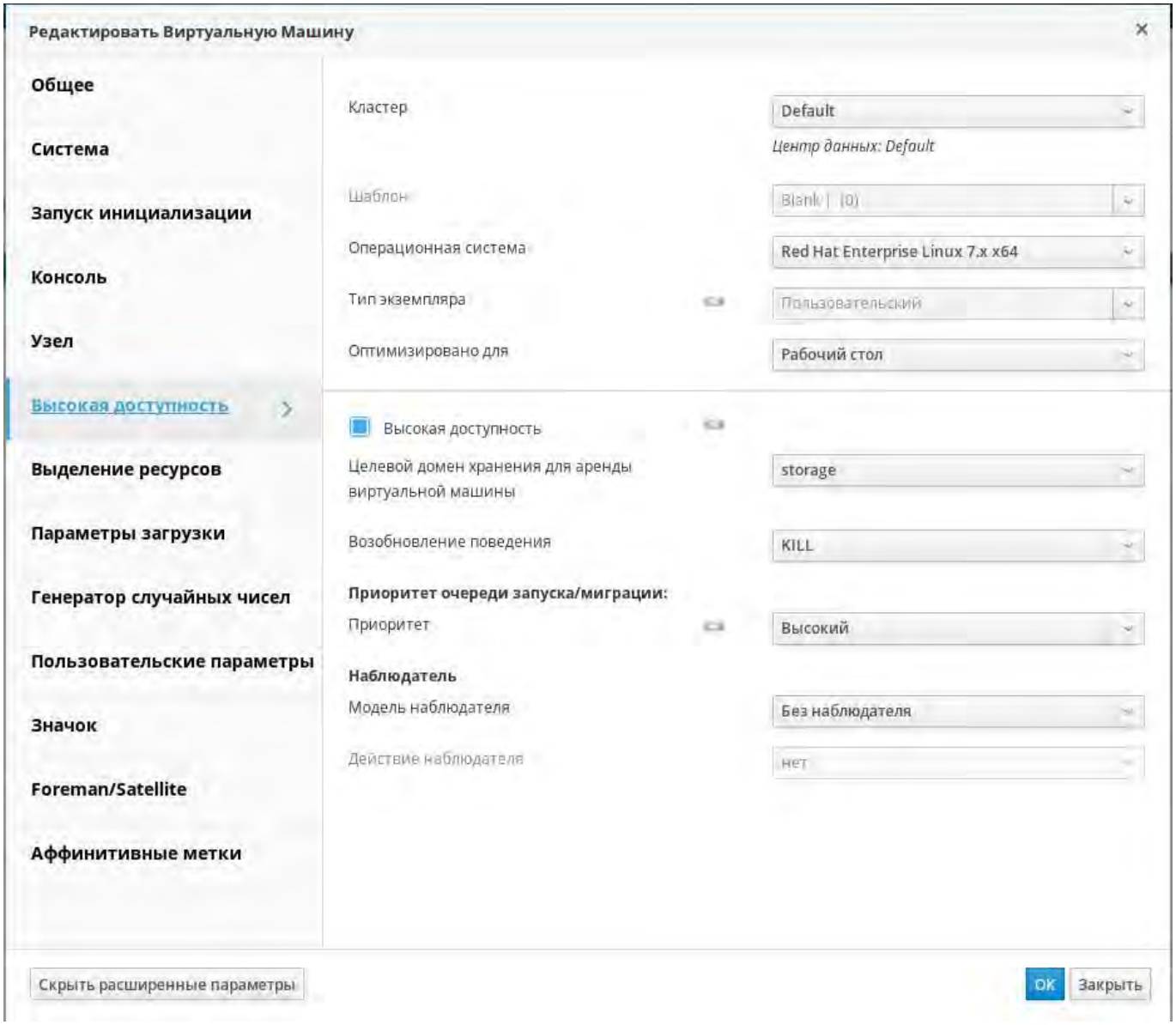
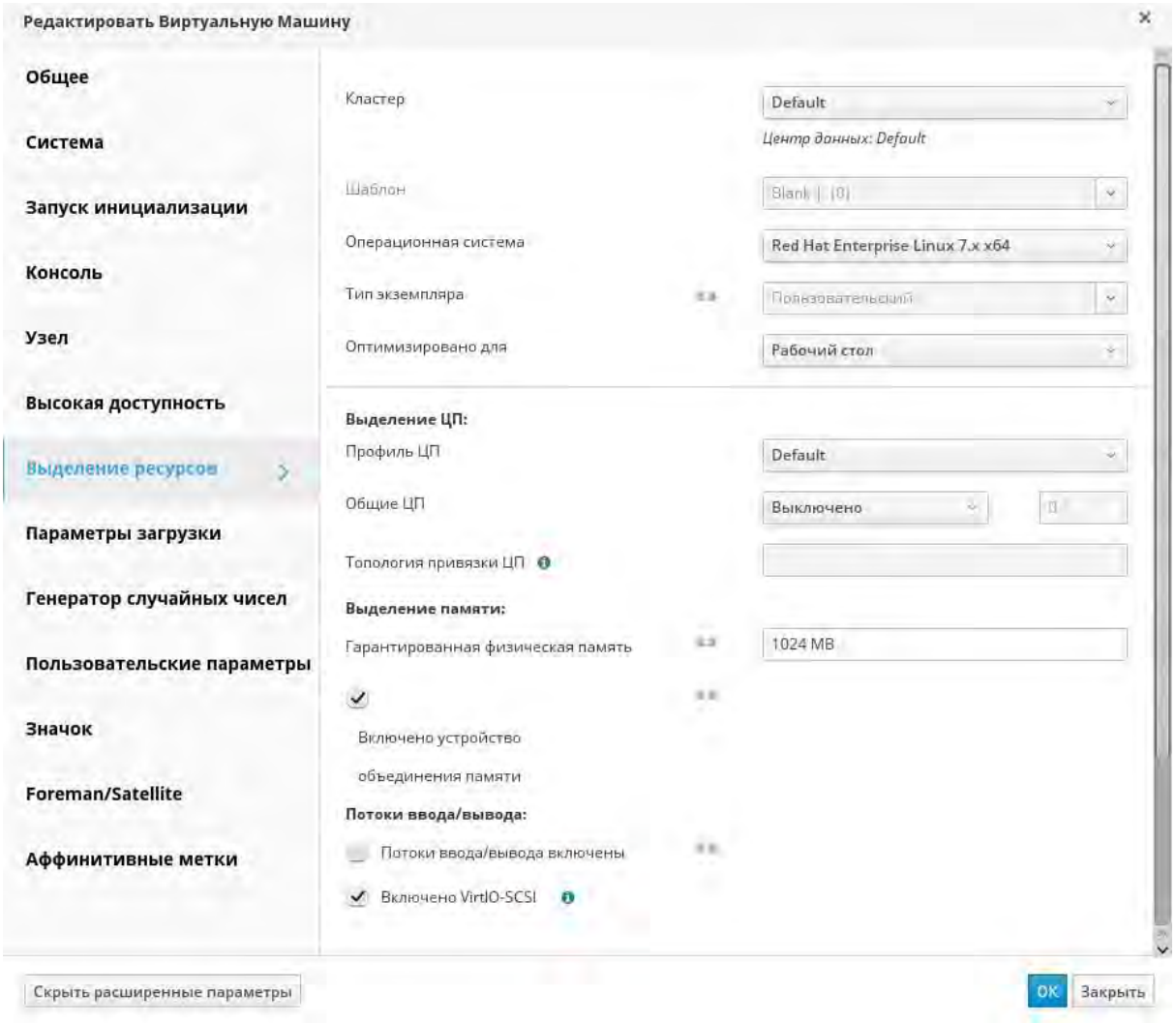


Рисунок SEQ Рисунок * ARABIC \s 1 40 – Вкладка «Высокая доступность»

Далее необходимо перейти во вкладку «Выделение ресурсов» (см. рисунок 3.33), все настройки оставив без изменений (рисунок 3.41):

– «Выделение ЦП» – данный параметр устанавливает приоритет использования ресурсов ЦП для ВМ на хосте;

– «Выделение памяти» – задает гарантированный объем оперативной памяти выделяемой ВМ.



После завершения всех настроек необходимо нажать на кнопку «**ОК**». ВМ будет создана и отобразится в списке (рисунок 3.42).

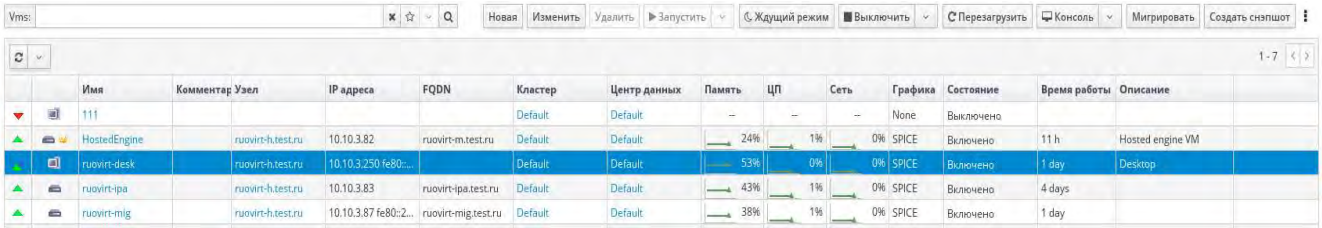


Рисунок 3.42 – Отображение созданной ВМ

Для установки операционной системы на ВМ необходимо:

– выбрать соответствующую ВМ из списка;

– нажать кнопку раскрытия списка, находящуюся на кнопке «Запустить» после чего из выпадающего списка выбрать позицию «Разовый запуск» (Рисунок 3.43);

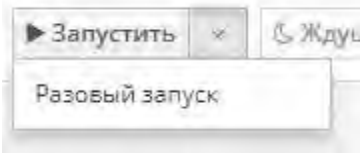


Рисунок 3.43 – Разовый запуск

– в открывшемся окне с параметрами разовой загрузки ВМ (см. рисунок 3.44) необходимо выбрать подменю «Параметры загрузки»;

– далее необходимо настроить загрузку с образа диска. Выставить маркер в поле «Прикрепить CD», в выпадающем меню необходимо выбрать образ системы и нажать на кнопку «ОК». В подменю «Параметры загрузки» можно также выбрать загрузку с жесткого диска, загрузку с CD-диска или по сети. Также существуют другие подменю параметров настройки данной ВМ: часовой пояс, выбор протокола по которому будут передаваться видео данные и т.д. Значения дополнительных параметров необходимо оставить по умолчанию.

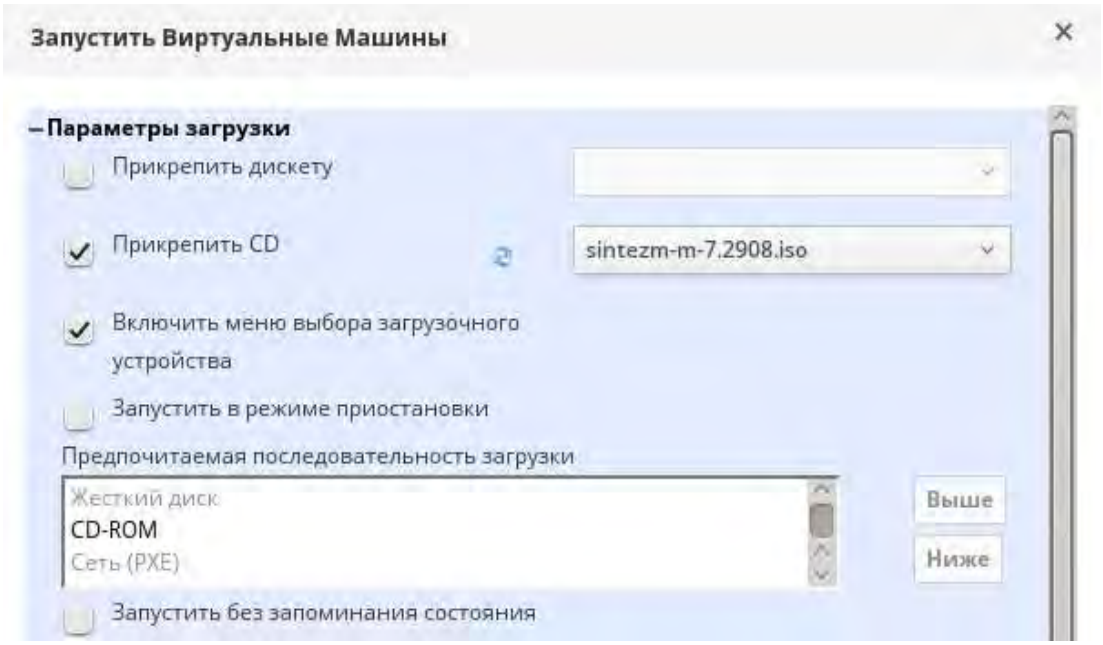


Рисунок 3.44 – Загрузка виртуальной машины с образа диска

Для установки ОС на созданную ВМ используется консоль виртуальной машины.

Для запуска консоли виртуальной машины необходимо выбрать ВМ и нажать на кнопку «Консоль» (рисунок 3.45).

Рисунок 3.45 – Запуск консоли

Примечание: для доступа к консоли виртуальной машины необходимо наличие пакета remote-viewer для возможности отображения видеоконсоли. Также запись о менеджере должна присутствовать в файле /etc/hosts.

Установка ОС выполняется согласно пункту 3.2 «Установка в конфигурации

3.4.4. Установка и настройка ВМ Сервера управления доступом

Сервер управления доступом устанавливается в виде виртуальной машины. Для этого необходимо в Менеджере ВМ создать виртуальную машину согласно пункту инструкции при развёртывании управления доступом будут использованы параметры представлены в «Таблица 3.3».

Для установки ОС на ВМ Сервера управления доступом необходимо произвести действия, описанные в пункте 3.1 данной инструкции, после чего в окне «Выбор программ» в качестве базового окружения выбрать позицию «Сервер-ИПА» (рисунок 3.46).

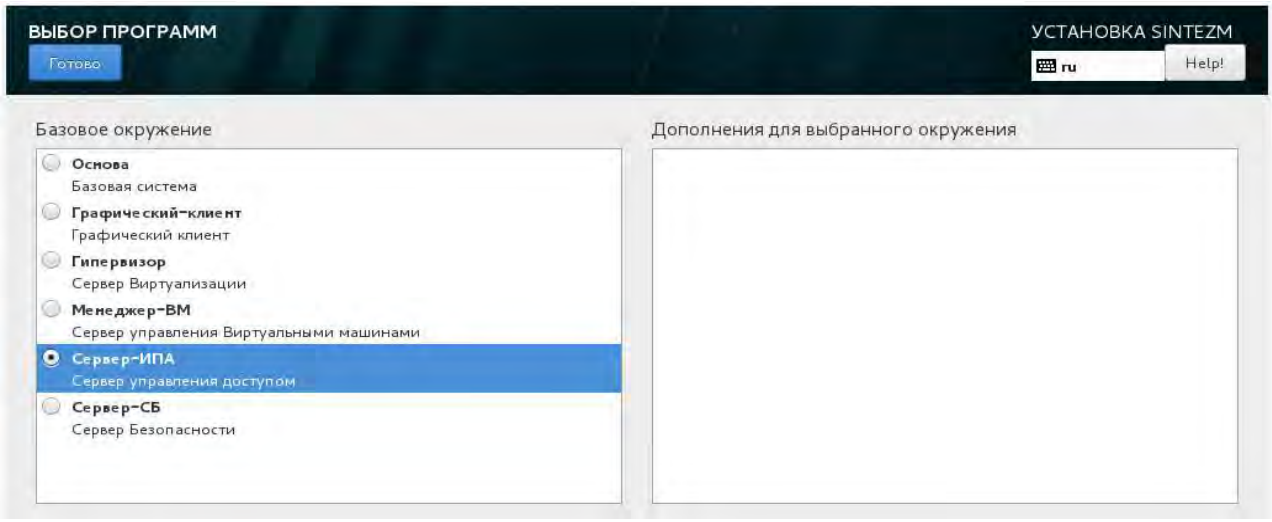


Рисунок 3.46 – Окно выбора программ

3.4.4.1. Настройка места установки

Настройка места установки при установке сервера управления доступом производится аналогично порядку, описанному в пункте 3.2.1.1.

3.4.4.2. Конфигурирование сети и имени узла

Конфигурирование сети и имени узла при установке сервера управления доступом производится аналогично порядку, описанному в пункте 3.2.1.2.

3.4.4.3. Назначение региональных настроек

Настройка даты и времени при установке сервера управления доступом производится аналогично порядку, описанному в пункте 3.2.1.3.

3.4.4.4. Предварительная настройка ОС

Предварительная настройка ОС для ВМ сервера управления доступом осуществляется аналогично порядку, описанному в пункте п. 3.4.1.4.

3.4.4.5. Настройка Средства управления доменными пользователями

Для непосредственной установки и настройки Средства управления доменными пользователями необходимо выполнить команду:

```
ipa-server-install --setup-dns --no-ntp --no-forwarders --reverse-zone=<ptr_net> --allow-zone-overlap --no-host-dns --admin-password=<password> --ds-password=<password> -domain=<domain.local> --realm=<REALM.LOCAL> --unattended
```

где параметры reverse-zone, admin-password, ds-password, domain и realm могут содержать значения, зависящие от требований к установке.

В параметре reverse-zone указывается зона обратного запроса DNS.

В параметре domain указывается домен.

В параметре realm указывается имя Kerberos realm для сервера управления доступом.

В параметрах admin-password и ds-password указывается пароль для административного пользователя (Внутренний администратор Средства управления доменными пользователями (admin)) и пароль, который будет использоваться сервером каталогов, соответственно.

В данной конфигурации эти параметры принимают следующие значения:

```
<ptr_net> - 2.10.10.in-addr.arpa.
<domain.local> - fintech.ru
<realm> - FINTECH.RU
<admin-password> - 12345678
<ds-password> - 12345678
```

Данная команда должна завершиться без ошибок.

По окончании выполнения команды Web-интерфейс Средства управления доменными пользователями будет доступен по полному доменному имени sintezm-ipa.fintech.ru. Для того что бы зайти на сервер управления доступом необходимо на АРМ добавить узлы самой ИПА в файл /etc/hosts, в виде записи:

```
10.10.10.73 sintezm-ipa.fintech.ru
```

Далее надо запустить web-браузер и в адресной строке браузера прописать URL

```
https://sintezm-ipa.fintech.ru
```

После чего на странице аутентификации необходимо ввести учётные данные в поле «Имя пользователя» значение admin, в поле «Пароль» – 12345678 (рисунок 3.47)

Рисунок 3.47 – Web-интерфейс Средства управления доменными пользователями

После получения доступа в web-интерфейс Средства управления доменными пользователями необходимо завершить настройку сервера управления доступом. Для этого необходимо включить две опции: ipauniqueid и postalcode. Это можно сделать

следующим образом: перейти по пунктам меню «ИПА Сервер» -> «Контроль доступа на основе ролей» -> «Права доступа». Найти правило под названием «System: Read следующих позиций:

- ipauniqueid;
- postalcode;
- st;
- carlicense.

После чего нажать на «Сохранить» (рисунок 3.48).

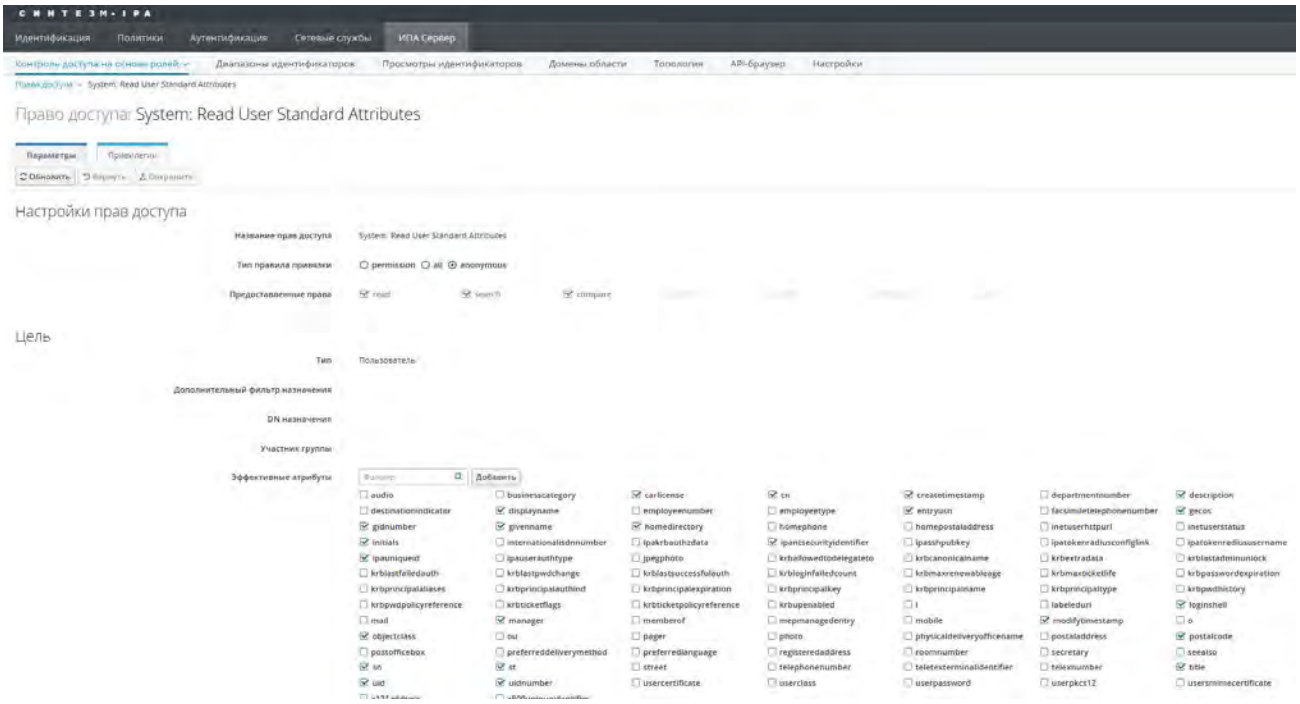
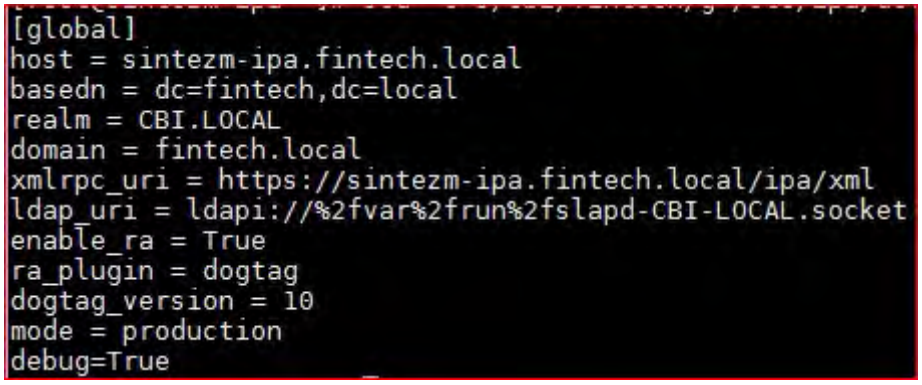


Рисунок 3.48 – Правило «System: Read User Standard Attributes»

Для настройки аудита необходимо добавить параметр debug=true в секцию [global] конфигурационного файла /etc/ipa/default.conf. Например:



Для настройки подключения к порталу средства управления виртуализации необходимо в конфигурационном файле /etc/nginx/nginx.conf привести опции в соответствие для секции http:

В файле /etc/httpd/conf.modules.d/00-lua.conf закомментировать строку:

```
LoadModule lua_module modules/mod_lua.so
```

, а так же переопределить или добавить глобальную опцию в файле /etc/httpd/conf/httpd.conf :

```
TraceEnable off
```

В файлах /etc/httpd/conf.d/*.conf привести опции в соответствие для всех секций VirtualHost где используется шифрование через SSL engine:

```
SSLProtocol         all -SSLv3
SSLHonorCipherOrder on SSLCipherSuite "EECDH+ECDSA+AESGCM
EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256
EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH+aRSA+RC4 EECDH EDH+aRSA
RC4 !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS +RC4 RC4"
```

3.4.4.6. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с выбранной схемой аутентификации согласно п.3.7.2.

3.4.4.7. Настройка централизованного аудита

Для функционирования централизованного аудита на сервере управления доступом (сообщения транслируются на сервер безопасности) необходимо привести файл /etc/rsyslog.d/rsyslog-send.conf к следующему виду:

```
module(load="omrelp")
```

```
if ( $programname == "dlogevent" ) then {
    action(
        type="omrelp"
        Target="[ip-адрес сервера безопасности]"
        Port="2514"
        queue.type="LinkedList"
        queue.size="10000"
        queue.filename="q_sendRule"
        queue.highwatermark="9000"
        queue.lowwatermark="50"
        queue.maxdiskspace="1g"
        queue.saveonshutdown="on"
        action.resumeRetryCount="-1"
        action.resumeInterval="3"
    )
}
```

, где `[ip-адрес сервера безопасности]` – адрес сервера безопасности на который будут пересылаться события безопасности.

А также привести файл /etc/rsyslog.d/rsyslog-ipa.conf к следующему виду:

```
$ModLoad imfile
# /var/log/httpd/error_log
$InputFileName /var/log/httpd/error_log
$InputFileTag ipa:
$InputFileStateFile ipa_log.state
$InputFileSeverity info
$InputFileFacility local1
$InputRunFileMonitor
# /var/log/krb5kdc.log
$InputFileName /var/log/krb5kdc.log
$InputFileTag krb5kdc:
$InputFileStateFile krb5kdc_log.state
$InputFileSeverity info
$InputFileFacility local1
$InputRunFileMonitor
```

После внесений изменений в файл перезагрузить сервисы rsyslog и dlogevent:

```
service rsyslog restart
service dlogevent restart
```

3.4.4.8. Настройка Apache Tomcad

Для повышения защищённости Apache Tomcat необходимо осуществить его дополнительное конфигурирование:

1) настройка ограничения доступа к внутренним приложениям минимально необходимым диапазоном адресов/доменов. Необходимо добавить в секцию <Context> конфигурационных файлов /etc/pki/pki-tomcat/context.xml, /etc/tomcat/context.xml, /usr/share/pki/server/conf/context.xml строку:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1|::1|0:0:0:0:0:0:0:1|[ip-адрес ИПЫ]|[диапазон ip]"/>
```

, где [диапазон ip] – соответствует wildcard ip адресов с которых будет разрешено подключение.

Например:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1|::1|0:0:0:0:0:0:0:1|10.0.57.*"/>
```

2) настройка логирования текущего web.xml. Необходимо добавить параметр logEffectiveWebXml="true" в файлы /etc/pki/pki-tomcat/context.xml, /etc/tomcat/context.xml, /usr/share/pki/server/conf/context.xml

```
# sed -i 's/<Context>/<Context logEffectiveWebXml="true">/g'
/etc/pki/pki-tomcat/context.xml /etc/tomcat/context.xml
/usr/share/pki/server/conf/context.xml
```

3) настройка использования дополнительных источников метаданных при развертывании веб-приложений. Необходимо добавить параметр metadata-complete="true" в элементы web-app для всех приложений.

```
# sed -i 's/<web-app/<web-app metadata-complete="true"/g' /etc/pki/pki-
tomcat/web.xml /etc/tomcat/web.xml /usr/share/pki/ca/conf/web.xml
/usr/share/pki/ca/webapps/ROOT/WEB-INF/web.xml
/usr/share/pki/ca/webapps/ca/WEB-INF/web.xml
/usr/share/pki/kra/conf/web.xml /usr/share/pki/kra/webapps/ROOT/WEB-
INF/web.xml /usr/share/pki/kra/webapps/kra/WEB-INF/web.xml
/usr/share/pki/server/conf/web.xml
/usr/share/pki/server/webapps/ROOT/WEB-INF/web.xml
```

4) отключение отображения отладочной информации если во время обработки запроса возникает ошибка. Необходимо:

— добавить в файл /var/lib/pki/pki-tomcat/conf/web.xml строки следующего содержания (рисунок 3.49)

```
<error-page>
    <error-code>404</error-code>
    <location>/404.html</location>
</error-page>

<error-page>
    <error-code>500</error-code>
    <location>/500.html</location>
</error-page>
```

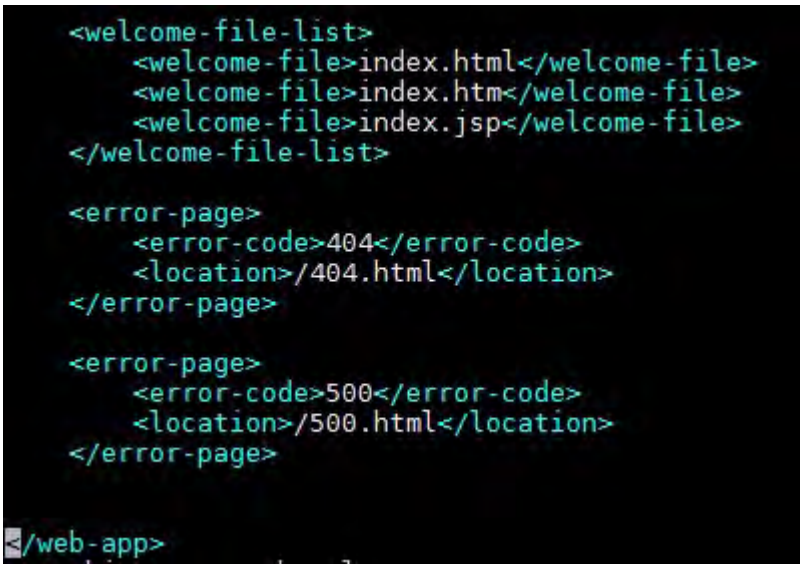


Рисунок 3.49 – Настройка web.xml

— Скопировать файлы которые будит отображаться при наступлении ошибки

```
# cp /usr/share/pki/ca/webapps/ca/404.html
/usr/share/pki/server/webapps/ROOT
# cp /usr/share/pki/ca/webapps/ca/500.html
/usr/share/pki/server/webapps/ROOT
```

— перезапустить Apache Tomcad

```
# systemctl restart  pki-tomcatd@pki-tomcat.service
```

5) Отключение заголовка X-Powered-By и изменение значения Server. Необходимо выполнить команду:

```
# sed -i 's/<Connector/<Connector xpoweredBy="false" server="-"/g' /etc/pki/pki-tomcat/server.xml /usr/share/pki/server/conf/server.xml /etc/tomcat/server.xml
```

6) Ограничение доступа к $CATALINA_HOME, $CATALINA_BASE, каталогу конфигурации Tomcat, каталогу исполняемых файлов, каталогу веб-приложений, catalina.properties, context.xml. logging.properties, server.xml, web.xml

Необходимо выполнить команды:

```
# chmod g-w,o-rwx /usr/share/tomcat /etc/tomcat /usr/share/java/tomcat /var/log/tomcat /var/cache/tomcat/temp /var/lib/tomcat/webapps /var/cache/tomcat/work
# chown pkiuser:pkiuser /usr/share/tomcat /etc/tomcat /usr/share/java/tomcat /var/log/tomcat /var/cache/tomcat/temp /var/lib/tomcat/webapps /var/cache/tomcat/work

# chmod g-w,o-rwx /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat/alias /usr/share/tomcat/bin /usr/share/pki/server/common /etc/pki/pki-tomcat /var/log/pki/pki-tomcat /usr/sbin/tomcat
# chown pkiuser:pkiuser /var/lib/pki/pki-tomcat /etc/pki/pki-tomcat/alias /usr/share/tomcat/bin /usr/share/pki/server/common /etc/pki/pki-tomcat /var/log/pki/pki-tomcat /usr/sbin/tomcat

# locate catalina.properties |xargs chmod g-w,o-rwx
# locate catalina.properties |xargs chown pkiuser:pkiuser

# locate context.xml |xargs chmod g-w,o-rwx
# locate context.xml |xargs chown pkiuser:pkiuser

# locate logging.properties |xargs chmod g-w,o-rwx
# locate logging.properties |xargs chown pkiuser:pkiuser

# locate server.xml |xargs chmod g-w,o-rwx
# locate server.xml |xargs chown pkiuser:pkiuser

# locate web.xml |xargs chmod g-w,o-rwx
# locate web.xml |xargs chown pkiuser:pkiuser
```

7) Настройка SSL протокола. Необходимо выполнить команды:

```
# sed -i 's/sslProtocol="SSL"/sslProtocol="TLSv1.2"/g' /etc/pki/pki-tomcat/server.xml
# sed -i 's/sslProtocol="SSL"/sslProtocol="TLSv1.2"/g' /usr/share/pki/server/conf/server.xml
# sed -i 's/sslProtocol="TLS"/sslProtocol="TLSv1.2"/g' /etc/tomcat/server.xml
```

8) Настройка ограничения размера файла журнала

```
# sed -i '/^[^#]/ s/\(^1catalina.org..*$\)/#\ \1/' /var/lib/pki/pki-tomcat/conf/logging.properties
# sed -i 's/1catalina.org.apache.juli.FileHandler/1catalina.java.util.logging.FileHandler/g' /var/lib/pki/pki-tomcat/conf/logging.properties
```

```
# cat << EOF >> /var/lib/pki/pki-tomcat/conf/logging.properties
1catalina.java.util.logging.FileHandler.level = FINEST
1catalina.java.util.logging.FileHandler.pattern = \${catalina.base}/logs/catalina%g.log
1catalina.java.util.logging.FileHandler.limit = 5000000000
1catalina.java.util.logging.FileHandler.count = 5
1catalina.java.util.logging.FileHandler.formatter = java.util.logging.SimpleFormatter
EOF
```

9) Настройка обработчиков в logging.properties

```
# sed -i 's/java.util.logging.ConsoleHandler.level\ =\ FINE/java.util.logging.ConsoleHandler.level\ =\ FINEST/g' /var/lib/pki/pki-tomcat/conf/logging.properties
```

10) Отключение автоматического развертывания приложений

```
# locate server.xml | xargs sed -i 's/autoDeploy="true"/autoDeploy="false"/g'
```

11) Отключение развертывания при запуске приложений

Указать параметр deployOnStartup="false" в секции «<Host» в /etc/pki/pki-tomcat/server.xml, /etc/tomcat/server.xml, /usr/share/pki/server/conf/server.xml

Рисунок 3.50 - Отключение развертывания при запуске

12) настройка ограничения доступа к веб-администрированию необходимым диапазоном адресов/доменов. Необходимо добавить в секцию «</Host>» (</Server></Service></Engine>) конфигурационного файла /var/lib/pki/pki-tomcat/conf/server.xml строку:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1|::1|0:0:0:0:0:0:0:1|[ip-адрес ИПЫ]|[диапазон ip]"/>
```

, где [диапазон ip] – соответствует wildcard ip адресов с которых будет разрешено подключение.

Например:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="127\.0\.0\.1|::1|0:0:0:0:0:0:0:1|10.0.57.*"/>
```

3.4.5. Установка и настройка ВМ Сервер безопасности

3.4.5.1. Установка ВМ Сервер безопасности

Сервер безопасности устанавливается в виде виртуальной машины. Для этого необходимо в Менеджере ВМ создать виртуальную машину согласно пункту 3.4.3 , данного документа.

Для установки ОС на ВМ Сервера безопасности необходимо произвести действия описанные в пункте 3.1 данной инструкции, после чего в окне «Выбор программ» в качестве базового окружения выбрать позицию «Сервер-СБ» (рисунок

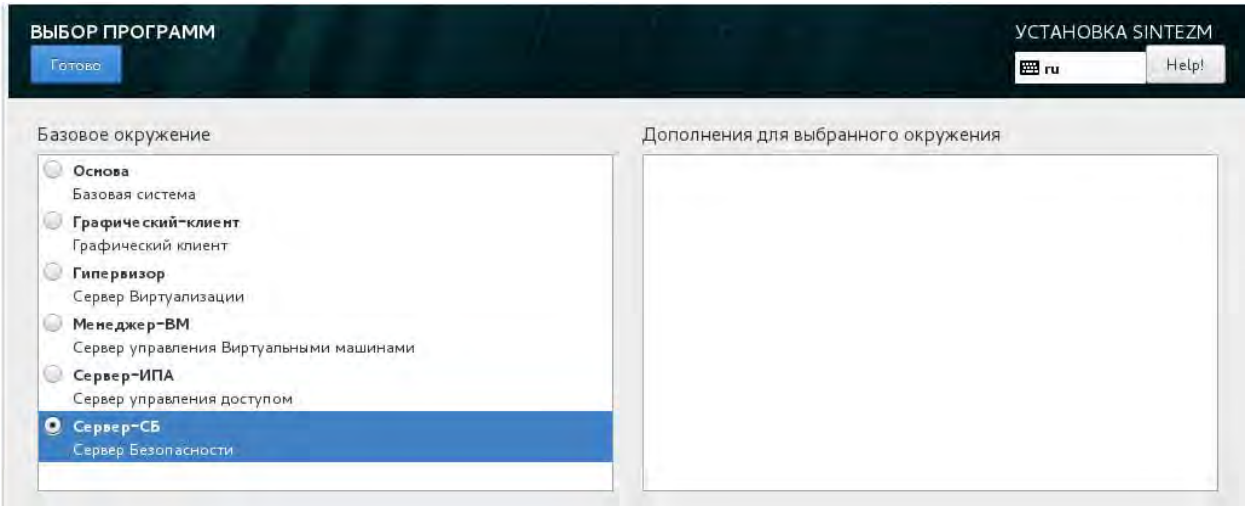


Рисунок 3.51 – Окно выбора программ

3.4.5.2. Настройка места установки для сервера виртуализации

Настройка места установки при установке сервера безопасности производится аналогично порядку, описанному в пункте 3.2.1.1.

3.4.5.3. Конфигурирование сети и имени узла

Конфигурирование сети и имени узла при установке сервера безопасности производится аналогично порядку, описанному в пункте 3.2.1.2.

3.4.5.4. Назначение региональных настроек

Настройка даты и времени при установке сервера безопасности производится аналогично порядку, описанному в пункте 3.2.1.3.

3.4.5.5. Предварительная настройка ОС

Предварительная настройка ОС для ВМ сервера безопасности осуществляется аналогично порядку, описанному в пункте п. 3.4.1.4.

3.4.5.6. Настройка сервера безопасности

3.4.5.6.1. Добавление сервера безопасности в Сервер управления доступом

Примечание. Выполнение данного пункта необходимо осуществить после установки и настройки Сервера управления доступом (см п.3.4.4).

После установки сервера безопасности узел необходимо добавить в сервер управления доступом. Данная операция осуществляется согласно п. 3.5 «Добавление узла в Сервер управления доступом» Руководство системного программиста» (ТАСП.62.01.12.000.005 32).

3.4.5.6.2. Инициализация БД хранения событий безопасности

Для настройки Сервера Безопасности необходимо предварительно провести инициализацию СУБД командой:

```
/usr/pgsql-9.5/bin/postgresql95-setup initdb
```

По окончанию выполнения данной операции необходимо отключить все типы авторизации для доступа к БД за исключением локальной. Для этого необходимо открыть файл pg_hba.conf на редактирование командой:

```
vim /var/lib/pgsql/9.5/data/pg_hba.conf
```

Найти строку:

```
local  all            all       ipeer
```

и заменить её на:

```
local  all            all       trust
```

Далее необходимо определить директорию формирования файла unix сокета, для этого необходимо в конфигурационном файле:

```
/var/lib/pgsql/9.5/data/postgresql.conf
```

изменить с:

```
#unix_socket_directories  =  '/var/run/postgresql,  /tmp'   #  comma-
separated list of directories
```

на:

```
unix_socket_directories  =  '/var/run/postgresql,  /tmp'    #  comma-
separated list of directories
```

После чего добавить в автозапуск и запустить сервис postgresql-9.5.service командами:

```
systemctl enable postgresql-9.5.service
systemctl start postgresql-9.5.service
```

Далее необходимо скопировать iso-файл дистрибутива КП «ЗОС «СинтезМ» на ВМ сервера безопасности и примонтировать его в директорию /mnt. Копирование iso-файла осуществляется командой scp:

```
scp [путь до iso-образа дистрибутива] root@[ip-адрес сервера безопасности]:/[путь до директории для сохранения]
```

Например:

```
scp sintez-m-7-x86_64.iso root@10.10.10.50:~
```

Монтирование iso-файла выполняется командой

```
mount sintez-m-7.x86_64.iso /mnt
```

После того как iso-файл примонтирован, необходимо переустановить rpm-пакет , для того чтобы в СУБД создалась база данных, которая требуется для работы Сервера Безопасности. Перед установкой пакета необходимо удалить его предыдущую версию командой:

```
rpm -e --noscripts --nodeps pszi-sb-db-[версия пакета]
```

Примечание Версию установленного пакета можно проверить командой: rpm –aq |grep pszi-sb-db

Установка rpm-пакета выполняется командой:

```
rpm -ihv --force /mnt/Packages/pszi-sb-db-[версия пакета].x86_64.rpm
```

3.4.5.6.3. Настройка портала Сервера безопасности

Далее необходимо отредактировать конфигурационный файл settings.py командой:

```
vim /opt/sb/epu/epu/settings.py
```

В данном файле надо найти строку начинающуюся с `DEFAULT_MANAGER = {` и привести весь конфигурационный блок к следующему виду:

```
DEFAULT_MANAGER = {
    'addr': '10.10.10.125',
    'hostname': 'sintezm-m.fintech.ru',
    'internalusername': 'admin',
    'internalpassword': '12345678',
    'ovirt_db_password': '12345678'
}
```

Затем необходимо отключить SELinux командой:

```
setenforce 0
```

З

```
SELINUX=permissive
```

Для настройки подключения к порталу сервера безопасности необходимо конфигурационном файле /etc/nginx/nginx.conf привести опции в соответствие для секции http:

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_prefer_server_ciphers on;
ssl_stapling on;
ssl_ciphers        'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-
RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-
AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-
ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-
SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-
SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-
GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-
SHA:AES:CAMELLIA:DES-CBC3-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!aECDH:EDH-DSS-DES-CBC3-
SHA:EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-
SHA:kEECDH+AES128:kEECDH:kEDH:kRSA+AES128:kEDH+3DES:!LOW:!SEED:!IDEA:!
SRP:!SSLv2:!SSLv3:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDSA+SHA
256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+aRSA:
!RC4:RC4:EECDH+AESGCM:AES256+EECDH:AES256+EDH:DHE-RSA-AES256-GCM-
SHA384:ECDHE-RSA-DES-CBC3-
SHA:EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:EECDH+ECDSA+SHA384:EECDH+ECDS
A+SHA256:EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH+aRSA+RC4:EECDH:EDH+
aRSA:!3DES:!DSS:RC4-MD5:RC4-SHA:DES-CBC-SHA:EDH-RSA-DES-CBC-SHA:EDH-
DSS-DES-CBC-SHA:EXP-RC4-MD5:EXP-DES-CBC-SHA:EXP-EDH-RSA-DES-CBC-
SHA:EXP-EDH-DSS-DES-CBC-SHA:DES-CBC3-MD5:DHE-DSS-AES128-SHA:RC2-CBC-
MD5:DES-CBC-SHA:DES-CBC-MD5:EXP-RC2-CBC-MD5:EXP-RC2-CBC-MD5:ECDH-
ECDSA-RC4-SHA:ECDH-ECDSA-AES128-SHA:ECDH-ECDSA-AES256-SHA:ECDH-RSA-
RC4-SHA:ECDH-RSA-AES128-SHA:ECDH-RSA-AES256-SHA:ECDHE-ECDSA-RC4-
SHA:ECDHE-RSA-RC4-SHA:ECDH-ECDSA-DES-CBC3-SHA:ECDH-RSA-DES-CBC3-
SHA:ECDHE-ECDSA-DES-CBC3-SHA:NULL-MD5:NULL-SHA:IDEA-CBC-SHA:EXP-ADH-
RC4-MD5:ADH-RC4-MD5:EXP-ADH-DES-CBC-SHA:ADH-DES-CBC-SHA:ADH-DES-CBC3-
SHA:KRB5-DES-CBC-SHA:KRB5-RC4-SHA:KRB5-IDEA-CBC-SHA:KRB5-DES-CBC-
MD5:KRB5-DES-CBC3-MD5:KRB5-RC4-MD5:KRB5-IDEA-CBC-MD5:EXP-KRB5-DES-CBC-
SHA:EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-RC4-SHA:EXP-KRB5-DES-CBC-MD5:EXP-
```

```
KRB5-RC2-CBC-MD5:EXP-KRB5-RC4-MD5';
fastcgi_param SSL_VERIFIED $ssl_client_verify;
fastcgi_param SSL_CLIENT_SERIAL $ssl_client_serial;
fastcgi_param SSL_CLIENT_CERT $ssl_client_cert;
fastcgi_param SSL_DN $ssl_client_s_dn;
add_header Strict-Transport-Security max-age=15768000;
```

Далее необходимо перезапустить сервисы nginx и sbuwsgi командами:

```
systemctl restart nginx
systemctl restart sbuwsgi.service
```

После чего станет доступен web-интерфейс Портала Управления по адресу http://10.10.10.50/ (рисунок 3.52)

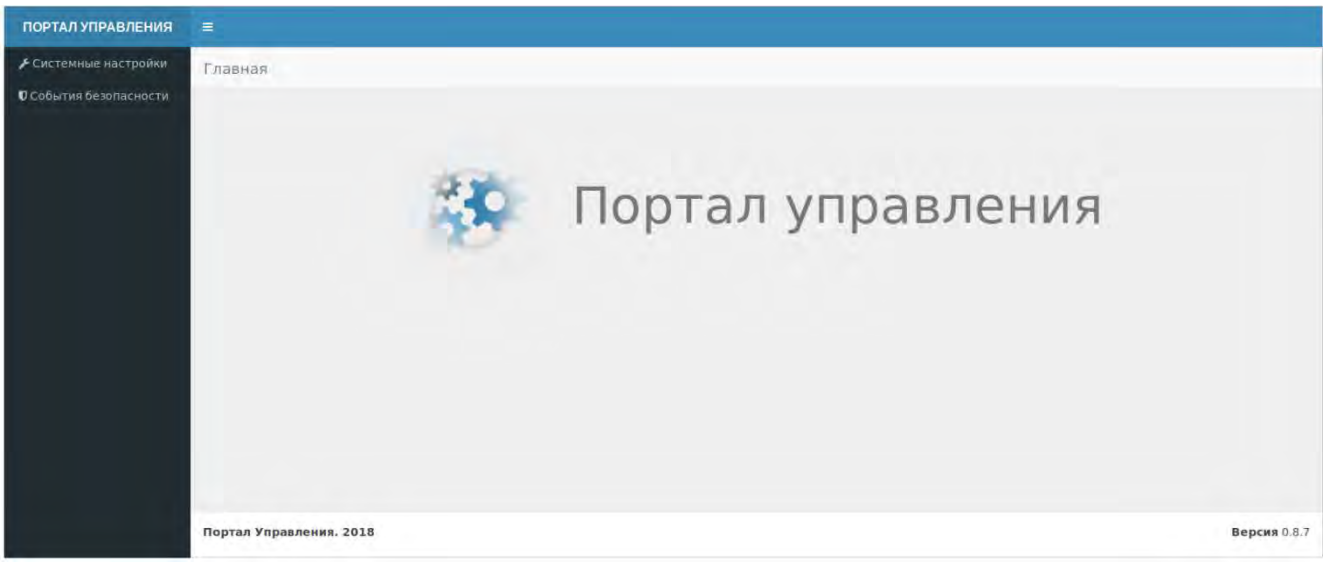


Рисунок 3.52 – Портал управления

3.4.5.6.4. Настройка сбора событий безопасности

Сервер безопасности является модулем КП «ЗОС «СинтезМ» и реализует функцию сбора событий безопасности, генерируемых различными агентами безопасности, и их представление на портале управления.

Настройка сервера безопасности заключается в конфигурировании перечня файлов, перечисленных ниже:

```
/etc/nginx/conf.d/arm-obi.conf;
/etc/dlogevent/dlogevent.conf;
/etc/cron.d/systemevents_cleaning_schedule;
/etc/cron.d/systemevents_zip_cleaning_schedule;
```

Для настройки блокировки доступа WEB-интерфейса для всех ВМ, кроме автоматизированного рабочего места администратора (АРМ ОБИ), локальный администратор на сервере безопасности приводит содержание конфигурационного файла /etc/nginx/conf.d/arm-obi.conf в следующий формат:

```
server {
    listen 80;
    listen [::]:80;
    root /opt/sb/epu/gui/;
    index index.html index.htm;
    try_files $uri $uri/ /index.html;
   location /rest/ {
            proxy_pass http://localhost:8000;
    }
location / {
    allow [ip-адрес];
    deny all;
}
}
```

, где [ip-адрес] соответствует ip-адресу автоматизированного рабочего места администратора (АРМ ОБИ).

Для того, чтобы открыть и отредактировать конфигурационный файл, локальный администратор в командной строке выполняет команду:

```
 # vim /etc/nginx/conf.d/arm-obi.conf
```

Настройка получения и отправки системных сообщений, за которые отвечает модуль dlogevent, сервера безопасности осуществляется через конфигурационные файлы каталога /etc/rsyslog.d/, а также /etc/dlogevent/dlogevent.conf.

Настройка получения системных сообщений от других хостов проводится через конфигурационный файл /etc/rsyslog.d/rsyslog-receive.conf. Для получения системных сообщений содержимое конфигурационного файла должно выглядеть следующим образом:

```
$ModLoad imrelp
$InputRELPServerRun 2514
```

Следующим этапом является настройка сохранения системных сообщений в базе данных сервера безопасности. Для успешного сохранения локальному

администратору необходимо привести конфигурационный файл /etc/dlogevent/dlogevent.conf к следующему виду:

```
[PREV]
path = /var/lib/dlogevent/prev.sqlite
[PSQL]
enable = 1
host =
dbname = epu_mod
uname = dlogevent
upass =
```

Помимо вышеуказанных настроек, локальному администратору также необходимо настроить расписание вызова модулей, используемое планировщиком задач cron. Настройка расписания производится при помощи конфигурационного файла /etc/cron.d/systemevents_cleaning_schedule. Для обеспечения стабильной работы вызываемых модулей, локальному администратору необходимо привести содержимое данного конфигурационного файла к следующему виду:

```
00       00       1       1-12/2       *       root       /usr/bin/python
/opt/sb/epu/systemevents/unload_cleaning.py mode shedule
00       00/2       *       *       *       root       /usr/bin/python
/opt/sb/epu/systemevents/unload_cleaning.py mode memory,
```

где:

– первые «00» - определяют минуты;

– следующие «00» - определяют часы;

– «1» - определяет число месяца (может принимать значение от 1 до 31 соответственно);

– «1-12» - определяет месяц(-ы) (значение после месяца(-ев) (например, «/2», как на примере выше) обозначает периодичность применения команды. В данном случае имеется в виду, что команда будет действовать каждый месяц с 1-го по 12-ый;

– «root» - имя пользователя, с привилегиями которого будет запущена команда;

– «/usr/bin/python /opt/sb/epu/systemevents/unload_cleaning.py mode schedule» - адрес запускаемого модуля.

В данном случае в указанном конфигурационном файле хранится команда запуска модуля «Архиватор событий безопасности» (unload_cleaning.py) для архивации и последующей очистки журнала аудита.

В конфигурационном файле /etc/cron.d/systemevents_zip_cleaning_schedule содержится расписание условной ротации архивов журналов безопасности. Ниже приведено содержание данного конфигурационного файла:

