АО "НТЦ ИТ РОСА"

ОПЕРАЦИОННАЯ СИСТЕМА РОСА "ХРОМ" 13 (НЕСЕРТИФИЦИРОВАННАЯ ВЕРСИЯ)

Руководство администратора

Часть 1. Установка

РСЮК.10502-01 32 01

Листов 46

2026

АННОТАЦИЯ

Данный документ является руководством администратора операционной системы РОСА "ХРОМ" 13 РСЮК.10502-01 (далее – ОС, Система) в вариантах "рабочая станция" (далее – ОС рабочей станции) и "сервер" (далее – серверная ОС).

ОС зарегистрирована в реестре российского ПО от 05.09.2016 №1607.

Предполагается, что читатель является системным администратором ОС Linux с опытом работы в интерфейсе командной строки. Также рекомендуется ознакомиться с принципами работы Системы в графическом интерфейсе пользователя, которые описаны в документе "ОС РОСА "ХРОМ". Руководство пользователя"(индекс РСЮК.10502-01 34 01).

В настоящем руководстве приведен состав ОС, инструкции по нескольким типам установки ОС (локальная, установка с использованием средств маскирования информации, установка в виртуальную машину, автоматизированная установка), общие сведения о работе в ОС, ее настройке и организации работы пользователей в ней.

Перед установкой, настройкой и эксплуатацией ОС рекомендуется внимательно ознакомиться с настоящим руководством.

Для разработки документа использованы ссылки на следующие стандарты:

– ГОСТ Р 2.105-2019 "Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам";

– ГОСТ 2.601 "Единая система программной документации. Виды программных документов";

– ГОСТ 19.101-77 "Единая система программной документации. Виды программ и программных документов";

– ГОСТ 19.105-78 "Единая система программной документации. Общие требования к программным документам";

– ГОСТ 19.503-79 "Единая система программной документации. Руководство системного программиста".

Настоящий документ подготовлен в соответствии с технологической инструкцией "РОСА. Регламент формирования документации к программным продуктам" (индекс РСЮК.11001-03 90 01).

Содержание

1 Безопасная установка и эксплуатация ОС . . . 4

1.1 Условия безопасной эксплуатации . . . 4
1.2 Доверенная загрузка . . . 4
1.3 Защита информации . . . 4
1.4 Безопасная конфигурация ОС и ее целостность . . . 5
1.5 Пользователи и администраторы . . . 5
1.6 Настройка точного времени . . . 6

2 Локальная установка . . . 7

2.1 Подготовка к установке . . . 7
2.2 Установка ОС на рабочую станцию . . . 7
2.3 Установка серверной версии ОС . . . 14
2.4 Парольная защита загрузчика ОС . . . 14

3 Установка с использованием средств маскирования информации . . . 16

3.1 Общие вопросы . . . 16
3.2 Разметка носителя с маскированием информации . . . 16
3.3 Поддержка tpm2 для автоматического ввода паролей . . . 17

4 Установка на виртуальную машину . . . 19
5 Автоматизированное развертывание . . . 20

5.1 Введение в kickstart-сценарии . . . 20
5.2 Типовой сценарий автоматизированной установки . . . 20
5.3 Дополнительные действия в kickstart-сценариях . . . 24

6 Сетевая загрузка с возможностью установки . . . 26

6.1 Технология Intel PXE . . . 26
6.2 Начальная настройка сервера для работы PXE . . . 26
6.3 Настройка сервера DHCP (BOOTP) . . . 27
6.4 Настройка веб-сервера . . . 28
6.5 Настройка сервера TFTP . . . 28
6.6 Настройка сети в LiveCD . . . 30

7 Обновление на платформу ОС РОСА13 . . . 32
8 Графическая установка с использованием VNC . . . 35
9 OEM-установка . . . 38
10 Установщик iso2img . . . 40
11 Подготовительные процедуры после установки . . . 41
Термины и сокращения . . . 44

1 БЕЗОПАСНАЯ УСТАНОВКА И ЭКСПЛУАТАЦИЯ ОС

1.1 Условия безопасной эксплуатации

Для безопасной эксплуатации ОС должна быть установлена на совместимую аппаратную часть, удовлетворяющую требованиям п. 1.4 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

Организационными или техническими средствами (с помощью пломб или замков) должна быть обеспечена защита физической целостности корпуса компьютера с установленной ОС от изменения аппаратной конфигурации.

Установку, настройку и обслуживание ОС должен проводить обладающий необходимыми компетенциями администратор ОС в соответствии с настоящим Руководством.

Эксплуатацию ОС должны выполнять обладающие необходимыми компетенциями пользователи в соответствии с документом "ОС РОСА "ХРОМ". Руководство пользователя" .

1.2 Доверенная загрузка

Для безопасной работы в ОС должна быть реализована её доверенная загрузка, обеспечиваемая внешними средствами АПМДЗ/СДЗ и/или организационными мерами, а именно:

- защитой BIOS паролем от изменения;
- отключением в BIOS загрузки с внешних носителей (DVD, подключаемых накопителей) согласно документации к аппаратуре после установки;
- защитой паролем режима изменения параметров загрузчика GRUB (п. 2.4).

1.3 Защита информации

Администратор должен обеспечить механизмы резервного копирования и необходимый объем носителей для защищенного хранения резервных копий данных пользователей согласно инструкциям, описанным в п. 6.2 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

При использовании парольной защиты для идентификации во всех случаях администратор должен использовать пароли достаточной степени сложности. При

использовании небезопасных паролей ОС предупреждает об этом; при получении такого предупреждения нужно изменить пароль на более сложный.

Рекомендуется произвести установку ОС с использованием механизма маскирования информации на носителе согласно п. 3.

Для предотвращения утечки информации с помощью записи её на съемные внешние накопители (флеш-накопитель, внешние HDD, DWD-RW и др.) должен быть организован процесс контроля их использования. Это возможно сделать как чисто организационными мерами, так и аппаратным отключением возможности подключения внешних накопителей на пользовательских компьютерах (с помощью настроек BIOS).

Для предотвращения несанкционированного доступа к информации в момент, когда авторизованный пользователь ОС делает перерыв в работе, он должен блокировать экран нажатием сочетания клавиш `META+L` на клавиатуре в графическом режиме или же командой `vlock`, если он работает в консольном текстовом режиме.

1.4 Безопасная конфигурация ОС и ее целостность

ОС также может быть сконфигурирована для безопасной работы с помощью файлов конфигурации, описанных в п. 6.5 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02). Необходимо контролировать с помощью программы AIDE целостность Системы путем создания базы данных после инсталляции, как показано в п.6.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02), и периодического осуществления контроля.

1.5 Пользователи и администраторы

Первый созданный инсталлятором пользователь при установке по умолчанию обладает доступом к правам администратора через команду sudo, т. е. является администратором ОС. Эту учетную запись необходимо применять только для настройки ОС, пользователи должны работать под отдельной учетной записью с пользовательскими правами. Подробнее об этом см. п. 2.2 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

1.6 Настройка точного времени

Для правильного ведения журналов событий и аудита в компьютере и ОС должно быть установлено актуальное системное время. Администратору необходимо контролировать установку правильного часового пояса и сохранение этого времени при выключении компьютера (поддерживать актуальность автономного питания BIOS с помощью встроенной батареи).

ОС сконфигурирована так, что время автоматически синхронизируется по сети Интернет с публичными серверами. Доступ к этой настройке имеют администраторы ОС, пользователь менять время по умолчанию не может.

2 ЛОКАЛЬНАЯ УСТАНОВКА

2.1 Подготовка к установке

Перед началом установки ОС рекомендуется выполнить следующие действия:

а) убедиться, что аппаратная конфигурация ПК удовлетворяет минимальным аппаратным требованиям, указанным в п.1.4 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02);

б) убедиться в подлинности DVD с дистрибутивом ОС (п.1.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02));

в) скопировать с DVD с дистрибутивом ОС образ на USB-носитель (если установка будет производиться с USB-носителя);

г) провести временную настройку BIOS/UEFI компьютера для обеспечения возможности загрузки с выбранного носителя, используя документацию на оборудование. В большинстве случаев выбор вариантов загрузки становится доступен при удержании клавиш `Del`, `F12` или `F2` при начале загрузки компьютера.

Для обеспечения доверенной загрузки ОС рекомендуется после успешной инсталляции режим загрузки с внешнего накопителя отключить.

2.2 Установка ОС на рабочую станцию

Выбор позиций меню при установке осуществляется стрелками на клавиатуре и нажатием клавиши `Enter` или же выбором элемента меню курсором и нажатием левой кнопки мыши.

Для того чтобы провести процедуру установки ОС, необходимо выполнить следующие действия:

а) вставить в устройство чтения DVD загрузочный диск изделия или USB-носитель с дистрибутивом ОС до того, как ПК начнет обращение к загрузочным дискам. Если обращение уже было произведено, и установка изделия не началась, необходимо перезагрузить ПК.

