

УТВЕРЖДЕН

ЛКНВ.11102-01 90 01-ЛУ

ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП
(ОС Альт 8 СП)

Руководство администратора
ЛКНВ.11102-01 90 01

Листов 510

Инд. № подл.	Подп. и дата	Взам. инв. №	Инд. № дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ содержит инструкции по установке и эксплуатации программного изделия (ПИ) «Операционная система Альт 8 СП» ЛКНВ.11102-01, сокращенное наименование – ОС Альт 8 СП, **релиз 10** для процессоров VLIW архитектуры **Эльбрус**.

Далее в документе будет использоваться альтернативное наименование ПИ: ОС Альт СП.

Версия: 1.2.

Документ предназначен для администратора ОС Альт СП и содержит общие сведения об ОС Альт СП, ее общей структуре, настройке, проверке, контрольных характеристиках развертывания и сообщениях администратору.

Также в документе приведены сведения, которые нужны для выполнения операций администрирования:

- установки и начального конфигурирования ОС Альт СП;
- конфигурирования параметров даты и времени, графической среды, средств ввода и вывода;
- конфигурирования сетей и сетевых служб;
- управления учетными записями и правами доступа пользователей;
- управления системными сервисами и служебными программами;
- настройки специализированного программного обеспечения;
- обновления программного обеспечения;
- просмотра системных журналов;
- управления автозапуском приложений;
- управления параметрами печати;
- работы с носителями информации;
- работы с руководствами, различными документами и дополнительными средствами.

СОДЕРЖАНИЕ

1. Общие сведения.....	14
1.1. Назначение и функции ОС Альт СП.....	14
1.2. Уровень подготовки администратора	15
2. Структура ОС Альт СП.....	16
2.1. Ядро ОС Альт СП.....	17
2.2. КСЗ.....	18
2.3. Системные библиотеки.....	20
2.4. Серверные программы и приложения.....	21
2.5. Прочие системные приложения.....	21
2.6. Программы веб-серверов.....	22
2.7. Интерактивные рабочие среды	22
2.8. Командные интерпретаторы	22
2.9. Графическая оболочка МАТЕ.....	22
2.10. Системы управления базами данных	22
2.11. Электронные справочники	23
3. Подготовительные процедуры.....	24
3.1. Настройка безопасной конфигурации компьютера.....	24
3.1.1. Процедура верификации	24
3.1.2. Настройка среды функционирования	24
3.2. Настройка опций безопасности	26
3.3. Описание механизмов устранения идентифицированных скрытых каналов.....	28
4. Функции и задачи администрирования ОС Альт СП.....	32
4.1. Функции администратора.....	32
4.2. Задачи администрирования	32
5. Установка ОС Альт СП.....	33
5.1. Запись установочного образа на USB-flash-накопитель	33
5.2. Способы первоначальной загрузки	34

5.3. Загрузка системы.....	35
5.4. Последовательность установки	37
5.4.1. Язык	38
5.4.2. Лицензионное соглашение	39
5.4.3. Дата и время.....	40
5.4.4. Подготовка диска	42
5.4.5. Перемонтирование	55
5.4.6. Установка системы.....	55
5.4.7. Сохранение настроек	57
5.4.8. Настройка сети	58
5.4.9. Администратор системы	60
5.4.10. Системный пользователь.....	62
5.4.11. Завершение установки	63
5.5. Обновление системы до актуального состояния	64
5.6. Проблемы при установке системы	65
6. Начало использования ОС Альт СП.....	66
6.1. Использование кабеля RS232 (COM) для подключения к консоли.....	66
6.2. Запуск ОС	67
6.3. Вход в систему.....	68
6.3.1. Идентификация и аутентификация в графической оболочке МАТЕ	68
6.3.2. Идентификация и аутентификация в консольном режиме	72
6.3.3. Виртуальная консоль	72
6.4. Блокирование сеанса доступа	73
6.4.1. Блокирование сеанса доступа после установленного времени бездействия (неактивности) пользователя или по его запросу	73
6.4.2. Блокировка виртуальных текстовых консолей	74
6.4.3. Настройка блокировки возможности пользователя изменять настройки блокировки системы.....	75
6.5. Завершение сеанса пользователя.....	76
6.5.1. Графический режим	76