```
0 1 * * * root cd /opt/security_events_files && ls -ltc | awk '{ if (!system("test -f " $9)) { size += $5; if (size > 50*2^30 ) system("rm " $9) } }'
```

В данном случае в конфигурационном файле указано условие ротации каталога /opt/security_events_files, содержащего файлы с архивами журналов событий безопасности, размер которого не должен превышать 50ГБ `(size > 50*2^30)`. В случае если суммарный размер хранящихся архивов в данной директории превышает 50 Гб, скрипт осуществит удаление самого старого из архивов.

3.4.5.6.5. Генерация инициализирующей последовательности

Генерация инициализирующей последовательности необходима для работы модуля dstreebog, при использовании доменной схемы аутентификации. Данное должно проводиться с АРМ ОБИ (необходимо наличие на АРМ/ВМ установленного агента безопасности администратора (admin-ab)) и персонального идентификатора пользователя СКЗИ «Рутокен ЭЦП 2.0 2100».

Для генерации инициализирующей последовательности нужно доменным администратором авторизоваться в АРМ ОБИ после чего зайти на веб-портал сервера безопасности, перейти в меню «Системные настройки» (рисунок 3.53).

Примечание. На целевом АРМ персональный идентификатор администратора (в качестве персонального идентификатора пользователя в КП «ЗОС «СинтезМ» применяется СКЗИ «Рутокен ЭЦП 2.0 2100» (сертификат № СФ/124-3673 ФСБ РФ) должен быть вставлен в USB порт.

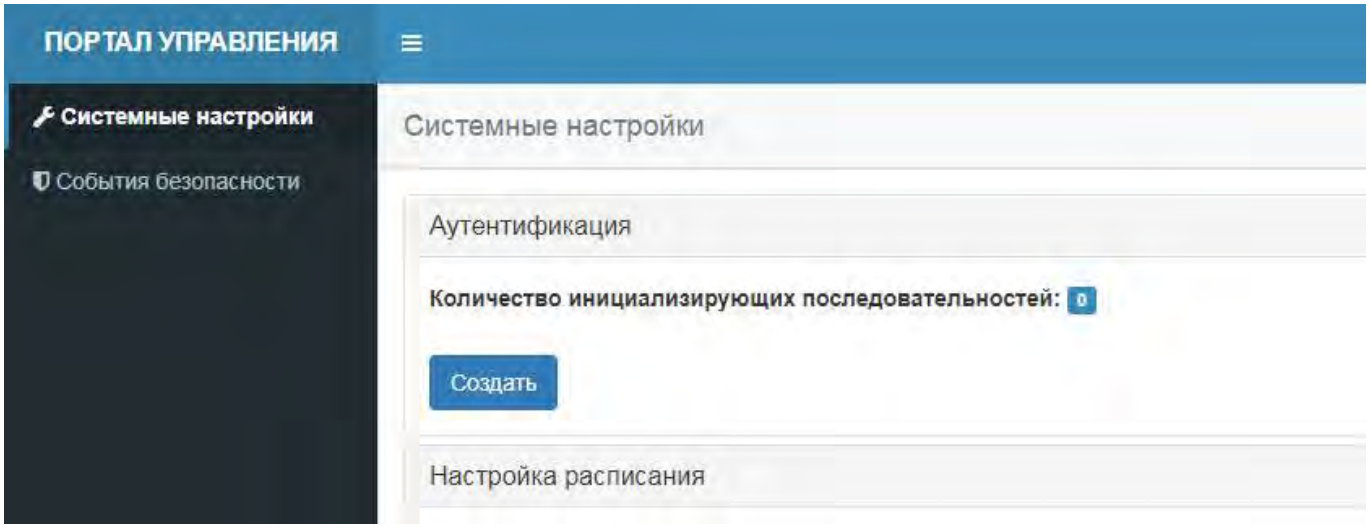


Рисунок 3.53 – Генерация инициализирующей последовательности

Перейти в раздел «Аутентификация», нажать на кнопку «Создать». В рабочей области отобразится форма «Введите пароль администратора» (Рисунок 3.54), где необходимо ввести PIN от подключенного персонального идентификатора.

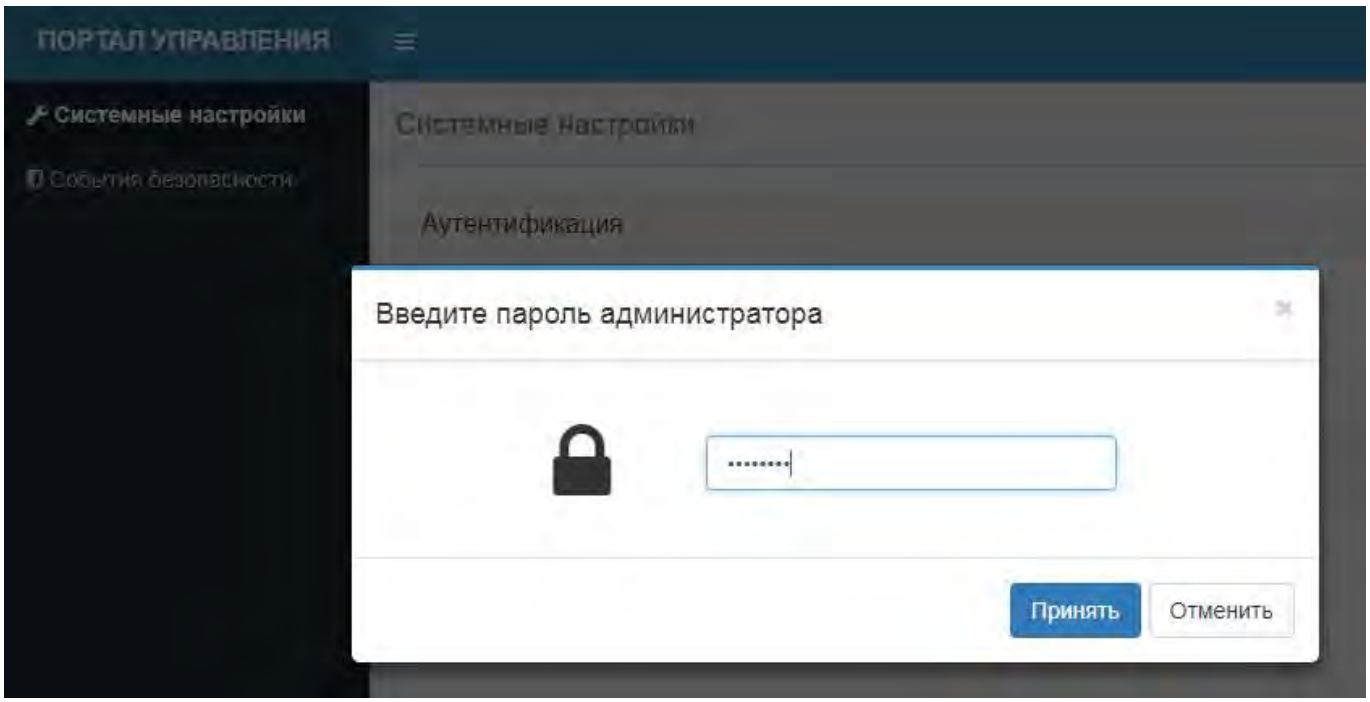


Рисунок 3.54 – Ввод пароля

При успешной генерации изменится счетчик «Количества инициализирующих последовательностей».

После чего необходимо осуществить перезагрузку модуля dstreebog командой

```
sudo systemctl restart dstreebog.service
```

3.4.5.6.6. Настройка базовой конфигурации

Настройка базовой конфигурации осуществляется в соответствии с выбранной схемой аутентификации согласно п. 3.7.2.

3.4.6. Создание учетной записи для доменного администратора

Для обеспечения возможности доменной аутентификации пользователей необходимо предварительно осуществить создание учетной записи доменного администратора. Для этого необходимо произвести следующие действия:

- подготовить персональный идентификатор для доменного администратора;
- отредактировать параметры учетной записи доменного администратора;
- добавить для пользователя роль доменного администратора;
- при необходимости сгенерировать инициализирующую последовательность на сервере безопасности (см. п 3.4.5.6.5);
- создать правило sudo для доменного администратора (при необходимости);
- включить доменную аутентификацию на АРМ ОБИ (см. п п.3.7.2);
- перезагрузить АРМ.

3.4.6.1. Подготовка персонального идентификатора для доменного администратора

Подготовка персонального идентификатора пользователя для доменного администратора выполняется на АРМ ОБИ командой cardtool-usermod. Для подготовки персонального идентификатора необходимо в консоли на АРМ ОБИ выполнить следующие действия:

- подключить персональный идентификатор в USB разъем на АРМ ОБИ;
- открыть на АРМ ОБИ эмулятор консоли и выполнить команду:

```
sudo cardtool-usermod
```

- далее необходимо следовать запросам программы:

• по запросу «[ ] Выбор ПИ» указать на персональный идентификатор прошивка которого будет осуществляется;

- по запросу «Выбор типа пользователя» указать, что прошивка персонального идентификатора осуществляется для доменного пользователя;
- по запросу «Использовать СБ по умолчанию» указать «y» если указан верный ip-адрес сервера безопасности или «n» для самостоятельного ввода ip-адрес сервера безопасности;
- по запросу «Имя пользователя:» указать логин пользователя, для которого выполняется прошивка персонального идентификатора, например protadm_d;
- по запросу «PIN пользователя:» указать PIN который будет использоваться пользователем в процессе аутентификации;
- по запросу «Использовать PIN администратора по умолчанию» указать «y» если PIN администратора для персонального идентификатора не был изменен ранее, или «n» для самостоятельного ввода PIN администратора для персонального идентификатора;
- на запрос «Установка флага администратора?» указать «y» для добавления метки администратора.

– дождаться окончания подготовки персонального идентификатора.

Процедура прошивки персонального идентификатора для администратора отображена на рисунке 3.55.

```
[root@sintezm-adm1 ~]# cardtool-usermod
Запуск cardtool-usermod [START]
[ ] Выбор ПИ
1) [OK]Slot #0: 3924582a
#? 1
Выбран [OK]Slot #0: 3924582a (пункт: 1)
Слот ПИ: 0
Серийный номер ПИ: 3924582a
[OK] Выбор ПИ
[ ] Выбор типа пользователя
1) Доменный
2) Локальный
#? 1
Выбран Доменный (пункт: 1)
[OK] Выбор типа пользователя
Использовать СБ по-умолчанию(10.10.3.84)? [y/n]n
Адрес СБ:10.10.10.50
Сервер Безопасности: 10.10.10.50
ПИ прикреплён к другому пользователю? [y/n]n
Имя пользователя:protadm_d
PIN пользователя:
Использовать PIN администратора по-умолчанию? [y/n]n
PIN администратора:
Установка флага администратора? [y/n]y
[ ] Инициализация ПИ
[OK] Инициализация ПИ
[ ] Установка PIN пользователя на ПИ
[OK] Установка PIN пользователя на ПИ
[ ] Установка имени пользователя на ПИ
[OK] Установка имени пользователя на ПИ
[ ] Установка флага администратора
[WR] Установка флага администратора
[OK] Установка флага администратора
[ ] Создание группы на СБ
[OK] Создание группы на СБ
[ ] Создание пользователя на СБ
[OK] Создание пользователя на СБ
[ ] Генерация ГОСТ ключей на ПИ
[OK] Генерация ГОСТ ключей на ПИ
[ ] Прикрепление ПИ к пользователю на СБ
[OK] Прикрепление ПИ к пользователю на СБ
[ ] Генерация сертификата
Using slot with index 0 (0x0)
[OK] Генерация сертификата
[ ] Загрузка сертификата на ПИ
Using slot with index 0 (0x0)
[OK] Загрузка сертификата на ПИ
Завершение cardtool-usermod [DONE]
```

Рисунок 3.55 – Прошивка персонального идентификатора для администратора безопасности

3.4.6.2. Редактирование параметров учетной записи доменного администратора

Для редактирования параметров учетной записи доменного администратора необходимо выполнить следующие действия:

– авторизоваться в средстве управления доменными пользователями. Для этого необходимо в адресной строке браузера ввести адрес сервера управления доступом, после чего в открывшемся окне (Рисунок 3.56) ввести логин и пароль доменного администратора. При первичном создании доменного администратора необходимо воспользоваться учетной записью внутреннего администратора Средства управления доменными пользователями (admin) создаваемой на этапе установки сервера управления доступом.

Рисунок 3.56 – Аутентификация в средстве управления доступом

– перейти в раздел «Идентификация» → «Пользователи» → «Активные пользователи» (Рисунок 3.57). В таблице представления пользователей выбрать пользователя которому необходимо назначить роль доменного администратора и для которого был подготовлен персональный идентификатор.

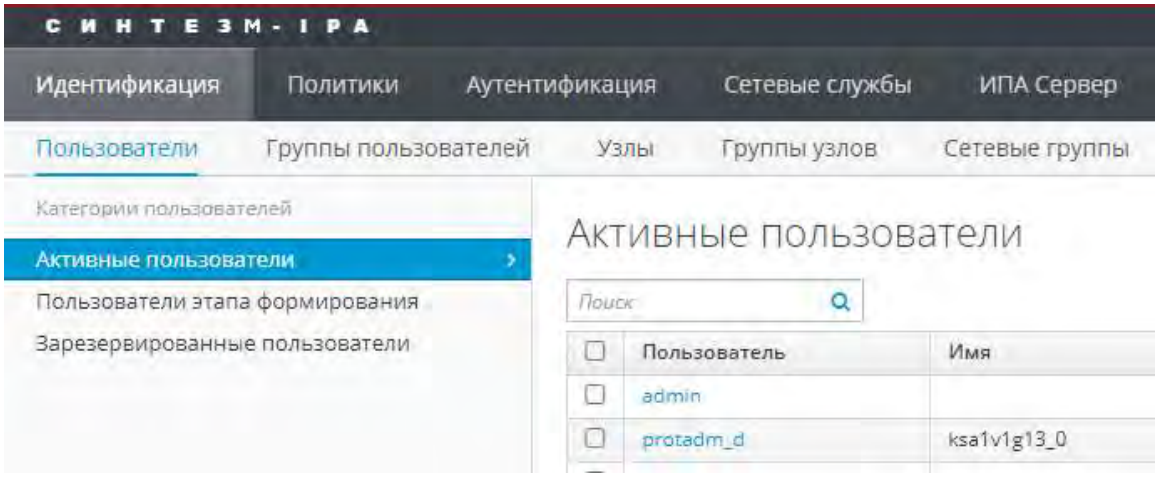


Рисунок 3.57 – Вкладка «Активные пользователи»

– в открывшемся окне параметров пользователя (Рисунок 3.58) необходимо, в разделе «Адрес эл.почты», заполнить поля «Область» и «Индекс»;

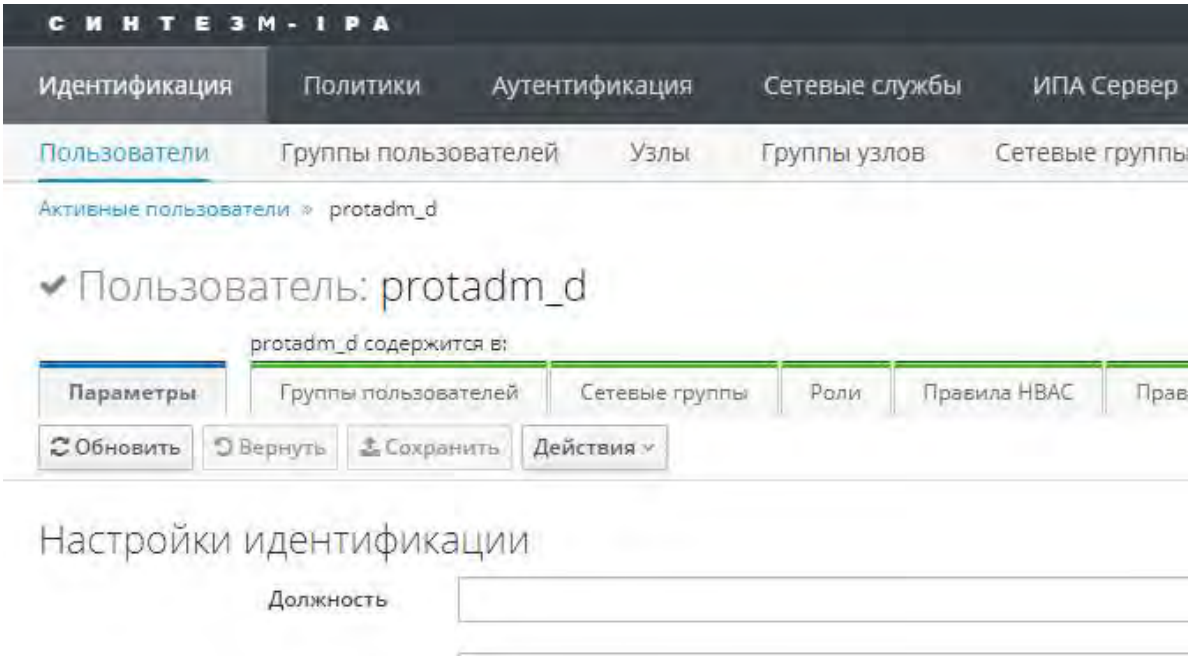


Рисунок 3.58 – Параметры пользователя

– поле «Область» должно содержать IP-адрес Сервера безопасности (Рисунок 3.59);

– поле «Индекс» должно содержать IP-адрес Менеджера виртуализации (Рисунок 3.59);

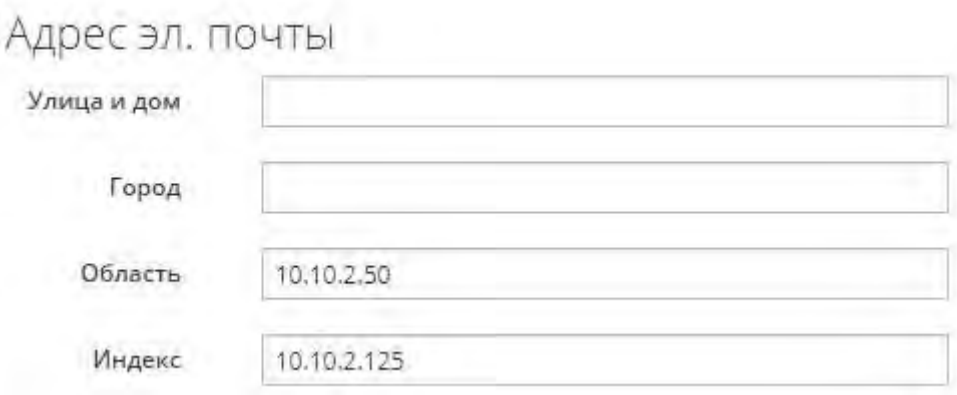


Рисунок 3.59 - Раздел «Адрес эл.почты»

3.4.6.3. Добавление пользователю роли доменного администратора

Для добавления пользователю роли доменного администратора необходимо выполнить следующие действия:

– авторизоваться в средстве управления доменными пользователями. Для этого необходимо в адресной строке браузера ввести адрес сервера управления доступом,

после чего в открывшемся окне (Рисунок 3.56) ввести логин и пароль доменного администратора. При первичном создании доменного администратора необходимо воспользоваться учетной записью внутреннего администратора Средства управления доменными пользователями (admin) создаваемой на этапе установки сервера управления доступом.

– перейти в раздел «Идентификация» → «Пользователи» → «Активные пользователи». В таблице представления пользователей выбрать пользователя которому необходимо назначить роль доменного администратора и для которого был подготовлен персональный идентификатор.

– в настройках пользователя выбрать вкладку «Группы пользователей» после чего нажать на кнопку «Добавить».

– в интерфейсе добавления группы выбрать из списка доступных групп (Доступно) группу «admins», после чего нажатием на кнопку > переместить группу «admins» из списка доступных в список Ожидаемых (Рисунок 3.60).

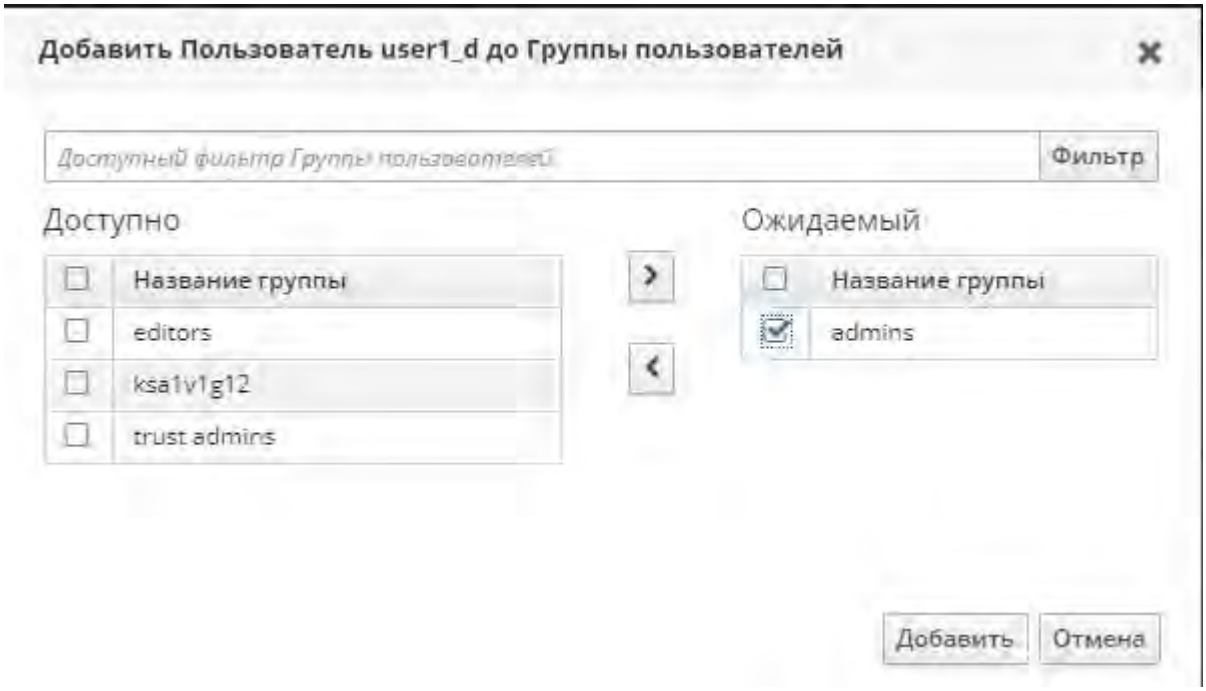


Рисунок 3.60 – Добавление группы

– нажать на кнопку «Добавить».

3.4.6.4. Создание правила sudo

Примечание: Создание правила Sudo для учетной записи осуществляется при необходимости назначения пользователю роли локального администратора в ОС.

Sudo (англ. *substitute user and do*, дословно «подменить пользователя и выполнить») –программа для системного администрирования UNIX-систем, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы. Основная идея — дать пользователям как можно меньше прав, при этом достаточных для решения поставленных задач. Правило sudo необходимо для выполнения операций требующих привилегий суперпользователя. Для создания правила sudo для доменного администратора необходимо

– авторизоваться в средстве управления доменными пользователями. Для этого необходимо в адресной строке браузера ввести адрес сервера управления доступом, после чего в открывшемся окне (Рисунок 3.56) ввести логин и пароль доменного администратора. При первичном создании доменного администратора необходимо воспользоваться учетной записью внутреннего администратора Средства управления доменными пользователями (admin) создаваемой на этапе установки сервера управления доступом.

– выполнить переход во вкладку главного меню «Политики» выбрать вкладку «Административный доступ», из выпадающего меню выбрать «Правила Sudo» (Рисунок 3.61);

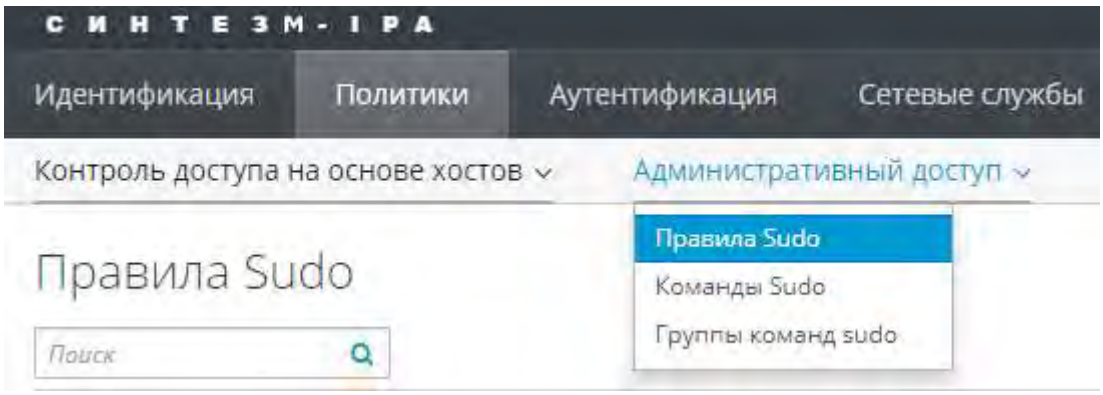


Рисунок 3.61 – Правила SUDO

– в интерфейсе «Правила Sudo» нажать на кнопку «Добавить»;

– в открывшемся окне (Рисунок 3.62) задать имя правила (например admin_sudo), после чего нажать на кнопку «Добавить и изменить»;

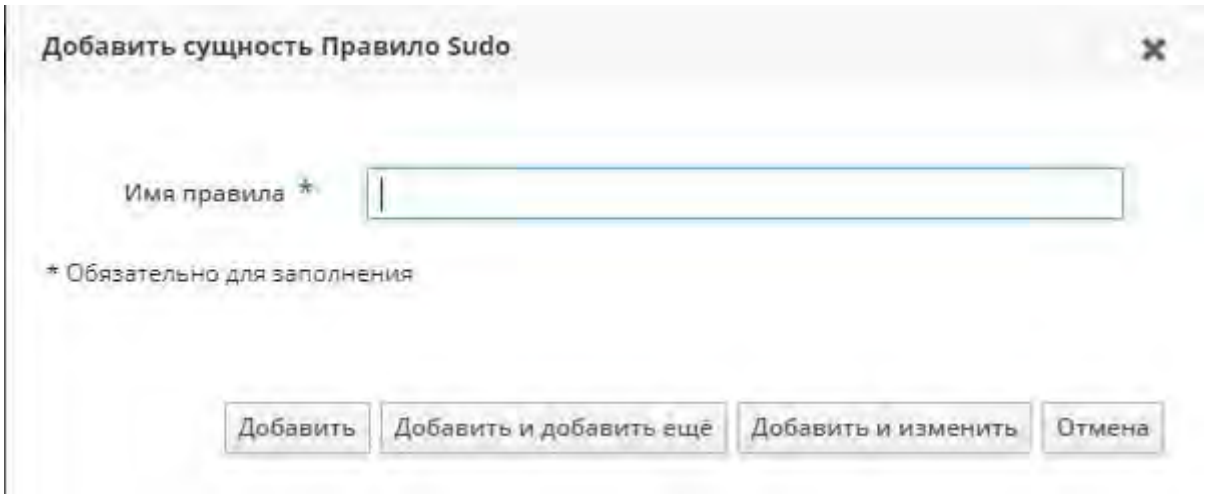


Рисунок 3.62 – Добавление правила Sudo

– в настройках правила, в секции "Параметры", нажать на кнопку "Добавить", ввести в появившемся окне (Рисунок 3.63) "!authenticate", выбрать "Добавить";

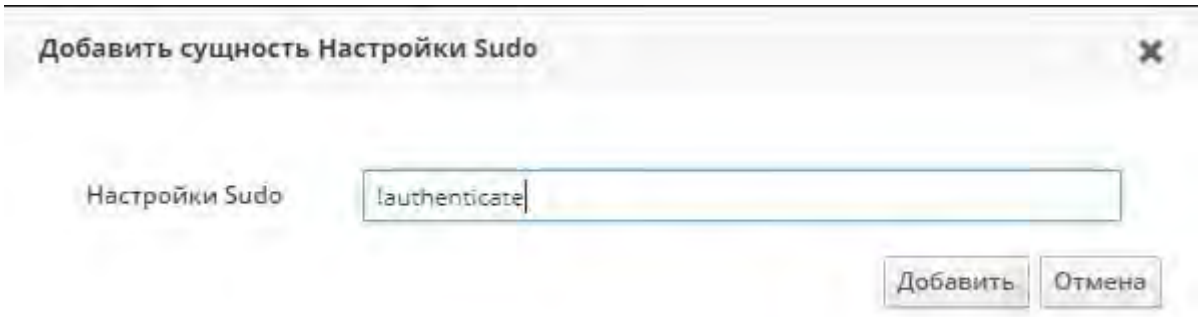


Рисунок 3.63 – Добавление параметра sudo

– в настройках правила, в секции «Кто», установить параметр «Указанные пользователи и группы», после чего добавить к правилу группу «admins»;

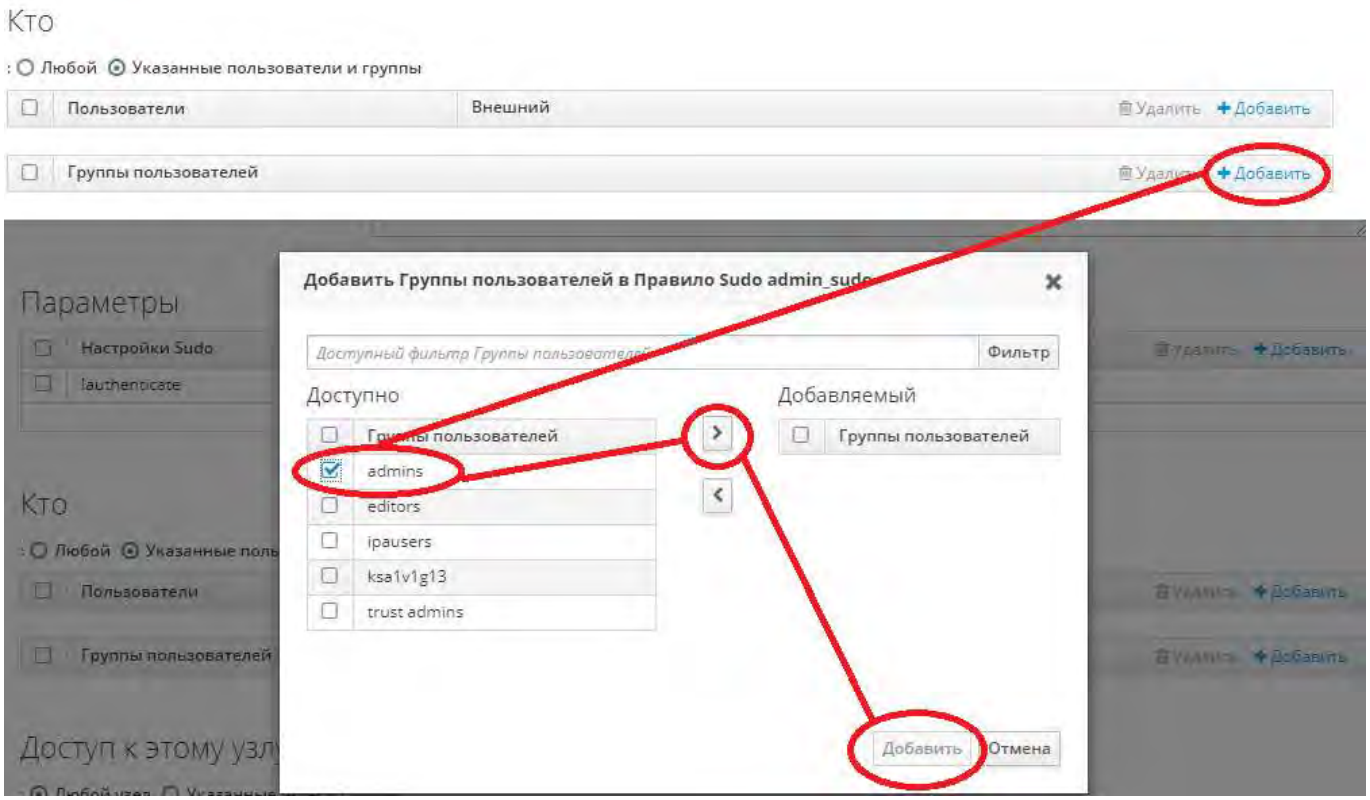


Рисунок 3.64 – Добавление группы к правилу

– в секции «Доступ к этому узлу», установить параметр «Любой узел»;

– в секции «Выполнение команд», установить параметр «Любая команда»;

– в секции «От имени», установить параметры «Любой» и «Любая группа»;

– после внесения всех изменений нажать на кнопку «сохранить» (Рисунок 3.65);

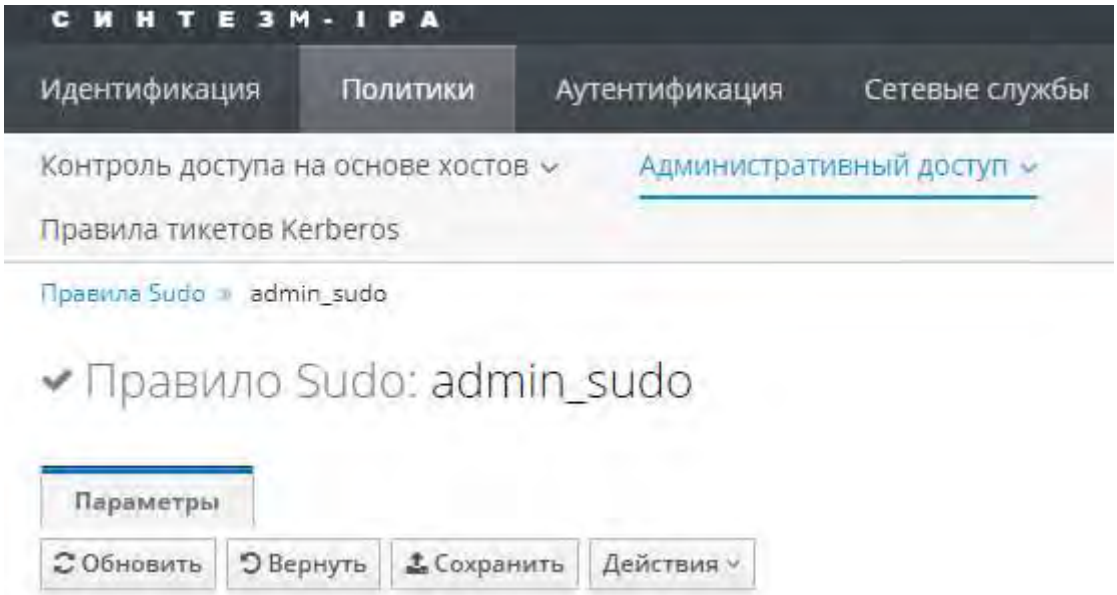


Рисунок 3.65 – Сохранение правила SUDO

3.4.7. Создание учетной записи системного администратора

Для обеспечения возможности управления средой виртуализацией (Менеджером ВМ) необходимо предварительно осуществить создание учетной записи системного администратора. Для этого необходимо произвести следующие действия:

– подготовить персональный идентификатор для системного администратора;

– отредактировать параметры учетной записи доменного системного администратора в Средстве управления доменными пользователями;

– добавить учетную запись для системного администратора на менеджере ВМ и назначить роль системного администратора на менеджере ВМ.

3.4.7.1. Подготовка персонального идентификатора для системного администратора

Подготовка персонального идентификатора пользователя для системного администратора выполняется на АРМ ОБИ командой cardtool-usermod. Для подготовки персонального идентификатора необходимо в консоли на АРМ ОБИ выполнить следующие действия:

- подключить персональный идентификатор в USB разъем на АРМ ОБИ;
- открыть на АРМ ОБИ эмулятор консоли и выполнить команду:

```
sudo cardtool-usermod
```

- далее необходимо следовать запросам программы:

• по запросу «[ ] Выбор ПИ» указать на персональный идентификатор прошивка которого будет осуществляется;

• по запросу «Выбор типа пользователя» указать, что прошивка персонального идентификатора осуществляется для доменного пользователя;

• по запросу «Использовать СБ по умолчанию» указать «y» если указан верный ip-адрес сервера безопасности или «n» для самостоятельного ввода ip-адрес сервера безопасности;

- по запросу «Имя пользователя:» указать логин пользователя, для которого выполняется прошивка персонального идентификатора, например systemadm_d;
- по запросу «PIN пользователя:» указать PIN который будет использоваться пользователем в процессе аутентификации;
- по запросу «Использовать PIN администратора по умолчанию» указать «y» если PIN администратора для персонального идентификатора не был изменен ранее, или «n» для самостоятельного ввода PIN администратора для персонального идентификатора;
- на запрос «Установка флага администратора?» указать «y» для добавления метки администратора.

– дождаться окончания подготовки персонального идентификатора.

3.4.7.2. Редактирование параметров учетной записи системного администратора

Для редактирования параметров учетной записи системного администратора безопасности необходимо выполнить следующие действия:

– авторизоваться в средстве управления доменными пользователями. Для этого необходимо в адресной строке браузера ввести адрес сервера управления доступом, после чего в открывшемся окне (Рисунок 3.66) ввести логин и пароль доменного администратора.

Рисунок 3.66 – Аутентификация в средстве управления доступом

– перейти в раздел «Идентификация» → «Пользователи» → «Активные пользователи» (Рисунок 3.67). В таблице представления пользователей выбрать

пользователя, которому будет назначена роль системного администратора и для которого был подготовлен персональный идентификатор.

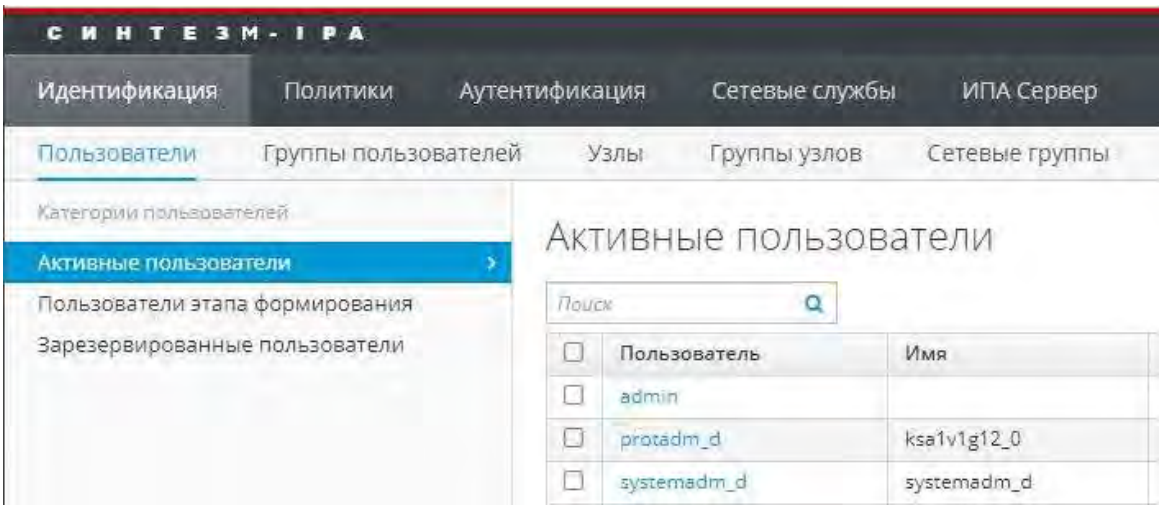


Рисунок 3.67 – Вкладка «Активные пользователи»

– в открывшемся окне параметров пользователя (Рисунок 3.68) необходимо, в разделе «Адрес эл.почты», заполнить поля «Область» и «Индекс»;

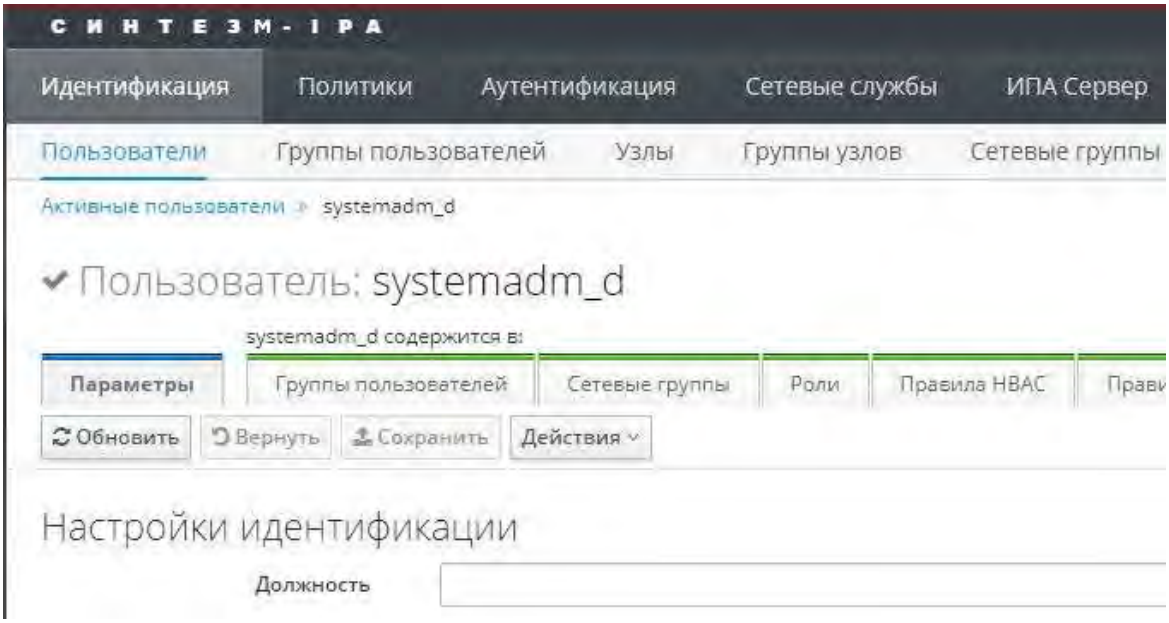


Рисунок 3.68 – Параметры пользователя

– поле «Область» должно содержать IP-адрес Сервера безопасности (Рисунок 3.69);

– поле «Индекс» должно содержать IP-адрес Менеджера виртуализации (Рисунок 3.69);

Рисунок 3.69 – Раздел «Адрес эл.почты»

3.4.7.3. Добавление учетной запись системного администратора на менеджере ВМ и назначение роли

Для добавления пользователя в менеджер ВМ и назначения роли системного администратора необходимо выполнить следующие действия:

– авторизоваться на портале администрирования средства управления средой виртуализации. Для этого необходимо в адресной строке браузера ввести адрес Сервера управления средой виртуализации, после чего в открывшемся окне (Рисунок 3.70) ввести логин и пароль внутреннего администратора менеджера ВМ (admin_internal), создаваемый на этапе установки менеджера ВМ, выбрав домен («Профиль») «internal».

Рисунок 3.70 – Аутентификация в менеджере ВМ

– перейти в раздел меню «Администрирование» → «Настройка» → «Системные разрешения». В поле «Поиск» выбрать домен, нажать кнопку вперед. В

таблице представления пользователей выбрать пользователя, которому необходимо назначить роль системного администратора и для которого был подготовлен персональный идентификатор (например: systemadm_d). В поле «Роль для связи» выбрать роль «SuperUser» (Рисунок 3.71).

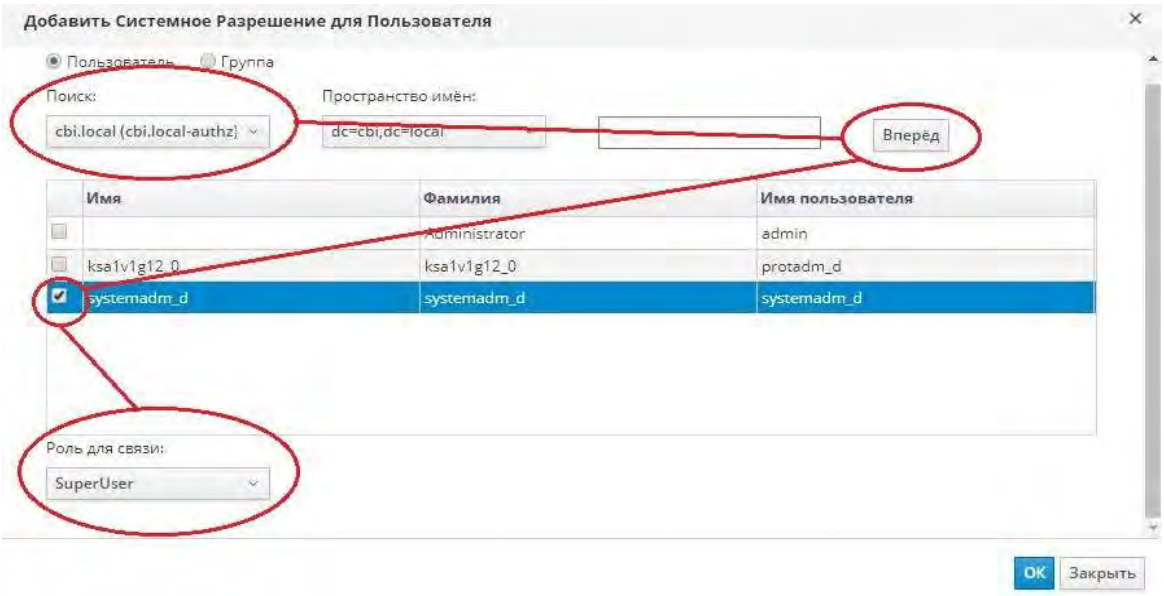


Рисунок 3.71 – Добавление системного администратора, назначение роли

3.5. Добавление узла в Сервер управления доступом

Для того чтобы ввести АРМ, ВМ или сервер в Сервер управления доступом необходимо выполнить команду:

```
ipa-client-install --enable-dns-updates --all-ip-addresses --mkhomedir
-N --server=<ipa_fqdn> --domain=<domain.local> --principal=<username> -
-password=<password> --unattended
```

где параметры server, domain, principal и password могут содержать значения, зависящие от требований к установке.

Примечание: Пред добавлением узла в Сервер управления доступом необходимо убедиться, что на узле добавляемом в сервер управления доступом были выполнены все предварительные операции указанные в п 3.4.1.4

При добавлении Менеджера ВМ в Сервер управления м необходимо дополнительно указать параметр «--no-ssh»

Параметр server соответствует полному доменному имени Сервера управления доступом.

В параметре domain указывается домен.

В параметре principal указывается имя пользователя, имеющего административные права.

В параметре password указывается пароль для пользователя, указанного в параметре principal.

В данной конфигурации эти параметры принимают следующие значения:

```
<ipa_fqdn> - sintezm-ipa.fintech.ru
<domain.local> - fintech.ru
<username> - admin
<password> - 12345678
```

3.6. Удаление узла из Средства управления доменными пользователями

Данная процедура осуществляется в два этапа:

1. На удаляемом узле выполняется команда:

```
ipa-client-install --uninstall
```

Далее необходимо зайти в web-интерфейс Средства управления доменными пользователями, доменным администратором. В web-интерфейсе перейти во вкладке имени хоста, который выводим из домена (рисунок 3.72). Затем нажать кнопку

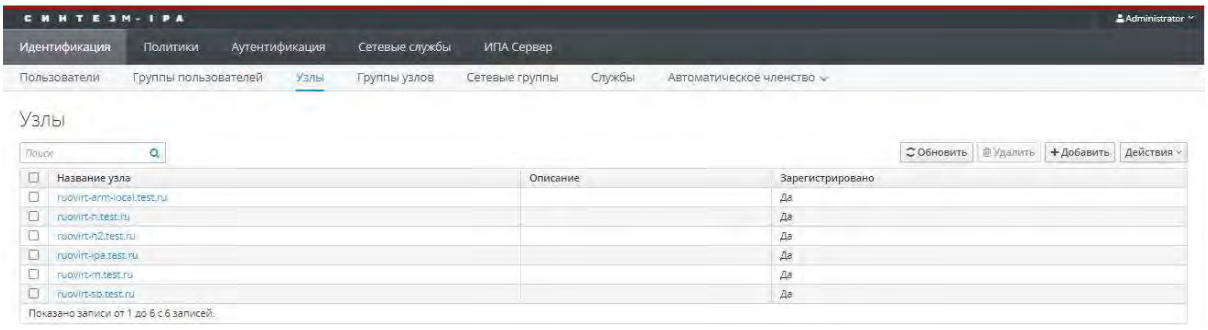


Рисунок 3.72 – Удаление хоста из Средства управления доменными пользователями

При удалении хоста из узлов будет предложено также удалить DNS-запись хоста host(s) managed by IPA DNS» для этого нажмите на кнопку «**Удалить**»

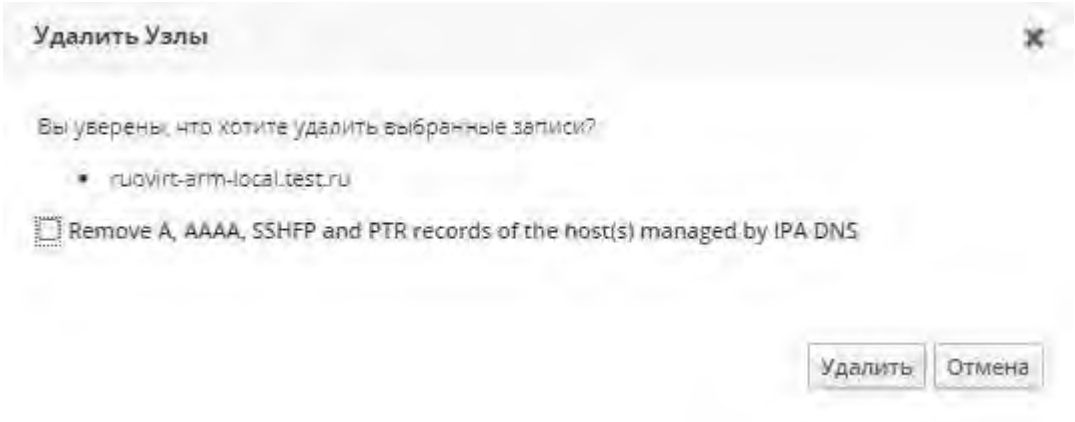


Рисунок 3.73 – Удаление DNS-записи хоста

После выполнения вышеописанных процедур АРМ будет выведен из домена и можно будет использовать локальную авторизацию.

3.7. Применение набора базовой конфигурации

За настройку базовых конфигураций КП «ЗОС «СинтезМ» в зависимости от роли средства на котором функционирует КП «ЗОС «СинтезМ» отвечает модуль /usr/bin/sz-user-policy входящий в состав пакета pszi-arm-config-1.4-0.el7.sz.noarch. В зависимости от переданных параметров модуль sz-user-policy обеспечивает:

– настройку модуля Mail Notification;

– настройку параметров автоматического завершения сеанса при бездействии;

– ограничения количества активных сессий для пользователей;

– настройку параметров аутентификации (локальная, доменная, использование персонального идентификатора) в том числе за счет вызова скриптов pszi-auth-conf-setup и pszi-auth-pam-setup;

– ограничение ролей на менеджере ВМ;

– создание учетных записей для администраторов (локального и доменного);

– установку пароля на загрузчик ОС GRUB;

– включение подсистемы самотестирования;

– запрет подключения пользователя root по протоколу ssh к ВМ, АРМ;

– ограничение на использование утилит /bin/su и /bin/sudo;

– удаление не используемых pam-модулей;

– ограничение виртуальных консолей управления.

Применение базовой конфигурации осуществляется командой:

```
sudo sz-user-policy [--параметры]
```

Примечание. Выполнение данной команды требует повышения привилегий и всегда должно осуществляться администратором с использованием утилиты sudo.

Параметры скрипта sz-user-policy представлены в таблице 3.7.

Таблица 3.7 –Параметры sz-user-policy

№	Параметр	Описание	Примечание
1.	--FSTEK	Инициализация конфигурации для КП «ЗОС «СинтезМ»	**Обязательный параметр** для данной конфигурации
2.	--local	Инициализация локальной схемы аутентификации	
3.	--domain	Инициализация доменной схемы аутентификации	
4.	--token	Инициализация аутентификации по персональному идентификатору	Данный параметр применяется для пользовательских АРМ/ ВМ
5.	--manager	Настройка ролей на менеджере ВМ	Данный параметр применяется только на менеджере ВМ, при необходимости ограничения возможности создания ролей
6.	-R, --rollback	Откат к предыдущей версии настроек	Используется в связке с 1,2,3 пунктами
7.	-T, --test	Запуск скрипта в тестовом режиме	Не модифицирует существующие настройки

3.7.1. Применение базового набора конфигураций для конфигурации «Операционная система»

Для применения базового набора конфигураций для конфигурации «Операционная система» и использования локальной аутентификации, на сервере/ВМ (серверной операционной системе) необходимо суперпользователем

выполнить команду (описание передаваемых параметров представлено в таблице 3.7):

```
sz-user-policy --FSTEK --local
```

Для инициализации двухфакторной аутентификации на сервере/ВМ (серверной операционной системе) необходимо выполнить действия описанные в пункте 3.7.3.

После выполнения команды необходимо перезагрузить техническое средство / ВМ.

Примечание. Перед перезагрузкой технического средства/ ВМ необходимо выполнить перерасчет эталонных значений контрольных сумм, в соответствии с п.3.12.3 настоящего документа.

Примечание. Аутентификации по протоколу ssh доступна только администратору.

Для инициализации локальной двухфакторной аутентификации на АРМ пользователя/ОБИ необходимо суперпользователем выполнить команду:

```
sz-user-policy --FSTEK --local --token
```

3.7.2. Применение базового набора конфигураций для конфигурации «Среда виртуализации»

Примечание. Перед применением данной схемы аутентификации необходимо наличие доменного администратора (3.4.6).

Применение базового набора конфигурации для Менеджера ВМ осуществляется командой:

```
sz-user-policy –FSTEK  --domain
```

Для применения базового набора конфигураций для конфигурации «Среда виртуализации» и использования доменной двухфакторной аутентификации на АРМ пользователя (клиентской операционной системе) необходимо локальным администратором выполнить команду:

```
sudo sz-user-policy --FSTEK --domain --token
```

Для выбора доменной схемы аутентификации на сервере/ВМ (серверной операционной системе) необходимо локальным администратором выполнить команду:

```
sudo sz-user-policy --FSTEK --domain
```

Для инициализации двухфакторной аутентификации на сервере/ВМ (серверной операционной системе) необходимо выполнить действия описанные в пункте 3.7.3.

Для вступления в силу внесенных изменений необходимо осуществить перезагрузку.

Примечание. Перед перезагрузкой необходимо выполнить перерасчет эталонных значений контрольных сумм, в соответствии с п.3.12.3 настоящего документа.

3.7.3. Инициализации двухфакторной аутентификации на сервере/ВМ (серверной операционной системе)

Для инициализации двухфакторной аутентификации на сервере/ВМ (серверной операционной системе), необходимо установить дополнительные пакеты и произвести настройку конфигурации стека аутентификации в /etc/pam.d/.

Для установки недостающих пакетов необходимо скопировать iso-файл дистрибутива КП «ЗОС «СинтезМ» и примонтировать его в директорию /mnt. Копирование iso-файла осуществляется командой scp:

```
scp [путь до iso-образа дистрибутива] root@[ip-адрес сервера безопасности]:/[путь до директории для сохранения]
```

Например:

```
scp sintez-m-7-x86_64.iso root@10.10.10.50:~
```

Монтирование iso-файла выполняется командой

```
mount sintez-m-7.x86_64.iso /mnt
```

После того как iso-файл примонтирован, необходимо установить пакеты pam_pkcs11-0.6.2-24.2.el7.sz.x86_64.rpm и pszi-pam-auth-rutoken-0.2-0.el7.sz.x86_64.rpm

```
yum install /mnt/Packages/ pam_pkcs11-0.6.2-24.2.el7.sz.x86_64.rpm
yum install /mnt/Packages/pszi-pam-auth-rutoken-0.2-0.el7.sz.x86_64.rpm
```

При настройке локальной двухфакторной аутентификации необходимо последовательно выполнить команды:

```
touch /etc/pam.d/mate-screensaver
pszi-auth-pam-setup --local --token --enable
pszi-auth-conf-setup --local --token --enable
```

При настройке доменной двухфакторной аутентификации необходимо последовательно выполнить команды:

```
touch /etc/pam.d/mate-screensaver
pszi-auth-pam-setup --domain --token --enable
pszi-auth-conf-setup -- domain --token --enable
```

После завершения выполнения команд, в секциях auth, account, password, session конфигурационных файлов, указанных в таблице 3.8 необходимо произвести замену «`system-auth`» на «`smartcard-auth`»

Таблица 3.8 – Перечень файлов

№	Конфигурационный файл
1.	/etc/pam.d/login
2.	/etc/pam.d/chsh
3.	/etc/pam.d/sudo
4.	/etc/pam.d/su
5.	/etc/pam.d/passwd
6.	/etc/pam.d/screen
7.	/etc/pam.d/gdm-autologin

Например:

```
#%PAM-1.0
auth       required     pam_sepermit.so
auth       substack     smartcard-auth
auth       include      postlogin
# Used with polkit to reauthorize users in remote sessions
-auth      optional     pam_reauthorize.so prepare
account    required     pam_nologin.so
account    include      smartcard-auth
password   include      smartcard-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed
```

```
in the user context
session    required     pam_selinux.so open env_params
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      smartcard-auth
session    include      postlogin
# Used with polkit to reauthorize users in remote sessions
-session   optional     pam_reauthorize.so prepare
```

Для обеспечения смены пароля необходимо добавить параметр «use_authtok» в файл /etc/pam.d/smartcard-auth.