б) выбрать язык, на котором будет производиться установка.

в) выбрать вариант установки "Запуск и установка ROSA Linux (live)" (рекомендуется) или же режим "Установка ROSA Linux", при котором установка идет

без предварительной загрузки ОС (рисунок 1). Такой режим применим для специальных случаев, например, при недостатке оперативной памяти или при необходимости ускорения установки.



Рисунок 1 – Выбор варианта установки

г) При проблемах с установкой может быть полезным пункт "Инженерное меню", в подменю которого доступны варианты с проверкой контрольной суммы образа перед установкой, проверкой оперативной памяти ПК или установкой в режиме упрощенной графики либо в текстовом режиме. Перед обращением в техническую поддержку при каких-либо проблемах настоятельно рекомендуется как минимум провести диагностику оперативной памяти (полный цикл) и попробовать загрузить установочный образ с предварительным тестированием контрольной суммы, что позволит исключить ошибки аппаратного обеспечения. При наличии сбоев оперативной памяти необходимо заменить ее на исправную, при сбое контрольной суммы образа следует использовать другой носитель или другой USB-порт. Пример "Инженерного меню" приведен ниже (рисунок 2) (конкретный внутренний номер

образа зависит от версии и может понадобиться при обращении в техническую поддержку).



Рисунок 2 – Инженерное меню

д) После загрузки в live-режиме появляется возможность полноценной проверки работы ОС на конкретном ПК с возможностью установки с помощью ярлыка инсталлятора на рабочем столе (рисунок 3). Перед установкой рекомендуется подключить ОС к сети (используя пиктограмму на панели задач), тогда часть параметров будет заполнена автоматически.

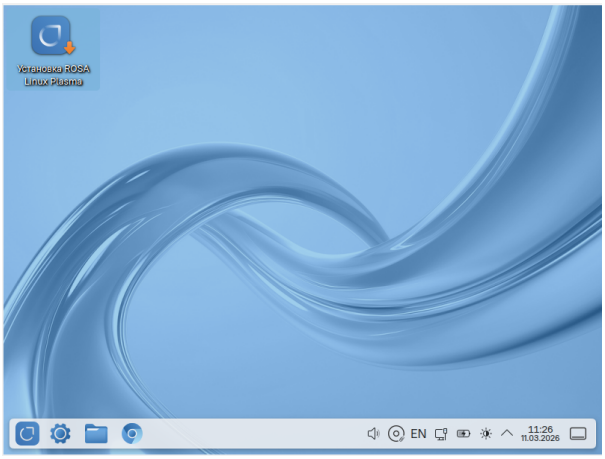

Рисунок 3 – Рабочий стол live-системы с ярлыком инсталлятора

Экран успешной проверки ОЗУ приведен ниже (рисунок 4). Для выхода из режима проверки необходимо нажать клавишу `Esc`, при этом произойдет перезагрузка ПК.

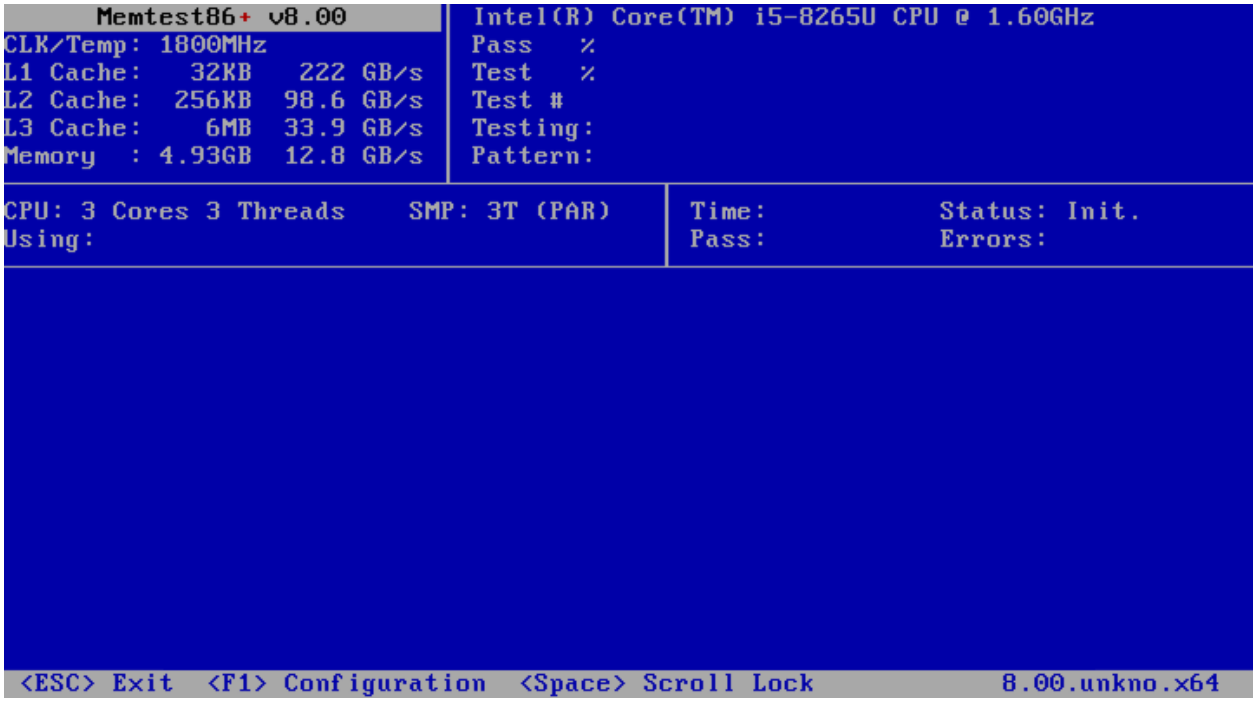

Рисунок 4 – Экран успешной проверки ОЗУ

е) Главный экран установщика ОС содержит семь разделов параметров, часть из которых заполнена автоматически, другая же часть (отмеченная красным цветом) требует вмешательства пользователя-установщика Системы (рисунок 5).

Для неотмеченных красным разделов возможно тоже может понадобиться дополнительная настройка, например, при подключении ОС к локальной сети рекомендуется изменить значение "Имя узла" на имя узла, соответствующее правилам вашей сети. В случае отсутствия подключения к сети или при ошибке автоопределения необходимо также правильно установить часовой пояс.

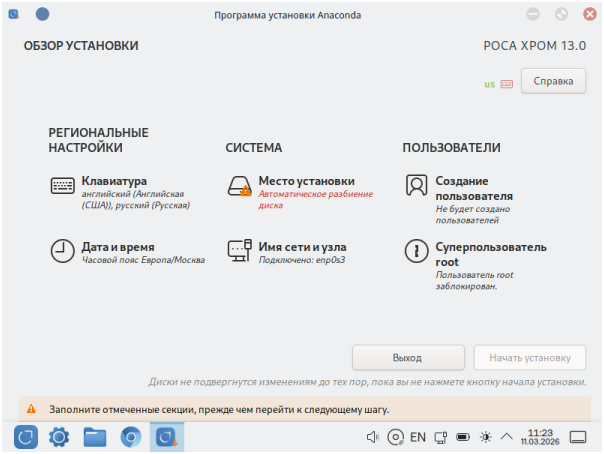

Рисунок 5 – Главный экран установщика Системы

ж) Для разметки установочного накопителя используется раздел "Место установки" (рисунок 6).

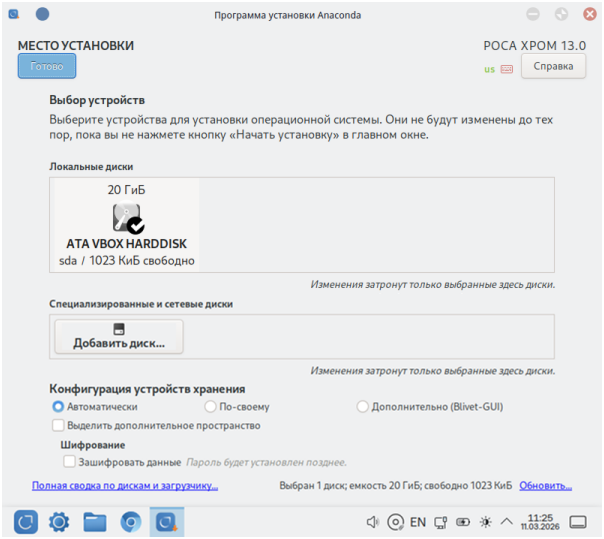

Рисунок 6 – Место установки системы

Если предполагается установка Системы на пустой носитель или же на выделенное на носителе пустое место, рекомендуется использовать автоматическую

разметку. Для этого достаточно нажать на кнопку Готово, при этом, кроме технического раздела /boot/efi, будет создан отдельный корневой раздел под ОС и раздел под файлы пользователей /home, а также раздел swap для расширения оперативной памяти. Стандартная разметка дает возможность быстрого восстановления работоспособности Системы при любых её отказах, для этого достаточно переустановить Систему в корневом разделе, не форматируя раздел с пользовательскими файлами.