6.5.2. Консольный режим	76
6.5.3. Настройки завершения сеанса пользователя.....	77
6.6. Выключение/перезагрузка компьютера.....	77
6.6.1. Графический режим	77
6.6.2. Консольный режим	78
7. Настройки системы	79
7.1. Центр управления системой.....	79
7.1.1. Графический интерфейс	80
7.1.2. Веб-интерфейс ЦУС.....	81
7.1.3. Установка и удаление модулей ЦУС	83
7.1.4. Права доступа к модулям ЦУС.....	84
7.1.5. Получение справочной информации	86
7.2. Выбор программ, запускаемых автоматически при входе в систему.....	87
7.2.1. Вкладка автоматического запуска программ	87
7.2.2. Вкладка настроек сессии	88
7.3. Режим киоск по ограничению запуска программ	89
7.3.1. Настройка ограничения в ЦУС	89
7.3.2. Управление режимом киоск в консоли.....	90
7.4. Задание хешей паролей.....	90
7.4.1. Смена алгоритма в консоли	91
7.4.2. Смена алгоритма в ЦУС	91
7.5. Настройка фильтрации пакетов с помощью утилиты iptables	92
7.5.1. Устройство фильтра iptables	93
7.5.2. Встроенные таблицы фильтра iptables	94
7.5.3. Команды утилиты iptables	95
7.5.4. Ключи утилиты iptables	98
7.5.5. Основные действия над пакетами в фильтре iptables.....	98
7.5.6. Основные критерии пакетов в фильтре iptables.....	99
7.5.7. Модули iptables.....	101
7.5.8. Использование фильтра iptables	104

7.5.9. Примеры команд iptables	104
7.6. Настройка экспорта аудита на удаленный узел	108
7.7. Настройка системы сигнализации на основе icinga	110
7.7.1. Настройка сервера мониторинга	112
7.7.2. Настройка агентов	130
7.7.3. Управление конфигурацией	137
7.7.4. Работа с Icinga	186
7.8. ГОСТ в OpenSSL	188
7.8.1. Поддержка шифрования по ГОСТ в OpenSSL	188
7.8.2. Создание ключей	188
7.9. Утилита уничтожения информации при удалении – dm-secdel	189
8. Средства удаленного администрирования	192
8.1. Вход в систему	192
8.2. Настройка подключения к Интернету	192
8.2.1. Конфигурирование сетевых интерфейсов	193
8.2.2. Объединение сетевых интерфейсов	196
8.2.3. Сетевые мосты	200
8.2.4. Настройка общего подключения к сети Интернет	202
8.2.5. Автоматическое присвоение IP-адресов (DHCP-сервер)	207
8.3. Соединение удаленных офисов (OpenVPN-сервер)	209
8.3.1. Настройка OpenVPN-сервера	209
8.3.2. Настройка клиентов	215
8.4. Доступ к службам из сети Интернет	217
8.4.1. Внешние сети	217
8.4.2. Список блокируемых хостов	218
8.5. Статистика	219
8.5.1. Сетевой трафик	219
8.5.2. Прокси-сервер	220
8.6. Обслуживание системы	221
8.6.1. Мониторинг состояния системы	221