```
password requisite pam_unix.so sha512 shadow use_authtok
```

После чего выполнить команду:

```
chmod 644 /etc/profile.d/autologout.*
```

Далее необходимо выполнить команду:

```
sudo setenforce 0
```

и внести изменения в конфигурационный файл /etc/selinux/config, заменив строку «SELINUX=enforcing» на «SELINUX= permissive».

3.7.4. Настройка блокировки учетных записей пользователей

Для включения блокировки учетных записей пользователей после определенного количества неудачных попыток входа необходимо внести изменения в конфигурации стека аутентификации в /etc/pam.d/, добавив в секцию auth (сразу после модуля pam_env.so) конфигурационных файлов /etc/pam.d/system-auth, /etc/pam.d/smartcard-auth, /etc/pam.d/password-auth вызов модуля pam_tally2.

Например:

```
auth        required      pam_env.so
auth        required      pam_tally2.so audit onerr=fail deny=5
unlock_time=30
auth        sufficient    pam_unix.so nullok try_first_pass
```

Описание параметров модуля pam_tally2 приведены в таблице 3.9.

Таблица 3.9 - Параметры модуля pam_tally2

Модуль	Параметр	Описание
pam_tally2.so	onerr=[fail|succeed]	При возникновении непредвиденной ошибки модуль вернёт PAM_SUCCES если установлено значение secced, иначе вернётся код ошибки
	file=/path/to/counter	Указание расположение файла счётчика. По умолчанию это файл /var/log/tallylog
	audit	Зарегистрирует имя пользователя в системном журнале, если пользователь не будет найден.
	silent	При данном параметре информативные сообщения перестают выводиться пользователю
	no_log_info	Не записывать информативные сообщения в лог через syslog
	deny=N	Запретить пользователю доступ после N неудачных попыток
	lock_time=N	Запретить доступ пользователю на N секунд после неудачной попытки
	unlock_time=N	Разрешить доступ через N секунд после неудачной попытки. Если этот параметр используется, пользователь будет заблокирован в течение указанного количества времени после того, как он превысит свой максимум допустимые попытки. В противном случае учетная запись заблокирована до тех пор, пока блокировка не будет удалена
	magic_root	Если модуль вызывается пользователем с uid = 0(root), счетчик не увеличивается.
	no_lock_time	Не используется поле .fail_loctime в /var/log/faillog для пользователя
	even_deny_root	учетная запись root может стать недоступной при включенной опции
	root_unlock_time=N	Этот параметр включает параметр even_deny_root. Разрешить доступ через N секунд пользователю root после неудачной попытки. Если этот параметр используется, пользователь root будет заблокирован в течение указанного количества времени после того, как он превысил максимально допустимый попытки.

3.7.5. Настройка удаленного входf на рабочие места

После проведения настройки ОС возможность удаленного входа по ssh на рабочие места и сервера для пользователей должна быть заблокирована.

Для блокировки возможности удаленного входа по ssh на рабочие места и сервера для пользователей необходимо провести настройку безопасной оболочки (ssh). Для этого в конфигурационном файле /etc/ssh/sshd_config необходимо

раскомментировать параметр «PasswordAuthentication» и установить его значение равным «no».

Для отключений уязвимых алгоритмов шифрования необходимо в конфигурационном файле /etc/ssh/sshd_config привести параметр Ciphers к следующему виду:

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128
MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160
```

Для установки запрета X11Forwarding необходимо выполнить команду

```
# sed -i 's/X11Forwarding yes/X11Forwarding no/g' /etc/ssh/sshd_config
```

Включить “хешироввние” имен хостов

```
# echo “HashKnownHosts yes” >> /etc/ssh/ssh_config
```

Для вступления изменений в силу необходимо перезапустить службу командой:

```
systemctl restart sshd.service
```

Пример конфигурационного файла ssh:

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

SyslogFacility AUTHPRIV
AuthorizedKeysFile      .ssh/authorized_keys

PasswordAuthentication no
Ciphers          aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128
MACs hmac-sha1,umac-64@openssh.com,hmac-ripemd160
ChallengeResponseAuthentication no

GSSAPIAuthentication no
GSSAPICleanupCredentials no
UsePAM yes

X11Forwarding no
UsePrivilegeSeparation sandbox         # Default for new installations.
AcceptEnv  LANG  LC_CTYPE  LC_NUMERIC  LC_TIME  LC_COLLATE  LC_MONETARY
LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
```

```
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
HashKnownHosts yes


Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

Безопасная оболочка (ssh) на пользовательских АРМ и ВМ должна быть отключена. Для отключения безопасной оболочки (ssh) на пользовательских АРМ и ВМ необходимо выполнить следующие команды:

```
systemctl stop sshd.service
systemctl disable sshd.service
```

3.7.6. Откат примененного базового набора конфигураций

Для отключения двухфакторной аутентификации на АРМ необходимо:

– загрузиться в режиме восстановления или технологическом режиме (см. п 3.8);

– дождаться инициализации ОС и запуска оболочки /bin/bash;

– ввести команду для отката базового набора конфигурации.

Команда для отката выглядит следующим образом

```
sz-user-policy --FSTEK --[примененная схема аутентификации] –R
```

, где `[примененная схема аутентификации]` – может принимать значение domain или local, в зависимости от типа примененной схемы аутентификации.

Для завершения отката примененной схемы аутентификации необходимо выполнить следующие команды:

```
touch /.autorelabel
echo “s” >> /proc/sysrq-trigger
exec /sbin/reboot –f
```

Примечание. Перед перезагрузкой системы необходимо выполнить перерасчет эталонных значений контрольных сумм, в соответствии с п.3.12.3 настоящего документа.

3.8. Настройка загрузчика GRUB

3.8.1. Краткое описание экранной формы загрузчика GRUB

Для того, чтобы начать работу с загрузчиком GRUB необходимо перезагрузить АРМ или ВМ на которой будет производиться настройка. При перезагрузке, перед загрузкой системы, появится экран оболочки GRUB (рисунок 3.74). Указанная экранная форма доступна в течении 5 с. После чего будет произведена загрузка выделенного загрузчика операционной системы, если пользователь не нажмёт любую клавишу на клавиатуре.

Примечание. Для остановки выполнения загрузки лучше использовать клавиши перемещения.

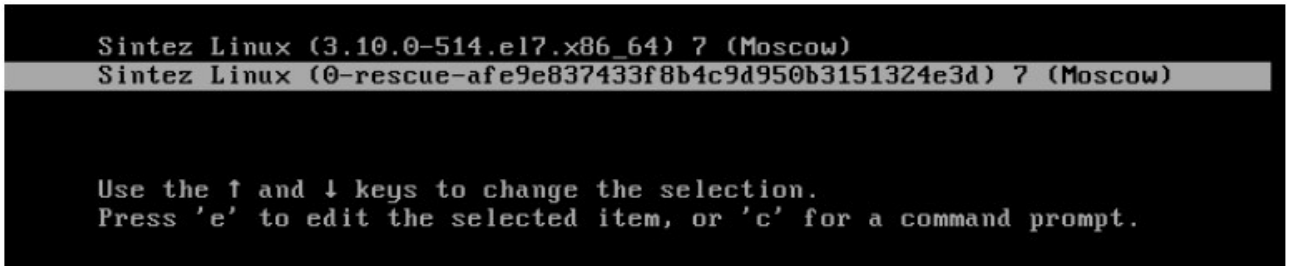


Рисунок 3.74 – Экранная форма оболочки GRUB

В оболочке GRUB пользователю представлены записи о доступных загрузчиках операционных систем, установленных на АРМ или ВМ.

Перемещаться между загрузчиками пользователь может, используя клавиши перемещения.

Для загрузки операционной системы необходимо выбрать требуемый загрузчик из списка и нажать клавишу «Enter».

После прохождения аутентификации пользователя в загрузчике GRUB (см. п 3.8.3) пользователю доступны две функции, которые привязаны к клавишам «e» и «c».

При нажатии клавиши «e» откроется экранная форма, в которой будут описаны все параметры загрузки операционной системы (рисунок 3.75).

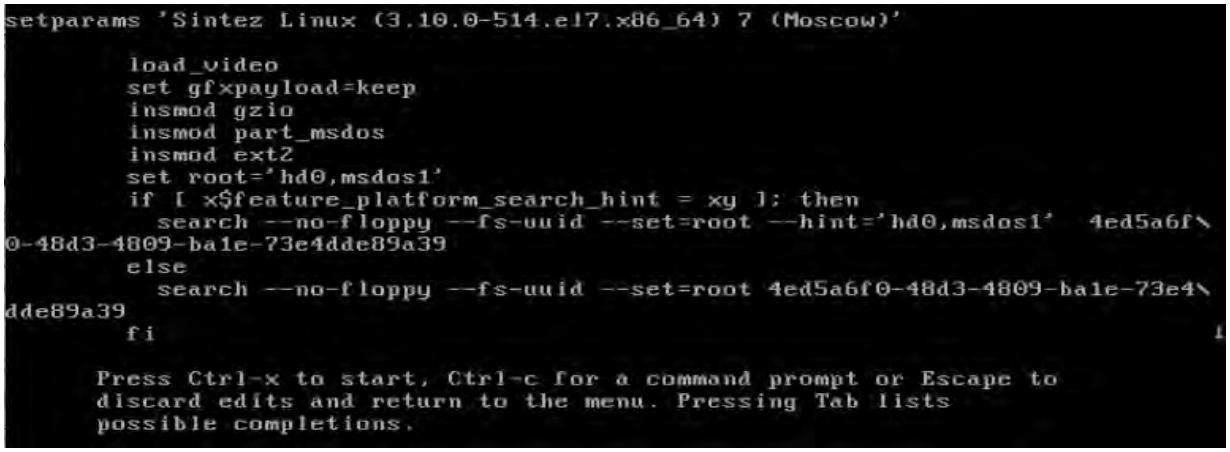


Рисунок 3.75 – Экранная форма GRUB с параметрами загрузки ОС

При нажатии клавиши «c» пользователь перейдёт в командную строку оболочки GRUB (рисунок 3.76).

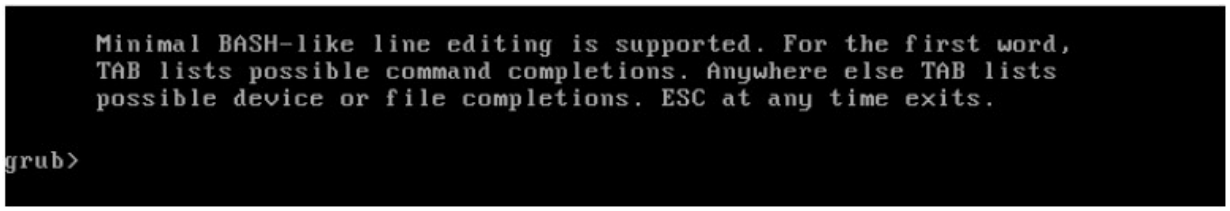


Рисунок 3.76 – Экранная форма GRUB с командной строкой

Клавиша «ESC» возвращает пользователя на предыдущий экран. Для загрузки операционной системы необходимо выбрать первую строку из списка GRUB, она является ссылкой на загрузку основной операционной системы.

3.8.2. Настройка разграничения доступа к оболочке GRUB

После загрузки операционной системы для того, чтобы разграничить доступ к оболочке GRUB на указанном АРМ или ВМ необходимо задать пароль суперпользователя, у которого будет доступ к оболочке GRUB.

```
# grub2-setpassword
```

После этого пользователю необходимо ввести пароль и подтверждение нового пароля (рисунок 3.77).

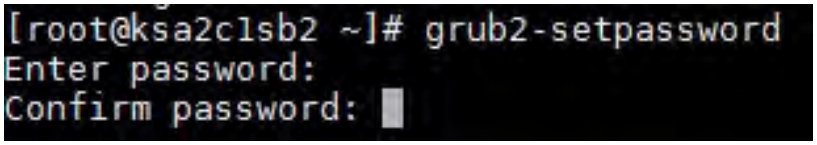


Рисунок 3.77 – Ввод и подтверждение пароля суперпользователя в GRUB

Если пароли пользователя не совпадут в командной строке появится сообщение:

```
# /usr/bin/grub2-mkpasswd-pbkdf2: error: passwords don't match
```

После задания пароля пользователя необходимо проинициализировать конфигурационный файл grub:

```
# grub2-mkconfig -o /boot/grub2/grub.cfg
```

3.8.3. Аутентификация в загрузчике GRUB

После установки пароля на загрузчик GRUB, при загрузке системы и выбора параметра «e» или «c», пользователю откроется экранная форма с предложением пройти аутентификацию в GRUB (рисунок 3.78):

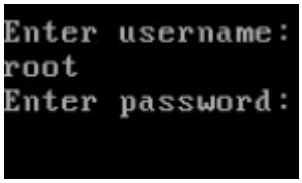


Рисунок 3.78 – Запрос аутентификации для изменений параметров GRUB

После ввода имени и пароля пользователя, который допущен к изменениям параметров GRUB, он перейдёт в стандартную экранную форму изменения параметров загрузчика.

3.8.4. Загрузка в режиме восстановления

Для того, чтобы загрузить операционную систему в режиме восстановления («rescue») необходимо при загрузке системы в оболочке GRUB выбрать строку, в имени которой, будет содержаться параметр «rescue» (рисунок 3.79):

Рисунок 3.79 - Выбор загрузки операционной системы в режиме «rescue»

3.8.5. Загрузка в технологическом режиме

Для загрузки в технологическом режиме аутентификации необходимо:

– дождаться на экране появления оболочки GRUB;

– при необходимости осуществить аутентификацию в загрузчике GRUB (см. п 3.8.3) после чего нажать на «e» для редактирования параметров загрузки;

Примечание. По умолчанию в GRUB используется имя пользователя «root», пароль «1234567890».

– в открывшемся окне (Рисунок 3.80) в строке начинающейся со значения «`linux16`» необходимо:

- изменить значение «`ro`» на «`rw`»;
- удалить (при наличии) параметр «`rhgb quiet`»;
- добавить параметр «`init=/bin/bash`»;

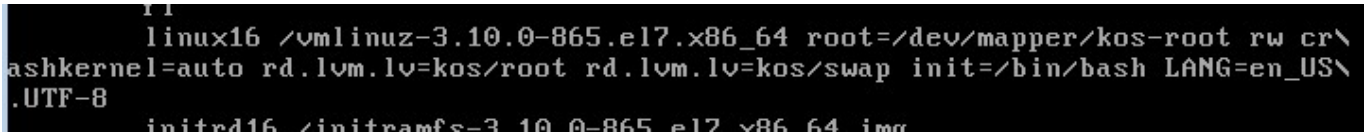


Рисунок 3.80 – Параметры загрузки

– после внесения изменений нажать «Ctrl+x»;

– дождаться инициализации ОС (Рисунок 3.81);

Рисунок 3.81 - Инициализация ОС

– ввести команды для инициализации переменных окружения:

```
export PATH=$PATH:/bin
export PATH=$PATH:/sbin
```

– примонтировать разделы командой:

```
mount –a
```

– для выхода из технологического режима необходимо выполнить команды

```
echo “s” >> /proc/sysrq-trigger
exec /sbin/reboot -f
```

3.9. Резервное копирование и восстановление системы с помощью режима «rescue».

Восстановление системы предназначено для восстановления работоспособности ОС, в случае некорректной работы, также при возникновении ошибок во время загрузки системы.

Для перехода в режим восстановления системы необходимо выполнить перезагрузку ОС, при необходимости с помощью кнопки «reset». Далее выполнить загрузку в режиме восстановления или выполнить аутентификацию в GRUB и приступить к загрузке в технологическом режиме.

3.9.1. Создание резервных копий системных директорий операционной системы.

Для создания резервной копий системных директорий, ОС необходимо предварительно загрузить в режим восстановления (см. п 3.8.4). После чего необходимо выполнить команду:

```
sudo /backup/backup.sh -b
```

После окончания архивации в директории /backup появятся архивные файлы всех системных директорий.

После завершения архивации пользователю необходимо записать на диск или съёмное usb-устройство вновь созданные файлы для защиты указанных файлов от потери или уничтожения.

3.9.2. Восстановление системных директорий из резервных копий.

Для восстановления системных файлов из архива необходимо перейти в режим восстановления (см. п 3.8.4) скопировать архивные файлы в директорию /backup и выполнить команду для разархивирования файлов для всех системных директорий:

sudo /backup/backup.sh –r

3.10.Настройка модулей операционной системы (non kernel)

3.10.1. Планировщик задач CRON

Планировщик задач в КП «ЗОС «СинтезМ» играет незаменимую роль в автоматизации администрирования операционной системы. Роль планировщика задач выполняет демон crond. Демон crond запускается системой инициализации systemd в момент запуска системы. После запуска, демон crond ежеминутно просматривает свои таблицы, в которых содержатся информация о периодичности запуска команд и запускает команды, когда значения полей минута, час, месяц и хотя бы одно из полей число и день недели, совпадают с текущим временем. Основной конфигурационный файл демона cron - */etc/crontab*:

```
cron:~#cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

В /etc/crontab задания выполняются с помощью команды run-parts, которая запускает скрипты и программы из указанных каталогов (/etc/cron.hourly, /etc/cron.daily и т.д.). Каждая строка запускает из соответствующего каталога задания

ежечасно, ежедневно, еженедельно и ежемесячно, соответственно строкам сверху вниз.

Примечание. Все команды в конфигурационном файле демона crond запущены от имени пользователя root.
crontab может содержать присваивания значений переменным shell, которые будут установлены перед запуском команды.

Также, если необходимо запускать какие-то команды по особому расписанию (не ежечасно, ежедневно, еженедельно и ежемесячно), то таблицы заданий помещаются в каталог */etc/cron.d/*.

Каждый пользователь системы имеет свой файл заданий crontab, в котором описано, в какое время и какие программы запускать от имени этого пользователя. Для редактирования файла crontab используется специальная одноименная программа crontab, позволяющая не прерывать процесс cron на время редактирования. Редактировать вручную таблицы cron не рекомендуется.

Файлы таблиц планировщика cron для пользователей хранятся в каталоге /var/spool/cron

Каждая строка планировщика имеет следующий формат:

```
* * * * * {пользователь} выполняемая_команда
- - - - -
| | | | |
| | | | ----- День недели (0 - 7) (Воскресенье =0 или =7)
| | | --------Месяц (1 - 12) (можно три буквы из названия месяца,
| | |         регистр не имеет значения от jan до dec)
| | --------- День (1 - 31)
| ----------- Час (0 - 23)
------------- Минута (0 - 59)
```

В примере показан формат одной из строки таблицы, состоящий из 7 полей. Первые 5 полей - значения, задающие периодичность выполнения команды (расписание). 6-е поле присутствует только в таблицах /etc/crontab и др.

расположенных в каталоге /etc/cron.d/. 7-е поле есть сама запускаемая команда. Командой может быть как простая команда, например, ls /proc >> /tmp/proc, или команда запуска написанного вами специального сценария. Со всей оставшаяся частью строки до символа перевода строки или символа %, будет выполнен вызов /bin/sh или другой оболочки, определенной в переменной SHELL в crontab. Знак процента (`%' ) в команде (если он не экранирован обратной косой чертой (`\')) будет соответствовать символу перевода строки и все данные после первого `%' будут посланы для команды на стандартный ввод.

Для указанных выше первых 5 полей, можно использовать **звездочку (*)**, что означает все допустимые значения. Например, если поставить звёздочку в значении месяца, команда будет выполняться каждый месяц в соответствии со временем, указанным в других параметрах.

Дефис (-) между целыми числами обозначает диапазон чисел. Например, 1-4 означает целые числа 1, 2, 3 и 4.

Список значений, разделенных запятыми (,), обозначает перечень. Например, перечисление 3, 4, 6, 8 означает четыре указанных целых числа.

Косая черта (/) используется для определения шага значений. Если после диапазона указать /<целое_число>. Например, значение минут 0-59/2, определяет, что задание будет запущено каждую вторую минуту.

Вся оставшаяся часть строки до символа перевода строки или символа %, будет выполнен вызов /bin/sh или другой оболочки, определенной в переменной SHELL в crontab Знак процента (`%' ) в команде (если он не экранирован обратной косой чертой (`\')) будет соответствовать символу перевода строки и все данные после первого `%' будут посланы для команды на стандартный ввод.

Пример crontab-файла:

```
# выполнить команды hello каждый понедельник  в 3:30
30 3 * * mon hello
# выполнить команду hello в первый день каждого месяца в 4:10
10 4 1 * * hello
# выполнять каждый день в 0 часов 5 минут, результат складывать в
log/daily
```

```
5 0 * * * $HOME/bin/daily.job >> $HOME/log/daily 2>&1
# каждый рабочий день в 22:00
0 22 * * 1-5 echo "Пора домой" | mail -s "Уже 22:00" john
23 */2 * * * echo "Выполняется в 0:23, 2:23, 4:23 и т. д."
5 4 * * sun echo "Выполняется в 4:05 в воскресенье"
0 0 1 1 * echo "С новым годом!"
15 10,13 * * 1,4 echo "Эта надпись выводится в понедельник и четверг в
10:15 и 13:15"
0-59 * * * * echo "Выполняется ежеминутно"
# каждые 5 минут
*/5 * * * * echo "Прошло пять минут"
```

Anacron

anacron — (англ. anachronistic cron) асинхронный или анахроничный cron. Anacron в отличие от cron не поддерживает запуск заданий по расписанию, вместо этого задания запускаются с заданным интервалом времени. Это очень удобно для систем, которые работают не регулярно, например, домашние рабочие станции или ноутбуки. Anacron хранит метки времени файлов в */var/spool/anacron*, чтобы записывать время выполнения заданий. При запуске anacron проверяет, прошло ли необходимое количество дней с тех пор, как задача была выполнена в последний раз, и при необходимости запускает ее. Задачи anacron хранятся в конфигурационном файле /etc/anacrontab. Синтаксис данного файла аналогичен /etc/crontab, за исключением полей таблиц:

```
* * * выполняемая_команда
- - -
| | |
| | --------- идентификатор
| ----------- задержка
------------- период
```

Период — период выполнения в днях. Задержка — задержка запуска в минутах. Идентификатор задания — любой непустой символ, кроме / \. Задержка чаще всего используется для того, чтобы позволить системе полностью загрузиться.

Демон cron при загрузке, а так же - после загрузки каждую минуту анализирует файл */etc/crontab*, каталог */etc/cron.d/* и каталог с пользовательскими таблицами заданий (*/var/spool/cron/crontabs*) и сверяет текущее время и строку в

просматриваемом файле и запускает указанную команду, когда значения полей минута, час, месяц и хотя бы одно из полей число и день_недели, совпадают с текущим временем.

В отличие от cron средство anacron сравнивает не текущее время со временем задания в crontab, а сколько прошло времени с последнего запуска задания, указанного в /etc/anacrontab и если прошел указанный промежуток времени, то задание запускается.

3.10.2. Безопасная оболочка (ssh)

SSH (от англ. secure shell - безопасная оболочка) это набор программ, которые позволяют регистрироваться на компьютере по сети, удаленно выполнять на нем команды, а также копировать и перемещать файлы между компьютерами. SSH организует соединение поверх каналов связи.

В КП «ЗОС «СинтезМ» SSH применяется на этапе пуско-наладки в процессе развертывания менеджера ВМ, в процессе управления гипервизорами (добавление, удаление), а также для обеспечения отказоустойчивого кластера.

Сервером SSH служит демон sshd, который запускается на UNIX-машине, а клиентом – программа ssh. Клиент ssh служит для обеспечения защищенной регистрации на удаленном компьютере.

Свободно распространяемая версия SSH состоит из следующих пакетов:

• openssh – основные файлы;

• openssh-clients – программа-клиент;

• openssh-server – ssh-сервер.

Для того, чтобы SSH начал работать, необходимо запустить демон sshd на той ЭВМ, к которой предполагается подключение. SSHD запускается самостоятельно, посредством менеджера служб systemd в режиме standalone, и обычно включен в автозагрузку по умолчанию.

3.10.2.1. Настройка SSH на сервере

Конфигурационный файл сервера sshd называется /etc/ssh/sshd_config. Справку по его синтаксису локальный администратор может получить по команде man 5 sshd_config. В пакете openssh-server находится конфигурационный файл с типовыми настройками.

3.10.2.2. Запуск демона sshd

Запуск демона sshd осуществляется автоматически при старте ОС и обеспечивается системным менеджером systemd.

Для запуска (перезапуска) демона sshd после загрузки ОС можно воспользоваться командой:

```
sudo systemctl restart sshd.service
```

Либо запустить демон sshd через команду:

```
sudo /usr/sbin/sshd [ключи]
```

Ключи, с которыми можно запускать sshd, перечислены в таблице 3.10.

Таблица 3.10 – Ключи сервера sshd

Ключ	Назначение
-b биты	Определяет число битов для ключа сервера (по умолчанию 768). Эту опцию можно использовать, только используется протокол SSH версии 1
-d	Режим отладки (DEBUG). В этом режиме сервер не переходит в фоновый режим, обрабатывает только одно соединение и подробно протоколирует свои действия в системном журнале. Ключ отладки особенно полезен для изучения работы сервера
-D	Также, как и при использовании предыдущего ключа, сервер sshd не будет переходить в фоновый режим. Однако в отличие от -d ключ -D не переводит сервер в режим отладки
-e	Отправлять отладочные сообщения не в системный журнал, а на стандартный поток ошибок
-f файл	Задает альтернативный файл конфигурации вместо /etc/ssh/sshd_con£ig
-g время	Предоставляет клиенту, не прошедшему аутентификацию, дополнительное время на ввод пароля. Значение 0 интерпретируется как бесконечное ожидание/
-h файл_ключа	Задает альтернативный файл открытого ключа (ключ узла). По умолчанию используется файл /etc/ssh/ssh_host_key. Этот ключ может понадобиться для того, чтобы запускать sshd от имени непривилегированного пользователя. Также ключ -h часто применяется при запуске sshd из сценариев, задающих различные настройки в зависимости от времени суток (в рабочее и нерабочее время)

Ключ	Назначение
- j	Используется, если нужно запускать sshd через суперсервер xinetd. Обычно демон sshd запускается отдельно при загрузке системы. Связано это с тем, что демону sshd требуется некоторое время для генерирования ключа сервера, прежде чем он сможет ответить на запросы клиентов. При запуске через суперсервер при каждом соединении суперсервер будет заново вызывать sshd, а тот заново генерировать ключ. Однако на современных компьютерах задержка практически не заметна. Поэтому вполне можно запускать sshd и через суперсервер
-к время	Задает время, спустя которое ключ сервера будет создан заново. По умолчанию время составляет 1 час. Эту опцию можно использовать только с протоколом SSH версии 1
-p порт	Указывает альтернативный порт, который демон sshd будет прослушивать вместо порта 22
-q	≪Тихий режим≫: не протоколировать сессию. Обычно протоколируется начало аутентификации, результат аутентификации и время окончания сессии
-t	Тестовый режим. Применяется для проверки корректности файла конфигурации
-4	Разрешается использовать IP-адреса только в формате IPv4
-6	Разрешается использовать IP-адреса только в формате IPv6

3.10.2.3. Использование SSH-клиента

Клиентская программа ssh находится в пакете openssh-clients вместе с типовым конфигурационным файлом /etc/ssh/ssh_conf. Настройки можно задавать и из командной строки, запуская ssh с соответствующими ключами. Основные ключи и аргументы перечислены в таблице 3.11.

Формат команды:

```
ssh [ключи] [ключи_с_аргументами] [логин_имя@]хост.домен
[команда]
```

Таблица 3.11 – Ключи программы ssh

Ключ	Назначение
-a	Отключает перенаправление аутентификации агента соединения
-A	Включает перенаправление аутентификации агента соединения
-c blowfish |3des | des	Позволяет выбрать алгоритм шифрования при использовании первой версии протокола SSH. Можно указать blowfish, 3des или des
-C	Отправлять отладочные сообщения не в системный журнал, а на стандартный поток ошибок
-f файл	Данная опция переводит ssh в фоновый режим после аутентификации пользователя. Рекомендуется использовать для запуска программы X11. Например: ssh - f host xterm
-i идент_файл	Задает нестандартный идентификационный файл (для нестандартной RSA/DSA-аутентификации)

Ключ	Назначение
-l логин_имя	Указывает, от имени какого пользователя будет осуществляться регистрации на удаленной машине
-p порт	Определяет порт, к которому подключится программа ssh (по умолчанию используется порт 22)
-к время	Задает время, спустя которое ключ сервера будет создан заново. По умолчанию время составляет 1 час. Эту опцию можно использовать только с протоколом SSH версии 1
-p порт	Указывает альтернативный порт, который демон sshd будет прослушивать вместо порта 22
-q	Переводит программу ssh в ≪тихий режим≫. При этом будут отображаться только сообщения о фатальных ошибках. Все прочие предупреждающие сообщения в стандартный выходной поток выводиться не будут
-v	Включает отображение всей отладочной информации
-x	Отключить перенаправление X11
-X	Включить перенаправление X11
-1	Использовать только первую версию протокола SSH (принудительно)
-2	Использовать только вторую версию протокола SSH (принудительно)
-4	Разрешается использовать IP-адреса только в формате IPv4
-6	Разрешается использовать IP-адреса только в формате IPv6

3.10.3. Менеджер пакетов YUM

3.10.3.1. Настройка расположения пакетов

Поиск пакетов начинается с просмотра директории /etc/yum.repos.d/, в которой находятся файлы с расширением repo. В этой директории repo-файлы хранятся по умолчанию, а дополнительные местоположения можно указать в конфигурационном файле YUM (обычно это файл /etc/yum.conf).

Типовой repo-файл содержит три раздела: в первом разделе перечислены источники обычных пакетов, во втором разделе – источники отладочных пакетов, и в третьем – источники пакетов исходного кода. Обычно пакеты дистрибутива доступны для загрузки из нескольких местоположений, которые называются зеркалами. Файл repo говорит программе yum о том, где она должна искать самые последние списки зеркал для каждого раздела.

Примечание. Следует обратить внимание на то, что конфигурация учитывает версию дистрибутива и архитектуру компьютера.

Помимо указания местоположения репозиториев, repo-файл содержит информацию о том, разрешено ли использование того или иного репозитория, и следует ли проверять загруженные пакеты с помощью подписей GPG.

3.10.3.2. Подключение внешних репозиториев

Для подключения внешних репозиториев необходимо любым доступным текстовым редактором отредактировать или создать файл repo в директории /etc/yum.repos.d/ и добавить в него соответствующую секцию:

```
[имя репозитория]
name=[имя репозитория]
baseurl=[тип расположения][расположение пакетов]
enabled=[статус репозитория]
gpgcheck=0
```

, где `[имя репозитория]` – задает имя репозитория;

`[тип расположения]` – указывает менеджеру пакетов yum откуда получать rpm пакеты для их установки, данный параметр может принимать значения следующие значения:

– `http://` - в случае если репозиторий пакетов располагается в сети

– `file:///` - в случае если репозиторий пакетов расположен локально на хосте.

`[расположение пакетов]` – указывает путь к расположению пакетов;

`[статус репозитория]` – может принимать значение включен - “1” или выключен - “0”;

В одном конфигурационном файле repo может содержаться несколько секций. Пример конфигурационного файла repo представлен ниже:

```
[base]
name=base
baseurl=http://files.fintech.ru/sintez/$releasever/os/$basearch/
enabled=0
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-sintez-release

[sintez]
name= sintez
```

```
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

3.10.3.3. Основные команды менеджера пакетов yum

Примечание. В КП «ЗОС «СинтезМ» для управления пакетами необходимо обладать привилегиям суперпользователя. В связи с этим управление пакетами возможно только локальным администратором с использованием утилиты sudo.

3.10.3.3.1. Установка/Удаление YUM -пакетов

Для инсталляции пакета с помощью yum или для его удаления (как с помощью rpm, так и с помощью yum) достаточно указать только имя пакета.

Для установки пакета необходимо выполнить команду yum с опцией install:

```
sudo yum install [имя пакета/путь до пакета]
```

Если вы хотите удалить пакет из системы, выполнить команду yum с опцией remove:

```
sudo yum remove [имя пакета/путь до пакета]
```

В случае удаления пакета с помощью команды yum remove будет выполнено пробное удаление, после чего вам надо будет подтвердить удаление. Если вы пытаетесь удалить пакет, от которого зависят какие-либо другие установленные в системе пакеты, то YUM предложит удалить их вместе с пакетом зависимостей.

3.10.3.3.2. Обновление YUM-пакетов

Для обновления всей системы или отдельных пакетов (а также нескольких пакетов с использованием групповых символов) используется команда yum update:

```
sudo yum update
```

3.10.3.3.3. Получение информации о YUM-пакетах

Для получения списка инсталлированных пакетов можно использовать команду yum list:

```
sudo yum list
```

3.10.3.3.4. Загрузка YUM-пакетов из репозиториев

Хотя команда yum автоматически загружает пакеты из репозиториев, вам может потребоваться загрузить пакеты и сохранить их, например, для использования на другом компьютере, не подключенном к сети или для проверки их содержимого. Для этого можно использовать команду yumdownloader:

```
sudo yumdownloader [имя пакета]
```

3.10.3.3.5. Поиск YUM-пакетов

YUM может искать пакеты по их именам и описаниям. Если же вам необходимо узнать, в каком пакете содержится еще не инсталлированная программа, можно воспользоваться командой yum provides для поиска пакета предоставляющего искомую программу.

```
sudo yum provides [название программы]
```

3.11.Настройка подсистемы печати

Сервер печати устанавливается на виртуальную машину сервер безопасности. Для настройки печати необходимо выполнить следующие действия:

– аутентифицироваться на сервере безопасности от имени привилегированного пользователя;

– сформировать ссылки на конфигурационные файлы сервера печати;

– настроить запрет на подключение к серверу безопасности (СБ) по 631 порту;

– настроить временную зону, объект, уровня секретности документа (рамка);

– повторный запуск сервисов, отвечающих за печать;

– добавление/удаление принтера.

3.11.1. Формирование ссылок на конфигурационные файлы

Базовый набор конфигураций, входящий в состав пакетов сервера печати (pszi-print, pszi-printing-server), содержит конфигурационные файлы обеспечивающие возможность обработки заданий на печать. Для применения базового набора конфигурации необходимо выполнить следующие команды:

```
ln -sf /usr/share/pszi-print/cupsd.conf_sb /etc/cups/cupsd.conf
```

```
ln -sf /usr/share/pszi-print/cups-browsed.conf_sb /etc/cups/cups-browsed.conf
ln -sf /usr/share/pszi-print/cups-files.conf_sb /etc/cups/cups-files.conf
```

3.11.2. Настройка веб-интерфейса сервиса печати CUPS

Управлять системой печати CUPS удобнее через Web. Все настройки CUPS хранятся в файле /etc/cups/cupsd.conf. Данный файл смоделирован по образу файла Веб сервера Apache. Файл конфигурации cupsd.conf начинается с ряда глобальных директив, которые оформлены в виде пар имя - значение. Для примера, чтобы изменить имя сервера, отправляемое другим системам, необходимо ввести директиву:

```
SeverName my.ptintserver.local
```

Данная строка определяет имя сервера как my.printserver.local. Пример конфигурационного файла, содержащего глобальные директивы:

```
Print-server:~# cat /etc/cups/cupsd.conf
# указание имени сервера
ServerName print-server.domain.local
# указание уровня логирования
LogLevel warning
SystemGroup lpadmin
# Разрешить доступ к серверу
Port 631
Listen /var/run/cups/cups.sock
Listen 192.168.56.3:631
# Включение/выключение функции обзора.
Browsing Off
#BrowseOrder allow,deny
#BrowseAllow all
#BrowseAddress @LOCAL
# указание типа аутентификации
DefaultAuthType Basic
<Location />
 Allow @LOCAL
 # Доступ к консоли управления только из локальной сети.
 Order deny,allow
</Location>
<Location /admin>
 # Доступ к администрированию только с определенной машины
```

```
 Allow From 127.0.0.1
 Allow From 192.168.56.10
 Order deny,allow
</Location>
<Location /admin/conf>
 # Доступ к изменению конфига только с аутентификацией, указанной в
DefaultAuthType
 AuthType Default
 Order deny,allow
</Location>
```

Как уже упоминалось выше, ServerName указывает имя сервера печати. LogLevel указывает подробность журналирования (по умолчанию при установке параметр равен info, если возникли какие-то проблемы с CUPS, а в протоколе нет ничего информативного, можно поднять уровень до максимального — debug2), Port указывает на каком порту будет доступен веб-интерфейс, Listen позволяет указать на каком IP адресе будет доступен веб-интерфейс, а так же прослушиваемый сокет.

Параметры, начинающиеся на Browsing, задают настройки "просмотра". В данном случае, под термином просмотр необходимо понимать возможность CUPS обнаруживать принтеры в сети. Данная возможность поддерживается на уровне протокола IPP. Обнаружение происходит посредством широковещательных рассылок, что при большом количестве серверов CUPS или при частом отключении/подключении принтеров может порождать дополнительную нагрузку на сеть. Так же, включение просмотра влечет за собой определенное бремя безопасности.

BrowseAllow и BrowseDeny

Указывают CUPS на стороне клиента адреса, от которых может приниматься или отвергаться, соответственно, информация о принтерах. Формат директив соответствует директивам Allow и Deny. В качестве аргумента для данной директивы может быть как отдельный IP, так и подсеть в формате 10.0.0.0/24 или 10.0.0.0/255.255.255.0 или 10.0.0.0-10.0.0.255, так и значение @LOCAL - обозначающее локальную сеть, а также имена хостов. Возможно использование нескольких данных директив.

Browsing

Указывает CUPS предоставлять свои серверы в общий доступ, либо нет. Значения может принимать On или Off соответственно.

BrowseAddress

Аналогична BrowseAllow, за исключением того, что она задает кому посылать пакеты, а не от кого принимать.

Далее в конфигурационном файле указана директива DefaultAuthTape, которая указывает механизм аутентификации, который будет использоваться для организации доступа по умолчанию. Basic – указывает использовать логины/пароли от локальной системы. None – указывает не использовать аутентификацию. При указании параметра Digest все пароли будут передаваться в зашифрованном виде, но тогда необходимо создать пользователей CUPS с помощью команды lppasswd, пользователи будут добавлены в файл /etc/cups/passwd.md5.

Существует также директива AuthClass, которая определяет, какие группы пользователей могут иметь доступ к подсистеме. Может принимать значения: Anonymous, User, System, Group. Параметр Anonymous указывает, что аутентификация производиться не должна. Параметр User говорит, что любой пользователь системы, корректно указавший имя/пароль, может иметь доступ. System – говорит, что доступ к подсистеме могут получить только пользователи - члены системной группы cups. Group указывает возможность пользоваться подсистемой только членам группы, которая должна быть указана в последующей директиве AuthGroupName.

Директива Order определяет порядок предоставления доступа к CUPS по умолчанию. Значение Deny, Allow определяет – отвергать попытки доступа, если право на доступ не указано явно. Если директива имеет значение Allow, Deny, то доступ будет предоставлен, если явно не запрещен.

После DefaultAuthType идут параметры, сгруппированные в разделы <Location /...>. Такие директивы определяют доступ к определенным функциям сервера.

На этом настройка доступа к веб-интерфейсу CUPS заканчивается. Остальные действия удобней выполнять через браузер. Для доступа к управлению необходимо ввести в веб-браузере строку http://ip.ad.dr.ess:631, в результате, должен появиться интерфейс управления CUPS. Если этого не произошло, следует проверить настройки еще раз.

Примечание. Перед манипуляциями с веб-интерфейсом необходимо сделать копию работающего конфига, так как после внесения каких-либо изменений в настройки, конфигурационный файл переписывается параметрами веб-интерфейса. В результате, все вышеуказанные настройки сбиваются.

Поэтому, настроив доступ к веб-интерфейсу, следует произвести настройки принтеров в Веб-интерфейсе, проверить работоспособность, а после проверки – восстановить настройки безопасности.

Для отключения доступа к веб-порталу сервиса печати необходимо в файле /etc/cups/cupsd.conf закомментировать строку «Port 631» (рисунок 3.82).

Рисунок 3.82 – Параметр «Allow remote access»

3.11.3. Настройка «Штампа»

Подсистемой печати осуществляется проставление на выходных печатных формах «штампа», содержащего следующую актуальную информацию:

- учетный номер распечатанного документа;
- дата и время печати;
- идентификатор принтера;
- идентификатор пользователя, выдавшего задание на печать;
- имя документа из которого производится печать;
- количество распечатанных страниц, экземпляров.

Кроме того в соответствии с параметрами заданными в конфигурационных файлах подсистемой печати проставляется дополнительно:

– временная зона;

– наименование системы или объекта;

– гриф документа.

Для настройки временной зоны и названия объекта автоматизации открыть текстовым редактором файл: /etc/pszi-print/sintez_autolabel.conf (рисунок 3.83).

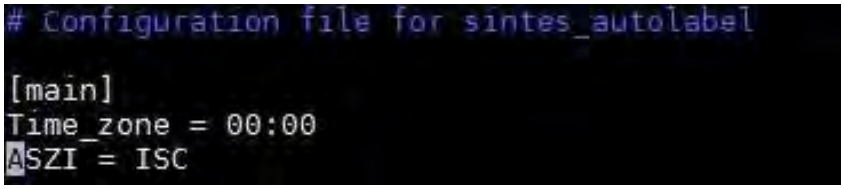


Рисунок 3.83 – Файл конфигурации

В рабочей области отобразится форма файла конфигурации, где параметр:

– «Time_zone» определяет смещение времени относительно даты, выставленной на сервере печати (сервере безопасности). Формат: чч:мм;

– «ASZI» определяет наименование объекта автоматизации.

Для задания грифа документа на печатающихся экземплярах документа необходимо в текстовом редакторе открыть файл /usr/share/pszi-print/sintez-autolabel, после чего внести изменения в строки 148, 159, 160, где прописано «Секретно»:

```
try:
        result = ld.search_s(basedn, ldap.SCOPE_SUBTREE)
    except:
        return 'Секретно'
    try:
        for contours in result[0][1].get('member'):
            try:
                if compare_ld_template in ld.search_s(contours,
ldap.SCOPE_SUBTREE)[0][1].get('member'):
                    return ld.search_s(contours,
ldap.SCOPE_SUBTREE)[0][1].get('description')[0]
```

```
            except TypeError as e:
            # TODO write in log
                continue
    except:
            return 'Секретно'
    return 'Секретно'
```

Примечание. Параметр гриф документа является информационным и проставляется автоматически для всех документов задание на печать которых было отправлено на сервер печати. Данная параметр применяется для принтеров при их добавлении через команду pszi-cupsfilter --config-

3.11.4. Запуск и остановка сервисов печати

После настройки сервера печати необходимо перезапустить cups, cups-browsed, pszi-printing-server командами:

```
service cups [Параметр]
service cups-browsed [Параметр]
service pszi-printing-server [Параметр]
```

, где [Параметр] – может принимать одно из трех значений в соответствии с таблицей 3.12.

Таблица 3.12 – Перечень параметров управляющей утилиты service

№ п/п	Параметр	Описание	Примечание
1.	start	Запуск службы	
2.	stop	Остановка службы	
3.	restart	Перезапуск службы	

3.11.5. Добавление/удаление принтера

Для добавления записи о принтере на сервере печати (сервере безопасности) выполнить команду:

```
pszi-cupsfilter --config-printer <Наименование принтера> <IP-адрес принтера>
```

Примечание. Параметр «Наименование принтера» является уникальным значением.

Для удаления записи о принтере выполнить команду:

```
pszi-cupsfilter --delete-printer <Наименование принтера>
```

Примечание. Для удаления задания, отправленного на принтер выполнить команду: pszi-cupsfilter --delete-cups-job <Номер задания>.

После настройки сервера печати и добавления принтеров необходимо убедиться, что на клиентской машине с которой будет осуществляется печать установлен пакет pszi-print (рисунок 3.84). Для проверки на клиенте необходимо выполнить команду:

```
rpm -qa |grep pszi-print
```

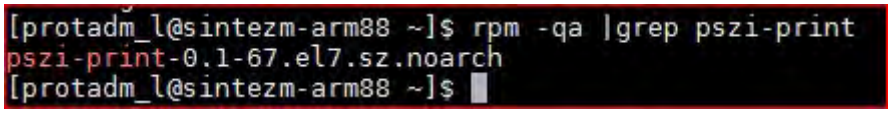


Рисунок 3.84 – Проверка наличия пакета pszi-print

3.12.Настройка подсистемы контроля целостности

Подсистема «Контроль целостности», реализуемая в рамках функции «Контроль целостности», осуществляет контроль над объектами файловой системы, используемыми компонентами, ПК и исполняемым кодом КП «ЗОС «СинтезМ». Осуществляемый контроль, в свою очередь, разделяется на следующие виды:

1. КЦ при загрузке ОС;
2. КЦ с определенным периодом (период задает локальный администратор безопасности);
3. КЦ по требованию локального администратора.

Контроль целостности осуществляется только локальным администратором. Ему доступны следующие функции:

- запуск задания проведения контроля целостности;
- запуск перерасчета эталонных значений контрольных сумм;
- настройка модуля AIDE;
- настройка расписания запуска периодической проверки контрольных сумм.

3.12.1. Настройка модуля AIDE

Настройка списка файлов для контроля целостности производится через конфигурационный файл /etc/aide.conf. В данном конфигурационном файле перечислены объекты файловой системы, по которым происходит контроль целостности. Помимо вышеупомянутого конфигурационного файла, объекты, для которых производится контроль целостности, также перечислены в /etc/aide.startup.conf. В данном конфигурационном файле перечислены файлы ядра ОС, ПСЗИ и конфигурационные файлы ЗОС, подлежащие КЦ.

Также для проведения контроля целостности используется файл дополнительной конфигурации /var/lib/aide/sintez/aide.conf. В данный файл необходимо вносить (или удалять) объекты файловой системы, подлежащие контролю целостности. Для того, чтобы внести какой-либо объект файловой системы для проведения КЦ, локальному администратору необходимо указать его полный адрес в файле /var/lib/aide/sintez/aide.conf. После включения нового элемента в КЦ локальному администратору необходимо провести перерасчет эталонных значений контрольных сумм.

Для того чтобы изменить список файлов, подлежащих контролю, необходимо отредактировать файл `/etc/aide.conf`. Для того чтобы получить подробную справку о том, как устроен данный файл, необходимо набрать в консоли `man aide.conf`.

В данном файле содержатся строки четырех типов:

– строки конфигурации, содержащие значения параметров и переменных;

– строки выборки, обозначающие, какие файлы надо внести в базу данных;

– макроопределения;

– строки, начинающиеся «с #» – комментарии.

Пример:

```
#AIDE conf
# Here are all the things we can check - these are the default
rules
#
```

```
#p: permissions
#ftype: file type
#i: inode
#n: number of links
#l: link name
#u: user
#g: group
#s: size
#b: block count
#m: mtime
#a: atime
#c: ctime
#S: check for growing size
#I: ignore changed filename
#md5: md5 checksum
#sha1: sha1 checksum
#sha256: sha256 checksum
#sha512: sha512 checksum
#rmd160: rmd160 checksum
#tiger: tiger checksum
#haval: haval checksum
#crc32: crc32 checksum
#DATAONLY: p+ftupe+i+l+n+u+g+s+m+c+md5
#L: p+ftype+i+l+n+u+g
#E: Empty group
#>: Growing logfile p+ftype+l+u+g+i+n+S
#The following are available if you have mhash support enabled:
#gost: gost checksum
#whirlpool: whirlpool checksum
#The following are available and added to the default groups R, L
and >
#only when explicitly enabled using configure:
#acl: access control list#selinux SELinux security context
#xattrs: extended file attributes
#e2fsattrs: file attributes on a second extended file system
```

```
# You can alse create custom rules - my home made rule definition
goes like this
MyRule = p+i+n+u+g+s+b+m+c+md5+sha1
# Next decide what directories/files you want in the database
/etc p+i+u+g #check only permissions, inode, user and group for
etc
/bin DATAONLY # apply the custom rule to the files in bin
/sbin MyRule # apply the same custom rule to the files in sbin
/var MyRule
!/var/log/.* # ignore the log dir it changes too often
!/var/spool/.*# ignore spool dirs as they change too often
!/var/adm/utmp$ # ignore the file /var/adm/utmp
```

В соответствии с данной конфигурации каталог `/bin` поставлен на контроль по правилу `DATAONLY`. Данная конфигурация включает файл из `/etc`, `/bin` и `/sbin`. Также она включает файлы из `/var` за исключением `/var/log`, `/var/spool` и `/var/adm/utmp`.

Для добавления конкретных файлов и директорий достаточно добавлять их абсолютные пути в файл и правила, по которым будет выполняться проверка? например:

```
/usr/bin DATAONLY
```

Для исключения файла или директории перед его именем необходимо поставить восклицательный знак например:

```
!/etc/aide.conf
```

, при этом файл `/etc/aide.conf` будет исключен из проверки на целостность.

3.12.2. Настройка расписания запуска периодической проверки

Для изменения расписания проведения периодической проверки контрольных сумм необходимо любым текстовым редактором отредактировать конфигурационный файл /etc/cron.d/counthash_timetable. Настройка расписания осуществляется в соответствии с пунктом 3.10.1 данной инструкции.

3.12.3. Запуск перерасчета эталонных значений контрольных сумм

Перерасчет эталонных значений контрольных сумм должен проводиться локальным администратором при внесении изменений в ОС.

Перерасчет эталонных значений осуществляется за счет вызова скрипта counthash с параметром –r.

```
counthash -r
```

, где параметр «-r» – перерасчет контрольных сумм объектов файловой системы.