По умолчанию ОС устанавливается на журналируемую ФС Ext4, но в инсталляторе также имеется возможность установки на Ext3, XFS и BTRFS. Кроме того, возможно форматировать и подключать диски с NTFS.

з) Для повышения защищенности информации есть возможность установить Систему на зашифрованный диск. Подробнее об установке системы с использованием средств маскирования рассмотрено в разделе 3.

и) Далее ввести учетные данные первого пользователя. По умолчанию он является администратором Системы, от его имени можно вводить консольные root-команды, используя sudo, и изменять критичные настройки Системы (рисунок 7). Подробнее о пользователях и администраторах см. раздел 2.2 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

Важно – При необходимости инсталляции ОС без создания пользователей данный раздел установки должен быть пропущен. Пользователь в Системе будет создан позднее, при первом запуске ОС;

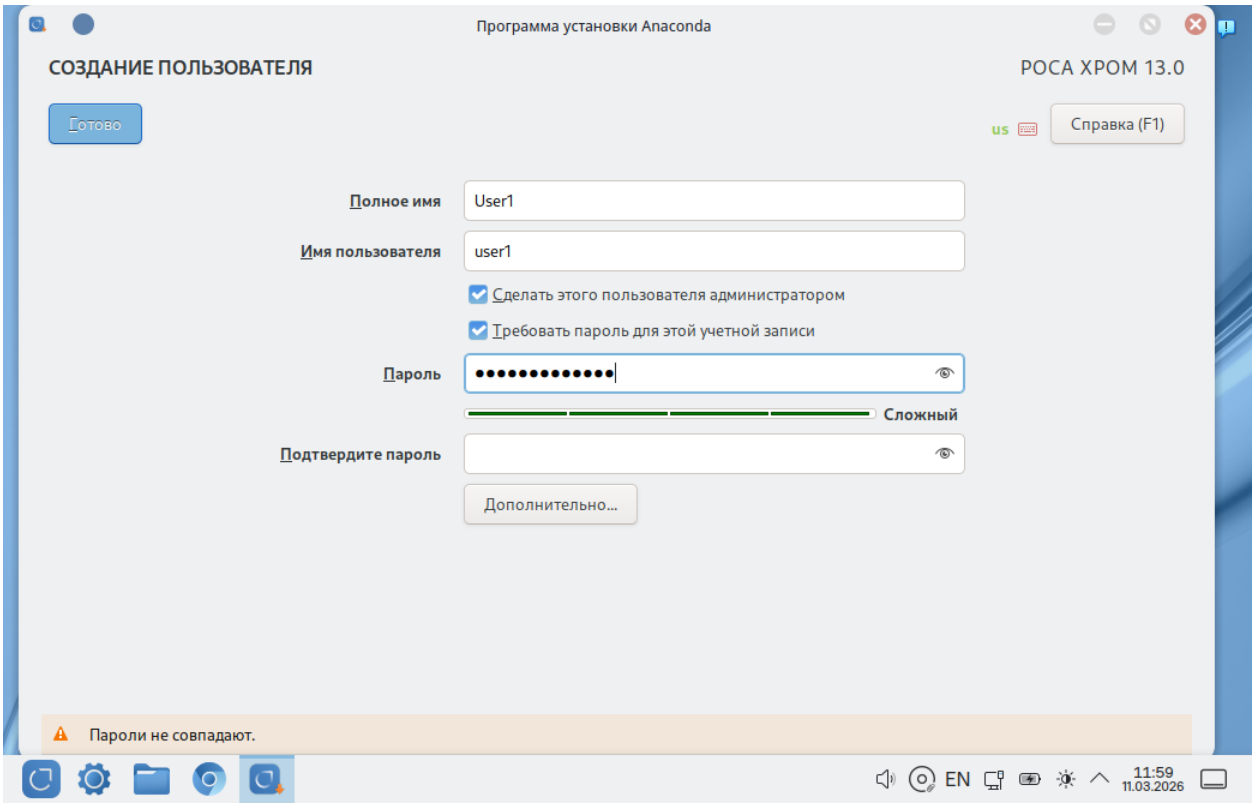

Рисунок 7 – Создание учетной записи пользователя

При вводе пароля контролируется его сложность: по длине, разнообразию знаков и по соответствию спискам часто применяемых паролей, но при этом сохраняется возможность использования небезопасных паролей при двойном нажатии на кнопку `Готово`.

к) Если при создании пользователя снять флажок "Сделать этого пользователя администратором", то обязательным останется следующее поле "Суперпользователь root", в которое необходимо ввести пароль суперадминистратора. Такая возможность оставлена для совместимости, при этом вводимый по умолчанию пользователь-администратор с правом sudo считается более безопасным вариантом.

л) После того как все обязательные пункты для установки заполнены, можно начать собственно установку ОС на ПК нажатием на кнопку `Начать установку` на главном экране установщика (рисунок 5).

м) Установка ОС может занять некоторое время, по завершении которого отобразится соответствующее сообщение (рисунок 8). После чего необходимо выполнить перезагрузку ПК, нажав кнопку `Перезагрузка системы`, в процессе которой необходимо извлечь установочный компакт-диск или флеш-накопитель.

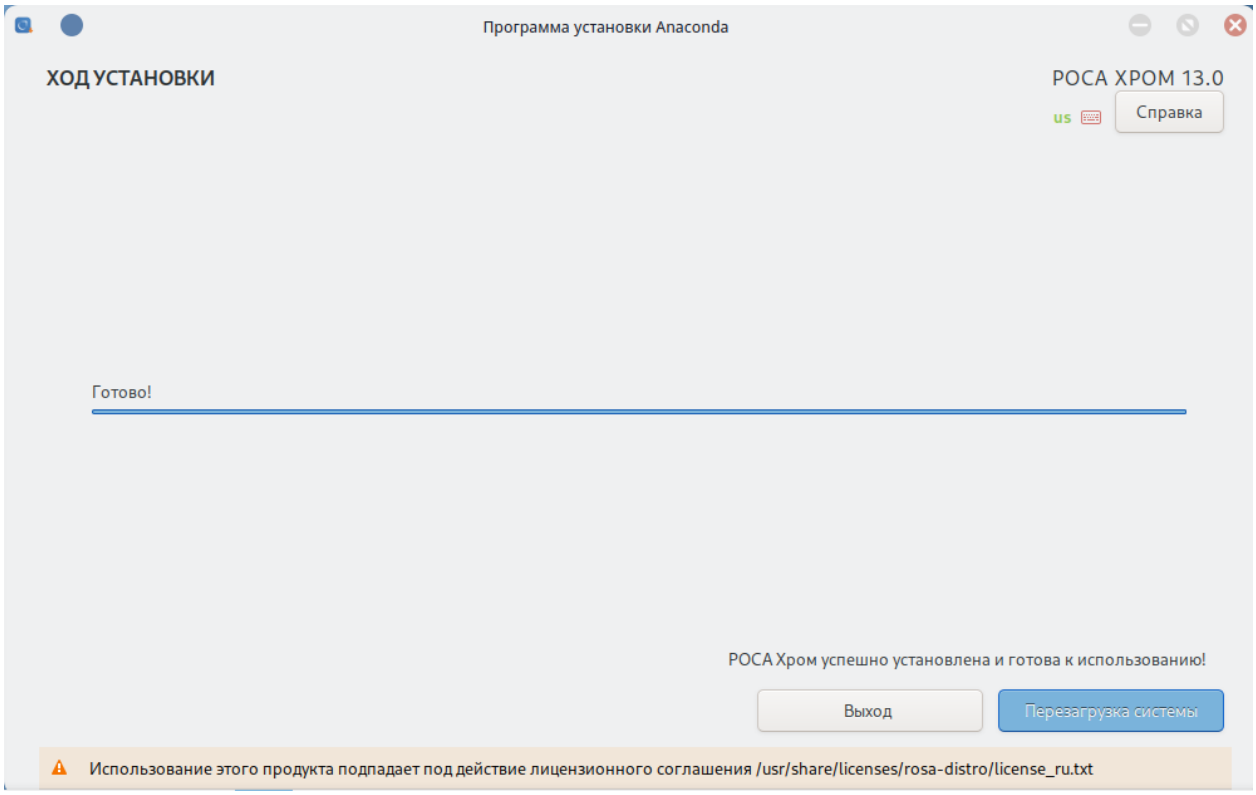

Рисунок 8 – Завершение процесса установки системы

н) После перезагрузки необходимо ввести (выбрать) логин и пароль учетной записи для выполнения входа в Систему. Если ОС была установлена на зашифрованные разделы, также понадобится ввести пароль для их расшифровки.