8.6.2. Системные службы	222
8.6.3. Обновление системы.....	223
8.6.4. Обновление систем, не имеющих выхода в Интернет	225
8.6.5. Локальные учетные записи	230
8.6.6. Администратор системы	231
8.6.7. Дата и время.....	231
8.6.8. Настройка прокси-сервера	232
8.6.9. Ограничение использования диска	233
8.6.10. Выключение и перезагрузка компьютера.....	234
8.6.11. FTP-сервер	236
8.6.12. Удостоверяющий центр.....	237
8.7. Сервер электронной почты (SMTP, POP3/IMAP).....	241
8.7.1. Сервер электронной почты	241
8.7.2. Сервер SMTP	242
8.7.3. Сервер POP3/IMAP	242
8.8. Сервер электронной почты postfix	242
8.8.1. Утилиты командной строки	243
8.8.2. Первичная настройка	245
8.8.3. Работа в режиме SMTP-сервера.....	246
8.8.4. SMTP-аутентификация	247
8.8.5. Триггеры ограничений.....	251
8.8.6. Алиасы и преобразование адресов	255
8.8.7. Настройка ограничений размера почтового ящика и отправляемого сообщения	256
8.9. Настройка удаленного подключения	256
8.9.1. OpenSSH, сервер протокола SSH (sshd).....	257
8.9.2. SSHD_CONFIG	270
8.9.3. USB/IP.....	281
8.10. Прокси-сервер (Squid).....	286
8.10.1. Настройка прозрачного доступа через прокси-сервер	287

8.10.2. Фильтрация доступа.....	287
8.10.3. Авторизация доступа	288
8.10.4. Кэширование данных.....	288
8.10.5. Настройка режима работы в качестве обратного прокси-сервера.....	289
8.10.6. Сбор статистики и ограничение полосы доступа	290
8.10.7. Кеширование DNS-запросов.....	290
9. Ограничение действий пользователя	291
9.1. Ограничение полномочий пользователей по использованию консолей	291
9.1.1. Настройка ограничения в ЦУС.....	291
9.1.2. Настройка ограничения в консоли	292
9.2. Ограничение неуспешных попыток входа в информационную систему...	293
9.3. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы	294
9.4. Блокировка макросов в приложениях	296
9.5. Настройка предупреждения пользователя при его входе в систему	296
9.6. Определение параметров уничтожения данных	297
9.7. Модуль AltNa.....	299
9.7.1. Запрет бита исполнения (SUID)	299
9.7.2. Блокировка интерпретаторов (запрет запуска скриптов)	301
9.7.3. Отключение возможности удаления открытых файлов.....	302
10. FreeIPA.....	303
10.1. Ввод рабочей станции в домен FreeIPA – установка клиента и подключение к серверу.....	303
10.1.1. Установка FreeIPA клиента.....	303
10.1.2. Настройка сети. FreeIPA.....	303
10.1.3. Подключение к серверу в ЦУС.....	305
10.1.4. Подключение к серверу в консоли.....	307
10.1.5. Вход пользователя.....	308
10.1.6. Удаление клиента FreeIPA	309
11. Настройка служб DNS (Bind).....	311

11.1. Общие сведения.....	311
11.2. Уменьшение времени ответа на DNS-запрос абонентов внутренней сети	312
11.3. Именованние компьютеров в интранет-сети.....	312
11.4. Примеры использования DNS-сервера Bind	312
12. Система мониторинга Zabbix	319
12.1. Установка сервера PostgreSQL	319
12.2. Установка Apache2	320
12.3. Установка PHP	320
12.4. Настройка и запуск Zabbix-сервера.....	320
12.5. Установка веб-интерфейса Zabbix.....	321
12.6. Установка Zabbix-агента (клиента)	325
12.7. Добавление нового хоста на Zabbix-сервере	325
12.8. Авторегистрация узлов	327
13. Postgresql	330
13.1. Состав	330
13.2. Настройка.....	330
13.3. Использование postgresql	331
13.3.1. Конфигурирование сервера.....	331
13.3.2. Конфигурирование ролей	332
13.3.3. Создание администратора БД и БД.....	333
13.3.4. Работа роли администратора БД	333
13.4. Настройка кластера postgresql.....	334
14. Функциональные возможности ОС	339
14.1. Управление системными сервисами, основные команды.....	339
14.1.1. Сервисы	339
14.1.2. Команды	340
14.2. Администрирование многопользовательской и многозадачной среды ...	343
14.2.1. Команда who	343
14.2.2. Команда ps	345