Для перерасчета эталонных значений контрольных сумм рассчитываемых при старте системы необходимо выполнить команду:

```
counthash –r startup.
```

или

```
service aide_startup init
```

3.13. Настройка подсистемы регистрации событий безопасности

Подсистема «Регистрация событий безопасности» состоит из следующих модулей:

– модуль auditd (протоколирование системных вызовов);

– модуль rsyslog (сбор системных сообщений и их передача для последующего анализа);

– модуль dlogevent (обработка системных сообщений, получаемых от rsyslog);

– модуль logrotate (автоматизация обработки журналов событий безопасности);

– сервер безопасности (сбор событий безопасности и их представление на портале управления).

3.13.1. Запуск и остановка модулей подсистемы регистрации событий безопасности

Запуск и функционирование модулей подсистемы обеспечивает системный менеджер systemd. Отслеживание и контроль состояния осуществляется с использованием утилиты systemctl.

В качестве параметра запуска утилита использует юнит. В качестве юнита выступают модули подсистемы «Регистрация событий безопасности». Для запуска модуля подсистемы «Регистрация событий безопасности» локальный администратор вводит команду следующего вида:

```
# systemctl start «юнит»
```

Для остановки модуля подсистемы «Регистрация событий безопасности» локальный администратор вводит команду следующего вида:

```
# systemctl stop «юнит»
```

Также утилита используется для отображения статуса юнита. По умолчанию любой юнит может принимать 2 статуса – запущен или нет. Для проверки статуса юнита локальному администратору необходимо ввести следующую команду:

```
# systemctl status юнит
```

Управление режимом запуска модуля audit и модуля rsyslog подсистемы «Регистрация событий безопасности» осуществляется за счет вызова управляющей утилиты systemctl или service.

```
# systemctl [параметр] auditd.service
```

`# systemctl [параметр] rsyslog.service`, где параметр может принимать значения в соответствии с таблицей 3.13.

Таблица 3.13 – Перечень параметров управляющей утилиты systemctl

№	Параметр	Описание	Примечание
1	start	Запуск службы	
2	stop	Остановка службы	
3	restart	Перезапуск службы	
4	status	Получение информации о текущем состоянии работы службы	
5	enable	Включение службы в автозагрузку при старте ОС	
6	disable	Исключение службы из автозагрузки при старте ОС	
7	reload	Перезагрузка правил фильтрации из конфигурационного файла	Применимо только для iptables, auditd

Управление режимом запуска модуля dlogevent подсистемы «Регистрация событий безопасности» осуществляется за счет вызова управляющей утилиты service.

`# service dlogevent [параметр]`, где параметр может принимать значения в соответствии с таблицей 3.14.

Таблица 3.14 – Перечень параметров управляющей утилиты service

№	Параметр	Описание
4.	start	Запуск службы
5.	stop	Остановка службы
6.	restart	Перезапуск службы

3.13.2. Модуль auditd

Модуль auditd обеспечивает протоколирование системных вызовов, работу средств сбора и просмотра записей аудита, работающих в программном окружении пользователя.

В состав auditd входят сам модуль и следующие утилиты:

– auditctl — управляет демоном auditd; с её помощью можно настраивать правила и следить за работой;

– ausearch — поиск событий в лог файле;

– aureport — утилита для создания отчетов.

Изменять и настраивать модуль auditd может только локальный администратор. Настройки auditd хранятся в конфигурационном файле /etc/audit/audit.conf. Правила аудита (настройка системы мониторинга действий в системе), загружаемые при старте модуля auditd, хранятся в соответствующих файлах директории /etc/audit/rules.d/. Для настройки правил аудита может использоваться команда auditctl (/usr/sbin/auditctl/) с различными параметрами (используемые параметры описаны ниже), добавление правил в данном случае осуществляется через командную строку.

В случае перезагрузки модуля auditd (перезагрузка модуля происходит при перезагрузке КП «ЗОС «СинтезМ», или по команде), правила, записанные при помощи команды auditctl вручную локальным администратором, перестают действовать.

Помимо вышеупомянутого способа, добавить правило аудита можно напрямую через файл /etc/audit/rules.d/audit.rules. Правила, добавленные напрямую через audit.rules, не перестают действовать при перезагрузке модуля.

Все настройки выполняются в конфигурационном файле /etc/audit/auditd.conf.

– log_file — путь к файлу, в котором хранятся системные сообщения

– log_format — формат, сохранения информации в файл с системными сообщениями;

– freq — число записей хранящиеся в буфере;

– flush — как будут синхронизироваться буфер с диском (none — не синхронизировать, incremental — переносить периодически с частотой в параметре freq; data — моментальная синхронизация, sync — синхронизировать при сбросе на диск);

– max_log_file — размер лог файла в Mb;

– max_log_file_action — что делать если лог превысил предыдущее значение;

– space_left — минимальный порог пространства, после чего сработает следующий параметр;

– space_left_admin — действия в случае окончания места для записи на диске (ignore — игнорировать; syslog — писать в syslog, email — отправлять письмо; suspend — остановить запись; single — сменить на однопользовательский режим; halt — остановить систему)

– disk_full_action — действия в случае переполнения диска (значения такие же как space_left_admin).

Для работы с правилами используется auditctl с опциями:

– l - показать все правила;

– a - создать новое;

– d - удалить правило;

– D - удалить все правила из списка.

Для создания правил используется команда следующего вида:

```
auditctl -a ”действие”,”список” -S  ”имя системного вызова” -F ”фильтры”
```

```
-K ”тег фильтрации”
```

В первом поле указываются действия, которые необходимо выполнить при том или ином событии: always (записать в журнал) и never (не писать).

Варианты возможных значений поля «список»:

– task - события, вызванные новыми процессами;

– entry - события, входа;

– exit - события, выхода;

– user - события, с параметрами пользователя;

– exclude - события исключения.

После «-S» указывается имя системного вызова, за которым устанавливается или прекращается наблюдение. При помощи опции «-F» устанавливаются параметры фильтра, а используя «-k» – устанавливается тег сообщения.

Например, команда добавления правила аудита, регистрирующего все попытки обращения к файлу /etc/passwd выглядит следующим образом:

```
auditctl -a always,exit -F arch=b32 -F path=/etc/passwd  -S open -k open32
```

Можно использовать дополнительные фильтры. Например, следить только за изменением атрибутов (a) и записью (w)

```
auditctl -a always,exit -S open -F path=/etc/passwd -F perm = aw
```

Для того чтобы правила, введенные локальным администратором через консоль, продолжали действовать после перезагрузки КП «ЗОС «СинтезМ» и модуля auditd соответственно, необходимо выполнить следующую команду для сохранения текущего списка правил в файл:

```
auditctl -l > /etc/audit/rules.d/audit.rules
```

После выполнения команды правила будут сохранены в файл /etc/audit/rules.d/audit.rules и будут загружаться после перезагрузки модуля.

Также локальный администратор может вручную составить новое правило аудита и добавить его в конфигурационный файл. Формат правила аналогичен параметрам передаваемым auditctl.

Для изменения правил аудита, локальному администратору необходимо открыть консоль и ввести команду:

```
vim /etc/audit/rules.d/audit.rules
```

В результате выполнения команды откроется файл audit.rules, в котором содержатся правила аудита. На рисунке 3.85 представлен фрагмент данного файла.

```
# This file contains the auditctl rules that are loaded
# whenever the audit daemon is started via the initscripts.
n The rules are simply the parameters that would be passed
# to auditctl.

# First rule - delete all
-D

# Increase the buffers to survive stress events.
# Make this bigger for busy systems
-b 320

# Feel free to add below this line. See auditctl man page
# 32
-a always,exit -F arch=b32 -S execve -S exit -S kill -F uid>=500

# 64
-a always,exit -F arch=b64 -S execve -S exit -S kill -F uid>=500

# don't show cron jobs
-a never,user -F subj_type=crond_t
```

Рисунок 3.85 – Фрагмент содержимого audit.rules

Vim – это текстовый редактор, позволяющий просматривать и модифицировать содержимое файла. После выполнения команды, представленной выше, файл откроется в режиме чтения. Для активации режима редактирования файла администратор нажимает клавишу с буквой «i» на клавиатуре.

Для выхода из редактора администратору необходимо нажать клавишу Esc и далее одну из следующих команд:

- :q — закрытие текстового редактора (без внесения изменений);
- :q! — закрытие текстового редактора (без сохранения внесенных изменений);
- :wq — сохранение и выход из Vim.

3.13.3. Модуль rsyslog

Основным конфигурационным файлом rsyslog является /etc/rsyslog.conf. В конфигурационном файле указываются глобальные директивы, модули и правила. Любой текст после знака хеша (#) является комментарием и не влияет на настройку модуля.

Правила состоят из части фильтра и части действия, формируемое в одной строке и разделённые одним или несколькими пробелами. Правило применяется сообщений аудита и определяется следующими частями:

- часть «фильтр», выбирающий подмножество сообщений аудита из всего множества сообщений аудита. Методы фильтрации разделяются на:

  - на основе метки объекта;
  - на основе метки важности;
  - на основе свойств сообщения аудита;
  - на основе выражения.

- часть «действие», определяющее действие с отфильтрованными сообщением аудита. Действиями могут быть:

  - сохранения сообщения аудита в файл;
  - отправка сообщения аудита по сети;
  - выполнение программы;
  - сохранение сообщения аудита в БД;
  - пропуск сообщения аудита;
  - выполнение нескольких вышеперечисленных действий.

Модульная конструкция rsyslog предоставляет множество модулей, обеспечивающие дополнительную функциональность. Большинство модулей предоставляют собой дополнительные модули ввода системного сообщения или модули вывода сообщения аудита. Для загрузки модуля в конфигурационном файле rsyslog.conf используется следующий синтаксис:

```
module(load=”MODULE”)
```

, где MODULE – название модуля. Например, для загрузки модуля ввода текстового файла(imfile), который позволяет rsyslog конвертировать любые стандартные текстовые файлы в системные сообщения rsyslog, указывается следующая строка в конфигурационном файле rsyslog.conf:

```
module(load=”imfile”)
```

Модули rsyslog разделены на следующие основные категории:

- модули ввода (Input Modules) – модули, собирающие системные сообщения из разных источников. Имя модуля ввода всегда начинается с префикса im (imfile, imjournal).
- модули вывода (Output Modules) – модули, предоставляющие возможность вывода сообщения аудита различными средствами, такими как отправка по сети, сохранение в БД, сохранение в файл. Имя модуля вывода всегда начинается с префикса om (omsnmp, omrelp).
- модули разбора (Parser Modules) – модули, предоставляющие создание пользовательских правил разбора и синтаксического анализа сообщения аудита. Имя модуля разбора всегда начинается с префикса pm (pmrfc5424, pmrfc3164).
- модули модификации сообщений (Message Modification Modules) – модули, модифицирующие содержимое сообщения аудита. Имена этих модулей начинаются с префикса mm (mmanon, mmnormalize, mmjsonparse).
- модули генерации сообщений аудита (String Generator Module) – модули, генерирующие сообщения аудита на основе содержимого входящего системного сообщения. Имя модуля генератора строк всегда начинается с префикса sm (smfile, smtradfile).
- библиотечные модули (Library Modules) – библиотечные модули, обеспечивающие функциональность других загружаемых модулей. Эти модули автоматически загружаются rsyslog при необходимости и не могут быть настроены.

Настройка модуля происходит через конфигурационные файлы. Перечень конфигурационных файлов rsyslog представлен в таблице 3.15.

Таблица 3.15 – Конфигурационные файлы rsyslog

№	Файл	Описание	Примечание
1.	/etc/rsyslog.d/rsyslog-audit.conf	Настройка взаимодействия с подсистемой аудита	
2.	/etc/rsyslog.d/rsyslog-dlog.conf	Вывод всех сообщений dlogevent в отдельный файл	Используется при отладке
3.	/etc/rsyslog.d/rsyslog-ipa.conf	Настройка взаимодействия с средства управления доступом IPA	
4.	/etc/rsyslog.d/rsyslog-ovirt.conf	Настройка взаимодействия с менеджером виртуализации	
5.	/etc/rsyslog.d/rsyslog-pipe.conf	Настройка передачи сообщений аудита в pipe файл	
6.	/etc/rsyslog.d/rsyslog-prog.conf	Настройка обработки неверного ввода пароля	
7.	/etc/rsyslog.d/rsyslog-receive.conf	Настройка получения событий безопасности с других хостов	
8.	/etc/rsyslog.d/rsyslog-send.conf	Настройка отправки событий безопасности на сервер безопасности	

1. Конфигурационный файл /etc/rsyslog.d/rsyslog-audit.conf настраивает получение системных сообщений с модуля auditd. Взаимодействие основано на лог-файле /var/log/audit/audit.log. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля imfile для чтения системных сообщений из файла ($ModLoad imfile);

– определение пути до лог-файла ($InputFileName /var/log/audit/audit.log);

– определение тега сообщений аудита ($InputFileTag tag_audit_log:);

– определение названия файла состояния, позволяющего определить новые сообщения аудита ($InputFileStateFile audit_log);

– определение метки важности сообщений аудита ($InputFileSeverity info);

– определение метки объекта ($InputFileFacility local6);

– активация слежения за лог-файлом ($InputRunFileMonitor).

2. Конфигурационный файл /etc/rsyslog.d/rsyslog-dlog.conf предназначен для отладки и выполняет вывод всех сообщений процесса dlogevent в файл /var/log/sec-events.log.

3. Конфигурационный файл /etc/rsyslog.d/rsyslog-ipa.conf настраивает сбор системных сообщений, генерируемых Средством управления доменными

пользователями. Сбор осуществляется за счет мониторинга журнала Средства управления доменными пользователями /var/log/httpd/error_log. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля imfile для чтения системных сообщений из файла ($ModLoad imfile);

– определение пути до лог-файла ($InputFileName /var/log/httpd/error_log);

– определение тега сообщений аудита ($InputFileTag tag_ipa_log:);

– определение названия файла состояния, позволяющего определить новые сообщения аудита ($InputFileStateFile ipa_log);

– определение метки важности сообщений аудита ($InputFileSeverity info);

– определение метки объекта ($InputFileFacility local6);

– активация слежения за лог-файлом ($InputRunFileMonitor).

4. Конфигурационный файл /etc/rsyslog.d/rsyslog-ovirt.conf настраивает сбор системных сообщений со средства управления средой виртуализации (менеджера ВМ). Данный конфигурационный файл применяется исключительно на ВМ в рамках которой функционирует менеджер ВМ, по умолчанию все строки конфигурационного файла закомментированы. Для настройки сбора событий с Менеджера ВМ необходимо раскомментировать все строки и перезапустить модуль rsyslog. Сбор осуществляется за счет мониторинга журнала менеджера ВМ /var/log/ovirt-engine/engine.log. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля imfile для чтения системных сообщений из файла ($ModLoad imfile);

– определение пути до лог-файла ($InputFileName /var/log/ovirt-engine/engine.log);

– определение тега сообщений аудита ($InputFileTag ovirt-engine:);

– определение названия файла состояния, позволяющего определить новые сообщения аудита ($InputFileStateFile ovirt-engine);

– определение метки важности сообщений аудита ($InputFileSeverity info);

– определение метки объекта ($InputFileFacility local6);

– активация слежения за лог-файлом ($InputRunFileMonitor).

5. Конфигурационный файл /etc/rsyslog.d/rsyslog-pipe.conf настраивает передачу всех системных сообщений собранных rsyslog в pipe файл, для их последующей обработки модулем dlogevent. Взаимодействие основано на pipe-файле /var/run/dlogevent.pipe. Конфигурационный файл состоит из следующих параметров:

– определение шаблона сообщения аудита ($template pipe_out,"«timereported:::date-unixtimestamp» |«source» |«programname» |«syslogtag» | «msg» | «syslogfacility-text» |«syslogseverity-text» \n");

– вывода всех полученных сообщений аудита в pipe файл с применением шаблона pipe_out (*.* |/var/run/dlogevent.pipe; pipe_out);

6. Конфигурационный файл /etc/rsyslog.d/rsyslog-prog.conf используется для настройки обработки события ввода неверного пароля пользователем при аутентификации. Данный конфигурационный файл применяется исключительно на ВМ в рамках которой функционирует сервер безопасности, по умолчанию все строки конфигурационного файла закомментированы. Для настройки работы необходимо на сервере безопасности раскомментировать все строки и перезапустить модуль rsyslog. Определение события ввода неверного пароля основано на UUID события безопасности, сгенерированного АРМ. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля omprog для запуска бинарных файлов (module(load="omprog"));

– проверки события безопасности на содержание UUID события ввода неверного пароля. В случае, если событие безопасности содержит данный UUID, производится запуск приложения анализа неверного пароля с передачей события безопасности в качестве аргумента (:msg, contains, "b7f8f4a1-2dea-4342-b36e-6e51b2d5ce0e» action(type="omprog" binary="/usr/share/pszi-dlogevent/rsyslog_analyse_wr_password")).

7. Конфигурационный файл /etc/rsyslog.d/rsyslog-receive.conf настраивает получение на сервере безопасности событий безопасности от АРМ и ВМ. Данный конфигурационный файл применяется исключительно на ВМ в рамках которой функционирует сервер безопасности, по умолчанию все строки конфигурационного файла закомментированы. Для настройки работы необходимо на сервере безопасности раскомментировать все строки и перезапустить модуль rsyslog. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля imrelp для загрузки RELP протокола для передачи событий безопасности ($ModLoad imrelp);

– запуск сервера RELP на порту 2514 ($InputRELPServerRun 2514).

8. Конфигурационный файл /etc/rsyslog.d/rsyslog-send.conf настраивает отправку на сервер безопасности событий безопасности от АРМ и ВМ. По умолчанию все строки конфигурационного файла закомментированы. Для настройки работы необходимо на АРМ и ВМ раскомментировать все строки и перезапустить модуль rsyslog. Конфигурационный файл состоит из следующих параметров:

– загрузка модуля omrelp для загрузки RELP протокола (протокол RELP используется для передачи событий безопасности ($ModLoad omrelp));

– передача сообщений аудита от модуля dlogevent на IP адрес сервера СБ по порту 2514 (:programname, isequal, "dlogevent" :omrelp:<IP_address_SB_server>:2514).

3.13.4. Модуль rsyslog-RELP

Модуль rsyslog-RELP получает события безопасности и отправляет их на сервер безопасности для дальнейших хранения и обработки. Передача осуществляется по протоколу RELP – сетевому протоколу с гарантированной доставкой. Подробнее об устройстве механизма передачи событий безопасности описано в документе Базовый Модульный Проект.

Конфигурация модуля rsyslog-RELP осуществляется через конфигурационные файлы:

- /etc/rsyslog.d/rsyslog-send.conf – для передачи событий безопасности;
- /etc/rsyslog.d/rsyslog-receive.conf – для получения событий безопасности.

Конфигурационный файл rsyslog-send.conf загружает модуль omrelp для отправки событий безопасности, которые, в свою очередь, формируются модулем dlogevent. События безопасности передаются на сервер безопасности. Конфигурационный файл состоит из следующих строк:

```
# загрузка модуля omrelp
$ModLoad omrelp
# :programname, isequal, "dlogevent" - отправление событий безопасности
от:
#  модуля dlogevent
# <ip адрес сервера СБ> - IP адрес сервера СБ (например, 10.10.10.10)
# 2514 – порт работы RELP сервера
:programname, isequal, "dlogevent" :omrelp:<ip адрес сервера СБ>:2514
```

Конфигурационный файл rsyslog-receive.conf загружает модуль imrelp для получения событий безопасности на сервере безопасности.

Конфигурационный файл состоит из следующих строк:

```
# загрузка модуля omrelp
$ModLoad imrelp
# запуск сервера RELP на порте 2514
$InputRELPServerRun 2514
```

3.13.5. Модуль Dlogevent

За обработку сообщений аудита и формирование на их основе событий безопасности отвечает модуль dlogevent.

В зависимости от роли средства вычислительной техники, на котором функционирует модуль dlogevent он выполняет следующие функциональные задачи:

а) задачи, решаемые модулем dlogevent, устанавливаемым на сервера, АРМ, ВМ:

– получение сообщения от rsyslog; формирование события безопасности на основе обработки одного или нескольких системных сообщений или событий безопасности;

– трансляция сформированных событий безопасности, в соответствии с перечнем заданным в инициализирующей БД, в rsyslog для их локального хранения и дальнейшей отправки на сервер безопасности;

б) задачи, решаемые модулем dlogevent, устанавливаемым на сервере безопасности:

- получение сообщения от rsyslog;
- запись событий безопасности в базу данных сервера безопасности.

Модуль dlogevent запускается при старте системы модулем инициализации системы init.d. Модуль init.d запускает dlogevent согласно параметрам, указанным в файле /etc/init.d/dlogevent. Параметры запуска приведены в таблице 3.16.

Таблица 3.16 – Параметры запуска модуля dlogevent

№	Параметр	Описание
1.	-s	Старт dlogevent
2.	-t	Остановка dlogevent
3.	-d	Подробный вывод действий при работе модуля
4.	-h	Вывод информации о параметрах запуска dlogevent

Далее происходит считывание инициализирующей БД init.sqlite формата sqlite3. Инициализирующая база /etc/dlogevent/init.sqlite предназначена для хранения шаблонов сообщений аудита и шаблонов сообщений событий безопасности, которые будут сформированы на основе сообщений аудита. Инициализирующая база устанавливается в систему КП «ЗОС «СинтезМ» при установке пакета pszi-dlogevent. База состоит из таблицы sec_events_table. Структура sec_events_table представлена в таблице 3.17.

Подробный вывод при работе модуля осуществляется в лог файл /var/log/dlogevent.log, который хранит записи о работе модуля в хронологическом порядке.

Таблица 3.17 – Структура таблицы sec_events_table базы данных init.sqlite

№	Имя поля	Описание	Пример
1.	id	Порядковый номер шаблона сообщения аудита	2
2.	syslog_tag	Имя процесса, генерирующего данное сообщение аудита	tag_audit_log
3.	message	Шаблон сообщения аудита	.*msg='sype=CARD_REMOVE user={user} auid=.*
4.	requred_event	Перечень id шаблонов сообщений аудита, необходимых для генерации события безопасности	
5.	output_to	Определение, куда необходимо выводить событие безопасности. Возможные варианты вывода: 0 – вывод не производится 1 – производится в rsyslog 2 – производится в БД событий безопасности 3 – производится в rsyslog и в БД событий безопасности	3
6.	security_event	Шаблон события безопасности	[{UUID}] Аутентификация: Пользователь {user} извлек ТК/ПИ
7.	event_tag	Тэг шаблона сообщения аудита	CARD_REMOVE
8.	action	Действие	CARD_REMOVE_ACTION
9.	UUID	Уникальный идентификатор шаблона сообщения аудита	4ede7c4b-a6b8-4fc6-a4b7-9caaf8df31da
10	enabled	Включен ли данный шаблон	1

Для добавления/редактирования/ удаления шаблонов сообщений необходимо использовать приложение sqlite3 из пакета sqlite-3.7.17-8.el7.x86_64. Пример выключения шаблона сообщения аудита (процесс редактирования шаблона сообщения аудита):

```
[root@sintezm ~]# sqlite3 /etc/dlogevent/init.sqlite
SQLite version 3.7.17 2013-05-20 00:56:22
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite>update sec_events_table set enabled=0 where id=153;
```

На основе инициализирующий БД init.sqlite осуществляется формирование структур шаблонов сообщений аудита по определенному алгоритму. Более подробное описание о процессе формирования структуры шаблонов сообщений представлено в документе «Базовый Модульный Проект».

Сервер безопасности

События безопасности, поступающие от АРМ и ВМ, хранятся в базе данных сервера безопасности. База данных событий безопасности сервера безопасности (БДСБСБ) предназначена для централизованного хранения событий безопасности и адаптацию событий безопасности в формат, удобный для последующего анализа. БДСБСБ основана на БД PostgreSQL и состоит из следующих таблиц:

- таблицы systemevents.systemevents.
- таблицы systemevents.systemevents_initialization
- таблицы systemevents.systemevents_action.

Формат таблицы systemevents.systemevents представлен в таблице 3.18.

Таблица 3.18 – Структура БДСБСБ

№	Имя поля	Описание	Пример
1.	– id	– Уникальный идентификатор события безопасности	– a2b4e424-2f09-4a06-9b35-759121f5a088
2.	– time	– Время генерации события безопасности	– 2018-04-25 23:26:49

№	Имя поля	Описание	Пример
3.	– message	– Сообщение события безопасности	– СБ. Очистка событий безопасности: Список событий безопасности был очищен 25-4-2018, 23-26. Создан файл 25-4-2018_23-26_cleaning.zip. (action: cleaning systemevents, object: no data, subject: ksa1v1admin, host: ksa1v1sb.vlad.ru, datetime: 1524662809456)
4.	– event_tag	– UUID события безопасности	2cd259e7-81dd-4e29-b – 1dc-7e105a01c0d4
5.	– host	– Хост, на котором произошло событие безопасности	– ksa1v1sb
6.	– checked	– Флаг просмотра события безопасности администратором	– F

Для того, чтобы производилась запись событий безопасности в БДСБСБ, необходимо подключение к БД. При подключении модуля dlogevent к БДСБСБ используется технологическая учётная запись СУБД PostgreSQL, с именем dlogevent. Создание пользователя происходит автоматически при установке пакета pszi-sb-db следующими командами:

```
createuser -U postgres -sw dlogevent
GRANT ALL ON SCHEMA systemevents TO dlogevent;
GRANT ALL ON TABLE systemevents TO dlogevent;
GRANT ALL ON TABLE systemevents_initialization TO dlogevent;
```

Шаблоны сообщений аудита

Шаблоны сообщений аудита используются dlogevent для обработки системных сообщений и формирования на их основе событий безопасности. Шаблоны сообщений аудита основаны на регулярных выражениях.

Регулярное выражение (regular expressions) – формальный язык поиска и осуществления манипуляций с подстроками в тексте, основанный на использовании метасимволов. Для поиска используется шаблон строки(строка-образец), состоящая из символов и метасимволов и задающая правило поиска.

Пример шаблона сообщения аудита запуска контроля целостности:

```
«.*type=start suffix={suffix} result={result}»
```

Пример сообщения системы о запуске контроля целостности:

```
«type=start suffix= result=success»
```

Метасимвол «.*» означает любое количество любых символов или их отсутствие.

В результате наложения шаблона на сообщение системы будут выделены следующие полезные данные, описанные в пункте 3.

Ключ полезного данного	Значение полезного данного
«suffix»	«»
«result»	«success»

На основе полученных полезных данных формируется событие безопасности. Пример события безопасности для запуска контроля целостности:

«[{UUID}] Запуск контроля целостности. Тип {suffix}. Результат: {result}»

Поскольку у данного шаблона сообщения аудита нет шаблонов сообщений аудита, от которого данный шаблон зависит и которые необходимы для формирования события безопасности, полезные данные берутся только из данного шаблона. В случае, если такие шаблоны сообщений аудита есть, полезная информация составляется из данного сообщения аудита и от зависимых сообщений аудита.

В результате подстановки полезных данных в событие безопасности получается следующее:

«[{UUID}] Запуск контроля целостности. Тип. Результат: success»

Значение полезного данного UUID берётся из инициализирующей базы init.sqlite. В результате получается сформированное сообщение события безопасности:

«[ab0ed56a-a47f-44a3-8378-b9b558dd1013] Запуск контроля целостности. Тип. Результат: success»

3.13.6. Модуль logrotate

Модуль logrotate предназначен автоматической ротации, сжатия, удаления, и пересылки журналов. Каждый файл журнала может обрабатываться ежедневно, еженедельно, ежемесячно или когда он становится слишком большим.

По умолчанию модуль logrotate запускается ежедневно службой cron в соответствии с расписанием /etc/cron.daily/logrotate.

По умолчанию используется конфигурационный файл `/etc/logrotate.conf` и файл состояния `/var/lib/logrotate.status`. Файл состояния содержит перечень, состоящий из имени файла журнала и даты его последней ротации. Пример файла состояния:

```
logrotate state -- version 2
"/var/log/nginx/error.log" 2018-5-10-3:21:1
"/var/log/yum.log" 2018-3-16-3:0:0
"/var/log/maillog" 2018-5-6-3:48:1
"/var/log/secure" 2018-5-6-3:48:1
"/var/log/messages" 2018-5-6-3:48:1
"/var/account/pacct" 2018-3-16-3:0:0
"/var/log/cron" 2018-5-6-3:48:1
```

Формат использования logrotate представлен ниже:

```
logrotate [-dv] [-f|--force] [-s|--state файл] файл_конфигурации+
```

Таблица 3.19 – Опции модуля logrotate

№	Опция	Параметр опции	Описание
1.	-d	–	Активирует режим отладки, в котором включена и опция -v (действия программы сопровождаются выводом подробной информации). В режиме отладки файлы системных сообщений, а также файл состояния logrotate, не подвергаются изменениям со стороны утилиты.
2.	-f	–	Принуждает logrotate произвести обращение журналов, даже если сама программа не считает это необходимым. Иногда это полезно после добавления новых записей в logrotate или если старый файл журнала был удалён вручную; таким образом будут созданы новые файлы и журналирование будет корректно продолжено.
3.	-m	команда	Указывает logrotate, какую команду использовать для отправки журналов по электронной почте. Эта команда может принять два аргумента: 1) тема письма и 2) получатель. Команда должна читать сообщение со стандартного входа и отсылать его электронной почтой получателю. Командой по умолчанию является /bin/mail -s.
4.	-s	файл	Предписывает logrotate использовать альтернативный файл состояния. Это полезно, если logrotate запускается от имени разных пользователей для разных наборов файлов системных сообщений. Файл состояния по умолчанию -- /var/lib/logrotate/status.
5.	--usage	–	Выводит краткую справку об использовании.

Всю необходимую информацию для осуществления ротации файлов журналов logrotate извлекает из группы конфигурационных файлов, заданных в

командной строке. Каждый файл конфигурации может установить глобальные опции и определить обрабатываемый файл журнала. Простой конфигурационный файл содержит примерно следующее:

```
# пример файла настроек logrotate
compress

/var/log/messages {
    rotate 5
    weekly
    postrotate
       /sbin/killall -HUP syslogd
    endscript
}
```

Строки, начинающиеся с «#» являются комментарием и не считываются модулем logrotate. Вторая строка задаёт глобальный параметр, определяющий что журналы после ротации будут сжаты.

Первые несколько строк устанавливают глобальные опции, в данном случае после обращения журналы сжимаются. Следующий раздел этого конфигурационного файла определяет обращение файла системных сообщений /var/log/messages. Журнал пройдёт через пятинедельный цикл обращений, прежде чем будет удалён. После обращения (циклического сдвига) журнала, но перед сжатием старого журнала, будет выполнена команда /sbin/killall -HUP syslogd.

В таблице 3.20 приведены директивы, которые могут быть включены в конфигурационный файл модуля logrotate.

Таблица 3.20 – Директивы конфигурационного файла logrotate

№	Директива	Используемая опция	Описание
1.	compress		Старые версии файлов журналов будут сжаты (по умолчанию gzip). См. также nocompress.
2.	compresscmd		Позволяет указать команду для сжатия файлов журналов. По умолчанию gzip. См. также compress.
3.	uncompresscmd		Директива позволяет указать команду для декомпрессии файлов журналов. По умолчанию gunzip.
4.	compressext		Если используется сжатие, определяет расширение сжатых файлов журналов. По умолчанию определяется из настроек команды сжатия.
5.	compressoptions		Программе сжатия может быть передана опция командной строки, если та их использует. Стандартно для gzip применяется "-9" (максимальное сжатие).
6.	copy		Создать копию файла журнала, не изменяя оригинал вовсе. Этот параметр может быть использован, например, для создания моментального снимка (среза) текущего файла журнала, или когда некоторой другой утилите требуется обрезать или подчистить файл. При использовании этого параметра не имеет силы директива create, так как старый файл журнала остаётся на своём месте.
7.	copytruncate		После создания копии, обрезать исходный файл журнала взамен перемещения старого файла журнала и создания нового. Это может найти применение в том случае, когда некоторой программе нельзя указать закрыть её журнал, и таким образом можно постоянно продолжать запись (добавление) в существующий файл журнала. Примите во внимание, что хотя между копированием файла и его обрезанием очень маленький промежуток времени, некоторая часть журналируемых данных может быть потеряна. При использовании этого параметра, не имеет силы директива create, так как старый файл журнала остаётся на своём месте.
8.	create	«режим» «владелец» «группа»	Непосредственно после обращения (перед выполнением скрипта postrotate) создать файл журнала (с тем же именем, что и только что сдвинутый журнал). Аргумент режим определяет режим доступа к файлу журнала в восьмеричном виде (единообразный с chmod(2)), владелец определяет имя пользователя, владеющего создаваемым файлом журнала, и группа определяет группу, к которой будет принадлежать файл журнала. Любые из этих атрибутов могут быть опущены; в этом случае вместо них для нового файла будут использованы атрибуты, имеющие те же значения, что и первоначальный файл журнала. Этот параметр может быть отключен использованием директивы nocreate.
9.	daily		Ежедневное обращение файлов журналов.
10.	delaycompress		Отложить сжатие предыдущего файла журнала до следующего циклического сдвига. Эта директива имеет силу только в комбинации с compress. Это может быть использовано в том случае, если некой

№	Директива	Используемая опция	Описание
			программе нельзя указать закрыть её файл журнала, и таким образом, можно некоторое время продолжать запись в предыдущий файл журнала.
11.	extension	расширение	Файлы журналов после обращение получат заданное расширение. Если используется сжатие, то после указанного расширения программа сжатия добавит ещё одно (обычно .gz).
12.	ifempty		Сдвигать файл журнала, даже если он пустой; это поведение можно изменить, применив директиву notifempty (по умолчанию активна ifempty).
13.	include	файл_или_каталог	Читает файл, переданный в качестве аргумента, так, как будто он включен построчно в тело конфигурационного файла с того места, где указана директива include. Если задан каталог, то содержащиеся в нём файлы будут прочитаны в алфавитном порядке, прежде чем переданы на обработку для включения. Файлы, не являющиеся обычными (такие как каталоги и именованные каналы), а также файлы, оканчивающиеся запрещёнными расширениями (определёнными параметром tabooext) -- будут проигнорированы. Директива include не может использоваться внутри определения файла журнала.
14.	mail	адрес	По окончании цикла обращения журнал будет отправлен электронной почтой на адрес. Если для отдельных журналов это не требуется, то можно применить директиву nomail.
15.	mailfirst		При использовании команды mail, посылать только что сдвинутый файл, а не закончивший цикл обращения файл журнала.
16.	maillast		При использовании команды mail, посылать не только что сдвинутый файл, а закончивший цикл обращения файл журнала (это задано по умолчанию).
17.	missingok		В случае отсутствия файла журнала перейти к обработке следующего, не выдавая сообщения об ошибке. См. также **nomissingok**.
18.	monthly		logrotate будет сдвигать файлы журналов раз в месяц (обычно первого числа каждого месяца).
19.	nocompress		Не сжимать с помощью gzip старые версии файлов журналов. См. также compress.
20.	nocopy		Не копировать исходный файл журнала и оставить его в штатном местоположении (это переопределяет параметр copy).
21.	nocopytruncate		После создания копии, не обрезать исходный файл журнала в его штатном местоположении (это переопределяет параметр copytruncate).
22.	nocreate		Не создавать новый файл журнала (это переопределяет директиву create).
23.	nodelaycompress		Не откладывать сжатие сдвинутого файла журнала до следующего цикла обращения (это переопределяет директиву delaycompress).
24.	nomail		Не отправлять старые файлы журналов почтой.

№	Директива	Используемая опция	Описание
25.	nomissingok		Если файл журнала не существует, выдать ошибку. Это установлено по умолчанию.
26.	noolddir		После обращения, журналы остаются в том же каталоге, где расположены текущие журналы (это переопределяет директиву olddir).
27.	nosharedscripts		Выполнять скрипты prerotate и postrotate для каждого обработанного журнала (это поведение задано по умолчанию, его можно переопределить параметром sharedscripts).
28.	notifempty		Не сдвигать журнал, если он пуст (это переопределяет параметр ifempty).
29.	olddir	директория	Переместить сдвинутые журналы в каталог. Заданный каталог должен размещаться на том же физическом устройстве, что и обращаемый файл журнала. При использовании этого параметра все старые версии журнала будут попадать в каталог. Этот параметр может быть переопределён параметром noolddir.
30.	postrotate/endscript		Строки с директивами, находящиеся между postrotate и endscript (которые сами должны располагаться на отдельных строках), будут выполнены после обращения журнала. Эти директивы могут находиться только внутри определения файла журнала. См. также prerotate.
31.	prerotate/endscript		Строки с директивами, находящиеся между prerotate и endscript (которые сами должны располагаться на отдельных строках), будут выполнены перед обращением журнала и только в случае, если журнал действительно будет сдвинут. Эти директивы могут находиться только внутри определения файла журнала. См. также postrotate.
32.	rotate	количество раз	Файл журнала будет сдвинут заданное количество раз, прежде чем будет удалён или послан по электронной почте на адрес, указанный в директиве mail. Если указано 0 раз, то старый журнал вместо обращения будет удалён.
33.	size	размер	Файлы журналов будут сдвинуты, когда станут больше указанного размера в байтах. Если размер оканчивается символом M, то размер интерпретируется в мегабайтах. Если использовать k, то можно задать размер в килобайтах. Таким образом, директивы size 100, size 100k, и size 100M являются верными.
34.	sharedscripts		Обычно скрипты prescript и postscript выполняются для каждого обрабатываемого журнала; это значит, что один и то же скрипт может выполняться несколько раз для одной конфигурационной записи, которая охватывает множество файлов (как в примере /var/log/news/*). Если параметр sharedscript указан, то скрипты будут выполнены только один раз, вне зависимости от количества журналов, подходящих под заданный шаблон. Однако если ни один из журналов, соответствующих шаблону, не требует обращения, то скрипты не будут выполнены вовсе. Этот параметр переопределяет директиву nosharedscripts.

№	Директива	Используемая опция	Описание
35.	start	число	Заданное число -- то, с которого начнётся счёт обращений. Например, если указать 0, после первого обращения (сдвига оригинального файла журнала) журналам будет присвоено расширение .0. Если указать 9, файлы журналов будут создаваться с расширением .9, пропустив 0-8. Файлы по-прежнему будут обращаться (сдвигаться) столько раз, сколько указано в директиве count.
36.	tabooext	[+] список_расширений	Изменяет текущий список запрещённых расширений (см. include). Если списку расширений предшествует знак +, то этот список прибавится к текущему, иначе заместит его. При первоначальном запуске список содержит следующие расширения: .rpmorig, .rpmsave, ,v, .swp, .rpmnew и ~.
37.	weekly		Файлы журналов будут сдвинуты, если текущий день недели меньше дня недели, в который произошло последнее обращение журнала, или если с тех пор прошло больше недели. Это почти то же самое, что и обращение журналов по понедельникам, но работает лучше, если logrotate не запускается каждую ночь.

3.13.7. Настройка централизованного аудита

Для настройки централизованного аудита на клиентской и серверной ОС, локальному администратору необходимо настроить пересылку событий безопасности на сервер безопасности, для этого необходимо привести файл /etc/rsyslog.d/rsyslog-send.conf к следующему виду:

```
module(load="omrelp")
if ( $programname == "dlogevent" ) then {
    action(
        type="omrelp"
        Target="[ip-адрес сервера безопасности]"
        Port="2514"
        queue.type="LinkedList"
        queue.size="10000"
        queue.filename="q_sendRule"
        queue.highwatermark="9000"
        queue.lowwatermark="50"
        queue.maxdiskspace="1g"
        queue.saveonshutdown="on"
        action.resumeRetryCount="-1"
        action.resumeInterval="3"
    )
}
```

, где `[ip-адрес сервера безопасности]` – адрес сервера безопасности на который будут пересылаться события безопасности.

После внесений изменений в файл перезагрузить сервисы rsyslog и dlogevent:

```
service rsyslog restart
service dlogevent restart
```

Настройка централизованного аудита для Менеджера ВМ осуществляется в соответствии с п 3.4.2.7.

Настройка централизованного аудита для Средства управления доменными пользователями осуществляется в соответствии с п 3.4.4.7.

3.14.Настройка подсистемы самотестирования

Управление перечнем запускаемых тестов обеспечивается за счет добавления/удаления соответствующей секции в конфигурационный файл

/etc/sintez/selftest.conf. Конфигурационный файл состоит из секции `[MAIN]`, а также одной или нескольких секций тестов.

Конфигурационный файл подсистемы самотестирования в общем виде выглядит следующим образом:

```
[AUDIT]
 base_url=/etc/sintez/tests/audit_test.py
 importance_lvl=INFO
 enabled=1

 [MAIN]
 importance_lvl=WARN
 mode=Permissive
 allowed_users = protadmin_l,(protadmin_d),root
 delay = 30
 add_restrict=/executive01,/executive02
```

, где:

– поле base_url определяет полный путь до файла скрипта.

– поле enabled определяет включен тест: 1, либо нет: 0. По умолчанию, если не задан — выключен.

– критичность теста importance_lvl — выставляется администратором. Если уровень критичности не задан, то по-умолчанию выставляется уровень INFO.

– секция MAIN в конфигурационном файле является управляющей. Уровень критичности теста не может быть ниже MAIN. Если же критичность выше, чем в MAIN то используется уровень критичности самого теста. В случае отсутствия критичности в секции MAIN, по умолчанию принимается значение MAIN: INFO.

– поле mode определяет режим запуска тестирования. Всего возможно два режима: Permissive (принимается по умолчанию): не прохождение теста не приводит к ограничениям, несмотря на остальные параметры. В противном случае - Enforcing. Только для MAIN.

– поле add_restrict позволяет подключать дополнительные исполняемые файлы, которые будут запущены в случае не прохождения теста. Указывается полное имя файла, включая путь и расширение. add_restrict может быть указан либо для конкретного теста, либо для всех — в секции MAIN.

– поле allowed_users: пользователи, которые будут сохранять доступ к системе в случае блокировки (по умолчанию: root, protadm_l, protadm_d). Только для MAIN.

– поле delay: время (в сек.) блокировки доступа в случае не прохождения тестов уровня WARN. Не может быть менее 10с и более 180с. По умолчанию: 30 с. Только для MAIN.

Комментирование строк в конфигурационном файле осуществляется символом “#”, т.е. строка идущая за символом “#” считается закомментированной.

Секция **[MAIN]** обязательная и соответствует глобальной настройке системы самотестирования. В этой секции задается глобальный уровень критичности системы самотестирования который может принимать следующие значения: INFO, WARN, CRITICAL.

При этом уровни критичности представленные в конфигурационном файле соответствуют накладываемым на систему ограничениям, где:

- INFO – соответствует отсутствию каких-либо ограничений.
- WARN – отключение сети и временный скринсейвер.
- CRITICAL - отключение сети, скринсейвер и запрет авторизации;

Помимо задания глобального уровня критичности в секции **[MAIN]** возможно объявить, в качестве переменных для параметра add_restrict, внешние модули которые будут запущены в процессе самотестирования в случае если тест завершиться неуспешно.

`[имя теста]` и `[имя секции]` - наименования теста и секции соответственно, данные параметры используются модулем самотестирования при генерации событий безопасности;

`[путь до теста]` – указывает расположение до исполняемого файла теста который будет запускаться модулем самотестирования;

`[уровень критичности теста]` – задает значение

`[статус теста]` – может принимать значение включен - “1” или выключен - “0”;

Для изменения расписания проведения самотестирования необходимо любым текстовым редактором отредактировать конфигурационный файл /etc/cron.d/security_self_test_timetable. Настройка расписания осуществляется в соответствии с пунктом 3.10.1 данной инструкции.

При установке пакета pszi_self-test во всех модулях его конфигурационного файла "/etc/sintez/selftest.conf" enabled выставлен на 0, а importance_lvl выставлен на INFO (INFO соответствует отсутствию реакции на возникающие при тестировании ошибки и только записывает информацию о данных событиях в лог).

Если параметр для переменной importance_lvl не задан, то выставляется параметр importance_lvl заданный в разделе [MAIN], если и он не установлен, то выставляется значение по-умолчанию соответствующее режиму WARN.

При этом следует иметь ввиду, что importance_lvl в разделе [MAIN] имеет приоритет перед importance_lvl выставленным в разделе какого-либо из модулей. т.е. если в [MAIN] importance_lvl установлен на уровень выше уровня, выставленного в каком-либо модуле, то информация по данному модулю записывается только в лог-файл и не ведет к возможному ограничению системы, если же параметр importance_lvl раздела [MAIN] ниже или соответствует importance_lvl из некоторого раздела, то в случае возникновения ошибки в данном модуле машина будет заблокирована в соответствии с выставленным в данном модуле уровне (importance_lvl). Порядок занчимости следующий INFO, WARN, CRITICAL, где INFO – минимальный уровень важности, а CRITICAL – максимальный.

3.15. Управление подсистемой ограничения программной среды

КП «ЗОС «СинтезМ» обеспечивает контроль установки и запуска компонентов программного обеспечения в соответствии с установленными правилами за счет реализации механизма замкнутой программной среды.

Реализации механизма замкнутой программной среды в КП «ЗОС «СинтезМ» основана на применении технологий IMA и EVM.

Механизмы IMA (Integrity Measurement Architecture, Архитектура Измерения Целостности) и EVM (Extended Verification Module, Расширенный Модуль Проверки) обеспечивают проверку целостности библиотек и исполняемых файлов и гарантируют подлинность подписанных файлов с момента включения механизмов. Во время запуска файла происходит проверка его подписи и, в случае несовпадения или отсутствия подписи, – отказ в доступе. Данная проверка происходит и во время старта операционной системы, что может привести к остановке загрузки ОС, в случае отсутствия правильной подписи файлов, участвующих в запуске ОС. Для настройки правил выбора файлов, попадающих под проверку, используется специальный файл с политиками, расположенный в /etc/sysconfig/ima-policy.

Примечание: Файл «/etc/sysconfig/ima-policy» создается только после включения механизма IMA/EVM (см. п 3.15.1 Включение IMA/EVM в режиме хэш подписей). До включения механизма, редактирования политики IMA возможно произвести за счет редактирования файла

IMA занимается вычислением значения хэш от содержимого файла. EVM вычисляет хэш от расширенных атрибутов файла, а также дополнительных характеристик, например номер иноды и UUID. Эти хэши записываются в дополнительные атрибуты файла: security.ima и security.evm соответственно. Таким образом EVM позволяет защитить атрибут security.ima от изменений, в случае изменения содержимого файла. Для вычисления хэш значения, IMA использует алгоритм SHA-1, а EVM применяет HMAC-SHA1. Таким образом, для использования EVM необходим симметричный ключ шифрования, загружаемый в ядро ОС.

Существует и другой режим работы IMA/EVM, когда подпись файлов осуществляется не значениями хэш, а сигнатурами. Для этого используется ассиметричное шифрование, при котором приватным ключом вычисляется от хэш значения содержимого файла сигнатура IMA, записываемая в соответствующий атрибут, а открытый ключ загружается в ядро ОС и используется для расшифровки сигнатуры.

Настройка IMA/EVM в КП «ЗОС «СинтезМ» доступна пользователю с ролью локального администратора.

Применение IMA и EVM обеспечивает контроль над программами в КП «ЗОС «СинтезМ», проверяя некоторые виды ресурсов перед их непосредственным выполнением. Рассматриваемые ресурсы представляют собой различные библиотеки, конфигурационные файлы, исполняемые файлы, архивы, скрипты и пр.

IMA осуществляет подсчет контрольных сумм файлов и различных программ до их загрузки в систему, а также поддерживает проверку контрольных сумм файлов, заданных политикой. EVM обеспечивает защиту файлов от атак, направленных на нарушение их целостности.

IMA проверяет файлы, в соответствии с политикой загружаемой при старте ОС. Файл политик находится в /etc/sysconfig/ima-policy.

Для функционирования ОС в конфигурации «Операционная система» и конфигурации «Среда виртуализации» необходимо отредактировать политику IMA входящую в набор базовых конфигураций и привести ее к следующему виду:

```
dont_measure fsmagic=0x9fa0
dont_appraise fsmagic=0x9fa0
dont_measure fsmagic=0x62656572
dont_appraise fsmagic=0x62656572
dont_measure fsmagic=0x64626720
dont_appraise fsmagic=0x64626720
dont_measure fsmagic=0x01021994
dont_appraise fsmagic=0x01021994
dont_appraise fsmagic=0x858458f6
dont_measure fsmagic=0x1cd1
dont_appraise fsmagic=0x1cd1
dont_measure fsmagic=0x42494e4d
dont_appraise fsmagic=0x42494e4d
dont_measure fsmagic=0x73636673
dont_appraise fsmagic=0x73636673
dont_measure fsmagic=0xf97cff8c
dont_appraise fsmagic=0xf97cff8c
dont_measure fsmagic=0x27e0eb
dont_appraise fsmagic=0x27e0eb
dont_measure fsmagic=0x6e736673
dont_appraise fsmagic=0x6e736673
```

```
measure func=BPRM_CHECK mask=MAY_EXEC fowner=0
appraise func=BPRM_CHECK mask=MAY_EXEC fowner=0
```

Политики IMA представляют собой текстовый файл определенного формата. Файл содержит следующие правила: dont_measure – для отключения подсчета хэш значения; dont_appraise – для отключения проверки подписи; measure и appraise – соответственно, для подсчета хэш значения и включения механизма IMA. Отключение подсчета и проверки необходимо для исключения работы подсистемы с псевдо-файловыми системами, например /proc. Данные правила записываются вместе с параметрами:

- fsmagic – указывает тип файловой системы, на которой расположен файл.
- func – указывает файловые операции, применяемые к файлу.
- fowner – указывает UID владельца файла.
- uid – процесс, получающий доступ к файлу, должен быть запущен указанным UID.

Возможные значения параметра func:

- BPRM_CHECK – файл является исполняемым.
- MMAP_CHECK – файл загружается в память процесса.
- FILE_CHECK – файл может быть открыт.
- MODULE_CHECK – файл загружается как модуль ядра.
- FIRMWARE_CHECK – файл загружается в ядро как прошивка.

3.15.1. Включение IMA/EVM в режиме хэш подписей

Для управления IMA/EVM используются скрипты install.sh и start.sh.

Скрипт install.sh обеспечивает включение механизма замкнутой программной среды за счет изменения системных настроек, создания ключей для подписи, загрузки файла политики, обновления образа initramfs.

Скрипт start.sh обеспечивает подпись файлов и перевод механизмов IMA/EVM в рабочий режим.

Настройка IMA/EVM осуществляется в следующем порядке:

1) Выполнение скрипта install.sh.

Для этого пользователю необходимо перейти в папку /opt/ima_evm_scripts/ и выполнить команду:

```
# ./install.sh
```

Скрипт выполняет настройку системы и подготавливает систему для запуска в режиме "fix".

2) Перезагрузка

Для применения внесенных в конфигурацию системы изменений необходимо произвести перезагрузку. Перезагрузка выполняется командой reboot

3) Выполнение скрипта start.sh.

Для этого пользователю после перезагрузки необходимо перейти в папку /opt/ima_evm_scripts и выполнить команду:

```
# ./start.sh -a
```

Скрипт подписывает файлы и подготавливает систему для запуска в режиме "enforce". Запуск скрипта `./start.sh` при первоначальном развертывании необходимо осуществлять с опцией «-a» в рамках которой осуществляет подпись всех исполняемых файлов, а также файлов, содержащих sticky bit, хеш значениям.

Помимо «-a», пользователь также может запустить скрипт со следующими опциями:

1. «-l» – подпись файлов из списка files_to_sign хэш значениями;

2. «-f» – конфигурирование системы для запуска в режиме «fix»;

3. «-h» – вывод справочной информации по работе скрипта с различными опциями.

Ниже приведен фрагмент процесса работы скрипта:

```
[root@ruovirt-ipa1 ima_evm_scripts]# ./start.sh -a
2018-08-02 14:34:00 Start sign all files
2018-08-02 14:34:01 Searching for files to sign
find: ‘/proc/11303/task/11303/fdinfo/5’: No such file or directory
find: ‘/proc/11303/fdinfo/6’: No such file or directory
2018-08-02 14:34:20 Signing all files...
2018-08-02 14:34:20 DEBUG: Signing file /boot/vmlinuz-3.10.0-
863.el7.x86_64
2018-08-02 14:34:20 DEBUG: Signing file
```

```
/boot/efi/EFI/sintez/fonts/unicode.pf2
2018-08-02 14:34:20 DEBUG: Signing file /boot/efi/EFI/sintez/gcdx64.efi
2018-08-02 14:34:20 DEBUG: Signing file /boot/efi/EFI/sintez/grubx64.efi
2018-08-02 14:34:20 DEBUG: Signing file /boot/vmlinuz-0-rescue-
7dfa7aba0c113f47a1ea0a8e37bc89b2
2018-08-02 14:34:20 DEBUG: Signing file /run/dlogevent.pid
2018-08-02 14:34:20 DEBUG: Signing file
/run/log/journal/7dfa7aba0c113f47a1ea0a8e37bc89b2/system.journal
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/certs/make-dummy-
cert
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/certs/renew-dummy-
cert
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/misc/CA
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/misc/c_hash
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/misc/c_info
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/misc/c_issuer
2018-08-02 14:34:20 DEBUG: Signing file /etc/pki/tls/misc/c_name
…
```

4) Перезагрузка ВМ

3.15.2. Проверка режима работы механизмов IMA/EVM

Для корректного включения механизмов IMA/EVM необходимо правильно создать файл политик и подписать файлы, подлежащие проверке. Для подписи файлов, ОС должна быть загружена в режиме "fix", что требует передачи правильных параметров в командную строку ядра: "`ima_tcb ima_appraise_tcb evm=fix ima_appraise=fix evmx509=/etc/keys/local_x509.der evmkey=/etc/keys/evm-user.blob`". После этого файлы можно подписать следующей командой: "evmctl ima_hash <путь_к_файлу>". Для загрузки ОС в режиме "enforce" достаточно убрать из параметров командной строки ядра "evm=fix ima_appraise=fix".