2.3 Установка серверной версии ОС

Установка серверной версии ОС осуществляется полностью аналогично установке на рабочую станцию (п. 2.2), за исключением того, что у серверной версии отсутствует live-режим. В меню начальной загрузки следует выбрать пункт "Установка ROSA Linux" для установки без предварительной загрузки ОС.

2.4 Парольная защита загрузчика ОС

Для повышения уровня безопасности возможно ограничить доступ к редактированию параметров загрузки, установив пароль на загрузчик GRUB2.

Этапы настройки пароля:

а) Генерация хеша пароля командой:

```
sudo grub2-mkpasswd-pbkdf2
```

Будет предложено ввести и подтвердить пароль. В результате отобразится хеш пароля, например:

```
Хэш PBKDF2 вашего пароля:
grub.pbkdf2.sha512.10000.7730DD2A5B6B5C31CD447BB9A8C313DC...
```

б) Создание конфигурационного файла с ограниченными правами доступа:

```
(umask 077 && touch /boot/grub2/user.cfg )
```

в) Запись сгенерированного хеша пароля в файл `/boot/grub2/user.cfg`:

```
echo "GRUB2_PASSWORD=grub.pbkdf2.sha512.10000.7730DD2A5B6B5C31CD
447BB9..." >
/boot/grub2/user.cfg
```

г) Обновление конфигурации GRUB2 применением изменений:

```
sudo update-grub2
```

После выполнения данных действий при попытке редактирования записей загрузчика GRUB2 (например, при нажатии клавиши `E` в меню загрузки) потребуется ввод пароля. Имя пользователя – root, пароль соответствует ранее заданному при генерации хеша.

3 УСТАНОВКА С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ МАСКИРОВАНИЯ ИНФОРМАЦИИ

3.1 Общие вопросы

В этом разделе будут рассмотрены только особенности установки ОС на компьютер пользователя с использованием средств маскирования информации на носителях. В документации к защищенным ОС используется термин "шифрование", если это шифрование является сертифицированным для защиты информации. В данном документе для несертифицированных к применению в РФ алгоритмов и программ шифрования используется термин "маскирование информации". Такое маскирование не обеспечивает гарантированной защиты информации, но значительно затрудняет неавторизованный доступ к ней.

3.2 Разметка носителя с маскированием информации

Для повышения защищенности информации есть возможность установить Систему с использованием маскирования информации, при этом разметку носителя можно осуществить автоматически, включив флажок "Зашифровать данные" или вручную.

Для режима разметки вручную в окне "Место установки" нужно выбрать в разделе "Конфигурация устройств хранения" переключатель "По-своему" и нажать на кнопку `Готово` , а потом разметить носитель с отдельным незашифрованным /boot (и /boot/efi для efi-BIOS). Корневой раздел Системы, swap-раздел и пользовательский раздел /home нужно при этом зашифровать (замаскировать), установив соответствующий флажок в поле "Зашифровать данные", затем кнопки `Применить` и `Готово` (рисунок 9).

Следует обратить внимание, что замаскированные разделы обозначены как LUKS-разделы. Рекомендуется использовать систему маскирования luks2.

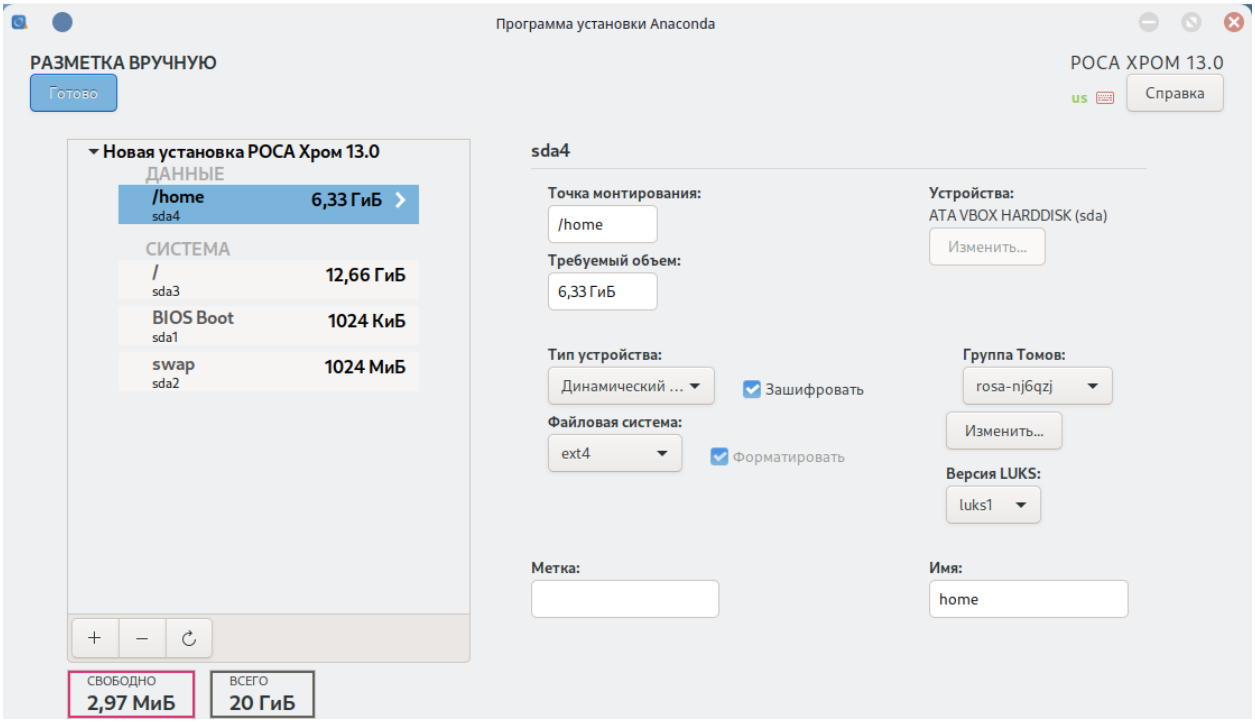

Рисунок 9 – Ручная разметка диска для использования маскирования

После этого можно выполнить установку в обычном режиме. При каждой загрузке Системы, использующей замаскированные разделы, у пользователя запрашивается пароль для расшифровки. Без ввода правильного пароля доступ к информации на носителях будет блокирован, причем эта блокировка сохраняется и при переносе носителя информации на другой ПК.

3.3 Поддержка tpm2 для автоматического ввода паролей

Современные СВТ с архитектурой x86_64 примерно с 2016-го года оснащаются встроенным модулем хранения конфиденциальной информации tpm2, который можно использовать для разблокировки замаскированного раздела LUKS. Пароль расшифровки маскированных разделов при этом будет храниться в tpm2 и вводиться автоматически. Пользовательская информация на изъятом из компьютера с tpm2 носителе будет недоступна при монтировании этого носителя на другом компьютере.

Для использования tpm2 в Системе, использующей разделы с маскированием информации, нужно ввести команду и следовать дальнейшим инструкциям:

```
sudo luksunlock
```

Для возврата к ручному вводу паролей используется команда:

```
sudo lukslock
```

4 УСТАНОВКА НА ВИРТУАЛЬНУЮ МАШИНУ

Образ ОС подготовлен для установки и работы на виртуальных машинах (далее – ВМ) в системах виртуализации ROSA Virtualization, Microsoft Hyper-V, VirtualBox, QEMU/KVM и ESXi VMWARE. В ОС предустановлены пакеты для поддержки совместимости (virtualbox-guest-addidtions, spice-vdagent и open-vm-tools), лишние из которых удаляются при установке в несовместимой среде.

Установка под управлением гипервизора должна осуществляться согласно документации к этому гипервизору с учетом минимальных требований ОС к аппаратному обеспечению (п. 1.4 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02)).

5 АВТОМАТИЗИРОВАННОЕ РАЗВЕРТЫВАНИЕ

5.1 Введение в kickstart-сценарии

Автоматизированная установка позволяет выполнить полностью автоматическую установку в соответствии с преднастройками, может применяться для автоматического развертывания множества компьютеров одинаковой конфигурации.

Для автоматизированной установки создается файл с настройками – kickstart-сценарий – сценарий быстрого развертывания. Затем в параметры cmdline ядра записывается путь к этому файлу, по DHCP автоматически настраивается сеть, а модуль anaconda-dracut в initramfs (образ файловой системы, загружаемый в оперативную память вместе с ядром) загружает этот kickstart-сценарий и сохраняет в файле /run/install/ks.cfg.

При установке в любом из режимов, в том числе в интерактивном графическом, в установленной Системе по адресу /root/anaconda-ks.cfg сохраняется kickstart-сценарий, описывающий произведенную установку, который можно взять за основу для пользовательского сценария в дальнейшем.