14.2.3. Команда <code>nohup</code>	348
14.2.4. Команда <code>nice</code>	349
14.2.5. Команда <code>renice</code>	350
14.2.6. Команда <code>kill</code> и <code>killall</code>	351
14.3. Основные утилиты для операций с файлами и каталогами.....	353
14.3.1. Команда <code>ls</code>	353
14.3.2. Команда <code>cp</code>	357
14.3.3. Команда <code>rsync</code>	358
14.3.4. Команда <code>mv</code>	359
14.3.5. Команда <code>dd</code>	360
14.3.6. Команда <code>s_rm</code>	360
14.3.7. Команда <code>s_fill</code>	361
14.3.8. Команда <code>cd</code>	361
14.3.9. Команда <code>pwd</code>	362
14.3.10. Команда <code>mkdir</code>	362
14.3.11. Команда <code>rmdir</code>	362
14.3.12. Команда <code>mount</code>	363
14.4. Создание, просмотр и редактирование файлов.....	363
14.4.1. Команда <code>cat</code>	363
14.4.2. Команда <code>less</code>	364
14.4.3. Команда <code>echo</code>	365
14.4.4. Команда <code>grep</code>	365
14.4.5. Команда <code>touch</code>	365
14.4.6. Команда <code>mknod</code>	366
14.5. Поиск файлов.....	367
14.5.1. Команда <code>find</code>	367
14.5.2. Команда <code>whereis</code>	369
14.6. Средства архивирования файлов	370
14.6.1. Команда <code>tar</code>	370
14.6.2. Команда <code>cpio</code>	371

14.7. Средства редактирования файлов.....	373
14.7.1. Текстовый редактор Vi	373
14.7.2. Редактор Vim	376
14.8. Средства настройки отложенного исполнения команд.....	381
14.8.1. Служба crond.....	381
14.8.2. Команда at	386
14.8.3. Команда batch	388
14.9. Control.....	388
14.10. Защищенный интерпретатор команд SSH.....	389
14.11. Средство управления процессами xinetd	390
14.12. Работа со смарт-картами	394
14.12.1. Двухфакторная аутентификация	394
14.13. Поддержка файловых систем.....	396
14.14. Поддержка сетевых протоколов	398
14.14.1. SMB.....	398
14.14.2. NFS.....	402
14.14.3. NTP	404
14.14.4. HTTP(S)	406
14.15. Управление печатью	406
14.15.1. Устройство CUPS	407
14.15.2. Установка принтера	416
14.15.3. Настройка сервера печати для сети.....	419
14.15.4. Команды управления печатью	420
14.16. Организация терминального доступа XRDP	424
14.16.1. Базовая настройка сервера терминалов	424
14.16.2. Настройка сервера.....	424
14.16.3. Настройки доступа пользователей	425
14.16.4. Подключение звука	425
14.16.5. Подключение USB-устройств.....	426
14.16.6. Настройка клиента для подключения к серверу терминалов	427

14.16.7. Управление XRDP	432
14.17. Timeshift	432
14.17.1. Настройка резервного копирования	434
14.17.2. Создание снимков	442
14.17.3. Восстановление системы	442
14.17.4. Работа с Timeshift в командной строке	444
14.18. Информация о системе и об аппаратной части компьютера	446
14.18.1. Команда inxi	446
14.18.2. Команда glxinfo	452
14.19. Xpra	452
14.19.1. Установка	453
14.19.2. Режимы работы	453
14.19.3. Использование	456
14.19.4. Клиент HTML5	464
14.19.5. Графический интерфейс	466
14.20. Установка корневого сертификата	468
15. Управление программными пакетами	469
15.1. Источники программ (репозитории)	470
15.1.1. Репозитории для APT	470
15.1.2. Добавление репозитория с использованием терминала	473
15.1.3. Программа управления пакетами Synaptic	475
15.2. Обновление информации о репозиториях в APT	476
15.3. Поиск пакетов (apt-cache)	476
15.4. Управление установкой (инсталляцией) компонентов программного обеспечения	477
15.4.1. Команда integrity-applier	478
15.5. Установка или обновление пакета командой apt	479
15.6. Удаление установленного пакета командой apt	481
15.7. Альтернативная установка дополнительного ПО	481
15.7.1. Программа управления пакетами Synaptic	482