Параметры командной строки доступны для просмотра в режиме EFI в файле `/boot/efi/EFI/sintez/grub.cfg, в режиме legacy - /boot/grub2/grub.cfg`. Для того, чтобы отредактировать параметры, пользователю необходимо открыть файл `/etc/default/grub` с помощью редактора vim. Далее для того, чтобы изменения вступили в силу, необходимо выполнить одну из следующих команд:

1

. 2. `grub2-mkconfig -o /boot/grub2/grub.cfg в режиме legacy`.

g

r

Для быстрой проверки состояния машины, пользователь может воспользоваться следующими командами:

1. `cat /proc/cmdline`

Данная команда предоставит параметры командной строки ядра в текущей загрузке. В результате выполнения в консоли появится текст, примерное содержание которого представлено ниже:

«BOOT_IMAGE=/vmlinuz-3.10.0-863.el7.x86_64 root=/dev/mapper/sintez-roo ro crashkernel=auto rd.lvm.lv=sintez/root rd.lvm.lv=sintez/swap ima_tcb ima_appraise_tcb evmkey=/etc/keys/evm-user.blob »

2. `cat /sys/kernel/security/evm`

Команда предоставит одно из двух значений: 1 в случае, если EVM функционирует, 0 – в противоположном случае. Ниже представлен результат выполнения команды проверки:

```
[root@ruovirt-evm ~]# cat /sys/kernel/security/evm
1[root@ruovirt-evm ~]#
```

3. keyctl show

Данная команда отображает загруженные ключи kmk-user и evm-key. Примерный результат выполнения команды представлен на скриншоте ниже:

```
[root@ruovirt-evm ~]# keyctl show
Session Keyring
 904601620 --alswrv      0     0  keyring: _ses
 966418820 --alswrv      0 65534   \_ keyring: _uid.0
 404766947 --alswrv      0     0       \_ user: kmk-user
 792571727 --alswrv      0     0       \_ encrypted: evm-key
```

3.15.3. Порядок обновления политик IMA и переподписи исполняемых файлов

Для редактирования политик IMA (например, добавления или удаления правил) локальному администратору необходимо произвести изменения в конфигурационном файле политик, перевести работу IMA/EVM в режим «fix» для обновления подписей, при необходимости переподписать исполняемы файлы и библиотеки, после чего перевести работу IMA/EVM в режим «enforce».

Переподпись исполняемых файлов необходимо осуществлять при установке программного обеспечения или его обновлении.

Обновление политик IMA и переподпись исполняемых файлов осуществляется в следующем порядке:

1) Для редактирования файла политик необходимо открыть файл политики при помощи тестового редактора vim: `# vim /etc/sysconfig/ima-policy`, и внести соответствующие изменения.

2) Для перевода IMA/EVM в режим «fix» необходимо перейти в папку /opt/ima_evm_scripts и выполнить команду:

```
# ./start.sh -f
```

3) Перезагрузка

Для применения внесенных в конфигурацию системы изменений необходимо произвести перезагрузку. Перезагрузка выполняется командой reboot

4) Переподпись исполняемых файлов и библиотек

Для переподписи после перезагрузки необходимо перейти в папку /opt/ima_evm_scripts и выполнить команду:

```
# ./start.sh -a
```

5) Перезагрузка ВМ

3.15.4. Утилиты для работы с IMA/EVM

* evm_create_keys.sh - создает ключи для подсистемы контроля целостности.

* evm_create_symkey.sh - создает симметричный ключ для подписи EVM.

* sign.sh - устанавливает флаг защиты от до записи и подписывает файлы, указанные в files_to_sign. Файлы из списка files_to_unsign подписываться не будут. Символьные ссылки игнорируются.

* grub-enforce-mode.sh - конфигурирует систему для загрузки в режиме "enforce".

Включение режима произойдет после перезагрузки.

* grub-fix-mode.sh - конфигурирует систему для загрузки в режиме "fix". Включение режима произойдет после перезагрузки.

* files_to_sign - список файлов, которые будут подписаны IMA/EVM. При необходимости подписать новые файлы, этот список нужно расширить, добавив путь к файлу или к директории, содержащей файлы для подписи.

* files_to_unsign - список файлов, остающихся без подписи IMA/EVM. Запуск этих файлов, после загрузки в режиме "enforce", будет невозможен.

* install.sh - выполняет настройку системы и подготавливает запуск режима "fix".

* start.sh - подписывает файлы и подготавливает запуск системы в режиме "enforce".

3.15.5. Управление автозагрузкой

Управление перечнем компонентов программного обеспечения, разрешенных для автоматического запуска при загрузке операционной системы осуществляется за счет вызова управляющей утилиты systemctl или chkconfig. При этом chkconfig применяется для обеспечения обратной совместимости с программным обеспечением старых версий запускаемых через SysV.

Задание перечня компонентов программного обеспечения, разрешенных для автоматического запуска при загрузке операционной системы, обеспечивается за счет применения в КП «ЗОС «СинтезМ»» systemd. Systemd – менеджер системы и служб, он оперирует специальными файлами конфигурации, которые называются юнитами. Каждый юнит отвечает за одну службу либо точку монтирования, либо подключаемое устройство.

Доступные файлы юнитов можно посмотреть в директориях /usr/lib/systemd/system/ и /etc/systemd/system/ (второй каталог имеет приоритет). Просмотр списка установленных файлов юнитов осуществляется командой: systemctl list-unit-files. Просмотр списка компонентов, поставленных в автозагрузку, осуществляется командой systemctl list-unit-files |grep enabled.

Управление перечнем компонентов программного обеспечения, разрешенных для автоматического запуска при загрузке операционной системы, осуществляется за счет вызова управляющей утилиты systemctl.

```
# systemctl [параметр] [юнит]
```

, где параметр может принимать значения в соответствии с таблицей 3.21.

Таблица 3.21 – Перечень параметров управляющей утилиты systemctl

№	Параметр	Описание
1	enable	Включение службы в автозагрузку при старте ОС
2	disable	Исключение службы из автозагрузки при старте ОС

3.16.Управление подсистемой фильтрации сетевого потока

По умолчанию после установки ОС модули подсистемы фильтрации сетевого потока неактивны.

Для включения подсистемы фильтрации сетевого потока необходимо запустить службы iptables, ebtables и добавить их в автозагрузку при страте системы.

Добавление в автозагрузку осуществляется командами:

```
# systemctl enable iptables.service
# systemctl enable ebtables.service
```

Запуск служб подсистемы фильтрации сетевого потока осуществляется командами:

```
# systemctl start iptables.service
# systemctl start ebtables.service
```

Подсистема фильтрации сетевого потока состоит из модулей пространства ядра ip_tables, ebtables и утилит пространства пользователя с аналогичными названиями iptables, ebtables.

Для просмотра списка загруженных правил фильтрация выполнить команды:

```
# iptables –L
# ebtables –L
```

Управление правилами фильтрации ip_tables осуществляется утилитой iptables.

Пример команды управления цепочками/правилами: iptables [-t таблица] [опции] [действие] [параметр].

Перечень цепочек:

– INPUT – цепочка, обрабатывающая входящие пакеты;

– PREROUTING – цепочка, обрабатывающая входящие пакеты;

– FORWARD – цепочка, обрабатывающая транзитные пакеты;

– OUTPUT – цепочка, обрабатывающая исходящие пакеты;

– POSTROUTING – цепочка, обрабатывающая исходящие пакеты.

Цепочки организованы в четырех таблицах. Эти таблицы выполняют, содержащиеся в них, правила из цепочки, соответствующей месту, где был совершен перехват сетевого потока. Перечень таблиц:

– raw содержит следующий перечень цепочек:

• PREROUTING – в эту цепочку входящие пакеты попадают раньше, чем в любую другую из цепочек iptables, и до обработки их системой определения состояния;

• OUTPUT – аналогично для пакетов, сгенерированных самим хостом.

Допустимые действия в таблице raw:

• RAWDNAT – выполняется проброс адресов и портов без учета состояния соединения.

Пример использования RAWDNAT действия:

```
iptables -t raw -A PREROUTING -i eth0 -d 212.201.100.135 -j  RAWDNAT --
to-destination 199.181.132.250
iptables -t rawpost -A POSTROUTING -o eth0 -s 199.181.132.250 -j RAWSNAT
--to-source 212.201.100.13
```

– mangle содержит следующий перечень цепочек:

• PREROUTING – позволяет модифицировать пакет до принятия решения о маршрутизации;

• INPUT – позволяет модифицировать пакет, предназначенный самому хосту;

• FORWARD – цепочка, позволяющая модифицировать транзитные пакеты;

• OUTPUT – позволяет модифицировать пакеты, исходящие от самого хоста;

- POSTROUTING – дает возможность модифицировать все исходящие пакеты, как сгенерированные самим хостом, так и транзитные.
- Допустимые действия в таблице mangle:
- TOS – изменяет поле TOS (тип сервиса) данного пакета.
- DSCP – изменяет поле DSCP (масштабируемый механизм классификации, управления трафиком и обеспечения качества обслуживания) в заголовке пакета.
- TTL – изменяет поле TTL (время жизни пакетов) данного пакета.

Пример использования TTL действия:

```
iptables -t mangle -I PREROUTING -j TTL --ttl-inc 1
```

Данная команда делает шлюз невидимым для многих служебных программ, предназначенных для определения маршрута следования данных в сетях TCP/IP:

- MARK – устанавливает или изменяет маркировку пакета.
- TCPMSS – устанавливает максимальный размер TCP-сегмента.
- TCPOPTSTRIP – выполняет удаление заданных TCP-опций из заголовка TCP-пакета.

Пример использования TCPOPTSTRIP:

```
iptables -t mangle -A POSTROUTING -p tcp -j TCPOPTSTRIP --strip-options
timestamp
```

Данная команда обеспечивает удаление штампов времени:

- TPROXY – реализует механизм прозрачного проксирования.
- – nat содержит следующий перечень цепочек:
- PREROUTING – в эту цепочку пакеты попадают до принятия решения о маршрутизации. Именно на данном этапе нужно проводить операции проброса (DNAT, REDIRECT, NETMAP);
- OUTPUT – через эту цепочку проходят пакеты, сгенерированные процессами самого хоста;
- POSTROUTING – через эту цепочку проходят все исходящие пакеты, целесообразно проводить операции маскарадинга (тип трансляции при которой адрес

отправителя подставляется динамически, в зависимости от назначенного интерфейсу адреса) (SNAT и MASQUERADE).

Допустимые действия в таблице nat:

- DNAT – подменяет адрес назначения для входящих пакетов, позволяя «пробрасывать» адреса или отдельные порты внутрь локальной сети.
- REDIRECT – подменяет номер порта в TCP- или UDP-пакете, а также подменяет адрес назначения на свой собственный.
- NETMAP – позволяет «пробросить» целую сеть.
- MIRROR – меняет местами адрес источника и назначения и высылает пакет обратно.
- – filter содержит следующий перечень цепочек:
- INPUT – эта цепочка обрабатывает трафик, поступающий непосредственно самому хосту;
- FORWARD – позволяет фильтровать транзитный трафик;
- OUTPUT – эта цепочка позволяет фильтровать трафик, исходящий от самого хоста.

Допустимые действия в таблице filter:

- ACCEPT – пропуск пакета.
- REJECT – заблокировать пакет и сообщить его источнику об отказе.
- DROP – заблокировать пакет, не сообщая источнику об отказе.
- TARPIT – задержка TCP-соединения.

Пример использования действия TARPIT:

– `iptables -I INPUT -p tcp --dport 25 -j TARPIT`, добавление правила блокирования порта, также необходимо добавить в таблицу raw соответствующее правило:

```
iptables -t raw -I PREROUTING -p tcp --dport 25 -j NOTRACK
```

Перечень опций представлен в таблице 3.22

Таблица 3.22 – Перечень опций

№	Опция	Описание	Примечание
1.	-A	Добавить одно или несколько правил в конец указанной цепочки	Если имя источника и/или назначения соответствует нескольким адресам, правило будет добавлено для всех возможных комбинаций адресов
2.	-D	Удалить одно или несколько правил из указанной цепочки	Существует две версии этой команды: правило может быть указано через его номер в цепочке (счёт первого правила начинается с 1) или через соответствие определения правила
3.	-I [номер правила]	В указанной цепочке вставить одно или более правил в позицию, заданную номером	Если указан номер 1 или не указан, правило или правила будут вставлены в начало цепочки
4.	-R	Заменить правило в указанной цепочке	Если имена источника и/или назначения соответствуют нескольким адресам, команда не будет выполнена с сообщением об ошибке
5.	-L	Показать все правила в выбранной цепочке	Если цепочка не указана, то команда применяется ко всем цепочкам
6.	-F	Сбросить выбранную цепочку (все цепочки в таблице, если ни одна не указана)	Это эквивалентно удалению по одному всех правил
7.	-Z	Обнулить счётчики количества пакетов и байтов во всех или указанной цепочке	Можно также указать -L, чтобы отобразить значения счётчиков непосредственно перед их обнулением
8.	-N	Создать новую, определённую администратором цепочку с заданным именем	В момент создания цепочки не должно быть уже существующих целей с указанным именем
9.	-X	Удалить цепочку, определённую администратором	При этом не должно быть ссылок на удаляемую цепочку. Если такие ссылки есть, необходимо сначала удалить или изменить правила, ссылающиеся на удаляемую цепочку. Если цепочка не указана, из таблицы будут удалены все цепочки кроме встроенных
10.	-E	Переименовать цепочку, определённую администратором	

Таблица 3.23 – Перечень параметров

№	Параметр	Описание	Примечание
1.	-p [!] [протокол]	Сетевой протокол применяемого правила или проверяемого пакета	Допустимые значения: tcp, udp, icmp, all. Также можно указывать

№	Параметр	Описание	Примечание
			в виде числа. Названия протоколов также можно брать из файла /etc/protocols. Знак «!» перед названием протокола инвертирует результат теста. Число 0 эквивалентно «all». Значение «all» соответствует всем протоколам и используется если данный параметр опущен
2.	-s [!] [адрес/маска]	Адрес источника	Адресом может быть сетевое имя, имя хоста, диапазон IP-адресов или одиночный IP-адрес
3.	-d [!] [адрес/маска]	адрес цели	Синтаксис аналогичен синтаксису параметра –s
4.	-j [назначение]	определение цели правила	
5.	-g [цепочка]	продолжить обработку в цепочке, определенной администратором	В отличие от опции –j (--jump), после возврата из вызванной цепочки, применение правил будет продолжено не в текущей цепочке, а в той цепочке, которая вызвала текущую через --jump
6.	-i [!] [наименование]	указывается наименование интерфейса, через который должен быть получен обрабатываемый пакет	только для пакетов, входящих в цепочки INPUT, FORWARD и PREROUTING
7.	-o [!] [наименование]	указывается наименование интерфейса, через который отправляется обрабатываемый пакет	только для пакетов, входящих в цепочки FORWARD, OUTPUT и POSTROUTING
8.	[!] -f	правило применяться ко второму и последующим фрагментам фрагментированного пакета	Так как у фрагмента невозможно определить номер порта источника или цели, равно как и тип ICMP, такие пакеты не обрабатываются правилами, содержащими номера портов или тип ICMP. Если перед флагом -f указан «!», то правило будет применяться только к первому фрагменту или к нефрагментированному пакету
9.	-c	инициализация в правиле счётчиков пакетов и байтов	при выполнении операций INSERT, APPEND, REPLACE

Встроенные действия:

- accept, разрешение на подключение;
- reject, запрет на подключение;
- drop, пакеты удаляются, информация не передается;

– mark, маркировка пакетов.

Пример команды управления правилами iptables:

1. `iptables -A INPUT --source 192.168.1.1 --jump ACCEPT`
`iptables -A INPUT --jump other_chain`

Эти команды добавляют к концу цепочки INPUT следующие правила: пропустить пакеты из 192.168.1.1, а всё, что останется – отправить на анализ в цепочку other_chain.

2. Добавить правило сетевой фильтрации:

```
iptables -I INPUT -s 202.54.1.2 -j DROP
```

3. Блокирование только входящего соединения:

```
iptables -A INPUT -m state --state NEW,ESTABLISHED -j ACCEPT
```

4. Блокировка конкретного IP-адреса:

```
iptables -A INPUT -s 1.2.3.4 -j DROP
iptables -A INPUT -s 192.168.0.0/24 -j DROP
```

5. Блокирование исходящего соединения:

```
iptables -A OUTPUT -p tcp -d [ip-адрес,порт/домен] -j DROP
```

6. Журналирование перемещения пакетов, сброс:

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF
A: "
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

7. Запрет, разрешения на трафик с определенных MAC-адресов:

```
iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source
00:0F:EA:91:04:07 -j ACCEPT
```

8. Заперт, разрешение ICMP Ping запросы:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```

9. Открыть диапазон портов

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport
7000:7010 -j ACCEPT
```

10. Открыть диапазон адресов

```
iptables -A INPUT -p tcp --destination-port 80 -m iprange --src-range 192.168.1.100-192.168.1.200 -j ACCEPT
iptables -t nat -A POSTROUTING -j SNAT --to-source 192.168.1.20-192.168.1.25
```

Сохранение правил осуществляется командой /sbin/service iptables save, что приводит к запуску утилиты iptables-save и сохранению правил в файл /etc/sysconfig/iptables. При этом если файл с правилами существовал, то старая версия сохраняется в /etc/sysconfig/iptables.save. Во время старта системы правила, содержащиеся в /etc/sysconfig/iptables, загружаются в модуль с помощью утилиты iptables-restore.

Помимо команд управления, правила iptables можно задавать в конфигурационном файле /etc/sysconfig/iptables.

Формат правил:

- A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
- A INPUT -p icmp -j ACCEPT
- A INPUT -i lo -j ACCEPT
- A INPUT -i eth0 -j ACCEPT
- A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
- A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
- A FORWARD -p icmp -j ACCEPT
- A FORWARD -i lo -j ACCEPT
- A FORWARD -i eth0 -j ACCEPT
- A INPUT -j REJECT --reject-with icmp-host-prohibited
- A FORWARD -j REJECT --reject-with icmp-host-prohibited

Управление правилами фильтрации ebtables осуществляется утилитой соответственно.

Модуль ebtables содержит три таблицы: broute, содержащую цепочку BROUTING; nat, содержащую цепочки PREROUTING, OUTPUT, POSTROUTING; filter, содержащую цепочки FORWARD, INPUT, OUTPUT.

Пример команды управления цепочками/правилами: ebtables [-t таблица] [опции] [действие] [параметр].

Перечень опций представлен в таблице 3.24.

Таблица 3.24 – Перечень опций

№	Опция	Описание	Примечание
1.	-A	Добавить одно или несколько правил в конец указанной цепочки	Если имя источника и/или назначения соответствует нескольким адресам, правило будет добавлено для всех возможных комбинаций адресов
2.	-D	Удалить одно или несколько правил из указанной цепочки	Существует две версии этой команды: правило может быть указано через его номер в цепочке (счёт первого правила начинается с 1) или через соответствие определения правила
3.	-I [номер правила]	В указанной цепочке вставить одно или более правил в позицию, заданную номером	Если указан номер 1 или не указан, правило или правила будут вставлены в начало цепочки
4.	-R	Заменить правило в указанной цепочке	Если имена источника и/или назначения соответствуют нескольким адресам, команда не будет выполнена с сообщением об ошибке
5.	-L	Показать все правила в выбранной цепочке	Если цепочка не указана, то команда применяется ко всем цепочкам
6.	-F	Сбросить выбранную цепочку (все цепочки в таблице, если ни одна не указана)	Это эквивалентно удалению по одному всех правил
7.	-Z	Обнулить счётчики количества пакетов и байтов во всех или указанной цепочке	Можно также указать -L, чтобы отобразить значения счётчиков непосредственно перед их обнулением
8.	-N	Создать новую, определённую администратором цепочку с заданным именем	В момент создания цепочки не должно быть уже существующих целей с указанным именем
9.	-X	Удалить цепочку, определённую администратором	При этом не должно быть ссылок на удаляемую цепочку. Если такие ссылки есть, необходимо сначала удалить или изменить правила, ссылающиеся на удаляемую цепочку. Если цепочка не указана, из таблицы будут удалены все цепочки кроме встроенных
10.	-E	Переименовать цепочку, определённую администратором	

Перечень параметров представлен в таблице 3.25

Таблица 3.25 – Перечень параметров

№	Параметр	Описание	Примечание
1.	-p [!] [протокол]	Сетевой протокол применяемого правила или проверяемого пакета	
2.	-i [!] [наименование]	Указывается наименование интерфейса, через который должен быть получен обрабатываемый пакет	Для пакетов, входящих во все цепочки
3.	-o [!] [наименование]	Указывается наименование интерфейса (порта), через который отправляется обрабатываемый пакет	Только для пакетов, входящих в цепочки FORWARD, OUTPUT и POSTROUTING
4.	-s [!] [адрес/маска]	Указывается MAC-адрес источника	Маска и адрес записывается как шесть шестнадцатеричных чисел, разделенных двоеточиями. Пример: Unicast = 00: 00: 00: 00: 00: 00/01: 00: 00: 00: 00: 00 Broadcast = ff: ff: ff: ff: ff: ff / ff: ff: ff: ff: ff: ff
5.	-d [!] [адрес/маска]	MAC-адрес цели	Синтаксис аналогичен синтаксису параметра –s
6.	--logical-in [!] [наименование]	Интерфейс (логический интерфейс) моста, через который принимаются пакеты	Используется для всех цепочек
7.	--logical-out [!] [наименование]	Интерфейс (логический интерфейс) моста, через который отправляются пакеты	Используется для цепочек FORWARD, OUTPUT и POSTROUTING

Пример команды управления правилами ebtables:

```
ebtables -A OUTPUT -d 00:1a:4a:16:01:07 -j DROP
```

Эта команда добавляют к концу цепочки OUTPUT следующие правила: запрет на исходящий трафик и удаление пакетов.

Для сохранения правил фильтрации ввести команду:

```
/usr/libexec/ebtables save
```

3.17.Управление средой виртуализации (Менеджер ВМ)

Управление средой виртуализации (Менеджер ВМ) осуществляется пользователем обладающим ролью системного администратора. Управление

проводиться через портал администрирования средства управления средой виртуализации предварительно авторизовавшись пользователем с ролью системного администратора. Для этого необходимо в адресной строке браузера ввести адрес Сервера управления средой виртуализации, после чего в открывшемся окне (Рисунок 3.68) ввести логин и пароль.

3.17.1. Создание сетей, интерфейсов

Для настройки сетевых мостов нужно нажать пункт меню Network на панели навигации слева, выбрать раздел «Networks».

Сетевой мост (bridge) – сетевое устройство, предназначенное для объединения сегментов подсети.

В появившейся окне (рисунок 3.86) системному администратору доступны следующие действия:

- новая сеть «Новая»;
- импорт сети «Импортировать»;
- редактирование сети «Изменить»;
- удаление сети «Удалить»;
- редактирование конфигурации сети.

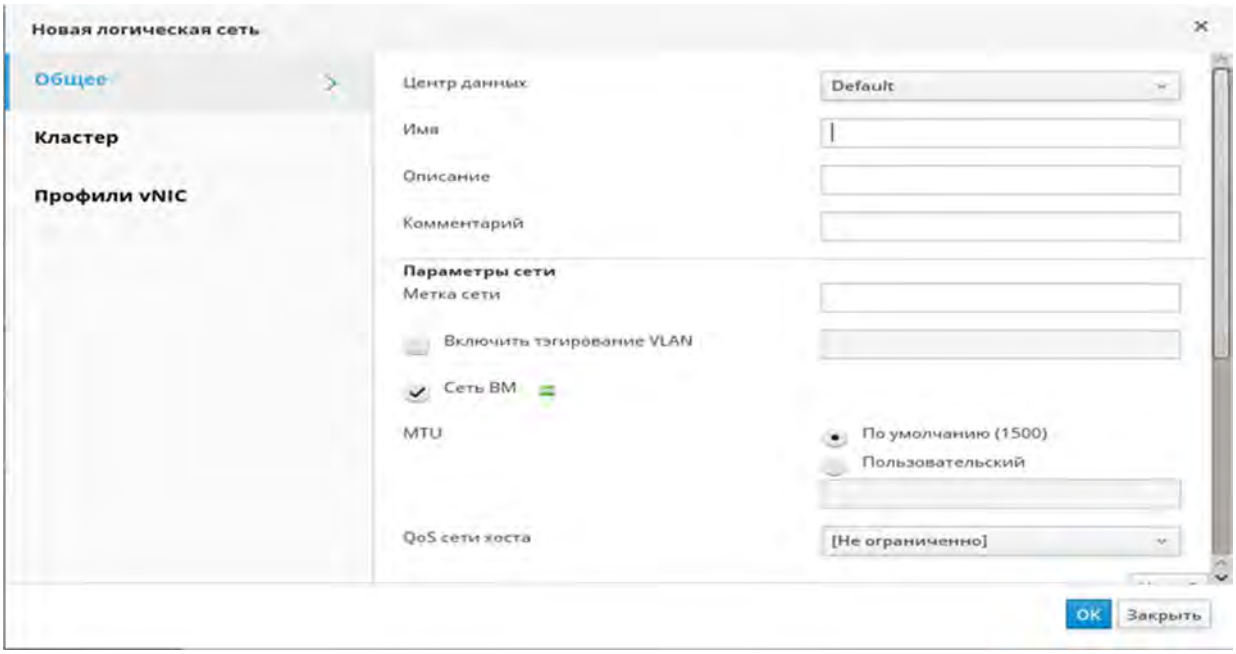


Рисунок 3.86 – Раздел сетевые настройки

Для создания логической сети нажать на кнопку «Новая» (рисунок 3.87).

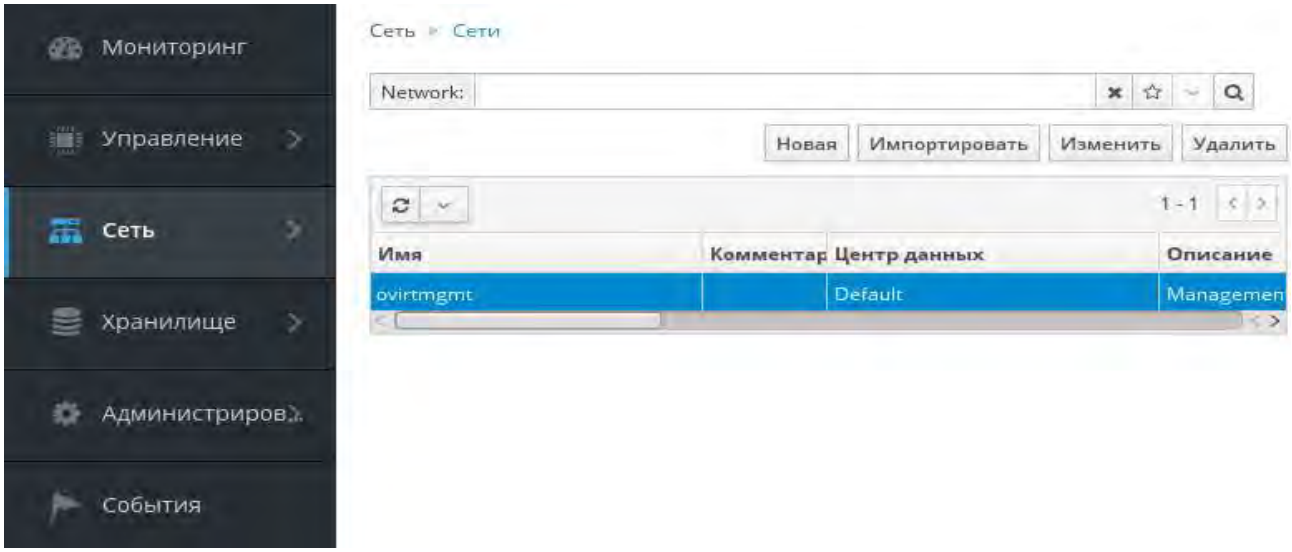


Рисунок 3.87 – Создание логической сети

Для создания логической сети системному администратору необходимо заполнить следующие поля:

– дата центр «Центр данных» является обязательным полем. В данном поле выбирается дата центр, к которому будет относится логическая сеть;

– наименование сети «Имя» является обязательным полем;

– описание «Описание» является необязательным полем;

– комментарии «Комментарий» является необязательным полем;

– метка сети «Метка сети» является необязательным полем. Функция сетевых меток обеспечивает возможность маркировки сетей и использования этой метки на интерфейсах хоста. Конфигурация сети может быть произведена путем управления сетевой меткой, а именно все хосты, помеченные данной меткой, будут прикреплены к конкретной сети;

– метка виртуальной сети «Включить тэгирование VLAN» является необязательным полем. Тоже самое что и метка сети;

– «Сеть VM»;

– максимальный размер полезного блока «MTU» является обязательным полем. По умолчанию максимальный размер полезного блока данных одного пакета, который может быть передан протоколом без фрагментации равен 1500 байт.

Системный администратор может назначить иную степень фрагментации. Для изменения степени фрагментации пакетов установить флаг выбора напротив позиции «Пользовательский», ввести необходимое значение.

Примечание. Степень фрагментации на сетевом коммутаторе должна совпадать со степенью фрагментации установленных на интерфейсах хоста.

– качество сервисов сети «QoS сети хоста» является необязательным полем. Функция управления объемом трафика;

– добавление внешнего подключения «Создать на внешнем провайдере». Данная функция необходима для создания виртуальных сетей;

– тип внешнего источника «Внешний поставщик» является обязательным полем. По умолчанию установлено значение «ovirt-provider-ovn»;

– также виртуальную сеть можно подключить в физической сети. Для подключения сети установить флаг выбора напротив позиции «Connect to physical network» является необязательным полем;

– при выставлении флага выбор напротив позиции «Connect to physical network», системному администратору будет доступна возможность выбора физической сети. «Data Center Network» является полем, где системному администратору необходимо выбрать к какому датацентру относится физическая сеть или ввести вручную датацентр, переключив флаг выбора с «Data Center Network» на «Customs».

Помимо назначения логической сети датацентру, системный администратор также может назначить логическую сеть для конкретного кластера, функционально входящего в датацентр.

Для назначения кластера выбрать пункт раздела «Кластер», расположенного в левой части рабочей области (рисунок 3.88).

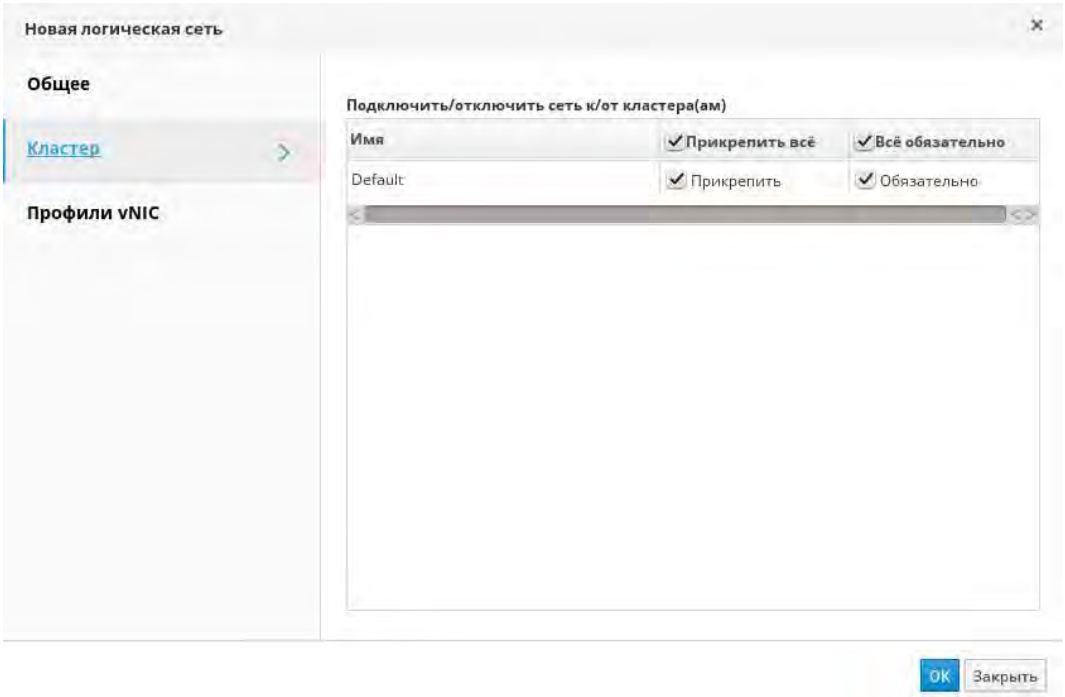


Рисунок 3.88 – Выбор раздела «Кластер»

В разделе «Кластер» представлен перечень кластеров относящиеся к конкретному датацентру. Для включения/исключения новой логической сети в кластер установить флаг выбора на против необходимой позиции или убрать флаг выбора соответственно.

В разделе «Профили vNIC» назначается связь между сервисами (QoS) и виртуальными сетевыми адаптерами (VNIC) (рисунок 3.89).

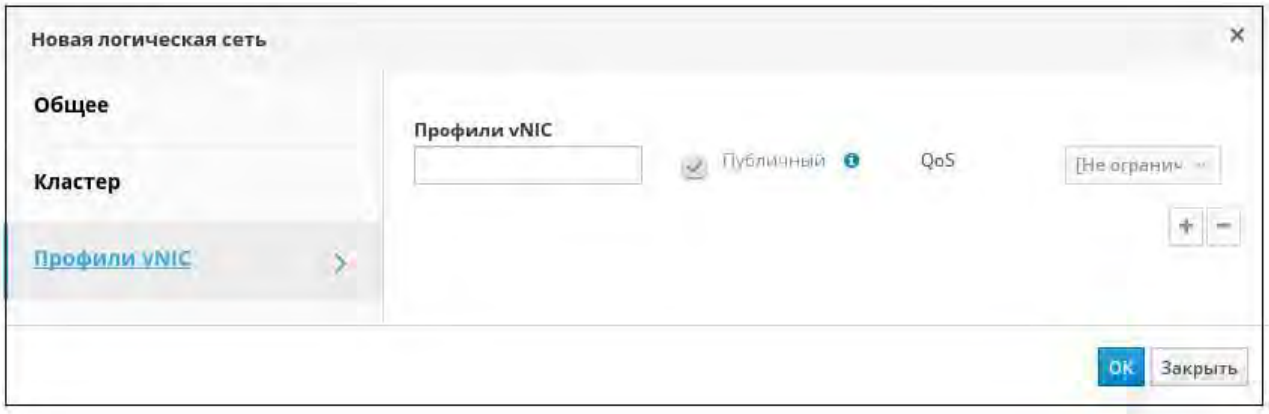


Рисунок 3.89 – Выбор раздела «Профили vNIC»

Для успешного завершения процесса создания новой логической сети нажать кнопку «ОК», в результате в разделе сетевые настройки (см. рисунок 2.7) отобразятся данные по вновь созданной сети.

Для настройки фильтрации сети перейти во вкладку конфигурации сети, нажав два раза ЛКМ на наименование сети (рисунок 3.90).

В открывшейся вкладке представлены следующие разделы:

– общие сведения «Общее»;
– профиль виртуальных интерфейсов «Профили vNIC»;
– подсети «Подсети»;
– гластера «Кластера»;
– хосты «Узлы»;
– виртуальные машины «Виртуальные машины»;
– шаблоны «Шаблоны»;
– разрешения «Разрешения».

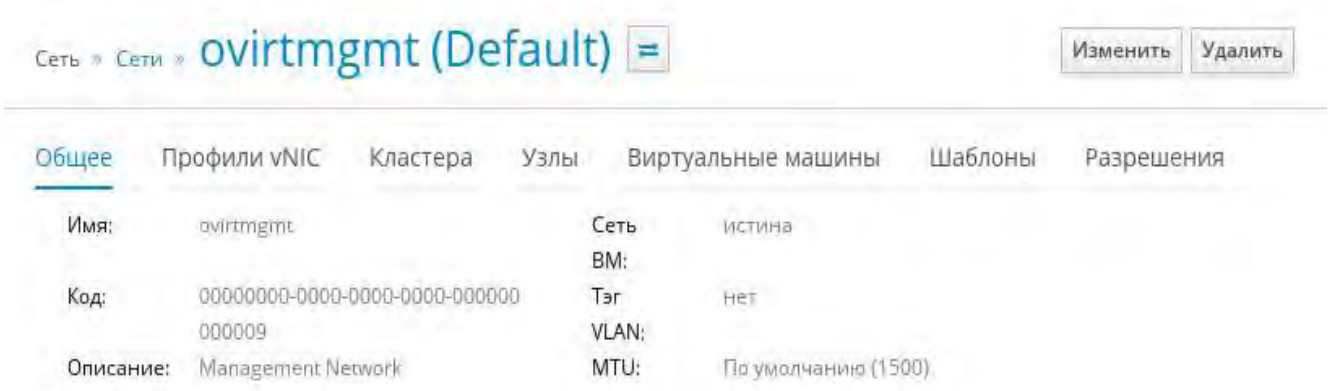


Рисунок 3.90 – Конфигурация сети

Перейти в раздел «Профили vNIC», где системный администратор обладает следующим перечнем действий над виртуальными интерфейсами (рисунок 3.91):

– создание «Новый»;
– редактирование «Изменить»;
– удаление «Удалить».

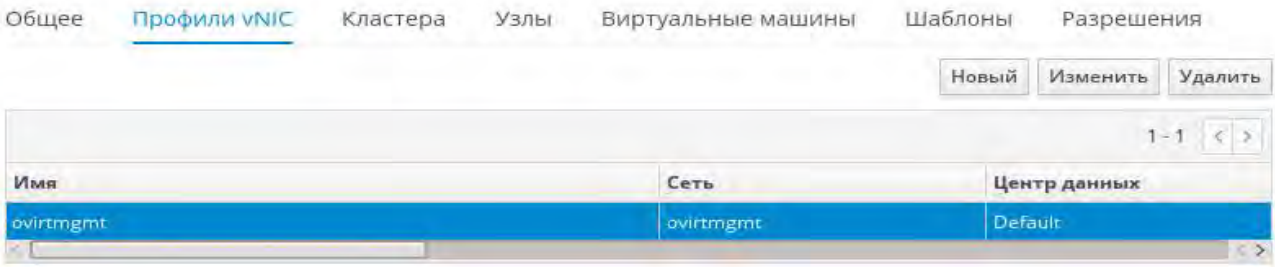


Рисунок 3.91 – Раздел виртуальных интерфейсов

Для назначения сетевых фильтров на виртуальную сеть нажать на кнопку «Изменить». В рабочей области отобразится форма конфигурации интерфейсов (рисунок 3.92). Системному администратору нужно выбрать поле «Фильтр сети».

Поле «Фильтр сети» представляет собой выпадающий список с перечнем правил фильтрации. Перечень правил фильтрации представлен в таблице 3.26.

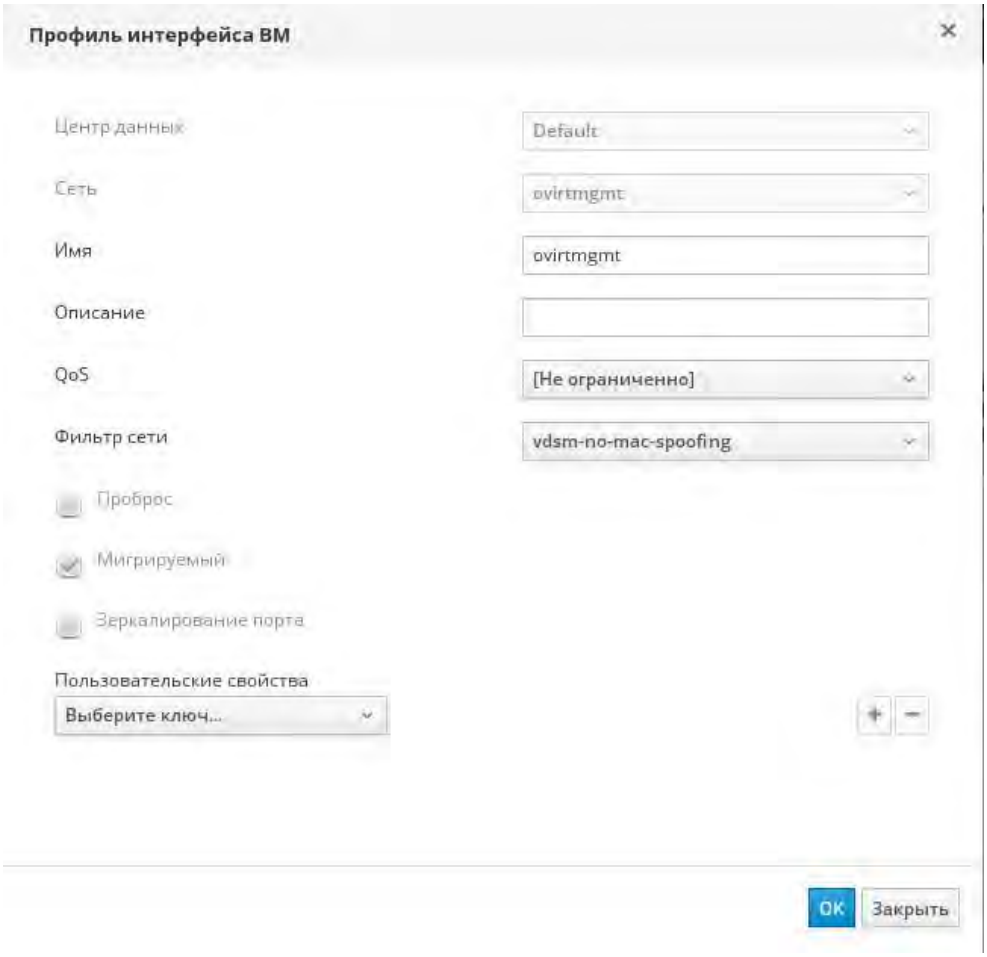


Рисунок 3.92 – Профиль интерфейсов

Таблица 3.26 – Правила фильтрации

№	Правило фильтрации	Описание
1.	vdsm-no-mac-spoofing	Предотвращает спуфинг MAC
2.	allow-arp	Принимает весь входящий и исходящий трафик протокола разрешения адресов (ARP) на гостевую виртуальную машину
3.	allow-dhcp	Позволяет гостевой виртуальной машине запрашивать IP-адрес через DHCP (с любого DHCP-сервера).
4.	allow-incoming-ipv4	Разрешает принимать весь входящий и исходящий трафик протокола ipv4
5.	allow-ipv4	Разрешает принимать весь входящий и исходящий трафик протокола ipv4
6.	clean-traffic	Предотвращает спуфинг MAC, IP и ARP. Этот фильтр ссылается на несколько других фильтров как на строительные блоки.
7.	no-arp-ip-spoofing	Эти фильтры предотвращают подмену ARP-трафика гостевой виртуальной машиной. Кроме того, они разрешают только сообщения ARP-запроса и ответа и требуют, чтобы эти пакеты содержали: no-arp-spoofing - MAC и IP-адреса гостя no-arp-mac-spoofing - MAC-адрес гостя no-arp-ip-spoofing - IP-адрес гостя
8.	no-arp-mac-spoofing	
9.	no-arp-spoofing	
10.	no-ip-multicast	Запрещает гостевой виртуальной машине отправлять многоадресные IP-пакеты.
11.	no-ip-spoofing	Запрещает гостевой виртуальной машине отправлять IP-пакеты с исходным IP-адресом, отличным от того, который находится внутри пакета. Этот фильтр является частью фильтра чистого трафика.
12.	no-mac-broadcast	Предотвращает исходящий трафик IPv4 на указанный MAC-адрес. Этот фильтр является частью фильтра clean-traffic.
13.	no-other-L2-traffic	Предотвращает весь сетевой трафик уровня 2, кроме трафика, указанного другими фильтрами, используемыми сетью. Этот фильтр является частью фильтра clean-traffic.
14.	no-other-rarp-traffic	Эти фильтры позволяют QEMU самостоятельно объявлять пакеты протокола обратного разрешения адресов (RARP), но предотвращают весь другой трафик RARP.
15.	qemu-announce-self	
16.	qemu-announce-self-rarp	

Для успешного завершения процесса назначения правил фильтрации нажать кнопку «ОК».

При отсутствии профиля виртуального интерфейса, системному администратору необходимо создать новый профиль виртуального интерфейса. Нажать на кнопку «Новый» раздела «Профили vNIC» (см. рисунок 3.91). Заполнить следующие поля:

– датацентр «Центр данных» является обязательным полем. По умолчанию установлено значение «Default»;

– сеть «Сеть» является обязательным полем. Определяется для какой сети создается интерфейс;

– наименование «Имя» является обязательным полем. Наименование должно быть уникальным;

– описание «Описание» является необязательным полем.

– политика приоритета сети «QoS» является обязательным полем. По умолчанию значение «Не ограниченно»;

– проброс «Проброс» является необязательным полем. Для обхода виртуальной сети и делегирования подключения на физический интерфейс используется функция проброса «Проброс». Для назначения данной функции установить флаг выбора напротив позиции «Проброс»;

– миграция «Мигрируемый» является необязательным полем. По умолчанию установлен флаг выбора. При миграции ВМ виртуальный интерфейс также мигрирует. Управление данной функцией доступно только с назначением проброса «Проброс»;

– дублирование (зеркалирование) сетевых интерфейсов (портов) является необязательным полем. При использовании функции проброса «Проброс» данная функция не доступна;

– пользовательские свойства «Пользовательские свойства» является необязательным полем. Назначение пользовательских свойств для применения к профилю виртуального интерфейса;

– разрешить всем пользователям использовать данный профиль «Разрешить всем пользователям доступ к этому профилю» является необязательным полем. По умолчанию установлен флаг выбора.

Для успешного завершения процесса создания профиля виртуального интерфейса нажать кнопку «ОК».

3.17.2. Назначение сетевых меток на конкретный хост

Сетевой интерфейс можно назначить как на физический сервер (гипервизор), так и на виртуальные машины. Назначение интерфейсов производится во вкладке меню «Управление». В зависимости от технического средства выбрать раздел «Хосты» (гипервизор) или «Виртуальные машины» (ВМ).

Для назначения сетевого интерфейса на физический сервере перейти в раздел «Хосты». Выбрать конкретный домен, нажатием ЛКМ по наименованию сервера (поле «Имя») перейти во вкладку конфигурации (рисунок 3.93).

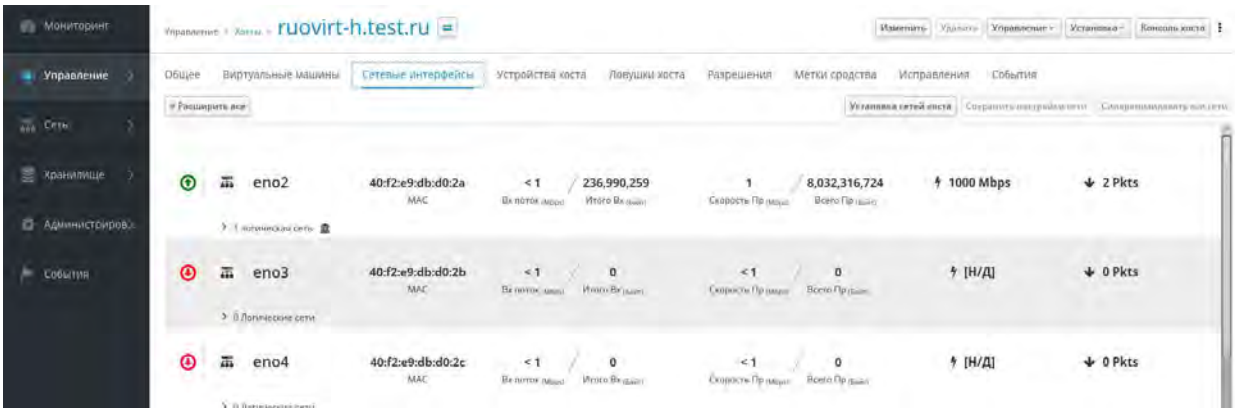


Рисунок 3.93 – Вкладка конфигурации

Для управления сетевыми интерфейсами перейти в раздел «Сетевые интерфейсы», выбрать хост, нажать на кнопку «Установка сетей хоста». В открывшейся экранной форме (ЭФ) (рисунок 3.94) системному администратору отображается перечень интерфейсов, относящихся к данному хосту (столбец «Интерфейсы», расположенный в левой части ЭФ) и соответствие с назначенными логическими сетями (столбец «Связанные логические сети»). В правой части расположены внешние логические сети «Внешние логические сети» созданные на ранних этапах.

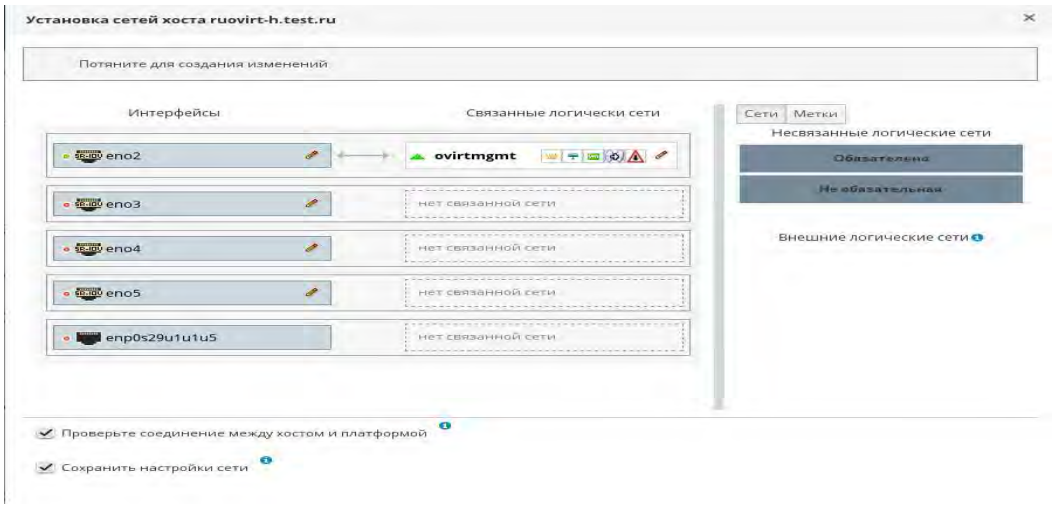


Рисунок 3.94 – Перечень интерфейсов

Для назначения сетевому интерфейсу логическую сеть, из поля «Внешние логические сети» перенести и установить выбранную логическую сеть напротив необходимого поля.

Для конфигурации логической сети нажать на пиктограмму редактирования (рисунок 3.95).

Рисунок 3.95 – Пиктограмма редактирования

При нажатии на пиктограмму в рабочей области отобразится форма по конфигурации сети (рисунок 3.96).

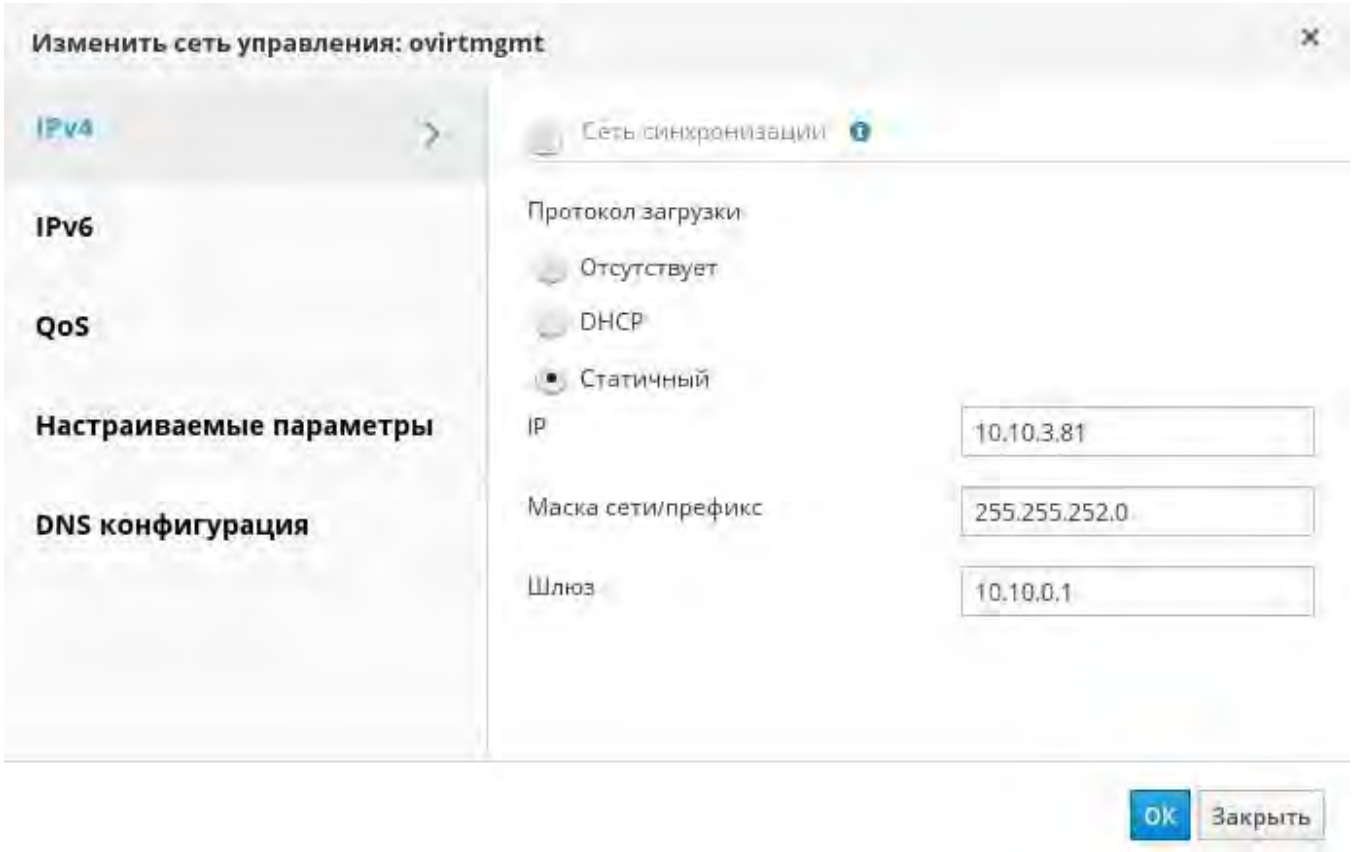


Рисунок 3.96 – ЭФ конфигурации сети

Выбрать какой протокол будет использоваться IPv4, IPv6. Задать протокол загрузки «Протокол загрузки» установив флаг выбора напротив необходимой позиции:

– не использовать протокол «Отсутствует»;

– протокол динамической настройки хоста «DHCP»;

– использовать статические значения «Статичный». При выборе типа «Static» системному администратору также нужно задать IP-адрес, маску подсети, шлюз.

Примечание. Каждая логическая сеть может иметь отдельный шлюз определенными от управления сетевой шлюз. Это гарантирует, что трафик, поступающий в логическую сеть, будет пересылаться с использованием шлюза логической сети вместо шлюза по умолчанию, используемого сетью управления.

Для переопределения приоритета трафика, необходимо перейти в раздел «QoS» вкладки, представленной на рисунке 3.97.

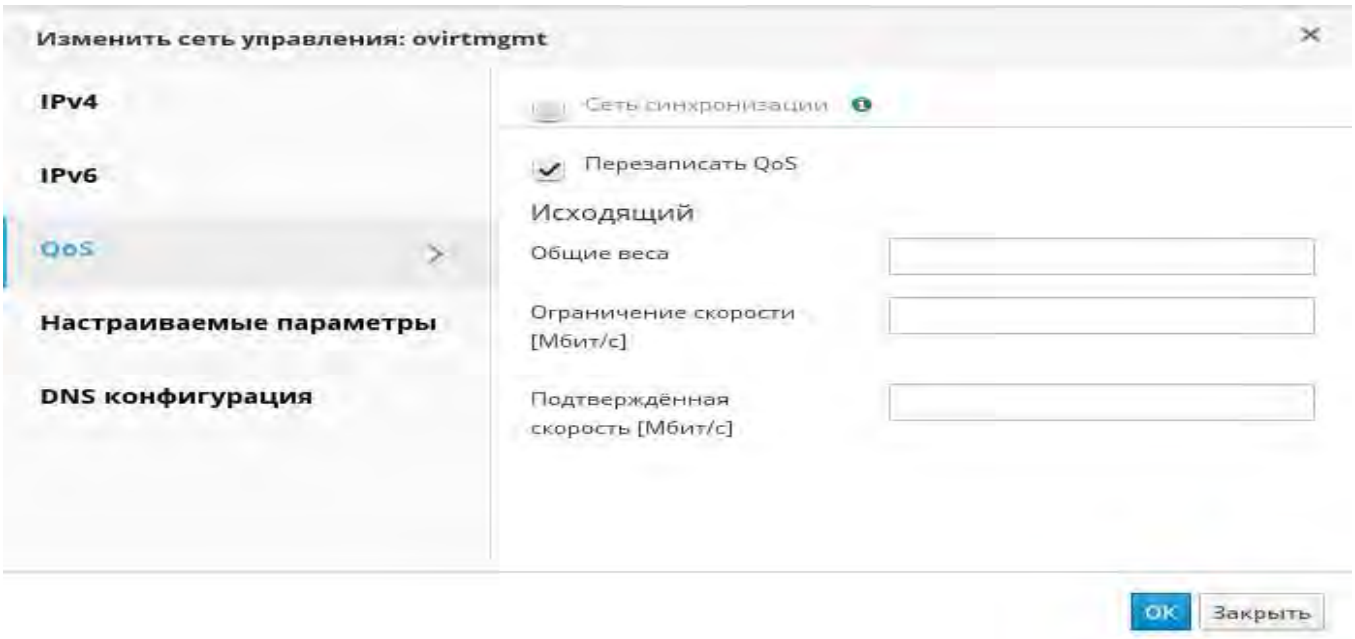


Рисунок 3.97 – раздел «QoS» вкладки конфигурации сети

Установить флаг выбора в поле перезапись приоритетов «Перезаписать QoS» и ввести нужные значения в следующие поля:

– «Общие веса» является обязательным полем. В этом поле определяется сколько логических связей должно быть выделено относительно других сетей. По умолчанию задаваемое значение должно попадать в интервал от 1 до 100;

– ограничение скорости [Мбит / с] «Ограничение скорости» является обязательным полем. Максимальная полоса пропускания;

– гарантирования скорость передачи [Мбит / с] «Подтвержденная скорость» является обязательным полем.

Для настройки сетевого моста (bridge), необходимо перейти в раздел «Настраиваемые параметры» вкладки, представленной на рисунке 3.98. В выпадающем списке выбрать пункт «bridge_opt». Ввести достоверный ключ и значение. Формат ключ-значения: key=value. Разделять несколько записей с помощью символа «пробел». Перечень допустимых параметров ключей представлен в таблице 3.27.

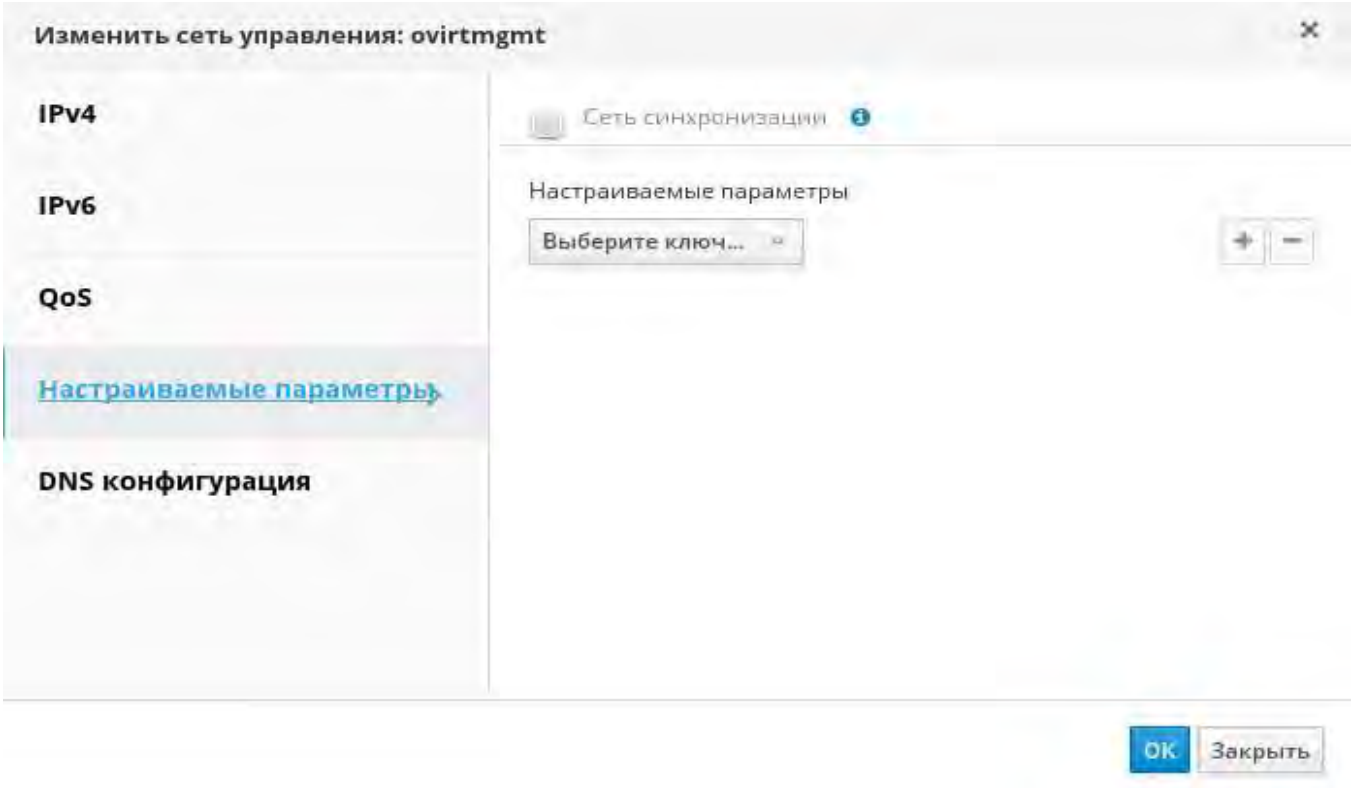


Рисунок 3.98 – раздел «Custom Properties» вкладки конфигурации сети

Таблица 3.27 – Параметры ключей

№	Ключ-значение	Описание	Примечание
1.	forward_delay=1500		Устанавливает время, в децисекундах. Мост будет находится в состоянии прослушивания и обучения. Если в это время не будет обнаружен коммутационный цикл, мост перейдет в состояние пересылки. Это позволяет проверять трафик и компоновку сети до нормальной работы сети.
2.	gc_timer=3765		Устанавливает время сбора мусора в децисекундах, после чего база данных пересылки проверяется и очищается от затухающих записей.
3.	hash_elasticity=4		Максимальная длина цепи, которая разрешена в хеш-таблице. Значение не вступает в силу до тех пор, пока не будет добавлена следующая новая группа многоадресной передачи. Если это не может быть выполнено после перезагрузки, происходит столкновение хэшей, и переход в состояние отключено.
4.	hash_max=512		Максимальное количество записей в хэш-таблице. Это значение вступает в силу немедленно и не может быть установлено на значение, меньшее, чем текущее количество записей в многоадресной группе. Значение должно быть не меньше двух

Для успешного завершения процесса настройки виртуальной сети нажать кнопку «ОК». В рабочей области отобразится форма «Настройка хост-сетей» («Setup Host Networks») (см. рисунок 2.14).

Для проверки подключения установить флаг выбора напротив поля «Проверка подключения между хостом и движком» («Verify connectivity between Host and Engine»).

Для неизменности сетевых настроек после перезагрузки среды установить флаг выбора напротив поля «Сохранить конфигурацию сети» («Save network configuration»).

Для назначения сетевого интерфейса на виртуальную машину перейти в раздел «Виртуальные машины» («Virtual Machines»). Выбрать наименование конкретной

ВМ, нажатием ЛКМ по наименованию ВМ (поле «Имя» («Name») перейти во вкладку конфигурации (рисунок 3.99).

Примечание. Назначение нового сетевого интерфейса для существующей ВМ осуществляется только когда машина находится в выключенном состоянии («Выключение»).

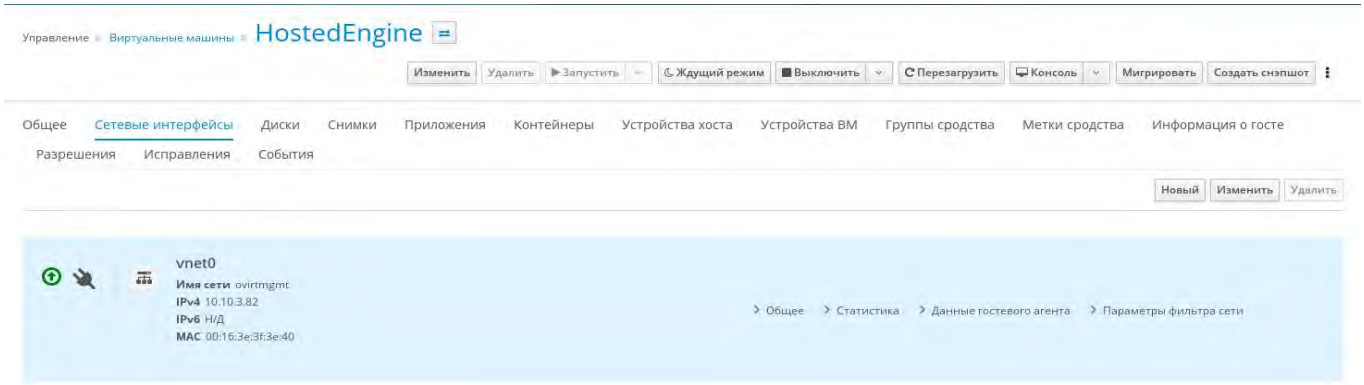


Рисунок 3.99 – ЭФ нового сетевого интерфейса для существующей ВМ

Для выключения виртуальной машины в меню управления ВМ нажать на пиктограмму выпадающего списка расположенной возле кнопки «Выключить» (рисунок 3.100). В выпадающем списке выбрать «Обесточить».

Рисунок 3.100 – Выбор процедуры выключения ВМ

После выполнения процедуры выключения ВМ в разделе «Сетевые интерфейсы» нажать на кнопку «Новый». В рабочей области визуализируется форма по созданию «Нового сетевого интерфейса» (рисунок 3.101). Выбрать профиль виртуального интерфейса, при необходимости задать Mac-адрес.

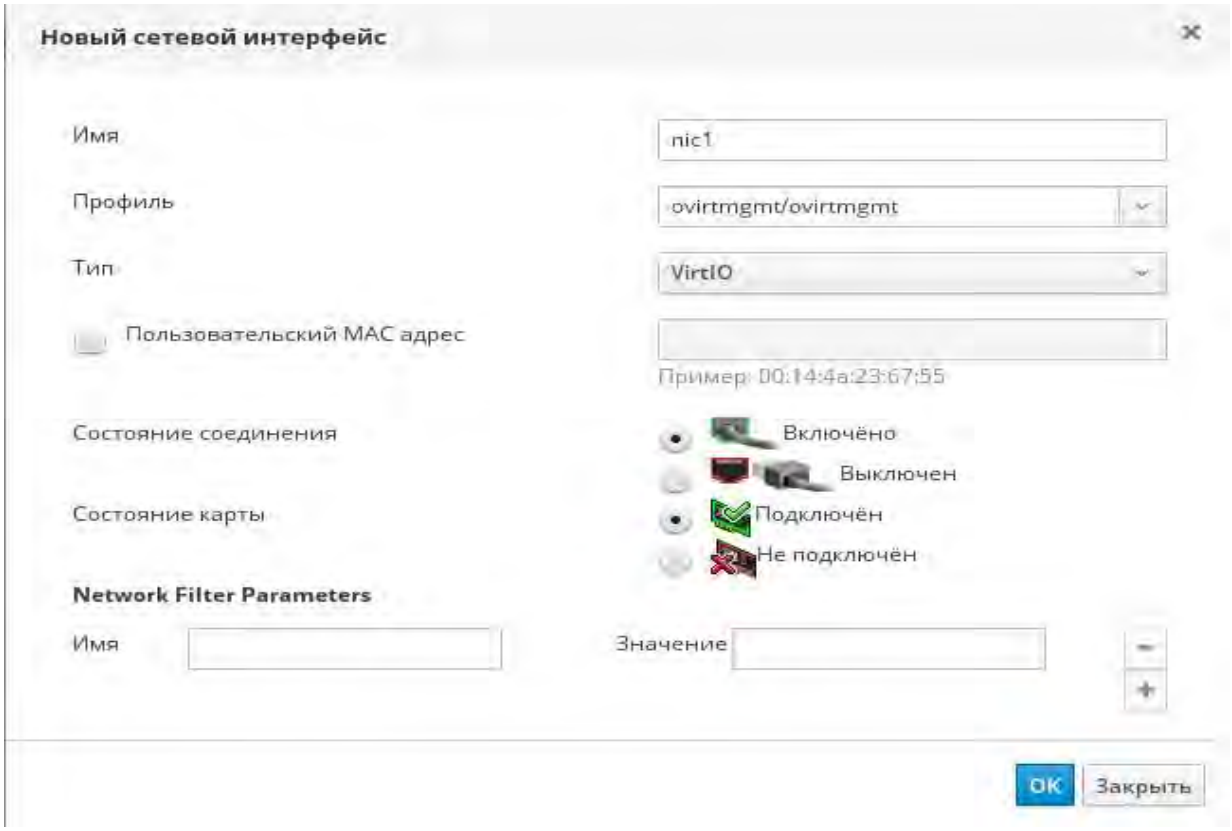


Рисунок 3.101 – ЭФ создания нового интерфейса ВМ

Для успешного завершения процесса создания виртуального интерфейса нажать кнопку «ОК». Запустить ВМ нажав на пиктограмму «Запустить», расположенную на меню управления (см. рисунок 3.99).

Примечание. В случае, когда сервер управления средой виртуализации (Менеджер ВМ) установлен не на физическом хосте (сервере), а на виртуальной машине тем самым используется «Хостинг-движок» («Hosted Engine»), для корректной работы виртуальных интерфейсов выполнить команду по ручной настройке виртуальной сети.

Для ручной настройки виртуальной сети нужно выполнить следующие действия:

– зайти на менеджер ВМ;

– выполнить команду:

```
vdsm-tool ovn-config <ip адрес менеджера> <ip адрес самого хоста> .
```

3.18.Управление защитой от переполнения буфера

Функция защиты буфера от переполнения реализована с помощью:

– использование битов в сегментах кода;

– рандомизация размещения адресного пространства (ASLR).

В КП «ЗОС «СинтезМ» предусмотрена возможность настройки параметра ASLR через интерфейс sysfs по адресу /proc/sys/kernel/randomize_va_space.

Пример команды настройки: sysctl –w kernel.randomize_va_space=[параметр]

Перечень параметров представлен в таблице 3.28.

Таблица 3.28 – Перечень параметров ASLR

№	Параметры	Описание	Примечание
1.	0	Технология ASLR отключена	
2.	1	Частичная рандомизация адресного пространства и использование случайного смещения	Адреса shared библиотек, стека, памяти выделяемой при помощи mmap, VDSO
3.	2	Полная рандомизация	К областям памяти указанных в п/п 2 добавляются адреса памяти, выделяемые при исполнении инструкции brk

3.19.Управление квотированием ресурсов

3.19.1. Включение дисковых квот

Для включения дисковых квот необходимо провести следующие настройки:

— настроить монтирование дисков с поддержкой механизма квотирования;

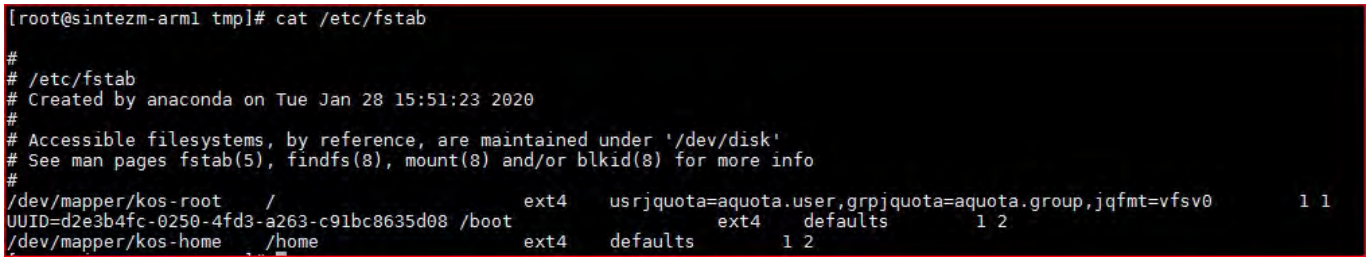
— произвести монтирование файловой системы с поддержкой механизма квотирования;

— провести первичную инициализацию механизма квотирования.

Для настройки монтирования дисков с поддержкой механизма квотирования необходимо отредактировать файл `/etc/fstab`

```
sudo vim /etc/fstab
```

добавив «usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0» для диска для которого настраивается квотирование. Например:



Для того, чтобы произвести монтирование файловой системы с поддержкой механизма квотирования необходимо выполнить команду

```
sudo mount -o,remount /
```

Для того, чтобы провести первичную инициализацию механизма квотирования необходимо выполнить команду:

```
quotacheck -vgum /
```

3.19.2. Настройка квот

Управление квотированием ресурсов выполняется с помощью конфигурирования файла /etc/security/limits.conf, а также с помощью утилит quota, setquota, quotaon, quotaoff.

В конфигурационном файле limits.conf задается ограничение ресурсов системы для пользователей или групп пользователей. Файл состоит из полей:

– domain;
– type;
– item;
– value.

Поле «domain» может содержать следующие атрибуты:

– наименование пользователя;
– наименование группы пользователей;

Примечание. Перед наименованием группы необходимо указать символ «@»)

– символ «*» – назначение ограничения, действующего по умолчанию.

Поле «type» задает тип ограничения: мягкое (soft) или жесткое (hard). Мягкое ограничение определяет число системных ресурсов, которое пользователь все еще

может превысить, жесткое ограничение превысить невозможно. При попытке сделать это, пользователь получит сообщение об ошибке.

Поле «item» может содержать следующие типы квотируемых ресурсов:

- core – ограничение размера файла core (Кб);
- data – максимальный размер данных (Кб);
- fsize – максимальный размер файла (Кб);
- memlock – максимальное заблокированное адресное пространство (Кб);
- nofile – максимальное число открытых файлов;
- stack – максимальный размер стека (Кб);
- cpu – максимальное время процессора (минуты);
- nproc – максимальное число процессов;
- as – ограничение адресного пространства;
- maxlogins – максимальное число одновременных регистрации в системе;
- locks – максимальное число файлов блокировки.

Управление квотированием ресурсов с помощью утилит.

/usr/bin/quota – утилита выводит сводку о использование пользователем дискового пространства.

Пример команды утилиты quota: quota [-v] [пользователь]

Опция «-v» обеспечивает вывод всех смонтированных файловых систем, на которых назначено ограничение ресурсов для конкретного пользователя.

/usr/sbin/setquota – редактор квот командной строки. В командной строке можно указать файловую систему, имя пользователя или группу пользователей, ограничения для файловой системы.

Примечание. Если наименование пользователя состоит из цифр, то утилита будет обрабатывать данное имя как

Пример команды: setquota [опции] [-F формат ограничения] [объект ограничения]

Перечень опций представлен в таблице 3.29.

Таблица 3.29 – Перечень опций утилиты setquota

№	Опции	Описание
1.	-u	Назначение ограничений на пользователя
2.	-g	Назначение ограничений на группу пользователей
3.	-a, -a | <файловая система>	Назначение ограничений на все файловые системы
4.	-t	Редактировать период снятий ограничений
5.	-T	Редактировать период снятий ограничений для пользователей или групп пользователей

/usr/sbin/quotaon – утилита включения квотирования файловой системы

Пример команды:

```
quotaon [опции] [-F формат ограничения] [все/ конкретная файловая система]
```

Утилита может запускать с перечнем опций, представленных в таблице 3.30

Таблица 3.30 – Перечень опций утилиты quotaon

№	Опции	Описание
1.	-a	Включить ограничения для всех файловых систем
2.	-f	Выключить ограничения
3.	-u	Работа с пользовательскими ограничениями
4.	-g	Работа с групповыми ограничениями

/usr/sbin/quotaoff – утилита отключения квотирования файловой системы

Пример команды:

```
quotaoff [опции] [-F формат ограничения] [все/ конкретная файловая система]
```

Утилита может запускать с перечнем опций, представленных в таблице 3.31.

Таблица 3.31 – Перечень опций утилиты quotaoff

№	Опции	Описание
1.	-a	Выключить ограничения для всех файловых систем
2.	-f	Выключить ограничения
3.	-u	Работа с пользовательскими ограничениями
4.	-g	Работа с групповыми ограничениями

3.20. Настройка Службы единого времени chrony

3.20.1. Настройка Службы единого времени chrony в качестве сервера точного времени

Для настройки данного сервиса в качестве сервера точного времени необходимо открыть файл настроек с использованием стандартного текстового редактора vim, выполнив команду:

```
vim /etc/chrony.conf
```

В открывшемся файле необходимо найти следующие строки:

```
#allow 192.168/16
#local stratum 10
```

В указанных строках необходимо убрать комментарий и указать значения подсети и маски подсети соответствующие параметрам локальной вычислительной сети в которой будет функционировать сервера точного времени.

Пример:

```
allow 10.10.10.0/24
local stratum 10
```

Далее изменить строку:

```
server 127.127.1.0 iburst
```

После чего перезапустить сервис chronyd:

```
systemctl restart chronyd.service
```

3.20.2. Настройка Службы единого времени chrony в качестве клиента

Для настройки данного сервиса в качестве сервера точного времени необходимо открыть файл настроек с использованием стандартного текстового редактора vim, выполнив команду:

```
vim /etc/chrony.conf
```

В открывшемся файле необходимо найти следующие строки:

```
server [ip-адрес] iburst
```

, где `[ip-адрес]` - ip-адрес сервера точного времени.

После чего перезапустить сервис chronyd:

```
systemctl restart chronyd.service
```

3.21. Управление приоритетом обслуживания

В КП «ЗОС «СинтезМ» реализована возможность управления приоритетами запуска процессов. Существуют одновременно две модели организации иерархии процессов – Linux Process Model и Cgroup Model.

Алгоритм планирования выполнения (Process Model) процессов (schedule_process) представлен в Функциональной спецификации п. 5. Управление правилами приоритетом обслуживания осуществляется утилитами nice, renice, chrt.

Команда nice используется для не запущенных процессов, команд.

Пример команды nice: nice [-n смещение] [--adjustment=смещение] [команда [аргумент].

nice -n13 pico myfile.txt, запуск команды «pico» на файл «myfile.txt» с привилегией «13».

Перечень команд представлен в таблице 3.32.

Таблица 3.32 – Перечень команд

№	Команда	Описание	Примечание
1.	-n	Увеличить nice на целое число N	По умолчанию 10
2.	--adjustment=N	Тоже самое что и «–n»	
3.	-- version	Вывод версии nice	

Все процессы в системе работают с определёнными приоритетами, также называемыми значениями «nice», которые могут изменяться от -20 (наивысший приоритет) до 19 (наименьший приоритет). Если значение приоритета не определено, каждый процесс будет назначаться по умолчанию значение «0» (рисунок 3.102).

Для вывода значений привилегий процессов используются команды:

- top;
- ps aux.

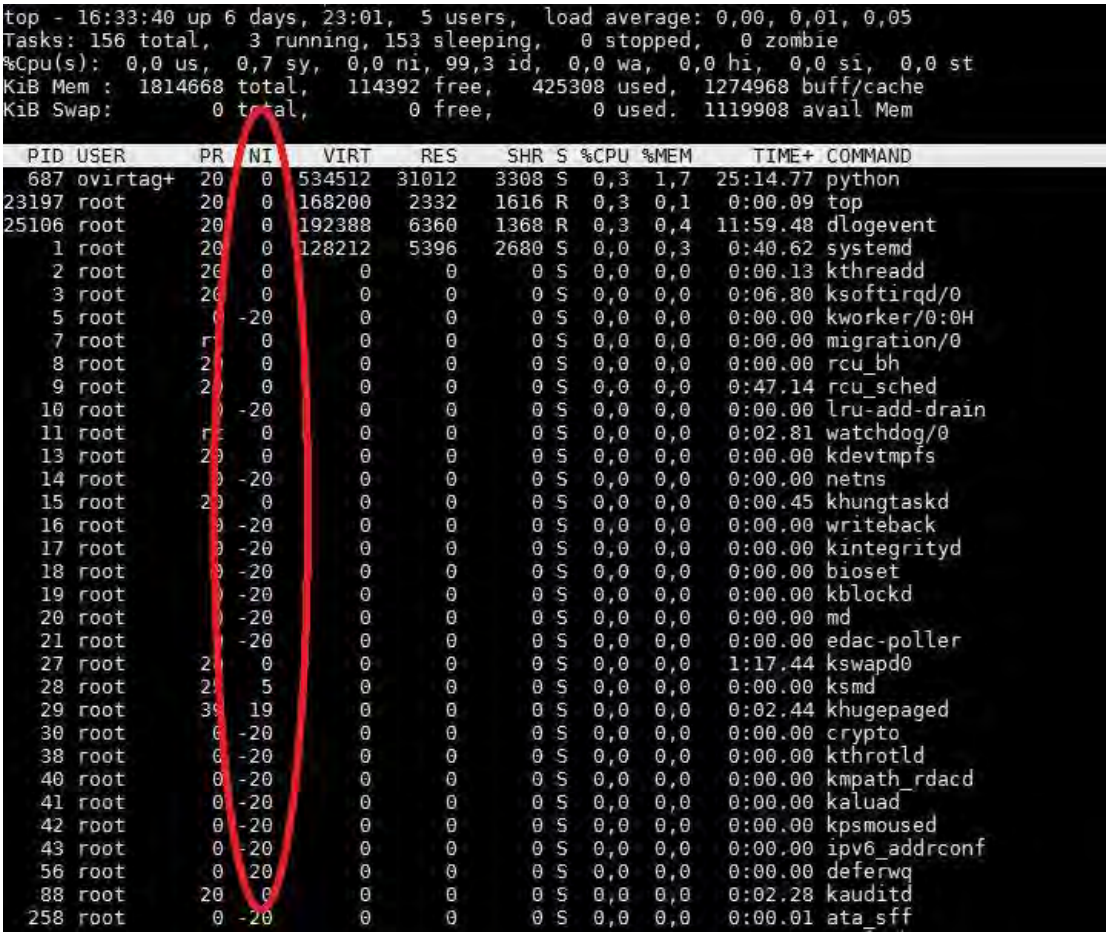


Рисунок 3.102 – Пример вывода информации топ процессов

Команда «renice» используется для запущенных процессов, когда приоритет обслуживания необходимо изменить в режиме реального времени, не прекращая работу процесса.

Пример команды renice:

```
renice [приоритет] [-p pid] [-g pgrp] [-u user]
renice [опция (-n)] increment [-p pid] [-g pgrp] [-u user]
```

– `renice -n 19 ПРОЦЕСС(PID)`, на существующий процесс назначается привилегия «19» (наименьшая степень привилегии)

– `renice +1 987 -u daemon root -p 32`, изменения приоритета процессу с PID 987 и 32, и всем процессам владельцы которых пользователь «daemon» и «root».

Таблица 3.33 – Перечень опций утилиты renice

№	Опции	Описание
1.	-g	Настройка привилегии для процессов равному идентификатору группы

2.	-n	Вместо изменения указанных приоритетов по указанным процессам, осуществляется наращивание значения приоритета для каждого процесса
3.	-u	Изменения приоритета по указанному идентификатору пользователя
4.	-p	Сброс привилегий процесса до значения по умолчанию

chrt - управление атрибутами процессов в режиме реального времени.

Пример команды chrt:

```
chrt [опции] [приоритет] [PID | команда (аргумент)]
```

Таблица 3.34 – Перечень опций утилиты chrt

№	Опции	Описание
1.	-p, --pid	Операция производится на существующем PID, не запуская новое задание (процесс)
2.	-b, --batch	Назначение политики планирования для SCHED_BATCH
3.	-f, --fifo	Назначение политики планирования для SCHED_FIFO
4.	-m, --max	Вывод максимального и минимального значений политик планирования
5.	-o, -- other	Назначение политики планирования для SCHED_OTHER
6.	-r, --rr	Назначение политики планирования для SCHED_RR
7.	-v, --version	Вывод информации о версии утилиты

Алгоритм планирования выполнения (Cgroups Model) процессов представлен в Функциональной спецификации п. 5. Управление правилами приоритетом обслуживания осуществляется cgroups.

Создание групп управления

В КП «ЗОС «СинтезМ» в соответствии с выполняемы задачами предусмотрено создание временных и постоянных групп управления (все действия по управления cgroups выполняются пользователем с правами суперпользователя).

Временные групп управления используются для назначения лимитов на ресурсы, потребляемой службой во время ее выполнения.

При создании постоянных групп управления конфигурация сохраняется после перезагрузки системы, поэтому ее можно использовать для управления службами, которые запускаются автоматически.

Создание временной группы

Пример команды: systemd-run --unit=name --scope --slice=slice_name <команда>, параметры команды представлены в таблице 3.35.

Таблица 3.35 – Описание параметров

№	Параметр	Описание	Примечание
1.	--unit=name	Задание наименование группы	Если параметр не указан, наименование сгенерируется автоматически
2.	--scope	При использовании этого параметра создается временная единица scope, вместо сервиса, который создастся автоматически	
3.	--slice=slice_name	Создание нового scope или сервиса	
4.	<команда>	Задать команду, выполняемую в сервисном модуле	
5.	--description	Создает описание	
6.	--remain-after-exit	Позволяет собирать информацию о времени выполнения после завершения процесса службы	
7.	--machine	Опция выполняет команду в контейнере	

Удаление групп управления

Пример команды: systemctl kill <наименование сервиса> --kill-who=PID,... --signal=signal , параметры команды представлены в таблице 3.36.

Таблица 3.36 – Параметры команды удаления

№	Параметр	Описание	Примечание
1.	<наименование сервиса>		Например: httpd.service
2.	--kill-who=<PID процесса>	Выбор перечень процессов из группы	

Настройка групп управления

Для управления ресурсами на основе приоритетов сперва необходимо создать группу приоритетов. В рамках данного примера будет использоваться группа limited. Создание группы осуществляется в конфигурационном файле /etc/cgconfig.conf. Группа содержит типы управляемых ресурсов и их параметры. Например группа

limited задающая параметры выделения оперативной памяти и процессорного времени будет выглядеть следующим образом:

```
group limited {
    memory {
         memory.limit_in_bytes = 20M;
  }
    cpuset {
        cpuset.cpus = 0;
        cpuset.mems = 0;
    }
    cpu {
        cpu.shares = 2;
        cpu.cfs_quota_us = 4000;
        cpu.cfs_period_us = 1000;
    }

}
```

Задание приоритета обслуживания для пользователя осуществляется за счет добавления соответствующей строки в /etc/cgrules.conf. В рамках нашего примера строка задающая приоритет для пользователя тест будет выглядеть следующим образом:

```
test cpu,cpuset,memory limited/
```

После внесения изменений в конфигурационный файл необходимо провести перезагрузку служб командой:

```
service cgconfig restart && service cgred restart
```

3.22.Настройка отказоустойчивости

Для обеспечения отказоустойчивого кластера, обеспечивающего работу экземпляров операционной системы на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и информации при выходе из строя одного из технических средств применяются набор модулей КП «ЗОС «СинтезМ»:

– keepalived;

– настройка синхронизации информации;

– настройка снимков (snapshot);

– настройка миграции ВМ между хостами серверов виртуализации.

3.22.1. Настройка keepalived

Настройка keepalived осуществляется в следующем порядке:

– Открыть файл настройки конфигурации keepaliveed:

```
sudo vi /etc/keepalived/keepalived.conf
```

– Нажатием клавиши «insert» выполнить переход в режим ввода.

– Внести изменения:

```
! Configuration File for keepalived
global_defs {
   notification_email {
     [email]
   }
   notification_email_from any@any.com
   smtp_server localhost
   smtp_connect_timeout 30
}

vrrp_instance VI_1 {
    state BACKUP
            nopreempt
    interface [имя интерфейса]
    virtual_router_id 51
    priority 150
    advert_int 1
    authentication {
        <strong>auth_type PASS
        auth_pass 31415926</strong>
    }
    virtual_ipaddress {
        [общий ip-адрес]

    }
}
```

, где **[общий ip-адрес]** – виртуальный ip-адрес назначаемый для обеспечения отказоустойчивости

[имя интерфейса] – имя сетевого интерфейса через который будет осуществляться сетевой обмен

[email] – адрес электронной почты на который будут отправляться уведомления о работе модуля keepalived

– Далее комбинацией клавиш «Shift+:» перейти в командный режим, выполнить «wq!» для сохранения внесенных изменений и нажатием «Enter» завершить сохранение внесенных изменений.

– Выполнить настройку автозапуска keepaliveed на АРМ администратора:

```
sudo systemctl enable keepalived
```

– Выполнить настройку keepaliveed на втором узле аналогично процедуре описанной выше, указав в качестве параметра «priority» значение **100** .

3.22.2. Настройка синхронизации информации

Синхронизация информации осуществляется в двустороннем режиме между двумя узлами за счет синхронизации файлов. Для настройки синхронизации информации необходимо на обоих узлах:

– выполнить установку пакетов obs-0.1-3.fc23.noarch.rpm, python-inotify-adapters-0.2.10-1.fc23.noarch.rpm, python-netifaces-0.10.4-3.el7.x86_64.rpm, на узлы синхронизация информации между которыми подразумевается, для этого выполнить команду:

```
sudo rpm -i obs-0.1-3.fc23.noarch.rpm python-inotify-adapters-0.2.10-1.fc23.noarch.rpm
```

– сгенерировать ssh ключ на первом узле, командой:

```
sudo ssh-keygen
```

– скопировать ssh ключ на другой узел, командой:

```
sudo ssh-copy-id <IP адрес>,
```

<IP адрес> = соответствует IP адресу второго узла.

– сгенерировать ssh ключ на втором узде, командой:

```
sudo ssh-keygen
```

– скопировать ssh ключ на первый, командой:

```
sudo ssh-copy-id <IP адрес>,
```

где <IP адрес> = соответствует IP адресу первого узла.

– на первом узле выполнить настройку конфигурационного файла «/etc/fobs/fobs.conf», для этого открыть файл для редактирования, командой:

```
sudo vim /etc/fobs/fobs.conf
```

- нажатием клавиши «insert» выполнить переход в режим ввода.
- внести изменения:

```
[fobs]
public_ip = [общий ip-адрес выделенный для keepalived]
timeout = 2
service = obs
```

– после внесения изменений выйти из режима ввода «esc», далее комбинацией клавиш «shift+:» перейти в командный режим, выполнить «wq!» для сохранения внесенных изменений и нажатием «Enter» завершить сохранение внесенных изменений.

– на первом узле выполнить настройку конфигурационного файла «/etc/obs/obs.conf», для этого открыть файл для редактирования, командой:

```
sudo vim /etc/obs/obs.conf
```

- нажатием клавиши «insert» выполнить переход в режим ввода.
- внести изменения:

```
[obs_pathes]
[path1]
in_dir = [директория]
out_dir = [имя пользователя]@[IP адрес]:/[директория]
```

, где path1 задает название секции, в конфигурационном файле может быть одна или более секций. Параметр in_dir задает директорию изменения которой будут отслеживаться сервисом obs. Параметр out_dir задает куда будут доводиться изменения.

– произвести на втором узле аналогичную настройку конфигурационных файлов «/etc/fobs/fobs.conf» и «/etc/obs/obs.conf».

– после завершения настройки необходимо на обоих узлах поставить службу fobs в автозагрузку и выполнить запуск сервиса:

```
sudo systemctl enable fobs
```

```
sudo systemctl start fobs
```

3.22.3. Настройка снимков (снэпшот)

Для создания снэпшота перейти в пункт меню «Управление», «Виртуальные машины». Оператору отобразится форма, в которой представлены виртуальные машины, зарегистрированные в системе. Выбрать ВМ, для которой необходимо создать снэпшот, перейти на форму «Создать снэпшот» посредством нажатия ЛКМ на кнопку «Создать снэпшот» (Рисунок 3.103).

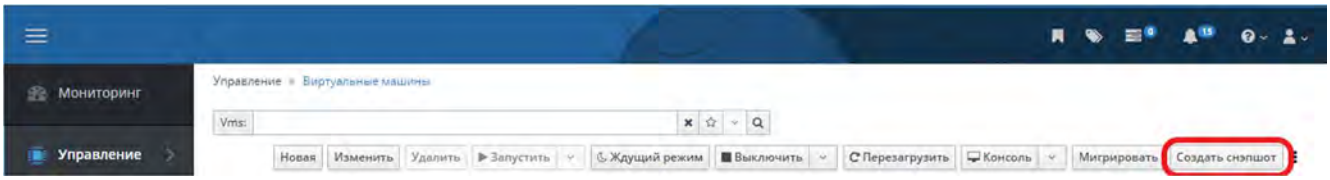


Рисунок 3.103 – «Создать снэпшот»

В форме «Создать снэпшот» оператору необходимо указать наименование снэпшота в поле «Описание» и установить флаг выбора напротив позиций, которые необходимо сохранить (Рисунок 3.104).

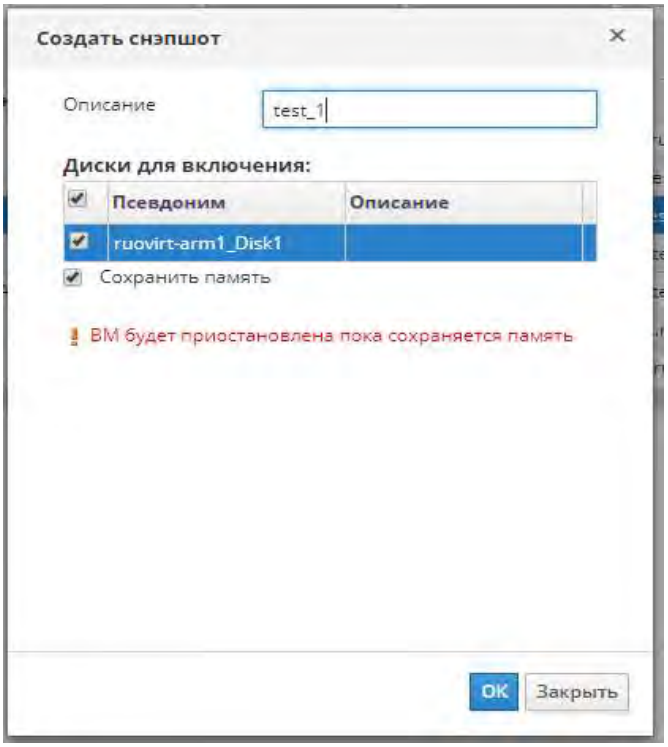


Рисунок 3.104 – форма «Создать снапшот»

– disk1;

– сохранить память.

Нажать кнопку «Ок», что приведет к запуску процесса создания снэпшота ВМ.

Для отслеживания статуса процесса создания снэпшота необходимо перейти в меню «События». В экранной форме поэтапно будет отображен процесс создания снэпшота (Рисунок 3.105).

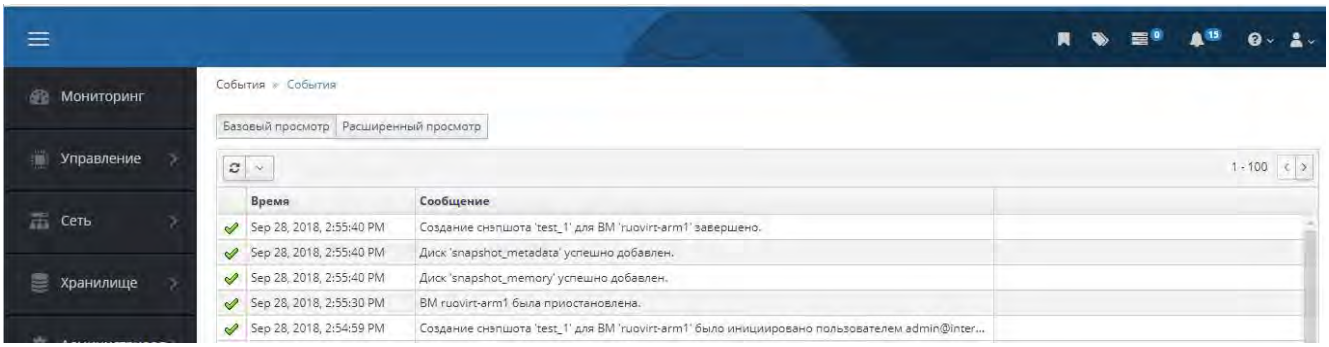


Рисунок 3.105 – Отображение событий

По завершению процесса отображается уведомление (Рисунок 3.106).

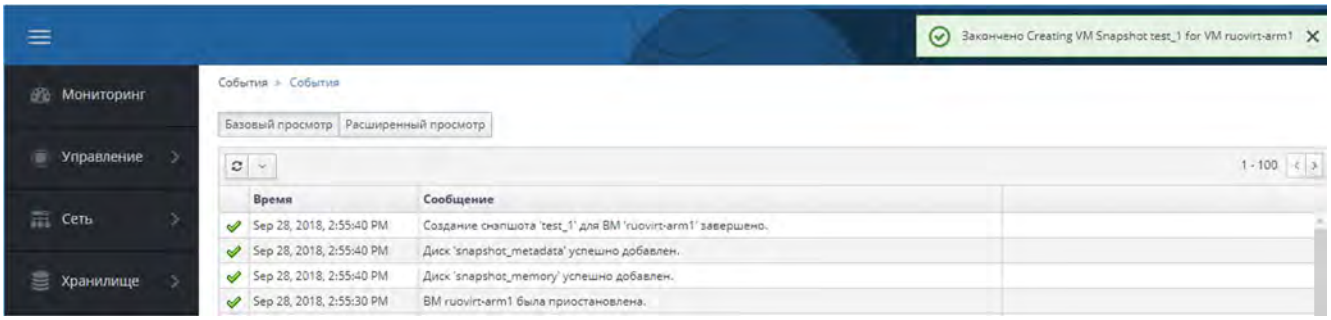


Рисунок 3.106 – Уведомление о завершении процесса

3.22.4. Настройка миграции ВМ между хостами серверов виртуализации

Для настройки миграции между хостами серверов виртуализации необходимо выполнить следующие этапы:

– добавление правил в межсетевой экран;

– добавление гипервизора в менеджер ВМ;

– изменение / настройка конфигурации ВМ.

Правила межсетевого экрана добавляются на том сервере виртуализации, котором создано хранилище на базе NFS.

Для добавления правил выполнить следующие команды:

```
firewall-cmd --permanent --add-service=nfs
```

```
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

Для добавления гипервизора в менеджер ВМ нужно перейти в веб-интерфейс портала администрирования менеджера ВМ и авторизоваться. В меню навигации выбрать «Управление», «Хосты». В разделе «Хосты» нажать на кнопку «Новый». В рабочей области отобразится форма добавления нового хоста (Рисунок 3.107), в которой необходимо добавить следующие параметры в подразделе «Общее»:

– «Узел кластера» - по умолчанию стоит значение «Default»;

– «Имя» - наименование добавляемого гипервизора, данное имя будет выводится в список хостов;

– «Имя хоста» - IP-адрес добавляемого гипервизора;

– «Пароль» - указывается пароль суперпользователя (root).

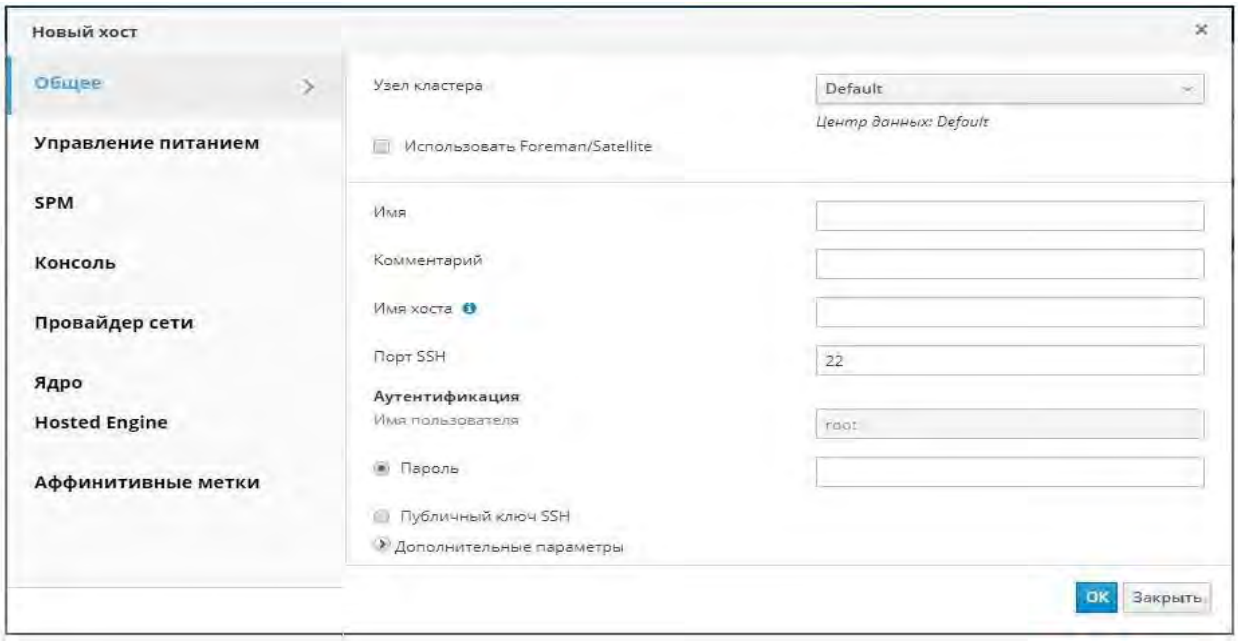


Рисунок 3.107 – Форма добавления нового хоста

В подразделе «Hosted Engine» (Рисунок 3.108) в выпадающем списке поля «Выберите действие развёртывания Hosted Engine» установить значение «Развернуть».

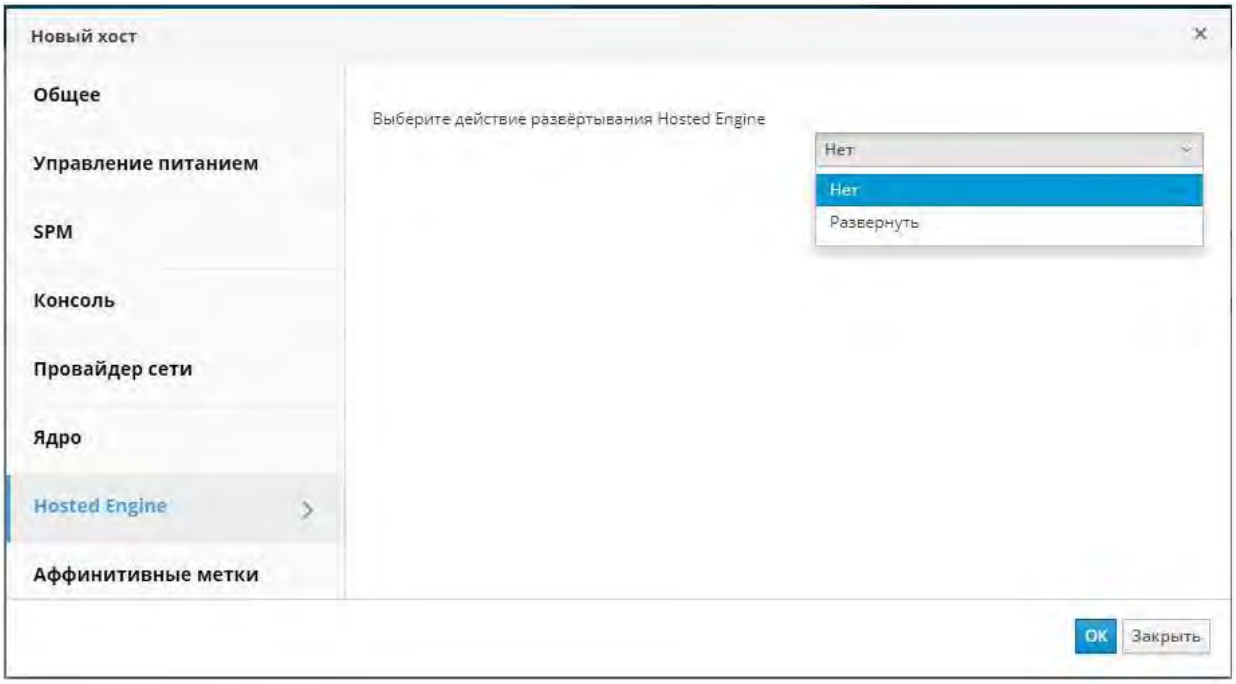


Рисунок 3.108 – Форма добавления нового хоста (Hosted Engine)

После внесенных параметров нажать кнопку «ОК».