5.2 Типовой сценарий автоматизированной установки

Для реализации типового сценария автоматизированной установки нужно создать файл, например, с именем a.ks, со следующим содержимым:

```
cmdline
# https://bugzilla.redhat.com/show_bug.cgi?id=1874434
liveimg --url=file:///dev/mapper/live-base

# Автоматически принять лицензионное соглашение
eula --agreed

# System language
lang ru_RU.UTF-8

# Keyboard layouts
keyboard --xlayouts=us,ru --switch=grp:alt_shift_toggle

# Network information
```

```
network --hostname=localhost.localdomain

# SELinux configuration
#selinux --disabled

# System services
services --enabled="chronyd"

autopart
# Partition clearing information
clearpart --all --initlabel

# System timezone
timezone Europe/Moscow --utc

# Passwords
rootpw 123456
user --groups=wheel,users --name=rosa --password=123456

%anaconda
pwpolicy root --minlen=6 --minquality=1 --notstrict --nochanges
--notempty
pwpolicy user --minlen=6 --minquality=1 --notstrict --nochanges
--emptyok
pwpolicy luks --minlen=6 --minquality=1 --notstrict --nochanges
--notempty
%end

reboot --eject
```

Примечание — С документацией по kickstart-сценариям можно ознакомиться по адресу https://pykickstart.readthedocs.io/en/latest/kickstart-docs.html.

Код приведенного выше сценария состоит из следующих командных строк:

а) Выполняется полностью автоматизированная установка: запускается X-сервер, автоматически запускается установка, не требующая настройки (возможны варианты без X-сервера и установка по VNC):

```
cmdline
```

б) Копируется на накопитель Система из LiveCD (также возможна установка из сетевого репозитория):

```
liveimg --url=file:///dev/mapper/live-base
```

в) Устанавливается язык ОС ru_RU.UTF-8 (в файле /etc/locale.conf):

```
lang ru_RU.UTF-8
```

г) Добавляются в ОС две раскладки клавиатуры: us и ru, а переключение раскладок настраивается на комбинацию клавиш `Alt+Shift`:

```
keyboard --xlayouts=us,ru --switch=grp:alt_shift_toggle
```

д) Включается служба systemd chronyd (можно перечислить несколько служб через запятые без пробелов):

```
services --enabled="chronyd"
```

Пример отключения sshd:

```
services --disabled="sshd"
```

е) Выполняется полностью автоматизированная разметка диска с удалением всех данных (возможно прописать детализированные инструкции по разметке диска):

```
clearpart --all --initlabel
```

ж) Устанавливается часовой пояс "Европа/Москва", а аппаратные часы (BIOS) будут выставлены по Гринвичу (рекомендуется):

```
timezone Europe/Moscow --utc
```

з) Устанавливается последовательность символов, например, "123456", в качестве root-пароля:

```
rootpw 123456
```

и) Создается пользователь с именем, например, "rosa", добавляется в группы wheel и users; устанавливается пароль пользователя, например, "123456":

```
user --groups=wheel,users --name=rosa --password=123456
```

Примечание — Группа wheel – специальная группа пользователей, используемая в некоторых системах UNIX для контроля доступа к команде su, которая позволяет пользователю маскироваться под другого пользователя (обычно суперпользователя).

Пароли можно записать в зашифрованном виде, например, установить пароль пользователю root:

```
rootpw --iscrypted $6$BHWkSXIw6TgPrdvJ$V1ARg/yAP.kRe5mo5FawOOvf7
SRm/GDM.Ly6RGGmSBR3Zc81/XzYlpoDnYKFMMPZodKBIVyBvjJ9evM1sey0E/
```

Хеш, приведенный выше, является результатом выполнения команды:

```
python3 -c "import crypt; print(crypt.crypt(input('clear-text
pw: '), crypt.mksalt(crypt.METHOD_SHA512)))"
```

Данная команда позволяет получить хеш введенного с клавиатуры пароля. Таким образом, можно избежать хранения пароля в открытом виде. Например, хеш пароля "123456" выглядит следующим образом:

```
user --groups=wheel,users --name=rosa
--password=$6$BHWkSXIw6TgPrdvJ$V1ARg/yAP.kRe5mo5FawOOvf7SRm/GDM.
Ly6RGGmSBR3Zc81/XzYlpoDnYKFMMPZodKBIVyBvjJ9evM1sey0E/
--iscrypted
```

к) По завершении установки необходимо перезагрузить ПК (в процессе перезагрузки необходим установочный носитель):

```
reboot --eject
```

Примечание — При установке на ВМ рекомендуется использовать установку с ISO-образа, подключенного как DVD, т.к. гипервизор умеет отключать виртуальный привод по команде извлечения диска из гостевой Системы. В таком случае после перезагрузки Система загрузится не с образа, а с диска с установленной ОС.

Параметры в cmline ядра и в kickstart-сценарии дополняют друг друга и могут использоваться в различных комбинациях.

5.3 Дополнительные действия в kickstart-сценариях

В kickstart-сценарий могут быть добавлены произвольные действия, выполняемые в интерпретаторе shell после завершения основной установки. Это позволяет настраивать Систему сразу после инсталляции.

Для выполнения действий в установленной Системе (в chroot) используется секция %post:

```
%post
<команды>
%end
```

Пример: запись даты и времени установки в файл /var/log/installtime.

```
%post
LC_ALL=C date > /var/log/installtime
%end
```

Если необходимо выполнить действия вне установленной Системы (в окружении LiveCD), в секцию %post добавляется параметр --nochroot:

```
%post –nochroot
LC_ALL=C date > "${INSTALL_ROOT}/var/log/installtime"
%end
```

Примечание — Дополнительно возможно загрузить внешние файлы с помощью утилит curl, wget и других средств сетевого доступа, при наличии доступа к локальному или внешнему веб-серверу.

Удаление и установка пакетов могут быть выполнены также внутри секции %post:

- Удаление ненужных пакетов:

```
%post
sudo dnf -q -y remove firefox-esr52
%end
```

- Установка дополнительных пакетов:

```
%post
dnf -q -y install sconfigs-detailed-audit
%end
```

Прямая установка пакетов через секцию %packages в данной конфигурации не поддерживается. Рекомендуется использовать утилиту dnf с ключом "-q" для подавления лишнего вывода, что повышает стабильность автоматизированной установки.

Для тестирования сценария автоматизированной установки можно воспользоваться встроенным HTTP-сервером на машине оператора:

а) Определить IP-адрес оператора:

```
ip a
```

б) Перейти в директорию с файлом сценария (например, a.ks) и запустить сервер:

```
python3 -m http.server
```

Примечание — В качестве альтернативы возможно использование других веб-серверов, например, nginx или Apache httpd.

в) На целевой машине при загрузке LiveCD в командную строку ядра необходимо добавить:

```
systemd.unit=anaconda.target
inst.ks=http://192.168.1.173:8000/a.ks
```

где:

- 192.168.1.173 – IP-адрес машины оператора,
- 8000 – порт запущенного HTTP-сервера.

Также рекомендуется добавить параметр inst.text. Данный параметр позволит запустить консольный режим установщика вместо графического. Установка будет произведена автоматически без участия оператора.

6 СЕТЕВАЯ ЗАГРУЗКА С ВОЗМОЖНОСТЬЮ УСТАНОВКИ

6.1 Технология Intel PXE

Возможность загрузки ОС по сети реализована с помощью стандартной технологии PXE, которая состоит из следующих этапов:

а) Встроенный в BIOS компьютера загрузчик PXE:

- получает IP-адрес по протоколу BOOTP (протокол, родственный DHCP);
- скачивает по протоколу TFTP с сервера TFTP файлы загрузчика, в т.ч. сам загрузчик и конфигурационный файл с описанием меню загрузки, а также элементы vmlinuz и initrd в качестве минимальной версии ОС;
- запускает минимальную версию ОС с указанными в конфигурационном файле параметрами.

б) Минимальная версия ОС, запущенная на клиентском компьютере:

- скачивает указанные в параметрах запуска initrd установочный образ и дополнительные компоненты полной версии ОС по протоколу HTTP с установленного на сервере PXE веб-сервера, сохраняя их в оперативной памяти;
- запускает скачанную полную версию ОС на клиенте.

Таким образом, на клиентском компьютере запускается тот же установочный образ LiveCD, что и при загрузке с USB-накопителя или DVD.

Следует учесть, что для сетевой загрузки ОС на клиентской системе требуется на 2 Гб оперативной памяти больше, чем для обычной установки.

6.2 Начальная настройка сервера для работы PXE

Для сетевой загрузки и установки на рабочих станциях необходим сервер, с которого будут загружаться образы ОС, и локальная сеть, по которой будет происходить загрузка. В качестве сервера можно использовать как установленную локально или в виртуальной машине версию ОС для рабочей станции, так и серверную версию ОС.