15.8. Обновление всех установленных пакетов apt-get	483
15.9. Обновление всех установленных пакетов Synaptic	483
15.10. Обновление ядра и модулей ядра	484
15.10.1. В консоли	484
15.10.2. Графический инструмент обновления ядра	485
15.11. Обновление изолированного окружения (chrooted environment)	489
15.12. Проверка подлинности пакетов	490
15.13. Получение уведомлений о выходе обновлений	490
15.14. Обновление систем, не имеющих выхода в Интернет	490
15.15. Единая команда управления пакетами (rpm)	490
16. Контрольные характеристики развернутой ОС Альт СП	492
17. Основы администрирования Linux	493
17.1. Общие принципы работы ОС	493
17.1.1. Процессы и файлы	493
17.1.2. Командные оболочки (интерпретаторы)	498
17.1.3. Командная оболочка Bash	498
17.1.4. Стыкование команд в системе Linux	500
17.2. Режим суперпользователя	502
17.2.1. Пользователи ОС	502
17.2.2. Назначение режима суперпользователя	503
17.2.3. Получение прав суперпользователя	503
17.2.4. Переход в режим суперпользователя	503
17.3. Управление пользователями	504
17.4. Система инициализации systemd и sysvinit	504
17.4.1. Запуск операционной системы	504
17.4.2. Примеры команд управления службами, журнал в systemd	505
17.4.3. Журнал в systemd	506
18. Сообщения администратору	508
Перечень сокращений	509

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Назначение и функции ОС Альт СП

ОС Альт СП представляет собой совокупность интегрированных программ, созданных на основе операционной системы (ОС) Linux.

ОС Альт СП предназначена для группового и корпоративного использования, автоматизации информационных, конструкторских и производственных процессов предприятий (организаций, учреждений) всех возможных типов и направлений.

ОС Альт СП поддерживает клиент-серверную архитектуру и может обслуживать процессы как в пределах одной компьютерной системы, так и процессы на других персональных электронных вычислительных машинах (далее – ПЭВМ) через каналы передачи данных или сетевые соединения.

ОС Альт СП обладает следующими функциональными характеристиками:

- обеспечивает возможность обработки, хранения и передачи информации в защищенной программной среде;
- обеспечивает возможность запуска пользовательского программного обеспечения (далее – ПО) в сертифицированном окружении;
- обеспечивает возможность функционирования в многозадачном режиме (одновременное выполнение множества процессов);
- обеспечивает возможность масштабирования системы: возможна эксплуатация ОС как на одной ПЭВМ, так и в информационных системах различной архитектуры;
- обеспечивает многопользовательский режим эксплуатации;
- обеспечивает поддержку мультипроцессорных систем;
- обеспечивает сетевую обработку данных, в том числе разграничение доступа к сетевым пакетам.

Для поддержки выполнения описанных функций в ОС Альт СП реализованы следующие возможности:

- управление процессами и информационными ресурсами;
- управление системными ресурсами;
- управление памятью;
- управление файлами и внешними устройствами;
- управление доступом к обрабатываемой информации;
- защита хранимых, обрабатываемых и передаваемых информационных ресурсов комплексом средств защиты (далее – КСЗ) ОС;
- администрирование;
- поддержка интерфейса прикладного программирования;
- поддержка пользовательского интерфейса.

1.2. Уровень подготовки администратора

Администратор ОС Альт СП должен иметь базовые знания в областях:

- принципы построения и функционирования современных вычислительных систем, механизмов защиты информации;
- работа с ОС семейства Linux;
- администрирование общесистемного и прикладного ПО;
- настройка средств защиты, используемых в составе ОС Альт СП;
- конфигурирование проводных подключений.