Система выдаст предупреждение о ненастроенном управлении питанием, нажать кнопку «ОК» (Рисунок 3.109).

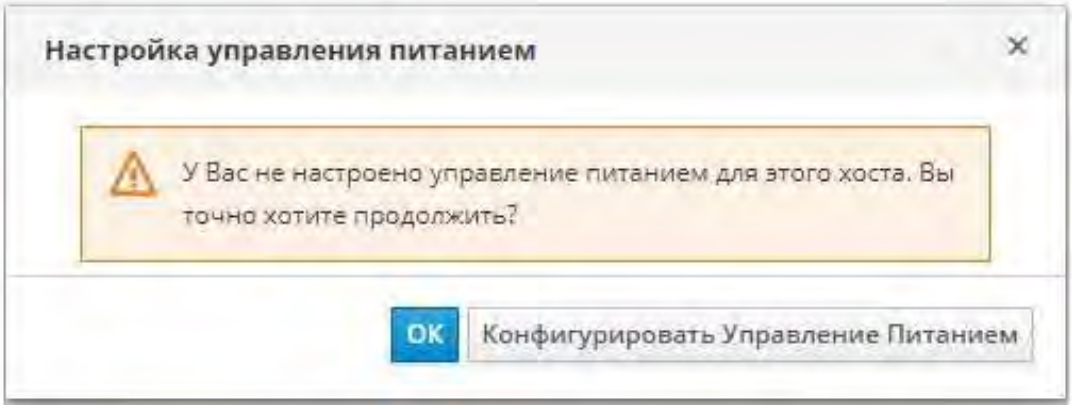


Рисунок 3.109 – Предупреждение настройки управления питанием

После успешного добавления сервера виртуализации, данные по хосту появятся в меню «Хосты».

Примечание: миграция в режиме реального времени не поддерживается в случае использования в качестве сетевого хранилища образов виртуальных машин NFS v4.2.

3.23.Настройка локальной парольной политики

За применение и настройку локальных парольных политик. Отвечают модули pam_cracklib.so и pam_pwquality.so. Библиотека pam_pwquality.so использует библиотеку cracklib и её словари для проверки и генерации пароля подходящих под парольную политику. Первоначально код был основан на модуле pam_cracklib, и модуль обратно совместим со своими опциями.

Модули обеспечивают проверку качества пароля. В первоначальной стадии только разбирает передаваемые в модуль параметры (функция _pam_parse) и возвращает PAM_SUCCESS.

Настройка локальной парольной политики заключается в редактировании конфигурационных файлов PAM (добавлении модулей pam_cracklib.so или pam_pwquality.so при их отсутствии) и задании необходимых параметров. Перечень параметров представлен в таблице 3.37.

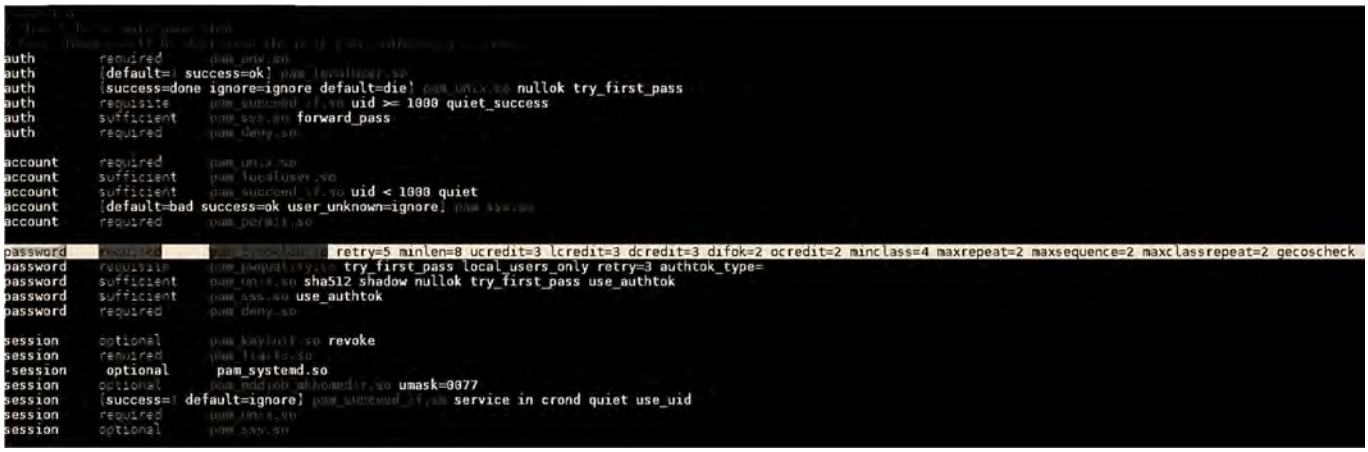


Рисунок 3.110

Например:

```
sudo vim /etc/pam.d/system-auth
```

```
password required pam_cracklib.so retry=5 minlen=8 ucredit=3
lcredit=3 dcredit=3 difok=2 ocredit=2 minclass=4 maxrepeat=2
maxsequence=2 maxclassrepeat=2 gecoscheck
```

, где «minlen=8» - минимальная длина для пароля учетной записи установлена 8 символов,

«ucredit=3» - максимальное разрешенное число использования символов верхнего регистра,

«lcredit=3» - максимальное разрешенное число использования символов нижнего регистра,

«dcredit=3» - максимальное разрешенное число использования цифр,

«difok=2» - сколько символов может быть такими же как в старом пароле,

«ocredit=2» - максимальное разрешенное число использования символов (не букв и не цифр),

«minclass=4» - минимальное количество обязательных классов символов для нового пароля (четыре класса - это цифры, верхние и нижние буквы и другие символы),

«maxrepeat=2» - максимальное количество разрешенных последовательных одинаковых символов в новом пароле (например, 11111),

«maxsequence=2» - отклонить пароли, если в строке более N символов верхнего и нижнего регистра или цифр (остановить пароли, такие как «QWERTY» или «12345»),

«maxclassrepeat=2» - максимальное количество разрешенных последовательных символов одного и того же класса в новом пароле (серии знаков препинания ("! @ # $%") также отклоняются),

«gecoscheck» - не позволяйте ни одному из слов в поле «полное имя» (GECOS) пользователя из / etc / passwd использовать его при выборе пароля.

Таблица 3.37 – Параметры pam_pwquality

Библиотека	Входящие параметры	Описание
pam_pwquality.so	debug	Включение режима откладки модуля. Информационные сообщения направляются в syslog.
	authtok_type=XXX	Создание подсказки для пароля. New XXX password: " and "Retype XXX password: ".

	retry=N	Запросить пароль у пользователя не более N раз перед возвратом с ошибкой. По умолчанию используется значение 1.
	difok	Количество символов в новом пароле, который не должен присутствовать в старом пароле. По умолчанию 5.
	minlen	Минимальный допустимый размер для нового пароля. Нельзя установить более низкое значение, чем 6. * нужно иметь в виду что опции dcredit, lcredit, ucredit, ocredit могут фактически увеличивать эту величину
	dcredit	если N>=0, определяет максимальный кредит минимально допустимой длины нового пароля, выделенный на включение в пароль цифр (N первых цифр не будут учитываться при сравнивании длины пароля с минимально допустимой; по умолчанию это значение 1); если N<0, определяет минимально допустимое количество цифр в новом пароле;
	ucredit	если N>=0, определяет максимальный кредит минимально допустимой длины нового пароля, выделенный на включение в пароль букв в верхнем регистре (N первое количество букв в верхнем регистре не будут учитываться при сравнивании длины пароля с минимально допустимой; по умолчанию это значение 1); если N<0, определяет минимально допустимое количество букв в верхнем регистре в новом пароле;
	lcredit	если N>=0, определяет максимальный кредит минимально допустимой длины нового пароля, выделенный на включение в пароль букв в нижнем регистре (N первых букв в нижнем регистре не будут учитываться при сравнивании длины пароля с минимально допустимой; по умолчанию это значение 1); если N<0, определяет минимально допустимое количество

		букв в нижнем регистре в новом пароле;
	ocredit	если N>=0, определяет максимальный кредит минимально допустимой длины нового пароля, выделенный на включение в пароль других символов (N первых таких символов не будут учитываться при сравнивании длины пароля с минимально допустимой; по умолчанию это значение 1); если N<0, определяет минимально допустимое количество других символов в новом пароле (по умолчанию это ограничение не накладывается).
	minclass	Минимальное количество обязательных классов символов для нового пароля. Номер по умолчанию равен нулю. Четыре класса - это цифры, верхние и нижние буквы и другие символы.
	maxrepeat	Отклонить пароли, содержащие более N одинаковых последовательных символов. Значение по умолчанию равно 0, что означает, что эта проверка отключена. ***static int consecutive(pwquality_settings_t *pwq, const char *new, void **auxerror)***
	maxsequence	Отклонить пароли, содержащие монотонные последовательности символов больше N. Значение по умолчанию равно 0, что означает, что эта проверка отключена. Примерами такой последовательности являются «12345» или «fedcb». ***static int sequence(pwquality_settings_t *pwq, const char *new, void **auxerror)***
	maxclassrepeat	Отклонить пароли, содержащие более N последовательных символов одного и того же класса. Значение по умолчанию равно 0, что означает, что эта проверка отключена.
	gecoscheck	Если отличное от нуля, проверьте, содержатся ли в новом пароле

		отдельные слова длиной более 3 символов из поля пользователя GECOS которое содержится в файле /etc/passwd. Значение по умолчанию равно 0, что означает, что эта проверка отключена. ***static int gecoscheck(pwquality_settings_t *pwq, const char *new, const char *user)***
	badwords = <список слов>	Слова, длиной более 3 символов, из этого списка, разделенного пробелами, индивидуально искажаются и запрещаются в новом пароле. По умолчанию список пуст, что означает, что эта проверка отключена.
	enforce_for_root	Модуль вернет ошибку при неудачной проверке, даже если пользователь, изменяющий пароль, является root. Эта опция отключена по умолчанию
	local_users_only	Модуль не будет проверять качество пароля для пользователей, которых нет в файле /etc/passwd
	use_authtok	Этот аргумент используется, чтобы заставить модуль не запрашивать у пользователя новый пароль, но использовать тот, который предоставляется ранее уложенным модулем пароля.
	dictpath=*/path/to/dict*	Путь к словарям cracklib

Несмотря на то, что параметр «minlen» задает минимальную длину пароля, длина фактического пароля пользователя может отличаться в меньшую сторону. Это связано с тем, что pam_pwquality.so объединяет понятие длины пароля с понятием «стойкость» (использование смешанных и небуквенных символов). Параметр «minlen» в данном случае является минимальной требуемой длиной для пароля, состоящего из всех строчных букв, при этом пользователи получают «кредиты» при использовании в паролях букв верхнего и нижнего регистра, цифр и не буквенно-цифровых символов.

По умолчанию пользователи получают максимум 1 кредит для каждого класса символов (цифры, верхние и нижние буквы и другие символы.). Поэтому, если

локальный администратор устанавливает «minlen = 12», пользователь может по-прежнему иметь пароль с 8 символами, если они используют все четыре класса символов.

Максимальный кредит для любого конкретного класса символов фактически настраивается. Четыре параметра «lcredit», «ucredit», «dcredit» и «ocredit» используются для установки максимального кредита для строчных, строчных, числовых (цифровых) и не буквенно-цифровых (других) символов, соответственно.

Помимо использования «кредитов» также можно использовать отрицательные значения для «lcredit», «ucredit», «dcredit» и «ocredit». Отрицательные значения заставляют пользователя использовать определенное количество символов каждого типа. Например, «ocredit = -2» потребует, чтобы все пользователи имели в своих паролях по меньшей мере два не-алфавитно-цифровых символа.

Для добавления сигнализации о истечении срока действия пароля необходимо настроить базу dlogevent /etc/dlogevent/init.sqlite, а также конфигурационный файл «/etc/rsyslog.d/rsyslog-mail.conf».

Для настройки событий в БД, в приложении «Терминал среды MATE» выполнить команду (для входа в БД):

```
sqlite3 /etc/dlogevent/init.sqlite;
```

Далее выполнить настройку, следующими командами:

```
insert into sec_events_table (id, syslog_tag, message, requred_event, output_to, security_event, event_tag, action, UUID, enabled) values (300,'login','.*expired password for user {user} .*','',3,'[{UUID}] Истёк срок действия пароля пользователя. Имя: {user}','PASS_EXPIRED_LOGIN','PASS_EXPIRED','d1da3012-157f-4d1d-9f1e-801feafd6bcf',1);
insert into sec_events_table (id, syslog_tag, message, requred_event, output_to, security_event, event_tag, action, UUID, enabled) values (301,'login','.* account {user} has expired .*','',3,'[{UUID}] Идентификация пользователя с истёкшим сроком действия. Имя: {user}','USER_EXPIRED_LOGIN','USER_EXPIRED','fee2911f-494e-42a7-9e54-8cf75e66aa4e',1);
```

Выполнить выход из БД:

```
.q
```

Далее поочередно выполнить следующие команды:

```
service dlogevent restart
service rsyslog restart
```

Для отображения событий безопасности в виде сообщений с использованием утилиты «mail» необходимо добавить идентификатор события в конфигурационный файл «/etc/rsyslog.d/rsyslog-mail.conf»:

- выполнить «`vim /etc/rsyslog.d/rsyslog-mail.conf`»;
- нажатием клавиши «`insert`» выполнить переход в режим ввода.
- в каждую из директорий «if ($programname == "dlogevent") then» добавить следующие идентификаторы событий, при их отсутствии:

```
‘be681734-bc1a-4c29-bea2-ceabab559b6f’,
‘0019fb58-ebb7-431e-a2b9-0e4adb17de76’,
‘dce7fb07-83c6-4af6-8214-7701c3bd01b3’,
‘22485898-4849-4fad-ba63-22f1ce789222’,
‘659d760c-03bb-43ed-b924-b3cae27d775b’,
‘1822a0a3-2e0d-4399-9739-6c6cb1ab188c’,
‘d1da3012-157f-4d1d-9f1e-801feafd6bcf’,
‘fee2911f-494e-42a7-9e54-8cf75e66aa4e’
```

Соответствие идентификаторов событий безопасности произошедшим действиям в системе представлено в Таблице 2.26 «Базового модульного проекта».

Далее комбинацией клавиш «`Shift+:`» перейти в командный режим, выполнить «`wq!`». Далее нажатием «`Enter`» завершить сохранение внесенных изменений.

3.24.Настройка параметров затирания объектов файловой системы

Параметры затирания объектов файловой системы задаются в строке 18 файла /usr/bin/shred_wrapper.

```
«  _shred="/usr/bin/shred -f -u -z "+ absfile»
```

Для возможности задания параметров необходимо чтобы в ОС был установлен пакет pszi-shred.

Примечание: для ОС в варианте установки клиентская операционная система пакет pszi-shred присутствует по умолчанию.

Для установки недостающего пакета необходимо скопировать iso-файл дистрибутива КП «ЗОС «СинтезМ» и примонтировать его в директорию /mnt. Копирование iso-файла осуществляется командой scp:

```
scp [путь до iso-образа дистрибутива] root@[ip-адрес куда копируется дистрибутив]:/[путь до директории для сохранения]
```

Например:

```
scp sintez-m-7-x86_64.iso root@10.10.10.50:~
```

Монтирование iso-файла выполняется командой

```
mount sintez-m-7.x86_64.iso /mnt
```

После того как iso-файл примонтирован, необходимо установить пакет pszi-shred-0.1-11.el7.sz.x86_64.rpm

```
rpm -ihv --noscripts --nodeps /mnt/Packages/pszi-shred-0.1-11.el7.sz.x86_64.rpm
```

Для задания параметров затирания объектов файловой системы необходимо отредактировать файл /usr/bin/shred_wrapper задав в строке 18 необходимые параметры в формате:

```
«  _shred="/usr/bin/shred [перечень параметров]"+ absfile»
```

Например

```
_shred="/usr/bin/shred -fuz -n 10"+ absfile
```

Перечень возможных параметров представлен в таблице 3.38.

Таблица 3.38 – Перечень параметров утилиты shred

№	Параметр	Описание
1.	-f	изменить права для разрешения записи, если необходимо
2.	-n N	переписать N раз
3.	-s N	очистить N байт (возможны суффиксы вида K, M, G)
4.	-u	обрезать и удалить файл после перезаписи

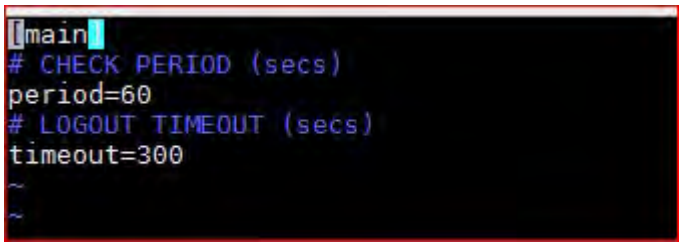
№	Параметр	Описание
5.	-x	не округлять размеры файлов до следующего целого блока; по умолчанию для нерегулярных файлов
6.	-z	перезаписать в конце с нулями, чтобы скрыть перемешивание

3.25.Настройка параметров автоматического завершения сессии

Параметры автоматического завершения сессии пользователя при бездействии задаются в конфигурационном файле /etc/autologout/autologout.conf. В данном конфигурационном файле задаются два параметра:

— параметр Period, задает промежуток времени в секундах через который служба autologout будет проверять бездействие пользователя;

— параметр timeout задет промежуток времени в секундах по истечении которого сессия пользователя будет закрыта.



После изменения значений конфигурационного файла, для применения изменений необходимо перезапустить службу autologout командой:

```
systemctl restart autologout
```

3.26.Конфигурация аудита безопасности веб-сервера nginx

При использовании nginx необходимо провести его дополнительное конфигурирование:

1) Ограничение доступа к каталогам и файлам NGINX.

Для настройки ограничения доступа к каталогам и файлам NGINX необходимо выполнить команды:

```
# find /etc/nginx -type d | xargs chmod 750
# find /etc/nginx -type f | xargs chmod 640
```

2) Установка тайм-аута keep-alive

Для задания парметра keepalive_timeout необходимо выполнить команду:

```
#    sed    -i    's/keepalive_timeout\    *65/keepalive_timeout    10/g'
/etc/nginx/nginx.conf /etc/nginx/nginx.conf.default
```

3) Скрытие информации о NGINX в файлах по умолчанию/

Для настройки необходимо выполнить команды:

```
# sed -i 's/NGINX//g' /usr/share/nginx/html/*.html
# sed -i 's/nginx//g' /usr/share/nginx/html/*.html
# sed -i 's/Nginx//g' /usr/share/nginx/html/*.html
```

4) Отключение скрытых файлов

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку (рисунок 3.111):

```
location ~ /\. { deny all; return 404; }
```

Рисунок 3.111 – Настрйока NGINX

5) Запрет на использование символических ссылок

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
disable_symlinks on;
```

6) Настройка заголовка X-Frame-Options

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
add_header X-Frame-Options "SAMEORIGIN";
```

7) Настройка заголовка X-Content-Type-Options

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
add_header X-Content-Type-Options "nosniff";
```

8) Настройка заголовка X-XSS-Protection

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
add_header X-XSS-Protection "1; mode=block";
```

9) Настройка политики Защиты Контента (CSP)

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
add_header Content-Security-Policy "default-src 'self'";
```

10) Настройка Referrer-Policy

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
add_header Referrer-Policy "no-referrer";
```

11) Настройка времени ожидания header и body

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующие строки:

```
client_body_timeout 10;
client_header_timeout 10;
```

12) Настройка Максимального размера тела запроса

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующие строки:

```
client_max_body_size 100K
```

13) Настройка Максимального числа и размера буферов для URI

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующие строки:

```
large_client_header_buffers 2 1k
```

14) Настройка количества подключений на IP-адрес

Для настройки необходимо:

— добавить в секцию http конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
limit_conn_zone $binary_remote_addr zone=limitperip:10m;
```

— добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
limit_conn limitperip 10;
```

15) Настройка ограничения скорости по IP-адресу

Для настройки необходимо:

— добавить в секцию http конфигурационного файла /etc/nginx/nginx.conf следующую строку:

```
limit_req_zone $binary_remote_addr zone=ratelimit:10m rate=5r/s;
```

— добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующие строки:

```
location / {
limit_req zone=ratelimit burst=10 nodelay;}
```

16) Настройка ограничения доступа по IP-адресам

Для настройки необходимо добавить в секцию server конфигурационного файла /etc/nginx/nginx.conf следующие строки:

```
location / {
allow [ip-адрес];
deny all;
}
```

17) Настройка перенаправления на HTTPS

Для настройки необходимо отредактировать nginx.conf, чтобы все незашифрованные порты, такие как порт 80, перенаправить на HTTPS через директиву return (company_host.com используется в качестве примера имени сервера).

```
server { listen 80; server_name company_host.com; return 301 https://$host$request_uri; }
```

18) Настройка доверенного сертификат

Отредактировать nginx.conf, чтобы использовать директивы ssl_certificate и ssl_certificate_key для веб-сервера, как показано ниже:

```
server {
listen 443 ssl http2;
listen [::]:443 ssl http2;
ssl_certificate /etc/nginx/cert.crt;
ssl_certificate_key /etc/nginx/nginx.key;
...
}
```

19) Настройка доступ к файлу закрытого ключа

Для настройки необходимо выполнить следующую команду:

```
chmod 400 /etc/nginx/nginx.key
```

20) Настройка использования только современных протоколов TLS

Для настройки необходимо выполнить следующую команду, чтобы изменить ssl_protocols, если они уже настроены:

```
sed -i "s/ssl_protocols[^;]*;/ssl_protocols TLSv1.2 TLSv1.3;/"
/etc/nginx/nginx.conf
```

Если ssl_protocols еще не настроены, это необходимо сделать вручную, открыв файл конфигурации и добавив директивы: server { ssl_protocols TLSv1.2 TLSv1.3; }

21) Настройка приоритета применения криптоалгоритмов

Для настройки необходимо отредактировать nginx.conf и добавив следующую строку:

```
ssl_prefer_server_ciphers on;
```

22) Настройка параметров Диффи-Хеллмана

Для настройки необходимо:

— сгенерировать стойкие DHE (Ephemeral Diffie-Hellman) параметры, используя следующие команды:

```
# mkdir /etc/nginx/ssl
# openssl dhparam -out /etc/nginx/ssl/dhparam.pem 2048
# chmod 400 /etc/nginx/ssl/dhparam.pem
```

— изменить конфигурацию сервера (nginx.conf):

```
http {
```

```
server {
ssl_dhparam /etc/nginx/ssl/dhparam.pem;
}
}
```

23) Настройка Online Certificate Status Protocol (OCSP)

Для настройки необходимо добавить директивы ssl_stapling и ssl_stapling_verify в файл конфигурации (nginx.conf):

```
server {
ssl_stapling on;
ssl_stapling_verify on;
}
```

24) Настройка HTTP Strict Transport Security (HSTS)

Для настройки необходимо убедиться, что приведенный ниже фрагмент кода можно найти в конфигурации для вашего сервера. Это гарантирует, что заголовок HSTS установлен со сроком действия шесть месяцев или 15768000 секунд.

```
server {
add_header Strict-Transport-Security "max-age=15768000;";
}
```

25) Настройка HTTP Public Key Pinning

Для настройки необходимо вставить хеш SHA-256 своего сертификата в конфигурацию сервера:

```
add_header Public-Key-Pins 'pinsha256="base64+primary==[хэш основного сертификата]";
pinsha256="base64+backup====[хэш запасного сертификата]";
maxage=5184000;
```

26) Настройка Perfect forward secrecy (PFS)

Для настройки необходимо добавить параметр в файл конфигурации (nginx.conf):

```
ssl_session_tickets off;
```

27) Настройка HTTP/2.0

Для настройки необходимо добавить параметр http2 в секцию server файла конфигурации:

```
server { listen 443 ssl http2; }
```

28) Настройка ведения журнала ошибок веб-сервера (error_log)

Для настройки необходимо отредактировать nginx.conf добавив в секцию http следующую строку:

```
error_log /var/log/nginx/error.log info;
```

29) Настройка ротации файлов журнала

Для настройки необходимо:

— изменить сжатие журнала с ежедневного на еженедельное выполнив команду:

```
# sed -i "s/daily/weekly/" /etc/logrotate.d/nginx
```

— изменить ротацию журнала с каждого года на каждые 13 недель выполнив команду:

```
# sed -i "s/rotate 52/rotate 13/" /etc/logrotate.d/nginx
```

3.27.Конфигурация аудита безопасности Apache HTTP Server

При использовании Apache HTTP Server необходимо провести его дополнительное конфигурирование:

1) Настройка индексов каталогов

Для настройки необходимо отключить возможность просматривать каталог указав в файле конфигураций (по умолчанию /etc/httpd/conf/httpd.conf) опцию -Indexes в директиве Options:

```
<Directory /var/www/html>
Options -Indexes
</Directory>
```

2) Настройка разрешенных методов HTTP-запросов

Для настройки необходимо запретить все методы кроме стандартных, ограничив их только реально необходимыми (GET, HEAD, POST), и разрешать остальные только для приложений, которым они нужны, для чего в файле

конфигураций (по умолчанию /etc/httpd/conf/httpd.conf) вставить в корневую секцию Directory:

```
<Directory />
<LimitExcept GET POST HEAD>
deny from all
</LimitExcept>
</Directory>
```

3) Настройка интерфейса CGI

Для настройки необходимо запретить (и разрешать только если необходимо) в файле конфигураций (по умолчанию /etc/httpd/conf/httpd.conf) директиву Options -ExecCGI

```
<Directory / >
Options -ExecCGI
</Directory>
```

4) Настройка использования символических ссылок

Для настройки необходимо запретить использование символических ссылок вставив в файле конфигураций (по умолчанию /etc/httpd/conf/httpd.conf) директиву Options –FollowSymLinks

```
<Directory / >
Options –FollowSymLinks
</Directory>
```

4. РЕГЛАМЕНТ ОБНОВЛЕНИЯ

4.1. Типы обновлений

В жизненном цикле КП «ЗОС «СинтезМ» предусмотрены следующие типы выпускаемых обновлений:

1) пакет обновления ОО – обновленная версия ОО с добавлением новых функциональных возможностей;

2) патч – исправление недостатков в ОО или пакете обновления ОО, выявленных на этапе эксплуатации изделия, выпускаемое по мере необходимости;

3) пакет модификаций – дистрибутив, содержащий все патчи, выпущенные за период после последней сертификации или инспекционного контроля. Выпускается в случае накопления большого количества патчей.

4.2. Оповещение потребителей о выпуске обновлений

Оповещение потребителей осуществляется инженерами Службы технической и сервисной поддержки разработчика. При формировании новой версии или обновления носитель передается инженеру Службы технической и сервисной поддержки разработчика. Потребителю направляется уведомление, что обновления готовы, и с ним согласуется способ их отправки и установки.

Разработчик ведет учет покупателей лицензии на дистрибутив ОО. Уведомление о выпуске обновлении программного обеспечения выполняется с использованием рассылки электронных почтовых сообщений с адреса электронной почты sintezm@fintech.ru.

Разработчик формирует документ с описанием обновления и отправляет его совместно с обновлением потребителю. Данный документ содержит описание обновления, процедур получения и контроля целостности обновления, процедур тестирования, установки, применения и верификации.

4.3. Предоставление обновлений потребителям

На сайте www.fintech.ru предоставляется возможность получения информации о необходимых обновлениях с описанием устраненных недостатков. Пользователи изделия информируются по электронной почте о выпуске обновлений изделия и устраненных в новых версиях недостатках.

Доставка обновлений программного обеспечения ОО до потребителей может осуществляться:

− с использованием сетевых протоколов передачи данных, за счет загрузки обновлений с сайта АО «ФИНТЕХ» (далее - разработчик).

− на DVD-дисках, промаркированных в соответствии с техническими условиями ТАСП.62.01.12.000.005 93 01.

Обновления, успешно прошедшие контроль влияния на безопасность ОО, публикуются в закрытой части сайта разработчика. Для получения обновлений с сайта разработчика, потребителю необходимо пройти по ссылке указанной в письме сформированном сотрудником Службы технической и сервисной поддержки разработчика по факту появления обновления.

Доступ потребителей к закрытой части сайта осуществляется с использованием учетной записи и пароля.

На сайте www.fintech.ru предоставляется возможность получения необходимых обновлений с описанием устраненных недостатков.

4.4. Проверка подлинности и целостности обновлений

Для проверки подлинности и целостности обновлений, до применения, необходимо осуществить процедуры контроля целостности и проверки подписи обновления.

4.4.1. Проведение контроля целостности обновления

При получении обновлений на оптическом носителе подсчет и проверка контрольной суммы, получаемой согласно ГОСТ 28147-89, осуществляется на ПЭВМ с КП «ЗОС «СинтезМ» в следующей последовательности:

1) установить оптический диск в устройство для чтения дисков;

2) в приложении «magma» перейти во вкладку «Диски и ISO»

3) выбрать привод, в котором находится рассчитываемый диск (по умолчанию указан /dev/sr0);

4) выбрать директорию для сохранения текстового документа с результатом расчета директорий, для этого нажать кнопку «Выбрать» в строке «Выберите директорию для сохранения;

5) нажать на кнопку «Рассчитать КС диска»;

6) ожидать завершения работы программы подсчета контрольной суммы;

7) сравнить значение контрольной суммы, сохраненное в выбранной директории, со значением, поставляемым с обновлением.

Подсчет контрольной суммы с использованием программы «ФИКС-Unix 1.0» осуществляется на ПЭВМ, с КП «ЗОС «СинтезМ» и программой «ФИКС-Unix 1.0» (ufix), в следующей последовательности:

1) установить оптический диск в устройство для чтения дисков;

2) создать временную директорию для монтирования оптического диска командой:

```
# mkdir /tmp/template_d
```

3) примонтировать диск командой:

```
# mount –o loop /dev/sr0 /tmp/template_d;
```

4) создать директорию для временного хранения результатов:

```
# mkdir /root/$(date +%Y-%m-%d)-ks-iso
```

5) последовательно выполнить команды для подсчета контрольной суммы:

```
# ufix -jR /tmp/template_d/ > /root/$(date +%Y-%m-%d)-ks-
iso/list.txt
# ufix -e /root/$(date +%Y-%m-%d)-ks-iso/list.txt
# ufix -h /root/$(date +%Y-%m-%d)-ks-iso/list.prj
# ufix -lv /root/$(date +%Y-%m-%d)-ks-iso/list.prj > /root/$(date
+%Y-%m-%d)-ks-iso/list.ks
```

6) открыть в браузере полученный файл /root/$(date +%Y-%m-%d)/list.html

7) сравнить значение контрольной суммы (строка «ВСЕГО»), выданной на экран, со значением, поставляемым с обновлением;

8) отмонтировать диск командой:

```
# umount /tmp/template_d
```

Проверка осуществляется путем сравнения значения контрольной суммы, полученной в результате подсчета программным средством, указанным в формуляре на изделие ТАСП.62.01.12.000.005 30 01, с контрольными суммами дистрибутивов компонентов изделия, приведенными в формуляре ТАСП.62.01.12.000.005 30 01.

При поставке обновлений с использованием сетевых протоколов передачи данных процедура контроля целостности обновления обеспечивается путем сравнения значения контрольной суммы (КС) обновления, полученной в результате расчета программным средством, указанным в формуляре ТАСП.62.01.12.000.005 30 01, с КС обновления указанной в документе с описанием обновления.

В случае обнаружения несоответствий при проведении проверки обновления необходимо обратиться к производителю.

4.4.2. Проверка подписи

Проверка подписи осуществляется командой:

```
# /opt/cprocsp/bin/amd64/cryptcp -verify ./signed_file -detached ./sign
```

, где: signed_file – файл подпись которого проверяется;

sign – файл подписи.

Например:

```
# /opt/cprocsp/bin/amd64/cryptcp -verify ./UPDATE_31092020.7z -detached ./UPDATE_31092020.7z.sgn
```

В случае успешного завершения проверки подписи на экране отобразиться сообщение (Рисунок 4.1):

```
«Signature's verified.
[ErrorCode: 0x00000000]»
```

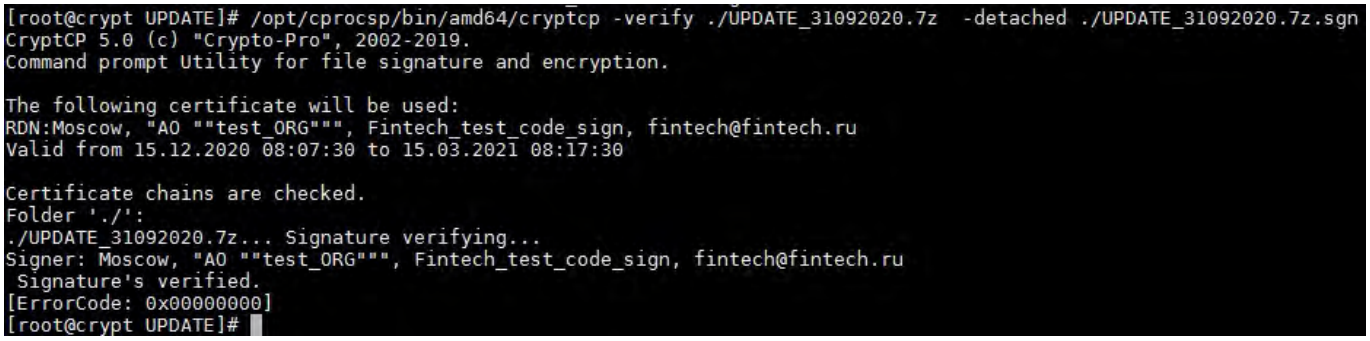


Рисунок 4.1 – Проверка подписи

В случае обнаружения внесения несанкционированных изменений в подписанный файл отобразиться сообщение (Рисунок 4.2):

```
«Error: Invalid Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:
748: 0x80090006
Error: Signature.
/dailybuildsbranches/CSP_5_0r0/CSPbuild/CSP/samples/CPCrypt/DSign.cpp:
863: 0x200001F9
[ErrorCode: 0x200001f9]»
```

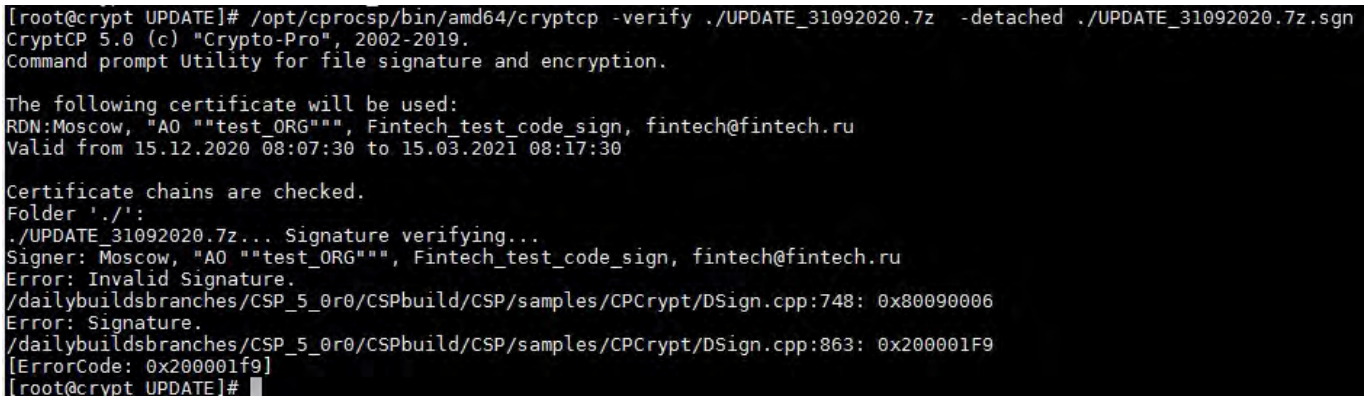


Рисунок 4.2 – Подпись не верна

4.5. Тестирование и отладка обновления

Тестирование и отладка обновления осуществляется в соответствии с п 2.4. документа «КП «ЗОС «СинтезМ» Документация по определению жизненного цикла (ТАСП.62.01.12.000.005 П1).

Проведение тестирования является обязательным перед передачей версии КП «ЗОС «СинтезМ» потребителю. Тестирование проводится сотрудниками отдела тестирования разработчика. Для тестирования и отладки программной продукции сотрудники отдела собирают стенд, выдается задание на тестирование. По результатам тестирования осуществляется устранение ошибок и осуществляется (при необходимости) доработка программного обеспечения.

Порядок проведения тестирования описан в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10»

4.6. Установки и применения обновления

В случае, если хост, на котором выполняется обновление программного обеспечения ОС является виртуальной машиной, до начала проведения обновления необходимо выполнить создание снимка (снапшота) виртуальной машины. Процедура создания снимков виртуальных машин описана в пункте 3.22.3. документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

В случае, если хост, на котором выполняется обновление программного обеспечения ОС является физическим АРМ или сервером, до начала проведения обновления необходимо выполнить создание резервных копий системных директорий операционной системы в соответствии с порядком описанным в п. 3.9.1 документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

Обновление ОО осуществляется в соответствии с порядком, описанным в документации поставляемой на обновление. Установка/обновление пакетов обновлений осуществляется менеджером пакетов yum в соответствии с порядком, описанным в п. 3.10.3. документа «КП «СинтезМ-ЗЭП» Руководство системного программиста (ТАСП.62.01.11.000.021 32 01)».

Инструкция по установке и применению обновления содержит следующую информацию:

- описание обновления;
- описание процедуры получения обновления;
- описание контроля целостности обновления;
- описание установки обновления;
- описание применения;
- описание процедур тестирования и верификации.

4.7. Контроль установки обновления

Для контроля установки обновления необходимо убедиться, что после установки обновления установленная версия обновляемых пакетов соответствует версии, указанной в документации на обновление.

Верификация применения обновления выполняется за счет тестирования каждой функция безопасности. Порядок проведения тестирования описан в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10».

4.8. Предоставление обновлений для внешнего контроля

Процедура предоставления обновлений для внешнего контроля включает следующие действия:

− разработчик и уполномоченная организация осуществляющая внешний контроль договариваются о форме предоставления обновления;

− разработчик предоставляет доступ к обновлениям в соответствии с выбранной формой представления;

− разработчик предоставляет доступ к программной и эксплуатационной документации на ОО, а также документации к обновлению.

Порядок проведения контроля указан в подразделе 2.2 документа «КП «ЗОС «СинтезМ» Свидетельство анализа влияния обновлений на безопасность ТАСП.62.01.12.000.005 Б9». Порядок проведения тестирования при внешнем контроле соответствует порядку представленном в документе «КП «ЗОС «СинтезМ» Тестовая документация ТАСП.62.01.12.000.005 Б10».

Результаты тестирования обновлений оформляются организацией, осуществляющей внешний контроль, в виде отчета и предоставляются разработчику. Разработчиком, на сайте разработчика, осуществляется публикация отчета или выписки из него содержащей результаты тестирования обновлений.

Состав Отчета о проведении анализа влияния обновлений на функции безопасности Операционной системы «СинтезМ-К» представлен в пункте 3 документа «КП «ЗОС «СинтезМ» Процедуры устранения недостатков».

5. ПРОВЕРКА ПРОГРАММЫ

Проверка работоспособности платформы КП «ЗОС «СинтезМ»

5.1. Проверка работоспособности сервера виртуализации

После загрузки КП «ЗОС «СинтезМ» на сервере виртуализации должно отобразиться приглашение для входа:

```
OS SintezM-K
localhost login:
```

Для проверки работоспособности функции гипервизора на сервере виртуализации необходимо проверить состояние служб vdsmd и libvirtd:

```
# systemctl status vdsmd
● vdsmd.service - Virtual Desktop Server Manager
   Loaded: loaded (/usr/lib/systemd/system/vdsmd.service; enabled;
vendor preset: enabled)
   Active: active (running) since Tue 2018-08-28 10:00:16 MSK; 1 day 6h
ago
 Main PID: 2368 (vdsmd)
# systemctl status libvirtd
● libvirtd.service - Virtualization daemon
   Loaded: loaded (/usr/lib/systemd/system/libvirtd.service; enabled;
vendor preset: enabled)
  Drop-In: /etc/systemd/system/libvirtd.service.d
           └─ unlimited-core.conf
   Active: active (running) since Tue 2018-08-28 09:59:55 MSK; 1 day 6h
ago
```

Состояние служб должно быть active (running).

Для проверки работоспособности режима Self Hosted Engine необходимо проверить состояние служб ovirt-ha-agent и ovirt-ha-broker, а также состояние виртуальной машины менеджера ВМ:

```
# systemctl status ovirt-ha-agent.service ovirt-ha-broker.service
● ovirt-ha-agent.service - oVirt Hosted Engine High Availability
Monitoring Agent
   Loaded: loaded (/usr/lib/systemd/system/ovirt-ha-agent.service;
enabled; vendor preset: disabled)
   Active: active (running) since Tue 2018-08-28 10:03:24 MSK; 1 day 6h
ago
 Main PID: 3189 (ovirt-ha-agent)
```

```
…
● ovirt-ha-broker.service - oVirt Hosted Engine High Availability
Communications Broker
   Loaded: loaded (/usr/lib/systemd/system/ovirt-ha-broker.service;
enabled; vendor preset: disabled)
   Active: active (running) since Tue 2018-08-28 10:02:39 MSK; 1 day 6h
ago
 Main PID: 2898 (ovirt-ha-broker)
...
```

Состояние служб должно быть active (running).

Проверка состояния виртуальной машины менеджера ВМ:

```
# hosted-engine --vm-status
--== Host 1 status ==--
conf_on_shared_storage             : True
Status up-to-date                  : True
Hostname                           : ruovirt-h.test.ru
Host ID                            : 1
Engine status                          : {"health": "good", "vm": "up",
"detail": "Up"}
…
        state=EngineUp
        stopped=False
```

Один из хостов должен иметь Engine status «Up».

5.2. Проверка работоспособности менеджера ВМ

На менеджере ВМ необходимо проверить состояние службы ovirt-engine:

```
# systemctl status ovirt-engine.service
● ovirt-engine.service - oVirt Engine
   Loaded:    loaded    (/usr/lib/systemd/system/ovirt-engine.service;
enabled; vendor preset: disabled)
   Active: active (running) since Thu 2018-08-30 14:31:35 MSK; 1 day 21h
ago
 …
```

Состояние службы должно быть active.

Также необходимо в браузере ввести URL: https://<IP менеджера ВМ>/, должен открыться веб-интерфейс менеджера ВМ (рисунок 5.1):

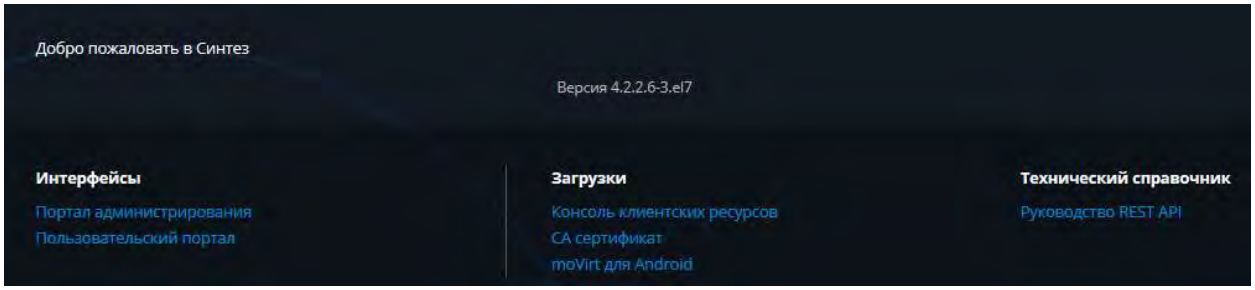


Рисунок 5.1 – Веб-интерфейс менеджера ВМ

При переходе в Портал администрирования либо в Пользовательский портал должна открыться форма аутентификации (рисунок 5.2):

Рисунок 5.2 – Форма аутентификации

5.3. Проверка работоспособности рабочей станции

После загрузки КП «ЗОС «СинтезМ» в варианте «Графический клиент» должен запуститься графический дисплейный менеджер с меню выбора пользователей. Если пользователи еще не созданы, необходимо нажать на кнопку «Нет в списке» после чего появится окно ввода имени пользователя (рисунок 5.3):

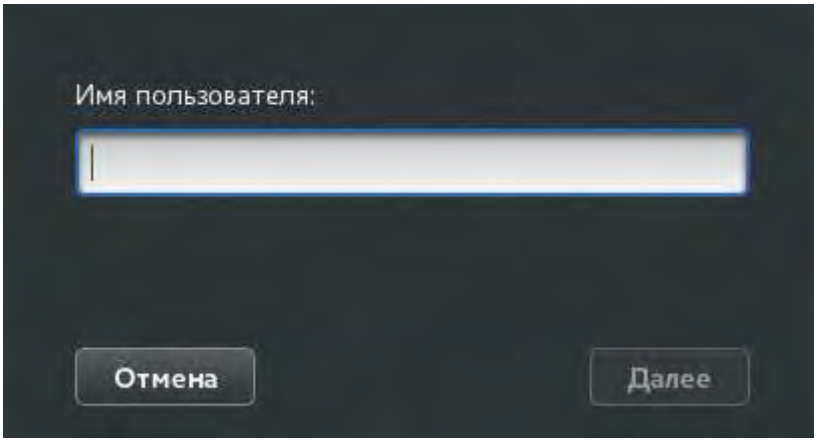


Рисунок 5.3 – Окно ввода имени пользователя

5.4. Проверка работоспособности сервера управления доступом

Для проверки работоспособности сервера управления доступом необходимо проверить состояние службы ipa:

```
# systemctl status ipa
```

● ipa.service - Identity, Policy, Audit

```
   Loaded: loaded (/usr/lib/systemd/system/ipa.service; enabled; vendor
preset: disabled)
   Active: active (exited) since Wed 2018-08-29 18:41:52 MSK; 2 days ago
  Process:   5093   ExecStart=/usr/sbin/ipactl   start   (code=exited,
status=0/SUCCESS)
      Main PID: 5093 (code=exited, status=0/SUCCESS)
        CGroup: /system.slice/ipa.service

Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting krb5kdc
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting kadmin
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting named Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting ipa_memcached
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting httpd Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting ipa-custodia
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting pki-tomcatd
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting ipa-otpd
Service
Aug 29 18:41:52 ruovirt-ipa.test.ru ipactl[5093]: Starting ipa-
dnskeysyncd Service
Aug 29 18:41:52 ruovirt-ipa.test.ru systemd[1]: Started Identity,
Policy, Audit.
```

Данный сервис является управляющим для следующего набора служб, непосредственно отвечающих за работу средства управления доменными пользователями:

```
krb5kdc, kadmin, named-pkcs11, ipa_memcached, httpd, ipa-custodia, pki-
tomcatd, ipa-otpd, ipa-dnskeysyncd.
```

Статус этих служб можно проверить следующей командой:

```
# for i in krb5kdc kadmin named-pkcs11 ipa_memcached httpd ipa-custodia
```

```
pki-tomcatd.target ipa-otpd.socket ipa-dnskeysyncd; do echo -n "$i";
systemctl status "$i" | grep Active; done
krb5kdc   Active: active (running) since Wed 2018-08-29 18:40:30 MSK; 2
days ago
kadmin   Active: active (running) since Wed 2018-08-29 18:35:43 MSK; 2
days ago
named-pkcs11   Active: active (running) since Wed 2018-08-29 18:41:09
MSK; 2 days ago
ipa_memcached   Active: active (running) since Wed 2018-08-29 18:36:00
MSK; 2 days ago
httpd   Active: active (running) since Wed 2018-08-29 18:41:22 MSK; 2
days ago
ipa-custodia   Active: active (running) since Wed 2018-08-29 18:36:06
MSK; 2 days ago
pki-tomcatd.target   Active: active since Wed 2018-08-29 18:41:52 MSK;
2 days ago
ipa-otpd.socket     Active: active (listening) since Wed 2018-08-29
18:36:02 MSK; 2 days ago
ipa-dnskeysyncd  Active: active (running) since Wed 2018-08-29 18:41:07
MSK; 2 days ago
```

5.5. Проверка работоспособности системных служб

Проверка работоспособности системных служб выполняется с помощью команды systemctl status <имя службы>. Для просмотра списка всех служб используется команда systemctl без параметров.

Например, чтобы проверить состояние сервиса синхронизации времени chronyd, необходимо ввести команду:

```
# systemctl status chronyd.service
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled;
vendor preset: enabled)

   Active: active (running) since Ср 2018-08-29 16:46:09 MSK; 2 days ago
 Main PID: 12783 (chronyd)
   CGroup: /system.slice/chronyd.service
           └─12783 /usr/sbin/chronyd
авг 29 16:46:09 ruovirt-h.test.ru systemd[1]: Starting NTP
client/server...
авг 29 16:46:09 ruovirt-h.test.ru chronyd[12783]: chronyd version 2.1.1
starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +DEBUG +ASYNCDNS +IPV6
+SECHASH)
авг 29 16:46:09 ruovirt-h.test.ru chronyd[12783]: Frequency -3.981 +/-
```

```
122.475 ppm read from /var/lib/chrony/drift
авг 29 16:46:09 ruovirt-h.test.ru systemd[1]: Started NTP client/server.
авг 29 16:46:13 ruovirt-h.test.ru chronyd[12783]: Selected source
10.0.1.117
```

В поле Active будет выведено текущее состояние службы. Также команда выведет последние сообщения из журнала для данной службы.

6. СООБЩЕНИЯ СИСТЕМНОМУ ПРОГРАММИСТУ

В таблице 6.1 представлены сообщения, которые может получить системный программист в ходе выполнения настройки, проверки программы. Описано содержание этих сообщений и действия системного программиста, которые необходимо предпринять по этим сообщениям.

Сообщения среды виртуализации доступны во вкладке «События» в портале администрирования средства управления средой виртуализации.

Таблица 6.1 – Сообщения системному программисту

Сообщение	Описание	Действие
ВМ <имя ВМ> запущена на хосте <имя хоста>	Информационное сообщение, сообщающее о запуске виртуальной машины	Действие не требуется
Invalid status on Data Center <имя датацентра>. Setting status to Non Responsive.	Сообщение информирует о проблемах в датацентре в среде виртуализации	Проверить состояние стореджей во вкладке Хранилище -> Домены. Проверить состояние серверов виртуализации во вкладке Управление _-> Хосты
Failed to check for available updates on host <имя хоста> with message 'Failed to run check-update of host …	Не удалось проверить наличие обновлений на сервере виртуализации	Действие не требуется
ВМ <имя ВМ> выключена.	Сообщение о выключении виртуальной машины	Проверить статус сообщения, было ли выключение ВМ инициировано администратором либо произошел сбой в работе ВМ
Внимание, мало места на диске. Домен <имя домена> имеет <число> GB/MB свободного места.	Заканчивается место в стореджe	Расширить место на стореджe; удалить неиспользуемые диски либо старые снимки систем если это возможно; добавить новый сторедж и перенести часть дисков на него
Не удалось получить доступ к хранилищу на хосте <имя хоста>	Сервер виртуализации не смог подключиться к стореджу	Открыть консоль сервера виртуализации, проанализировать файл журнала /var/log/messages. Проверить наличие сетевой доступности до системы хранения данных

Не удалось завершить создание ВМ	Произошла ошибка при создании ВМ	Проанализировать ошибки в списке Событий во время создания ВМ
Не удалось завершить создание снэпшота	Произошла ошибка при создании снимка ВМ	Проанализировать ошибки в списке Событий во время создания снимка
Не удалось запустить/завершить запуск ВМ	Произошла ошибка при запуске ВМ	Проанализировать ошибки в списке Событий во время запуска ВМ
Автоограничение для хоста <имя хоста> было запущено	Сработало управление по питанию для хоста	Проверить что хост был успешно перезагружен по питанию, виртуальные машины, работавшие на нем, запустились на других серверах
Миграция не удалась	Произошла ошибка при миграции виртуальной машины	Проанализировать ошибки в списке Событий во время миграции. Проверить что запущен SeLinux на серверах виртуализации. Проверить политику миграции в свойствах кластера, по умолчанию время, дающееся на процесс миграции, ограничено.
ВМ <имя ВМ> был установлен в статус Неизвестный	Произошел сбой в работе среды виртуализации	Проверить состояние серверов виртуализации, стореджей. Если сервер виртуализации был перезагружен, нажать в свойствах хоста кнопку «Подтвердить Узел был перезагружен»
ВМ <имя ВМ> была приостановлена из-за ошибки отсутствия места на хранилище	Закончилось место в сторедже	Освободить место на сторедже; расширить место на сторедже
ВМ <имя ВМ> была приостановлена из-за проблем ввода-вывода хранилища	Проблемы с подключение к стореджу	Проверить сетевую доступность к стореджу на сервере виртуализации
Установка хоста <имя хоста> провалилась	Произошла ошибка добавления сервера виртуализации в менеджер	Проанализировать файлы журналов /var/log/ovirt-engine на менеджере ВМ, /var/log/vdsm /var/log/messages на сервере виртуализации

В таблице 6.2 описаны наиболее часто встречающиеся проблемы и ошибки, возникающие при работе пользователя с интерфейсами.