Для того чтобы ОС могла работать в качестве сервера PXE, необходимо установить и настроить серверные пакеты. Для настройки понадобятся сервера DHCP и TFTP (простейший веб-сервер для загрузки по HTTP уже предустановлен), а также загрузчик syslinux:

```
dnf install dhcp-server tftp-server syslinux
```

6.3 Настройка сервера DHCP (BOOTP)

Конкретная настройка DHCP-сервера специфична для каждой локальной сети. В качестве примера можно рассмотреть по шагам простейший случай:

а) установить на сервере PXE для текущего сетевого соединения статический IP-адрес 192.168.1.1 и маску подсети 255.255.255.0;

б) заменить содержимое файла настройки /etc/dhcpd.conf на следующее:

```
  option domain-name "rosa.lan";
  option domain-name-servers ns1.rosa.lan, ns2.rosa.lan;
  default-lease-time 3600;
  max-lease-time 7200;
  authoritative;allow booting;
  allow bootp;
  filename "pxelinux.0";
  subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers 192.168.1.1;
  option subnet-mask 255.255.255.0;
  option domain-search "rosa.lan";
  option domain-name-servers 192.168.1.1;
  range 192.168.1.10 192.168.1.100;
  }
```

в) включить сервис DHCP командой:

```
sudo systemctl enable --now dhcpd
```

г) статус запущенного сервера (должен быть active) можно проверить командой:

```
systemctl status dhcpd
```

Правильность подключения можно проверить, войдя в сеть с клиентского компьютера: он должен получить от сервера DHCP IP-адрес 192.168.1.10.

6.4 Настройка веб-сервера

В предустановленном на образах ОС языке Python есть простой веб-сервер, который можно использовать для тестовой PXE-установки (потребуется ISO-образ ОС), последовательно выполнив следующие команды:

а) создать папку для веб-сервера:

```
mkdir -p "$HOME/webserver"
```

б) перейти в папку $HOME/webserver :

```
cd "$HOME/webserver"
```

в) создать папку для ISO-образа:

```
mkdir -p ISO
```

г) монтировать папку для ISO-образа:

```
sudo mount -o loop "<путь к ISO-образу>" "$HOME/webserver/ISO"
```

д) запустить HTTP-сервер из папки:

```
python3 -m http.server
```

Далее необходимо скопировать в папку $HOME/webserver файл kickstart-сценария a.ks, создание которого описано в п.5.2.

Консоль, в которой будет работать веб-сервер, следует оставить открытой. Проверить правильность его настройки можно, открыв на компьютере браузер по адресу http://192.168.1.1:8000.

В браузере должны быть выведены файлы из директории веб-сервера, в том числе должны быть доступны папка ISO, ее содержимое и файл kickstart-сценария a.ks, а в консоли веб-сервера должен быть выведен лог запросов к нему.

6.5 Настройка сервера TFTP

Для настройки сервера TFTP нужно выполнить следующие действия:

а) скопировать в папку сервера TFTP компоненты первоначального загрузчика:

```
( cd /usr/share/syslinux && cp -v menu.c32 pxelinux.0
ldlinux.c32 libutil.c32 /var/lib/tftpboot/ )
```

б) скопировать минимальную версию ОС из ISO-образа в папку TFTP-сервера (от имени пользователя, но не root):

```
( cd "$HOME/webserver/ISO/isolinux" ; sudo cp -v initrd0.img
vmlinuz0 /var/lib/tftpboot/ )
```

в) создать папку для дополнительных конфигурационных файлов TFTP-сервера:

```
mkdir -p /var/lib/tftpboot/pxelinux.cfg
```

г) открыть на редактирование файл /var/lib/tftpboot/pxelinux.cfg/default (будет создан, если не существует):

```
nano /var/lib/tftpboot/pxelinux.cfg/default
```

Содержимое файла /var/lib/tftpboot/pxelinux.cfg/default:

```
  default menu.c32
  prompt 0
  timeout 300
  ONTIME local
  menu title #================ PXE BOOT ===============#
  label 1
  menu label ^1) Automatically install ROSA
  kernel /vmlinuz0
  append initrd=/initrd0.img systemd.unit=anaconda.target
  enforcing=0
  root=live:http://192.168.1.1:8000/ISO/LiveOS/squashfs.img
  inst.text inst.ks=http://192.168.1.1:8000/a.ks
  label 2
  menu label ^2) Install ROSA
  kernel /vmlinuz0
  append initrd=/initrd0.img enforcing=0
  root=live:http://192.168.1.1:8000/ISO/LiveOS/squashfs.img
```

Для сохранения данных и выхода из редактора nano нажимают клавиши `Ctrl+O` и `Ctrl+X` соответственно.

В строках, начинающихся с append, определены параметры cmdline ядра для вариантов загрузки в меню. В первом случае запускается автоматизированная консольная установка по kickstart-сценарию, а во втором случае запускается LiveCD. При отсутствии выбора со стороны пользователя какого-либо пункта меню в течение 300 секунд будет произведена загрузка первого пункта.

Следует обратить внимание, что приведенный выше kickstart-сценарий автоматически стирает весь диск, т.е. в приведенной конфигурации, если не выбрать второй пункт меню, будет произведена автоматическая установка с форматированием диска. При запуске ОС по PXE можно выбрать нужный пункт меню. При необходимости можно адаптировать меню под свои потребности (дополнительная информация доступна по ссылке https://wiki.syslinux.org/wiki/index.php?title=PXELINUX).

д) запустить и добавить в автозагрузку TFTP-сервер:

```
sudo systemctl enable --now tftp
```

е) выполнить настройки BIOS клиентской машины на загрузку по сети (PXE) и произвести загрузку.

6.6 Настройка сети в LiveCD

По умолчанию при запуске LiveCD, включая режим работы исключительно установщика ОС, настройка сети осуществляется автоматически по протоколу DHCP.

В случае необходимости задания статических сетевых параметров соответствующая конфигурация может быть передана в ядро через параметр cmdline, используя синтаксис, поддерживаемый модулем dracut network-legacy.

Пример задания параметров сети вручную:

```
ip=192.168.122.50::192.168.122.1:255.255.255.0:::off
```

где:

- 192.168.122.50 – IP-адрес сетевого интерфейса;
- 192.168.122.1 – шлюз по умолчанию;
- 255.255.255.0 – маска подсети;

– off – отключение автоматической настройки через DHCP.

Примечание — Дополнительные сведения о параметрах и форматах можно найти на справочной странице dracut.cmdline(7).

7 ОБНОВЛЕНИЕ НА ПЛАТФОРМУ ОС РОСА13

Обновление с платформы 2021.1 (ОС РОСА "ХРОМ" 12) на платформу ОС РОСА "ХРОМ" 13 осуществляется с помощью загрузки и устновки пакета update-r12-to-r13. Загрузка пакета может быть выполнена из командной строки или с использованием графической программы "Пакеты" (dnfdragora).

Установка пакета из командной строки выполняется командой:

```
sudo dnf install update-r12-to-r13
```

Так как в процессе обновления заменяются все графические библиотеки, обновление должно выполняться в консольном режиме. Запуск процедуры обновления из рабочей графической сессии не рекомендуется. Для запуска обновления необходимо выполнить скрипт update-r12-to-r13 из TTY с правами администратора:

```
sudo update-r12-to-r13
```

Если в Системе установлена графическая оболочка, например KDE Plasma, запуск процедуры обновления также может быть выполнен из менеджера входа GDM, если соответствующий вариант запуска доступен в списке сеансов. В этом случае перед входом в Систему в менеджере входа выбирается сеанс обновления (рисунок 10), предоставляемый пакетом update-r12-to-r13, после чего выполняется вход под учетной записью пользователя с правами администратора и запускается процедура обновления.



Рисунок 10 – Запуск скрипта обновления

Важно:

– **Обновление системы:** Обновление следует выполнять из стандартных репозиториев РОСА, предварительно протестировав совместимость стороннего ПО с ОС РОСА "ХРОМ" 13 для сохранения его работоспособности.

– **Резервное копирование:** Перед обновлением необходимо создать резервную копию Системы и пользовательских данных, а также подготовить загрузочный флеш-накопитель с ОС РОСА "ХРОМ" 12 на случай сбоя.

– **Альтернативная установка:** При невозможности выполнить обновление с помощью скрипта update-r12-to-r13 вследствие нестандартной конфигурации Системы допускается ручная переустановка ОС до версии 13 с сохранением пользовательских данных, если каталог /home в ОС версии 12 был размещен на отдельном разделе. В таком случае при установке ОС версии 13 в инсталляторе должен быть выбран ручной способ разметки диска: для корневого раздела должно быть указано форматирование, а раздел с пользовательскими данными /home должен быть подключен без форматирования.

– **Логирование:** Журнал процесса обновления сохраняется в файле /var/log/update_platform.log.

– **Лицензирование:** Для платных версий ОС РОСА "ХРОМ" перед началом обновления требуется ввести ключа доступа к новой платформе.

– **Обновление оболочки:** При переходе на ОС версии 13 сохраняется оболочка KDE Plasma 5, а последующее обновление до Plasma 6 выполняется через установку и запуск скрипта update-kde5-to-kde6.