Таблица 6.2 – Типовые ошибки

Текст сообщения	Тип ошибки	Действия пользователя

Учётная запись заблокирована как следствие неудачных попыток ввода пароля	Превышение числа попыток неправильного ввода пароля определённого локальным администратором	Локальный администратор должен разблокировать пользователя выполнив команду: sudo /sbin/pam_tally2 –user <username> --reset
Sorry that didn’t work. Please try again.	Попытка входа в систему в период времени, когда доступ запрещён	Локальный администратор должен изменить временной период, когда доступ запрещён
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пин-кода для смарткарты	Необходимо ввести правильный пин-код
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пароля	Необходимо ввести правильный пароль
Не сработало. Попробуйте ещё раз	Попытка осуществить авторизацию несуществующим локальным пользователем	Необходимо использовать данные существующих локальных пользователей
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пин-кода для смарткарты	Необходимо ввести правильный пин-код
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пароля	Необходимо ввести правильный пароль
Не сработало. Попробуйте ещё раз	Попытка несанкционированного входа на ВМ (Пользователю не присвоен HBAC)	Обратитесь к доменному администратору для организации доступа к ВМ
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пин-кода для смарткарты	Необходимо ввести правильный пин-код
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пароля	Необходимо ввести правильный пароль
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пин-кода для смарткарты	Необходимо ввести правильный пин-код
Sorry that didn’t work. Please try again.	Попытка ввода неправильного пароля	Необходимо ввести правильный пароль
The username or password is incorrect	Попытка ввода неправильного пароля в web-интерфейсе Менеджера ВМ	Необходимо ввести правильный пароль
Unable to log in. Verify your information or contact the system administrator	Попытка авторизации на портале Менеджера ВМ несуществующим пользователем	Необходимо произвести авторизацию существующим пользователем
The user <username@domain> is not authorized to perform login	Попытка авторизации на портале Менеджера ВМ доменным пользователем, у которого нет прав	Системный администратор должен выдать права на авторизацию в портале Менеджера ВМ

Пароль или имя пользователя некорректные	Попытка ввода неправильных логина или пароля во время авторизации в средстве управления доменными пользователями	Необходимо ввести корректные учётные данные
Пользователь заблокирован	Попытка авторизации заблокированным пользователем в средстве управления доменными пользователями	Необходимо обратиться к доменному администратору для разблокирования пользователя
Пароли не совпадают	При смене пароля для пользователя введены несовпадающие новые пароли	Необходимо ввести одинаковые пароли в соответствующие поля
Слишком простой пароль: Пароль не прошёл проверку орфографии – слишком простой. Всё равно использовать?	При создании нового пользователя был введён слишком простой пароль.	Необходимо ввести пароль удовлетворяющий требованиям безопасности
Слишком простой пароль: Пароль не прошёл проверку орфографии – основан на слове из словаря. Всё равно использовать?	При создании нового пользователя был введён пароль, который может быть подобран по словарю	Необходимо ввести пароль удовлетворяющий требованиям безопасности
Слишком простой пароль: В пароле должно быть не менее 8 символов. Всё равно использовать?	При создании нового пользователя был введён пароль, длинна которого меньше заданной согласно требованиям безопасности	Необходимо ввести пароль удовлетворяющий требованиям безопасности
Срок действия учётной записи истек; обратитес…	Попытка входа в систему с учётной записью, у которой окончился срок действия	Необходимо обратиться к локальному администратору для изменения срока действия учётной записи
Время действия учётной записи истекло	Попытка входа в систему с учётной записью, у которой окончился срок действия	Необходимо обратиться к локальному администратору для изменения срока действия учётной записи
Не сработало. Попробуйте ещё раз	Совершена попытка входа в систему пользователем, у которого заблокирован локальный пароль	Необходимо обратиться к локальному администратору для разблокирования локального пароля
Пользователь заблокирован	Попытка авторизации заблокированным доменным пользователем в средстве управления доменными пользователями	Необходимо обратиться к доменному администратору для разблокирования пользователя
Unable to log in because the user account is disabled or locked. Contact the system administrator	Попытка авторизации заблокированным доменным	Необходимо обратиться к доменному администратору для

	пользователем на портале Менеджера ВМ	разблокирования пользователя
Не сработало. Попробуйте ещё раз	Попытка авторизации заблокированным доменным пользователем на АРМ Пользователя.	Необходимо обратиться к доменному администратору для разблокирования пользователя
The directory '/home/<username>' already exists. Please choose a new directory, or disable home directory creation	Попытка создания локального пользователя с указанием домашней директории другого локального пользователя	Необходимо указать уникальное имя домашней директории локального пользователя
Учётная запись с именем пользователя <username> уже существует	Попытка создать локального пользователя с именем существующего пользователя	Необходимо использовать уникальное имя пользователя
Идентификатор пользователя <UUID> уже используется	Попытка создания локального пользователя с UUID совпадающим с существующим	Необходимо создавать локального пользователя с уникальным UUID
I won't delete <username> home directory (/home/<username) for reason: - Каталог не существует или запись невозможна	Выполняется попытка удаления пользователя у которого отсутствует домашняя директория	В экранной форме с предупрежнением необходимо нажать «Да» для удаления пользователя
Вы не можете удалить пользователя <username> из его основной группы	Выполняется попытка удаления группы, у которой существет основной пользователь	Необходимо сперва удалит или перенести в другую группу основного пользователя группы удаляемой группы.
Локальная учётная запись заблокирована как следствие неудачных попыток ввода пароля	Превышение числа попыток неправильного ввода пароля определённого локальным администратором	Локальный администратор должен разблокировать пользователя
Не сработало. Попробуйте ещё раз	Совершена попытка входа в систему пользователем, у которого заблокирована локальная учётная запись	Необходимо обратиться к локальному администратору для разблокирования локальной учётной записи
Constrait violation: Password is too shot	Совершена попытка задать слишком короткий пароль доменного пользователя на Сервере-ИПА	Необходимо ввести пароль удовлетворяющий требованиям безопасности
Введённый пользователь заблокирован	Превышение числа попыток неправильного ввода пароля определённого доменным администратором на портале ИПА	Доменный администратор должен разблокировать пользователя в личной карточке пользователя на Сервер-ИПА
Unable to log in because the user account is disabled or locked. Contact the system administrator	Превышение числа попыток неправильного ввода пароля определённого доменным	Доменный администратор должен разблокировать пользователя в личной

	администратором на портале Менеджера ВМ	карточке пользователя на Сервер-ИПА
Не сработало. Попробуйте ещё раз	Превышение числа попыток неправильного ввода пароля определённого доменным администратором при авторизации на ВМ	Доменный администратор должен разблокировать пользователя в личной карточке пользователя на Сервер-ИПА
bash: /usr/sbin/<utilname>: Отказано в доступе	Произведена попытка выполнения утилиты <utilname> локальным непривилигированным пользователем	Данная утилита должна выполняться только пользователем имеющим административные права
<username> is not in the sudoers file. The incident will be reported	Локальным пользователем произведена попытка выполнения какой-либо команды с правами администратора	Необходимо обратиться к локальному администратору для настройки прав на выполнения команд
passwd: только root может выбирать имя учётной записи	Произведена попытка смены пароля непривилигированным локальным пользователем	Смена пароля пользователя должна производиться только локальным администратором
Authentication is required to run system-config-users	Требуется ввод пароля пользователя root для запуска утилиты	Необходимо использовать sudo для запуска утилиты
Error executing command as another user: Request dismiss	Вызов утилиты в консоле ВМ непривилигированным пользователем	
Ошибка ИПА 2100: ACIError Недостаточно прав для доступа: Insufficient access rights	Осуществлена несанкционированная попытка смены пароля пользователю (на Сервер-ИПА)	Смену пароля пользователя может осуществлять только доменный администратор
Ошибка ИПА 2100 ACIError Недостаточно прав для доступа: Insufficient 'write' privilege to the 'nsAccountLock' attribute of entry 'uid=user_td, cn=users,cn=accounts, dc=cbi, dc=local'.	Осуществлена несанкционированная попытка деактивации пользователя (на Сервер-ИПА)	Деактивировать пользователя может только доменный администратор
Ошибка ИПА 2100 ACIError Недостаточно прав для доступа: Insufficient 'delete' privilege to delete the entry 'uid=user_td, cn=users, cn=accounts, dc=cbi, dc=local'.	Осуществлена несанкционированная попытка удаления пользователя (на Сервер-ИПА)	Удалить пользователя может только доменный администратор
Ошибка ИПА 2100: ACIError Недостаточно прав для доступа: Insufficient 'moddn' privilege to move an entry to 'cn=deleted users, cn=accounts, cn=provisioning, dc=cbi, dc=local'.	Осуществлена несанкционированная попытка консервации пользователя (на Сервер-ИПА)	Законсервировать пользователя может только доменный администратор

Ошибка ИПА 2100: ACIError Недостаточно прав для доступа: Insufficient 'write' privilege to the 'krbLoginFailedCount' attribute of entry 'uid=user_td, cn=users, cn=accounts, dc=cbi, dc=local'.	Осуществлена несанкционированная попытка разблокирования пользователя (на Сервер-ИПА)	Разблокировать пользователя может только доменный администратор
Ошибка ИПА 2100: ACIError Недостаточно прав для доступа: Insufficient 'add' privilege to add the entry 'cn=automember rebuild membership, cn=tasks, cn=config'.	Осуществлена несанкционированная попытка перестроить записи автоматического участия (на Сервер-ИПА)	Перестроить записи автоматического участия может только доменный администратор
"/path/to/file" E212: Невозможно открыть файл для записи Нажмите ENTER или введите команду для продолжения	Осуществлена несанкционированная попытка изменить содержимое системного файла	Содержимое данных файлов может изменять только локальный администратор безопасности
<username> is not in the sudoers file. This incident will be reported.	Осуществлена несанкционированная попытка получить административные права для изменения системных файлов	
bash: /path/to/utilmane: Отказано в доступе	Осуществлена несанкционированная попытка запустить утилиту <utilname>	Данная утилита должна запускаться только локальным администратором безопасности
<username> is not in the sudoers file. This incident will be reported.	Осуществлена несанкционированная попытка получить административные права для изменения системных файлов	
iptables v1.4.21: can't initialize iptables table `filter': Permission denied (you must be root) Perhaps iptables or your kernel needs to be upgraded	Осуществлена попытка изменить правила iptables непривилигированным пользователем	Правила iptables должен изменять только локальный администратор безопасности
Problem getting a socket, you probably don't have the right permissions.	Осуществлена попытка изменить правила ebtables непривилигированным пользователем	Правила ebtables должен изменять только локальный администратор
bash: /path/to/utilmane: Отказано в доступе	Осуществлена несанкционированная попытка запустить утилиту <utilname>	Данная утилита должна запускаться только локальным администратором
"/etc/profile E212: Невозможно открыть файл для записи Нажмите ENTER или введите команду для продолжения	Осуществлена несанкционированная попытка изменить содержимое файла /etc/profile	Содержимое файла /etc/profile может изменять только локальный администратор

	непривилигированным пользователем	
"/etc/bashrc E212: Невозможно открыть файл для записи Нажмите ENTER или введите команду для продолжения	Осуществлена несанкционированная попытка изменить содержимое файла /etc/bashrc непривилигированным пользователем	Содержимое файла /etc/bashrc может изменять только локальный администратор
bash: /path/to/utilmane: Отказано в доступе	Осуществлена несанкционированная попытка запустить утилиту <utilname>	Данная утилита должна запускаться только локальным администратором
Попытка соединения не удалась <Browser> не может установить соединение с сервером <IP>.	На сервере безопасности не работает сервис nginx	Доменный администратор безопасности должен перезапустить сервис nginx командой systemctl restart nginx.service
В браузере отображается пустой интерфейс портала сервера безопасности без каких-либо данных	На сервере безопасности не работает сервис sbuwsgi	Доменный администратор безопасности должен перезапустить сервис sbuwsgi командой systemctl restart sbuwsgi.service
На портале сервера безопасности продолжительное время не регистрируются события безопасности	На сервере безопасности не работает сервис dlogevent или rsyslog	Доменный администратор безопасности должен перезапустить сервисы dlogevent и rsysylog командами systemctl restart rsyslog.service service dlogevent restart
На портале сервера безопасности продолжительное время крутятся шестерёнки	На сервере безопасности не работает сервис postgresql-9.5.service	Доменный администратор безопасности должен перезапустить сервис postgresql-9.5.service командой systemctl restart postgresql-9.5.service
В лог-файле /var/log/nginx/error.log содержится запись вида: *799 connect() to unix:///run/epu.sock failed (2: No such file or directory) while connecting to upstream, client: 127.0.0.1, server: <sb_hostname>, request: "GET /rest/systemevents/system_event_alert/ HTTP/1.0", upstream: "uwsgi://unix:///run/epu.sock:", host: "localhost:8000", referrer: "http://<IP>/events"	На сервере безопасности не работает сервис postgresql-9.5.service	Доменный администратор безопасности должен перезапустить сервис postgresql-9.5.service командой systemctl restart postgresql-9.5.service
в браузере отображается сообщение «403 forbidden nginx/1.10.2»	Осуществлена попытка	Доменный администратор

	несанкционированного доступа не с АРМ Администратора	безопасности должен разрешить доступ к порталу СБ с требуемого АРМ Пользователя
Error opening config file (Отказано в доступе) NOTE - using built-in logs: /var/log/audit/audit.log Error opening /var/log/audit/audit.log (Отказано в доступе)	Осуществлена попытка несанкционированного запуска утилиты ausearch	Только локальный администратор может запускать утилиту ausearch
Argument is required for -<option>	Утилита ausearch запущена без параметров для указанной опции.	При запуске утилиты ausearch необходимо указывать требуемые параметры опций.
<no matches>	Утилита ausearch запущена с неверными опциями и параметрами или отсутствуют данные удовлетворяющие параметрам поиска	Необходимо задать корректные опции и параметры поиска
Summary Report ========== Error opening config file (Отказано в доступе) NOTE - using built-in logs: /var/log/audit/audit.log Error opening /var/log/audit/audit.log (Отказано в доступе)	Осуществлена попытка несанкционированного запуска утилиты aureport	Только локальный администратор может запускать утилиту aureport
-<option> is an unsupported option	Утилита aureport запущена с неподдерживаемой опцией	Утилиту aureport необходимо запускать только с поддерживаемыми опциями
tail: невозможно открыть «/var/log/messages» для чтения: Отказано в доступе tail: больше нет файлов	Недостаточно прав на чтение лог-файла	Локальный администратор безопасности должен выдать права на чтение лог-файла
tail: невозможно открыть «/var/log/messag» для чтения: Нет такого файла или каталога tail: больше нет файлов	Неверно задано имя лог-файла	
dmesg: неверный ключ — «key»	Утилита dmesg запущена с неподдерживаемым ключом	
tail: невозможно открыть «/var/log/messages» для чтения: Отказано в доступе tail: больше нет файлов	Недостаточно прав на чтение лог-файла	Локальный администратор должен выдать права на чтение лог-файла

grep: /var/log/messages: Отказано в доступе	Недостаточно прав на чтение лог-файла	Локальный администратор должен выдать права на чтение лог-файла
head: невозможно открыть «/var/log/messages» для чтения: Отказано в доступе	Недостаточно прав на чтение лог-файла	Локальный администратор должен выдать права на чтение лог-файла
cat: /var/log/messages: Отказано в доступе	Недостаточно прав на чтение лог-файла	Локальный администратор должен выдать права на чтение лог-файла
error: cannot stat /etc/logrotate.conf: Нет такого файла или каталога	Отсутствует конфигурационный файл для сервиса logrotate	Восстановите файл logrotate.conf из резервной копии или создайте его.
error: /etc/logrotate.conf:4 unknown option '<words>' -- ignoring line	В конфигурационном файле /etc/logrotate.conf содержится неправильная опция.	Исправьте неправильную строку на поддерживаемую опцию
Не приходят собдытия от какого-либо ВМ/Сервера	Неправильно указан IP-адрес СБ в конфигурационном файле /etc/rsyslog.d/rsyslog-send.conf	Необходимо прописать правильный IP-адресс Сервера Безопасности в конфигурационном файле /etc/rsyslog.d/rsyslog-send.conf на ВМ/Сервере.
There are no enabled repos. Run "yum repolist all" to see the repos you have. To enable custom repositories: yum-config-manager --enable <repo>	Отсутствует файл содержащий список репозиториев	Необходимо файл с репозиториями либо восстановить из резервной копии или создать его.
Не найдена команда: clear Пожалуйста, воспользуйтесь /bin/yum --help	Для утилиты yum использована неподдерживаемая команда	
Skipping unreadable repository '/etc/yum.repos.d/sintez-base.repo' There are no enabled repos. Run "yum repolist all" to see the repos you have. To enable custom repositories: yum-config-manager --enable <repo>	Недостаточно прав для запуска утилиты yum	Только локальный администратор может запускать утилиту yum
-bash: <util> /bin/bash: плохой интерпретатор: Отказано в доступе	Попытка запустить неподписанную утилиту или утилиту у которой изменились права	
sysctl: "kernel.randomize_va_space" must be of the form name=value	Синтаксическая ошибка задания параметра sysctl	
sysctl: cannot stat /proc/sys/kernel/randomize_v_space: Нет такого файла или каталога	Ошибка в написании параметра kernel.randomize_va_space	
/usr/sbin/counthash: line <number>: /var/log/sintez/counthash.log: Отказано в доступе	Осуществлена попытка несанкционированного запуска утилиты counthash	Данную утилиту может запускать только локальный администратор

touch: невозможно выполнить touch для «/path/to/file»: Отказано в доступе chmod: невозможно получить доступ к «/path/to/file»: Отказано в доступе		
sh: /usr/sbin/prime_self_test: Отказано в доступе	Осуществлена попытка несанкционированного запуска утилиты prime_self_test	Данную утилиту может запускать только локальный администратор
Cannot access config file:/etc/aide.conf:No such file or directory No config defined Configuration error	Отсутствует конфигурационный файл /etc/aide.conf, необходимый для работы утилиты counthash	Необходимо конфигурационный файл /etc/aide.conf либо восстановить из резервной копии, либо создать его.
85:Error in expression:<expression> Configuration error	В конфигурационном файле /etc/aide.conf содержится ошибка	
-bash: ulimit: -h: неправильная опция	Утилита ulimit запущена с неподдерживаемым параметром	
-bash: ulimit: <limit_parametr>: cannot modify limit: Операция не позволена	Данная ошибка возникает, когда пользователь/администратор пытается изменить какое-либо ограничение на значение больше разрешённого системой	
renice: failed to set priority for <digit> (process ID): Операция не позволена	Осуществлена попытка несанкционированного изменения приоритета процесса	Приоритет процессов может изменять только локальный администратор
renice: failed to get priority for <digit> (process ID): Нет такого процесса	Данная ошибка возникает, когда пытаются поменять приоритет у несуществующего процесса	
renice: bad value <value>	Данная ошибка возникает, когда утилиту renice запускают с неправильными параметрами.	
mount: only root can use "--options" option	Недостаточно прав на монтирование контроллеров ресурсов	Только локальный администратор может монтировать контроллеры ресурсов
mount: mount point </mount/path> does not exist	Отсутствует точка монтирования для монтирования контроллеров ресурсов	локальный администратор должен создать точку монтирования
cgcreate: can't create cgroup /group0: Cgroup, operation not allowed	Недостаточно прав для создания контрольной группы	Только локальный администратор может

		создавать контрольные группы
cgcreate: cgroup controller and pathparsing failed ((null))	Данная ошибка возникает, когда отсутствует обязательный параметр <path>	
cgcreate: can't create cgroup /<cgroup_name> Cgroup one of the needed subsystems is not mounted	Данная ошибка возникает, когда пытаюются создать группу для несуществующего контроллера	
cgcreate: can't find uid/gid of user/group <digit>	Данная ошибка возникает, когда в команде создания котрольной группы вместо имери пользователя/группы владельца используют uid/gid	
<quota_util>: неверный ключ — «key»	Данная ошибка возникает, когда для утилит работы с квотам использут неподдерживаемый ключ	
<quota_util>: Cannot open quotafile /home/aquota.user: Отказано в доступе	Данная ошибка возникает, когда утилиты работы с квотам запускают от непривилигированного пользователя	
Bad number of arguments.	Данная ошибка возникает, когда утилиты работы с квотам запускают без указания обязательных аргументов	
<quota_util>: Mountpoint (or device) /home not found or has no quota enabled. <quota_util>: Cannot find filesystem to check or filesystem not mounted with quota option.	Данная ошибка возникает, когда утилиты работы с кватами применяют к файловой системе не поддерживающей квотирование	
quotaon: Cannot stat() given mountpoint /<mount_point>: Нет такого файла или каталога Skipping... quotaon: No correct mountpoint specified.	Данная ошибка возникает при попытке включить квотирование на несуществующей файловой системе	
не удалось открыть «file.txt»: Превышена дисковая квота	Данная ошибка возникает, когда превышена дисковая квота	локальный администратор должен изменить настройки квоты
Invalid arguments, see --help	Данная ошибка возникает, когда утилита /usr/sbin/pszi-cupsfilter вызывается без аргументов или с	

	неправлиьными рагументами	
lpadmin: Запрещено lpadmin: The printer or class does not exist. /usr/sbin/pszi-cupsfilter: line 17: /etc/cron.d/pszi-printer-test.crontab: Отказано в доступе	Недостаточно прав для выполнения утилиты /usr/sbin/pszi-cupsfilter	Утилиту /usr/sbin/pszi-cupsfilte может запускать только локальный администратор.
lpadmin: The printer or class does not exist.	Попытка удалить несуществующий принтер	
Ошибка входа в GRUB	Данная ошибка возникает, когда пользователь вводит неправильные логин и/или пароль для входа в GRUB	
iptables v1.4.21: no command specified	Данная ошибка возникает, когда для утилиты iptables не задана ни одна команда	
iptables v1.4.21: option "-<option>" requires an argument	Данная ошибка возникает, когда для утилиты iptables не заданы аргументы для используеиой опции	
iptables v1.4.21: unknown option "<option>"	Данная ошибка возникает, когда для утилиты iptables использована неизвестная опция	
Bad argument <argumetn>	Данная ошибка возникает, когда для утилиты iptables используется некорректный аргумент	

7. ОГРАНИЧЕНИЯ ПРИ ЭКСПЛУАТАЦИИ

7.1. Роли пользователей

Учетные записи, используемые в КП «ЗОС «СинтезМ» разделяются на два типа:

- доменные;
- локальные (в том числе технологические).

Учетные записи пользователей КП «ЗОС «СинтезМ», хранящиеся на Сервере управления доступом, именуются доменными. Данные о таких пользователях распространяются Сервером управления доступом на АРМ пользователей.

Доменные пользователи могут быть как служебными (данные субъекты осуществляют действия, выполняемые автоматически, без участия человека), так и сопоставленными лицу.

Учетные данные пользователей, хранящиеся локально на пользовательских АРМ, именуются локальными.

Локальные пользователи могут быть как служебными (данные субъекты осуществляют действия, выполняемые автоматически, без участия человека), так и сопоставленными лицу. В КП «ЗОС «СинтезМ» присутствуют служебные локальные пользователи. Данные субъекты действуют только в рамках одного компьютера или виртуальной машины, от имени данных пользователей функционируют системные сервисы защищенной операционной системы (ОС).

В КП «ЗОС «СинтезМ» выделены следующие роли:

- доменный администратор;
- локальный администратор;
- системный администратор;
- пользователь.

Примечание: далее по тексту при использовании терминов «доменный администратор», «локальный администратор», «системный администратор» для

уточнения субъекта, которым выполняется действие, подразумевается пользователь которой обладает указанной ролью.

Каждой роли КП «ЗОС «СинтезМ» сопоставляются действия (права), предопределенные в программных компонентах системы. Действия в свою очередь объединяются в логическую структуру – роль.

Распределение функциональных возможностей администраторов в ОС, менеджере ВМ, сервере управления доступом в соответствии с назначенной ролью представлен в Таблице 6.

Таблица 6 – Перечень функциональных возможностей ролей администраторов КП

№ п/п	Роль КП	Сервер управления доступом	ОС	Менеджер ВМ
1.	Доменный администратор	Управление: - группами пользователей; - пользователями; - политикой паролей; - правилами доступа к хосту; - правилами автомонтирования; - делегированием полномочий.		-
2.	Локальный администратор	-	Управление: - идентификацией и аутентификацией; - пользователями; - политиками паролей; - атрибутами безопасности; - разграничением доступа; - регистрацией событий безопасности; - ограниченной программной средой; - обеспечением надежного функционирования; - фильтрацией сетевых потоков.	-
3.	Системный администратор	-	-	Управление: - созданием ВМ; - ВМ;

				- доступом к ВМ; - пользовательскими данными; - сетевой конфигурацией; - шаблонами - датацентрами, кластерами, хранилищами.

Управление ФБО осуществляется пользователями, имеющими роль администратора, за счет применения разграничения доступа к конфигурационным файлам, а также разграничения доступа к параметрам на уровне интерфейсов управления.

7.2. Требования к среде функционирования

При использовании КП «ЗОС «СинтезМ» сотрудниками эксплуатирующей организации должны быть обеспечены следующие требования:

– СВТ на котором функционирует КП «ЗОС «СинтезМ» должно соответствовать требованиям заявленным в пункте 1.5;

– установка, конфигурирование и управление КП «ЗОС «СинтезМ» в должна проводиться соответствии с эксплуатационной документацией;

– должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует КП «ЗОС «СинтезМ»;

– должна быть обеспечена доверенная загрузка ОС (блокирование попыток несанкционированной загрузки, контроль доступа субъектов доступа к процессу загрузки, контроль целостности компонентов загружаемой операционной среды);

– должны быть обеспечены необходимые ресурсы для выполнения функциональных возможностей безопасности операционной системы, хранения резервных копий, создаваемых операционной системой, а также защищенное хранение данных операционной системы и защищаемой информации;

– должно быть обеспечено ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации;

– должен обеспечиваться доверенный маршрут между ОС и пользователями ОС (администраторами, пользователями);

– должен обеспечиваться доверенный канал передачи данных между ОС и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;

– должна быть обеспечена невозможность отключения (обхода) компонентов ОС;

– должны быть реализованы меры, препятствующие несанкционированному копированию информации, содержащейся в ОС, на съемные машинные носители информации (или за пределы информационной системы);

– должен осуществляться контроль вноса (выноса) в (из) контролируемую зону (контролируемой зоны) съемных машинных носителей информации;

– должна осуществляться проверка целостности внешних модулей уровня ядра, получаемых от заявителя (разработчика, производителя), перед их установкой в операционную систему;

– должно быть обеспечено выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;

– персонал, ответственный за функционирование КП «ЗОС «СинтезМ», должен обеспечивать функционирование КП «ЗОС «СинтезМ», в точности руководствуясь эксплуатационной документацией;

– лица, ответственные за эксплуатацию КП «ЗОС «СинтезМ», должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержались в тайне и были недоступны лицам, не уполномоченным использовать данную учетную запись;

– должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

– запрещается подключение bluetooth-устройств к хостам, функционирующим под управлением ОС;

– не должно быть возможности для передачи сетевых пакетов между хостами, функционирующими под управлением ОС, и FTP-серверами, к которым возможен доступ непривилегированных пользователей;

– должно быть исключено использование отчуждаемых носителей информации с содержимым, сформированным нарушителем;

– должны использоваться антивирусные средства;

– должно использоваться только лицензионное ПО фирм-производителей. В случае необходимости использования иного программного обеспечения, его применение должно быть санкционировано администратором безопасности. В любом случае стороннее ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПО СКЗИ;

– необходимо регулярно устанавливать пакеты обновления безопасности, обновлять антивирусные базы;

– при подключении к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов;

– должна быть установлена только одна операционная система, правом установки и настройки которой должен обладать только администратор;

– должна быть отключена возможность удаленного управления ОС;

– необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации), неиспользуемые протоколы, сервисы и службы рекомендуется отключить.

7.3. Ограничения для администратора

Администратору запрещается:

– включать автомонтирование образов дисков в формате ISO на АРМ непривилегированного пользователя;

– включать использование файловой системы UDF на АРМ пользователя;

– выполнять команду «pg_dumpall -g» с указанием директории, доступ на чтение к которой предоставлен пользователю;

– использовать ключ «-php-docroot» для uwsgi;

– использовать ключа «--protect-args» для rsync;

– запускать mod_wsgi в режиме демона;

– использовать файловые журналы для пакета mariadb-libs;

– устанавливать параметр max_message_unix_fds пакета dbus равным нечетному числу;

– настраивать пакет sssd на кэширование паролей;

– открывать на сервере порты для подключений по протоколу SMB1;

– включать проброс TCP посредством изменения значения параметра AllowTcpForwarding в файле /etc/ssh/sshd_config;

– выполнять SQL-команды формата "INSERT ... ON CONFLICT DO UPDATE".

Администратору запрещается предоставлять непривилегированному пользователю следующие права:

– право на запуск службы Systemd;

– право на доступ к журналам и конфигурационным файлам СУБД из состава КП «ЗОС «СинтезМ», а также право на запуск серверных частей СУБД;

– право на изменение параметра max_message_unix_fds пакета dbus;

– право на изменение файла /etc/mailcap;

– право на использование утилиты sudo;

– привилегию CAP_NET_ADMIN;

– право на доступ к настройкам пакета ansible;

– право на доступ к файлу /dev/fuse;

- право на доступ к журналам Менеджера ВМ (ovirt-engine);
- право на доступ к каталогу хранения временных файлов sqlite;
- право на доступ к утилите pam_console_apply;
- право на доступ к файлу /dev/wcnss_wlan;
- права на запись в файлы httpd.conf и .htaccess;
- право на использование компиляторов из состава ОС;
- право на редактирование переменных среды;
- право на чтение файлов /proc/*/environ;
- право на запись в файлы /etc/passwd и /etc/shadow;
- право на запись в конфигурационный файл загрузчика grub;

- право на доступ к чтению записей аудита.

8. ПРИЕМКА СРЕДСТВА

Действий по приемке поставленного средства включают

— проверка общих требований;

— проверка целостности ПО;

— проверка комплектности;

— проверка механических требований;

— проверка маркировки;

— проверка упаковки.

Приемка поставленного средства осуществляется в соответствии с документом Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01).

8.1. Проверка общих требований

Проверка изделия на соответствие общим требованиям проводится путем выполнения следующих действий:

— проверить наличие всех документов в соответствии с КП «ЗОС «СинтезМ». Ведомость эксплуатационных документов ТАСП.62.01.12.000.005 20 01;

— просчитать количество листов каждого документа, сверить его с указанным на титульном листе и убедиться, что все листы без деформаций и помарок;

— проверить обозначения в колонтитулах документов.

Изделие считается удовлетворяющим требованиям если:

— эксплуатационная документация оформлена и изготовлена в соответствии с требованиями ЕСПД;

— состав документов соответствует указанному в документе КП «ЗОС «СинтезМ». Ведомость эксплуатационных документов ТАСП.62.01.12.000.005 20 01, количество листов каждого документа совпадает с указанным на титульном листе, замечаний по другим пунктам проверки не выявлено.

Проверка компакт-дисков изделия на соответствие требованиям проводится путем внешнего осмотра компакт-диска.

Изделие считается удовлетворяющим требованиям, если внешний осмотр показал, что компакт-диски соответствует требованиям, изложенным в Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01), а именно:

— для компакт-дисков с эксплуатационной документацией используются компакт-диски типа CD-R Printable 700 Мбайт (область печати: 33-118 мм; тип футляра: слим-бокс или конверт);

— для компакт-дисков с загрузочным модулем изделия используются компакт-диски типа DVD-R Printable 4,7 Гбайт (область печати: 33-118 мм; тип футляра: слим-бокс или конверт).

8.2. Проверка целостности ПО

Проверка целостности ПО проводится сверкой контрольных сумм изделия со значениями, указанными в формуляре, компакт-диске с загрузочным модулем и этикетке к диску с загрузочным модулем.

Подсчет и проверка контрольной суммы, получаемой согласно ГОСТ 28147-89, осуществляется на ПЭВМ с КП «ЗОС «СинтезМ» в следующей последовательности:

8) установить оптический диск в устройство для чтения дисков;

9) в приложении «magma» перейти во вкладку «Диски и ISO»

10) выбрать привод, в котором находится рассчитываемый диск (по умолчанию указан /dev/sr0);

11) выбрать директорию для сохранения текстового документа с результатом расчета директорий, для этого нажать кнопку «Выбрать» в строке «Выберите директорию для сохранения;

12) нажать на кнопку «Рассчитать КС диска»;

13) ожидать завершения работы программы подсчета контрольной суммы;

14) сравнить значение контрольной суммы, сохраненное в выбранной директории, со значением, указанным в формуляре, диске и на этикетке компакт-диска.

Подсчет контрольной суммы с использованием программы «ФИКС-Unix 1.0» (сертификат соответствия ФСТЭК России № 680, действителен до 26.02.2021 года, знак соответствия № М 370006) осуществляется на ПЭВМ, с КП «ЗОС «СинтезМ» и программой «ФИКС-Unix 1.0» (ufix), в следующей последовательности:

9) установить оптический диск в устройство для чтения дисков;

10) создать временную директорию для монтирования оптического диска командой:

```
# mkdir /tmp/template_d
```

11) примонтировать диск командой:

```
# mount –o loop /dev/sr0 /tmp/template_d;
```

12) создать директорию для временного хранения результатов:

```
# mkdir /root/$(date +%Y-%m-%d)-ks-iso
```

13) последовательно выполнить команды для подсчета контрольной суммы:

```
# ufix -jR /tmp/template_d/ > /root/$(date +%Y-%m-%d)-ks-
iso/list.txt
# ufix -e /root/$(date +%Y-%m-%d)-ks-iso/list.txt
# ufix -h /root/$(date +%Y-%m-%d)-ks-iso/list.prj
# ufix -lv /root/$(date +%Y-%m-%d)-ks-iso/list.prj > /root/$(date
+%Y-%m-%d)-ks-iso/list.ks
```

14) открыть в браузере полученный файл /root/$(date +%Y-%m-%d)/list.html

15) сравнить значение контрольной суммы (строка «ВСЕГО»), выданной на экран, со значением, указанным в формуляре, диске и на этикетке компакт-диска;

16) отмонтировать диск командой:

```
# umount /tmp/template_d
```

Изделие считается удовлетворяющим требованиям в случае совпадения контрольных сумм, выданных программами подсчета, со значениями, приведенными в соответствующем разделе формуляра, компакт-диске и на этикетке компакт-диска.

8.3. Проверка комплектности

Проверка комплектности проводят путем сравнения комплекта поставки изделия с комплектностью, указанной в разделе 4 формуляра.

Программное изделие считается выдержавшим проверку, если его комплектность соответствует комплектности в разделе 4 формуляра.

8.4. Проверка механических требований

Проверка механических требований проводится путем внешнего осмотра.

Изделие считается удовлетворяющим требованиям, если при внешнем осмотре не обнаружено:

— сколов, царапин, деформаций, других механических повреждений и дефектов рабочей поверхности компакт-диска;

— маркировка диска не имеет дефектов;

— слим-бокс (или конверт) не поврежден, крышка слим-бокса обеспечивает плотное закрытие;

— размеры этикетки обеспечивают ее вложение в слим-бокс или наклеивание на конверт, сама этикетка не имеет повреждений;

— эксплуатационная документация не имеет повреждений и замятостей обложек и переплетов.

8.5. Проверка маркировки

Проверка маркировки проводится путем внешнего осмотра и сверки контрольных сумм и заводского номера изделия:

— на компакт-диске с загрузочным модулем;

— на этикетке компакт-диска с загрузочным модулем;

— в формуляре.

Проверка маркировки компакт-диска с загрузочным модулем осуществляется путем внешнего осмотра. При проверке производится, визуальная сверка маркировки диска с загрузочным модулем с шаблоном, представленным в Комплекс программ

«Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01).

Проверка маркировки компакт-диска с комплектом эксплуатационной документации осуществляется путем внешнего осмотра. При проверке производится, визуальная сверка маркировки диска с комплектом эксплуатационной документации с шаблоном, представленным в Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01).

Изделие считается удовлетворяющим требованиям если:

— маркировка компакт диска с загрузочным модулем изделия проведена в соответствии с требованиями изложенными в Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01), контрольные суммы и заводские номера соответствуют указанным в формуляре на изделие;

— маркировка компакт диска с комплектом эксплуатационной документации изделия проведена в соответствии с требованиями изложенными в Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01);

— упаковка компакт дисков с загрузочным модулем и комплектом эксплуатационной документации имеет этикетки, оформленные в соответствии с требованиями изложенными в Комплекс программ «Защищенная операционная система «СинтезМ». Технические условия (ТАСП.62.01.12.0000.005 93 01) и данные этикетки соответствуют данным, записанным в формуляре.

8.6. Проверка упаковки

Проверка упаковки изделия проводится путем внешнего осмотра.

Изделие считается удовлетворяющим требованиям, если:

— упаковка не имеет следов механических повреждений, качество упаковки соответствует требованиям настоящих ТУ;

— компакт-диск с загрузочным модулем изделия упакован в штатный пластмассовый футляр или специальный конверт, и опечатан специальной наклейкой;

— компакт-диск с комплектом эксплуатационных документов упакован в штатный пластмассовый футляр или специальный конверт;

— компакт-диск с загрузочным модулем и комплект ЭД упакованы в прозрачную папку-конверт на молнии;

— упаковочный лист заполен, форма упаковочного листа соответствует представленной в ТУ.

9. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные и выходные данные КП «ЗОС «СинтезМ» в части базовой операционной системы представлены в таблице 7.1.

Таблица 7.1 – Входные и выходные данные КП «ЗОС «СинтезМ» в части базовой операционной системы

Наименование модуля			Назначение модуля	Входные данные		Выходные данные	
				Источник	Данные	Получатель	Данные
Ядро	Драйвера сетевого интерфейса		Обеспечение работы сетевой карты	Ethernet интерфейс	Системные прерывания	Виртуальная машина	Ethernet кадры
	Драйвера файловых систем		Обеспечение упорядоченного хранения данных на блочном устройстве, журналирования и поиска данных	Процессы	Файлы	Блочное устройство	Данные в формате файловой системы
	Модули управления сетью	Драйвер сетевого моста	Обеспечение сетевого взаимодействия	Физические и виртуальные сетевые интерфейсы	Ethernet кадры	Физические и виртуальные сетевые интерфейсы	Ethernet кадры
		NetFilter/ EbTables	Управление сетевым взаимодействием	Сетевое устройство	Ethernet кадры	Сетевое устройство	Легитимные Ethernet кадры
				Файл	Правила сетевого взаимодействия	Оперативная память	Структуры данных netfilter/x_tables.h
	Служба аппаратной виртуализации KVM		Обеспечение работы аппаратной виртуализации по технологии Intel-VT	Процесс гостевой виртуальной машины	Команды процессору Запрос страниц памяти	Аппаратные ресурсы	Инструкции процессора VMX Адреса страниц памяти
	Модуль работы с блочными устройствами		Обеспечение работы с жесткими дисками и подключаемыми	Драйвера файловых систем	Данные в формате файловой системы	Жесткий диск Система хранения данных	SATA-команды SCSI-команды

Таблица 7.1 – Входные и выходные данные КП «ЗОС «СинтезМ» в части базовой операционной системы

Наименование модуля		Назначение модуля	Входные данные		Выходные данные	
			Источник	Данные	Получатель	Данные
		системами хранения данных				
	Модули управления памятью	Управление трансляцией между физическими и виртуальными адресами оперативной памяти	Оперативная память	Адреса страниц	Процессы операционной системы	Адреса страниц виртуальной памяти
Загрузчик ОС		Обеспечение загрузки операционной системы	GRUB	Конфигурационный файл /boot/grub/grub.cfg	Оперативная память	Ядро ОС Образ начальной инициализации
Система виртуализации (Менеджер виртуализации)		Управление средой виртуализации	База данных Менеджера ВМ	SQL -запросы	vdsm	JsonRPC-запрос
Система виртуализации (Гипервизор)		Обеспечение работы виртуальных машин	vdsm	XML	libvirt	Параметры запуска Службы ВМ (QEMU)
			libvirt	Параметры запуска Службы ВМ (QEMU)	Оперативная память	Служба ВМ (QEMU)
			Сервер Spice-сессий	Служба ВМ (QEMU)	Клиент Spice	Удаленный рабочий стол

Входные и выходные данные КП «ЗОС «СинтезМ» в части пользовательского графического окружения представлены в таблице 7.2.

Таблица 7.2 – Входные и выходные данные КП «ЗОС «СинтезМ» в части пользовательского графического окружения

Наименование модуля		Назначение модуля	Входные данные		Выходные данные	
			Источник	Данные	Получатель	Данные
Ядро	Драйвера сетевого интерфейса	Обеспечение работы сетевой карты	Ethernet интерфейс	Системные прерывания	Виртуальная машина	Ethernet кадры
	Драйвера файловых систем	Обеспечение упорядоченного хранения	Процессы	Файлы	Блочное устройство	Данные в формате

Таблица 7.2 – Входные и выходные данные КП «ЗОС «СинтезМ» в части пользовательского графического окружения

Наименование модуля		Назначение модуля	Входные данные		Выходные данные	
			Источник	Данные	Получатель	Данные
		данных на блочном устройстве, журналирования и поиска данных				файловой системы
	Модуль работы с блочными устройствами	Обеспечение работы с жесткими дисками и подключаемыми системами хранения данных	Драйвера файловых систем	Данные в формате файловой системы	Жесткий диск Система хранения данных	SATA-команды SCSI-команды
	Модули управления памятью	Управление трансляцией между физическими и виртуальными адресами оперативной памяти	Оперативная память	Адреса страниц	Процессы операционной системы	Адреса страниц виртуальной памяти
Загрузчик ОС		Обеспечение загрузки операционной системы	GRUB	Конфигурационный файл /boot/grub/grub.cfg	Оперативная память	Ядро ОС Образ начальной инициализации
Сервисные компоненты	httpd -служба веб-сервера Apache	Обеспечение работы веб-приложений	Веб-браузер клиента (пользователя)	Веб-запрос	Веб-приложение	веб-запрос
Сервисные компоненты	java-openjdk-виртуальная машина Java	Обеспечение работы приложений java	Операционная система Приложение java	Байт-код Файлы Сокеты	Операционная система Приложение java	Байт-код Файлы Сокеты
	Php-интерпритатор	Интерпретация приложений на языке PHP	Веб-сервер	Веб-запросы	Веб-приложение	Веб-запрос

Таблица 7.2 – Входные и выходные данные КП «ЗОС «СинтезМ» в части пользовательского графического окружения

Наименование модуля		Назначение модуля	Входные данные		Выходные данные	
			Источник	Данные	Получатель	Данные
	postgresql-server - служба СУБД	Управление базами данных	Приложение	SQL-запрос	Приложение	Содержимое таблиц БД
	Mono- модуль сервера приложений	Обеспечение работы приложений Mono	Операционная система Приложение mono	Байт-код Файлы Сокеты	Операционная система Приложение java	Байт-код Файлы Сокеты
Сервисные компоненты	Geos-модуль работы с информацией о геолокации	Формирование SQL-запросов гео-данных и обработка гео-данных	Приложение для работы с гео-данными	Поток гео-данных, извлеченных из базы данных гео-локации	Приложение для работы с гео-данными	Топологический граф
	QT 4.8- кроссплат-форменная библиотека разработки ПО на языке программирования C++	Обеспечение работы приложений, написанных с использованием библиотеки QT	Приложение QT	Параметры функций	Приложение QT	Параметры функций
	QT 5.7- кроссплат-форменная библиотека разработки ПО на языке программирования C++	Обеспечение работы приложений, написанных с использованием библиотеки QT	Приложение QT	Параметры функций	Приложение QT	Параметры функций
Служба единого времени chrony		Обеспечение синхронизации времени	Клиент единого времени	UDP пакет в формате протокола NTP	Системный вызов clock_settime	Unix-время (количество секунд начиная с 01.01.1970 00:00:00 UTC)

Таблица 7.2 – Входные и выходные данные КП «ЗОС «СинтезМ» в части пользовательского графического окружения

Наименование модуля	Назначение модуля	Входные данные		Выходные данные	
		Источник	Данные	Получатель	Данные
Клиент службы имен	Обеспечение получения IP адреса по имени хоста	Имя хоста	Системный вызов gethostbyname	DNS запрос	Служба сервера имен

ПРИЛОЖЕНИЕ А
ПЕРЕЧЕНЬ ТЕРМИНОВ

(справочное)

Автоматизированная система **–** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

Автоматизированная система в защищенном исполнении – автоматизированная система, предназначенная для обработки информации ограниченного доступа и реализующая информационную технологию выполнения установленных функций в соответствии с требованиями нормативных документов по защите информации ФСБ России *(далее АСЗИ или Система)*

Виртуальный сетевой мост – построенная на базе технологии Linux Bridge программная реализация коммутатора, предназначенного для соединения нескольких узлов (ВМ, физических серверов, АРМ и технических средств) сети и обеспечивающего «жесткое» подключение физических и виртуальных интерфейсов сетевых адаптеров в вертикальную сетевую инфраструктуру.

Защищаемая информация – информация, содержащая охраняемые сведения, а также информация, для которой ее владельцем установлены требуемые характеристики безопасности.

Дистрибутив ПО **–** программное обеспечение, представленное в унифицированной форме, которая дает возможность выполнить установку ПО в автоматизированной системе в защищенном исполнении.

Исполняемый файл – файл, содержимое которого является готовой к исполнению компьютерной программой (в том числе двоичное представление машинных инструкций, скрипты bash, файлы сценариев python и т.д.).

Комплекс средств автоматизации – совокупность всех компонентов автоматизированной системы за исключением персонала.

Метаданные дистрибутива ПО – формализованное описание общих сведений и специальных характеристик программного обеспечения, представленное в форматах XML и JSON.

Метка безопасности – набор атрибутов, однозначно сопоставляемых с субъектами доступа, объектами доступа и назначающих их характеристики.

Монтирование – процедура подключения файловой системы, находящейся на СФХ в иерархию файлов и каталогов файловой системы ВМ.

Пользователь – конкретное должностное лицо, обладающее определенными правами доступа к объектам доступа, для выполнения функциональных обязанностей которого в автоматизированном режиме в АСЗИ создаётся виртуальная машина или выделяется рабочая станция.

Пользовательские виртуальные машины – виртуальные машины, предназначенные для исполнения программных средств Системы, с которыми непосредственно взаимодействуют ее пользователи.

Сетевое файловое хранилище (СФХ) – специализированное хранилище файлов и каталогов, подключенное к локальной сети.

Терминальный клиент – бездисковый АРМ обеспечивающий, взаимодействие пользователя с ресурсами АСЗИ посредством протокола SPICE.

Терминальный сервер – инфраструктурная ВМ обеспечивающая, выдачу терминальным клиентам ip-адресов по протоколу DHCP, а также загрузку образа ОС на терминальные клиенты, с использованием PXE, по локальной сети.

Узел – физические серверы, пользовательские ВМ, ВМ СПО, инфраструктурные ВМ, ТК или рабочие станции, зарегистрированные в Средстве управления доменными пользователями.

Web-клиент – пользовательское приложение, посредством которого осуществляется взаимодействие пользователя с web-сервисами.

ПРИЛОЖЕНИЕ Б

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

(обязательное)

АИС	–	автоматизированная информационная система
АРМ	–	автоматизированное рабочее место
АСЗИ	–	автоматизированная система в защищенном исполнении
ВМ	–	виртуальная машина
КСА	–	комплекс средств автоматизации
НСД	–	несанкционированный доступ
ОС	–	операционная система
ПСЗИ	–	программное средство защиты информации
СХД	–	система хранения данных
DHCP	–	(англ. *Dynamic Host Configuration Protocol* протокол динамической настройки узла) сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу *DHCP* и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок
Ebtables	–	средство для фильтрации пакетов для программных мостов Linux, работает преимущественно на втором (канальном) уровне сетевого стека
iSCSI	–	(*англ. Internet Small Computer System Interface*) протокол, который базируется на TCP/IP и разработан для установления взаимодействия и управления системами хранения данных, серверами и клиентами
Intel VT	–	(Intel Virtualization Technology) виртуализация режима реальной адресации (режим совместимости с 8086)
FC		(*англ. fibre channel –волоконный канал*) – семейство протоколов для высокоскоростной передачи данных
GRUB		(англ. *GRand Unified Bootloader*) загрузчик операционной системы от проекта GNU. GRUB позволяет пользователю иметь несколько установленных операционных систем и при включении компьютера выбирать одну из них для загрузки
KVM	–	(*англ. Kernel-based Virtual Machine*) – программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86, которая поддерживает аппаратную виртуализацию на

		базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine)
libvirt	–	это отлаженная и со всех сторон протестированная библиотека, с помощью которой любое приложение может быть легко обучено управлению виртуальными серверами
Linux	–	общее название Unix-подобных операционных систем, основанных на одноименном ядре
Linux Bridge	–	Бридж (англ. *bridge*, мост) – это способ соединения двух сегментов Ethernet на канальном уровне, то есть без использования протоколов более высокого уровня, таких как IP. Пакеты передаются на основе Ethernet-адресов, а не IP-адресов (как в маршрутизаторе). Поскольку передача выполняется на канальном уровне (уровень 2 модели OSI), все протоколы более высокого уровня прозрачно проходят через мост
LDAP	–	(англ. *Lightweight Directory Access Protocol* «облегчённый протокол доступа к каталогам») протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ITU-T протокола DAP. LDAP – относительно простой протокол, использующий TCP/IP и позволяющий производить операции аутентификации, поиска и сравнения, а также операции добавления, изменения или удаления записей
SELinux	–	(*англ. Security-Enhanced Linux – Linux с улучшенной безопасностью*) –реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа
SSH	–	(*от англ. secure shell - безопасная оболочка*) это набор программ, которые позволяют регистрироваться на компьютере по сети, удаленно выполнять на нем команды, а также копировать и перемещать файлы между компьютерами
SPICE	–	(*сокр. от англ. «Simple Protocol for Independent Computing Environments», то есть «Простой протокол для независимой вычислительной среды»*) –протокол, используемый в рамках проекта с аналогичным названием (но пишется строчными буквами: Spice). Проект представляет собой систему отображения удаленного дисплея, построенную для виртуальной среды, которая позволяет просматривать виртуальный «рабочий стол» вычислительной среды не только на машине, на которой он запущен, но и откуда угодно через Интернет, причем для просмотра можно использовать широкий спектр машинных архитектур
	–	*(Network File System*) протокол сетевого доступа к файловым системам. За основу взят протокол вызова удалённых процедур (ONC RPC). Позволяет подключать (монтировать) удалённые файловые системы через сеть
oVirt	–	свободная, кроссплатформенная система управления виртуализацией
REST	–	(*сокр. от англ. Representational State Transfer «передача состояния представления»*) архитектурный стиль взаимодействия компонентов распределённого приложения в

		сети. REST представляет собой согласованный набор ограничений, учитываемых при проектировании распределённой гипермедиа-системы
UDP	–	(англ. *User Datagram Protocol* –протокол пользовательских датаграмм) –один из ключевых элементов TCP/IP, набора сетевых протоколов для Интернета. С UDP компьютерные приложения могут посылать сообщения (в данном случае называемые датаграммами) другим хостам по IP-сети без необходимости предварительного сообщения для установки специальных каналов передачи или путей данных
USB	–	*(ю-эс-би, англ. UniversalSerial Bus*) последовательный интерфейс для подключения периферийных устройств к вычислительной технике. Получил широчайшее распространение и фактически стал основным интерфейсом подключения периферии к бытовой цифровой технике.
PXE	–	*(англ. Preboot eXecution Environment, произносится пикси*) среда для загрузки компьютера с помощью сетевой карты без использования локальных носителей данных (жёсткого диска, USB-накопителя и т.п.)
QEMU	–	свободная программа с открытым исходным кодом для эмуляции аппаратного обеспечения различных платформ

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	Номер документа	Входящий номер сопрово-дительного докум. и дата	Подп.	Дата
	изме-ненных	заме-ненных	новых	аннули-рованных					