8 ГРАФИЧЕСКАЯ УСТАНОВКА С ИСПОЛЬЗОВАНИЕМ VNC

Графическая установка с применением технологии VNC (Virtual Network Computing) позволяет запускать графический интерфейс установщика ОС на удалённой машине оператора без необходимости постоянного локального доступа к целевому оборудованию. Этот способ особенно полезен в случаях, когда установка производится на удалённый компьютер, не имеющий локальных устройств ввода и отображения (монитор, клавиатура, мышь), либо физический доступ к нему затруднён.

Поддержка VNC-установки встроена в стандартные образы ОС РОСА "ХРОМ".

Перед началом установки по VNC должно быть обеспечено выполнение следующих условий:

- установочный ISO-образ ОС РОСА "ХРОМ" загружен на целевую машину;
- обеспечена возможность первичного запуска образа (локально или через средства удалённого управления);
- целевая Система загружена с установочного образа;
- имеется сетевое соединение между целевой Системой и рабочим местом администратора;
- на стороне администратора установлен VNC-клиент.

Установка по VNC реализуется встроенными средствами установщика ОС Anaconda.

Для выполнения установки ОС с использованием VNC необходимо последовательно выполнить следующие действия:

а) На целевой машине выполнить загрузку Системы с установочного ISO-образа.

б) В меню загрузчика GRUB выбрать "Инженерное меню → Установка по VNC" (рисунок 11).

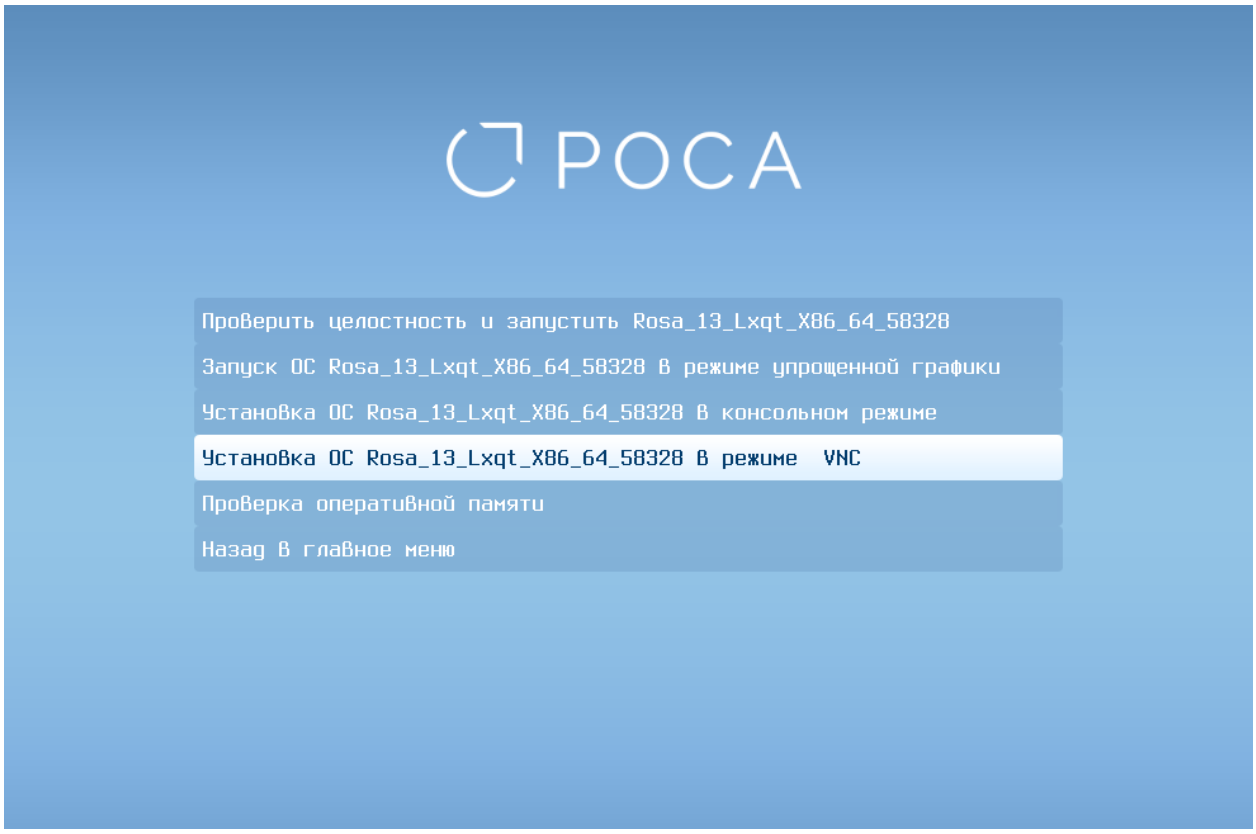

Рисунок 11 – Инженерное меню → Установка по VNC

в) Система автоматически запускает установщик ОС Anaconda.

г) После запуска установщика ознакомиться с информацией (рисунок 12), отображаемой в консоли, содержащей:

- IP-адрес целевой системы;
- номер дисплея VNC (например, " : 1").

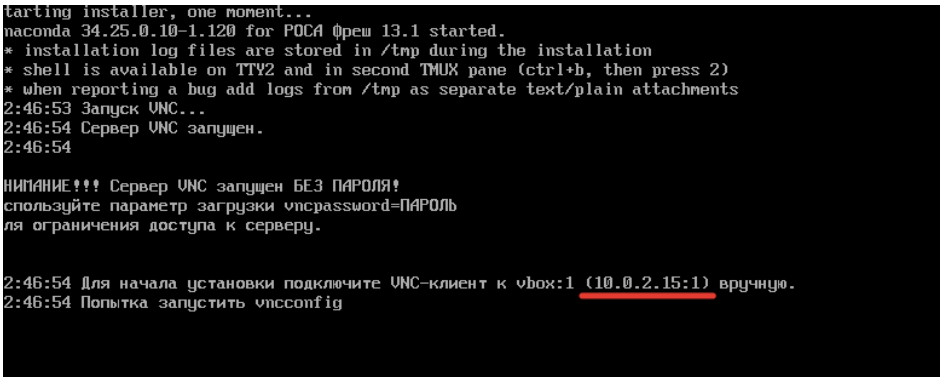

Рисунок 12 – Информация о IP-адресе и номер дисплея VNC целевой системы

д) На рабочем месте администратора необходимо запустить VNC-клиент и выполнить через него подключение к целевой системе, указав адрес в формате:

```
IP-адрес:номер_порта
Например: 192.168.1.100:1
```

е) После установления соединения на целевом компьютере автоматически откроется окно графического установщика ОС Anaconda, идентичное локальному интерфейсу установки. Можно приступить к стандартному графическому процессу установки (об этом подробнее см. раздел 2), управляя им удалённо.

9 OEM-УСТАНОВКА

OEM-установка предназначена для массового развёртывания ОС на однотипные компьютеры. В этом методе на жёсткий диск целевой машины побайтово копируется ISO-образ, а не клон уже установленной Системы. После копирования машины могут быть переданы конечным пользователям без дополнительной настройки.

При первом запуске администратор подтверждает установку ОС, после чего у него отсутствует возможность вмешаться в процесс. После завершения установки, при первом старте Систмы, будет предложено создать пользователей и подтвердить лицензионное соглашение.

Преимущества OEM-установки:

– размер образа для OEM-установки равен размеру стандартного ISO, что значительно меньше по сравнению с клон-образом уже установленного диска;
– после подтверждения пользователем установки исходный ISO-образ остаётся на первом разделе, что позволяет при неповреждённой файловой системе вернуть Систему к состоянию "первого старта";
– создание ISO-образа для OEM-установки происходит быстрее и проще, что снижает вероятность ошибок.

При выполнении OEM-установки автоматически создаётся отдельный служебный раздел, содержащий эталонный ISO-образ ОС. Данный раздел используется для хранения исходного образа Системы и обеспечивает возможность быстрого восстановления или повторной установки ОС с возвратом к состоянию "первого запуска" без использования внешнего установочного носителя.

OEM-образ формируется в два этапа:

а) Сборка образа на ABF. Необходимо, чтобы в сборке присутствовал пакет oem-install. С 2025 года данный пакет включается во все стандартные образы ОС РОСА "ХРОМ". Он не мешает установке через Anaconda и будет автоматически удалён на этапе initial-setup.

б) Пересборка с помощью скрипта oem-iso-rebuilder. Основная задача этого скрипта – заменить конфигурационный файл загрузчика GRUB2 в ISO-образе, чтобы при загрузке запускался oem-install вместо Live OS или Anaconda. Кроме того, скрипт меняет таблицу разделов на GPT и даёт возможность добавить файлы, влияющие на поведение OEM-установки.

Пример пересборки:

```
sudo oem-iso-rebuilder\ ./ ROSA.CHROME.PLASMA6.13.0.x86_64.iso
```

После запуска утилита предложит приостановить выполнение, чтобы добавить собственные конфигурационные файлы. По завершении будет получен новый образ с расширением .oem.iso.

Установка OEM-образа производится побайтовым копированием ISO-образа на носитель, для этого можно использовать утилиту dd:

```
dd if=./ROSA.CHROME.PLASMA6.13.0.x86_64.oem.iso of=/dev/sda
bs=4M
```

При пересборке ISO допускается добавить в его корень следующие файлы:

– oem-install.cfg – конфигурация разметки дисков, например:

```
PARTITONS=btrfs
ROOTSIZE=70000
SWAPSIZE=10000
EFISIZE=200
```

Подробнее обо всех параметрах можно узнать, выполнив команду:

```
/usr/libexec/oem-install --help
```

– anaconda-ks.cfg – kickstart-файл, который обычно создаётся Anaconda, будет скопирован в /root установленной Системы;

– oem-install.css – стили интерфейса GUI для oem-install, шаблон доступен в /usr/share/oem-install/oem-install.css.

10 УСТАНОВЩИК ISO2IMG

Утилита iso2img представляет собой простой скриптовый инструмент, позволяющий в один шаг установить ОС РОСА "XPOM" из ISO-образа в образ виртуальной машины (qcow2, vmdk, vdi и др.). При этом будет создан пользователь rosa с паролем rosa и правами администратора.

Установка и использование утилиты iso2img:

```
sudo dnf install iso2img
sudo iso2img Rosa.iso
```

В результате будет получен, например, файл Rosa.qcow2, который можно запустить напрямую:

```
qemoo Rosa.qcow2
```

Для получения дополнительных параметров необходимо обратиться к справке через команду:

```
iso2img –help
```

11 ПОДГОТОВИТЕЛЬНЫЕ ПРОЦЕДУРЫ ПОСЛЕ УСТАНОВКИ

После завершения установки ОС необходимо выполнить ряд подготовительных процедур, направленных на обеспечение безопасной и корректной работы Системы. Перечень мероприятий зависит от ролей, которые будет выполнять данная Система, требований к защите информации и политики безопасности организации.

Первоначальная настройка включает в себя следующие административные действия:

– Настройка системы аудита. Определяется перечень критически важных событий, подлежащих регистрации. По умолчанию активировано отслеживание основных системных событий. При необходимости следует расширить список контролируемых операций и определить действия при обнаружении инцидентов безопасности. Об этом подробнее см. разделы 6.6 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02) и 6.5.7 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка поведения служб при фиксации событий безопасности. Устанавливаются параметры реакции на критические события: запись в журнал, уведомления, обработка правилами службы auditd. Об этом подробнее см. разделы 6.6.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02) - 6.6.4 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка параметров хранения журналов аудита. Об этом подробнее см. раздел 6.6.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Установка пароля на загрузчик GRUB2. Ограничение доступа к параметрам загрузки делает невозможным изменение загрузочных настроек неавторизованными пользователями. Об этом подробнее рассмотрено в разделе 2.4.

– Создание учетных записей, групп и ролей. Формируется структура пользователей и групп в соответствии с функциональными обязанностями. Для каждой категории устанавливаются необходимые уровни доступа. Об этом подробнее см. главу 3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02)с и раздел 2.2.7 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка прав доступа к данным. Для создаваемых каталогов и файлов следует определить корректные права и владельцев, предотвращая несанкционированный доступ. Об этом подробнее см. раздел 6.1 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Определение политики установки и запуска программ. Настраиваются допустимые источники пакетов, методы установки и правила запуска системных и прикладных компонентов. Об этом подробнее см. разделы 2.6 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02) и 2.4.1 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка механизмов идентификации и аутентификации. Устанавливаются требования к паролям, сроки их действия, правила блокировки учётных записей и ограничения по числу неуспешных попыток входа. Об этом подробнее см. разделы 3.2 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02) и 3.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Организация резервного копирования. Создаются резервные копии системных настроек, данных и журналов. Определяется периодичность и набор инструментов для резервирования. Об этом подробнее см. раздел 6.2 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02)с.

– Настройка доверенных серверов точного времени. Корректное время необходимо для журналирования, сетевых взаимодействий и систем безопасности; рекомендуется использовать chrony. Об этом подробнее см. раздел 4.7 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Проверка целостности системных файлов. Настраиваются механизмы контроля целостности, позволяющие выявлять изменения критически важных компонентов. Об этом подробнее см. раздел 6.3 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка отказоустойчивости (при необходимости). При эксплуатации в критически важных средах может потребоваться настройка кластеров высокой доступности. Об этом подробнее см. раздел 6.7 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка квот и ограничений ресурсов. Определяются допустимые значения использования дискового пространства и памяти пользователями или группами. Об этом подробнее в разделе 6.5 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Настройка ограничений пользовательских сеансов. Устанавливаются параметры блокировки экрана, ограничения по времени бездействия и правила принудительного завершения сеансов. Об этом подробнее см. раздел 2.2.5 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02) и раздел 6.5.8 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

– Использование встроенной документации. Для получения справочной информации рекомендуется использовать встроенную систему документации `man`. Об этом подробнее см. раздел 2.3.8 "ОС РОСА Хром. Руководство администратора. Часть 2. Эксплуатация" (индекс – РСЮК.10502-01 32 02).

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин/Сокращение	Определение
АПМДЗ	Аппаратно-программный модуль доверенной загрузки
БД	База данных
ВМ	Виртуальная машина
ЗПС	Замкнутая программная среда
ИТ	Информационные технологии
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
СДЗ	Средство доверенной загрузки
СУБД	Система управления базой данных
УЗ	Учетная запись
ЦС	Центр сертификации
ФС	Файловая система
ACL	Access Control List – список контроля доступа
AIDE	Advanced Intrusion Detection Environment – усовершенствованная система обнаружения вторжений
API	Application programming interface – программный интерфейс приложения
BIOS	Basic Input/Output System – базовая подсистема ввода-вывода
CA	Certification authority – центр сертификации (удостоверяющий центр)
CIFS	Common Internet File System – протокол, являющийся частью протокола SMB, для удаленного подключения нескольких платформ – Windows, Linux или macOS, для идентификации и чтения файлов системы NTFS в Windows и HFS в macOS, чтобы совместно использовать эти файлы и принтеры между машинами с Windows и Linux
CSV	Comma separated values – текстовый формат, предназначенный для представления табличных данных
DHCP	Dynamic host configuration protocol – протокол динамической настройки сетевой конфигурации узла
DNS	Domain name system – система доменных имен
ENC	External node classifier – классификатор внешних хостов
ESR	Extended support release – релиз с расширенной (долговременной) поддержкой
Ext4	Fourth Extended Filesystem – журналируемая файловая система

Термин/Сокращение	Определение
Ext3	Third Extended Filesystem – журналируемая файловая система
GUI	Graphical User Interface – графический пользовательский интерфейс
HTTP	Hypertext transfer protocol – протокол передачи гипертекста
HTTPS	Hypertext transfer protocol secure – защищенная версия протокола передачи гипертекста
IP	Internet protocol – протокол межсетевого взаимодействия
IPv4	Internet Protocol Version 4 – версия 4 интернет-протокола
IPv6	Internet Protocol Version 6 – версия 6 интернет-протокола
IPP	Internet Printing Protocol – Интернет-протокол печати
IPA	Identity, policy and audit – система идентификации, политик и аудита (СИПА)
IPC	Interprocess Communication – средство межпроцессного взаимодействия
LDAP	Lightweight directory access protocol – протокол доступа к каталогам
LDAPS	Lightweight directory access protocol secure – защищенная версия протокола доступа к каталогам
LUKS	Linux Unified Key Setup – система шифрования дисков, которая хранит данные в зашифрованном физическом разделе
MAC	Media access control – уникальный идентификатор сетевого оборудования
MBR	Master boot record – главная загрузочная запись
MTA	Mail transfer agent – агент передачи почтовых сообщений
NTFS	New Technology File System – это проприетарная файловая система, разработанная компанией Microsoft
NTP	Network time protocol – протокол сетевого времени
SMB	Server Message Block – протокол соединения с устройствами со старыми версиями ОС Microsoft для подключения к серверам и обмена файлами
SMTP	Simple mail transfer protocol – протокол передачи почтовых сообщений
SSH	Secure shell – защищенная оболочка
SSL	Secure sockets layer – уровень защищенных сокетов
TCP	Transmission control protocol – протокол управления передачей данных
TFTP	Trivial file transfer protocol – протокол передачи файлов
TTY	Teletype – телетайп
UDP	User datagram protocol – протокол пользовательских датаграмм

Термин/Сокращение	Определение
URL	Uniform resource locator – сетевой адрес ресурса
USB	Universal Serial Bus – стандарт для подключения и передачи данных между ПК и периферийными устройствами
XFS	Журналируемая файловая система
YAML	Yet another markup language – язык разметки