2. СТРУКТУРА ОС АЛЫТ СП

ОС Альт СП состоит из набора компонентов, предназначенных для реализации функциональных задач пользователями (должностными лицами для выполнения определенных должностными инструкциями повседневных действий). ПИ ОС Альт СП поставляется в виде дистрибутива и комплекта эксплуатационной документации.

Структура ОС Альт СП представлена на рис. 1.

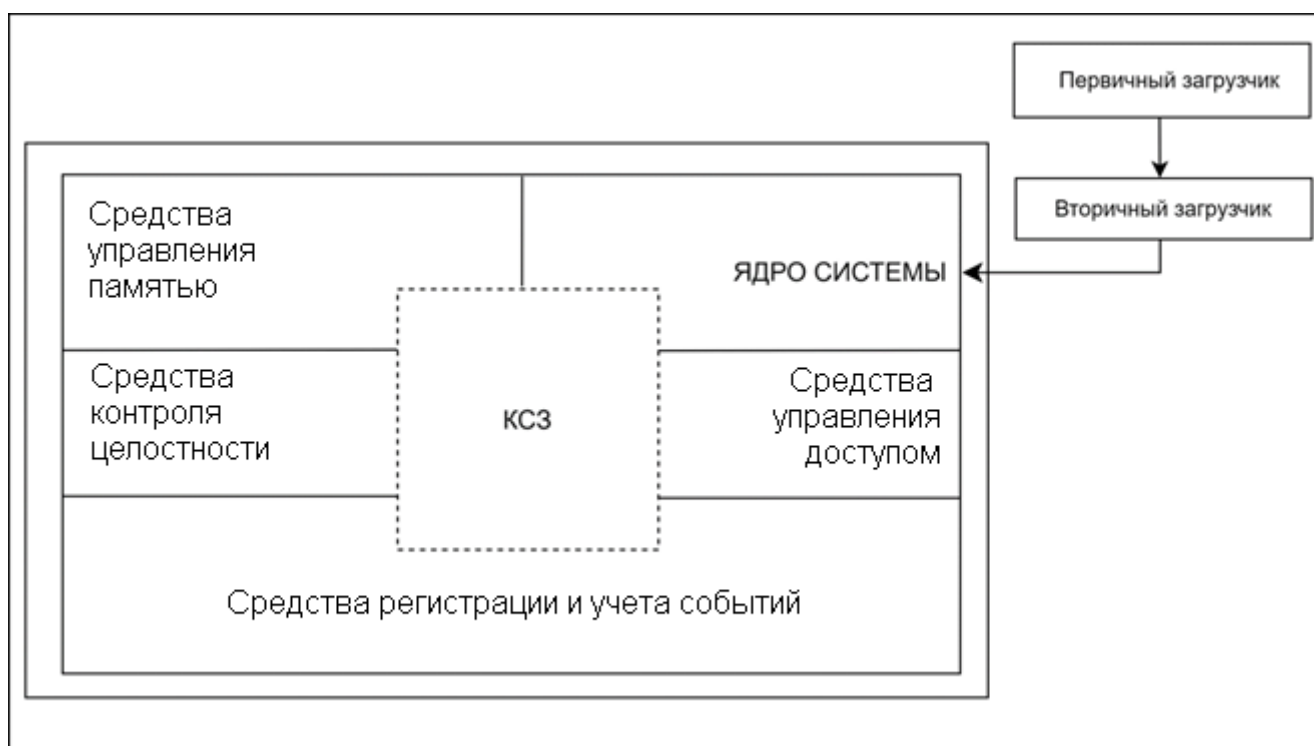


Рис. 1 – Структура ОС Альт СП

В состав ОС Альт СП входят следующие компоненты:

- ядро системы;
- средства управления доступом;
- средства регистрации и учета событий;
- средства контроля целостности;
- средства управления памятью.

В структуре компонентов ОС Альт СП выделены следующие функциональные элементы:

- ядро ОС;
- системные библиотеки;
- утилиты и драйверы;
- комплекс средств защиты информации;
- системные приложения;
- системы мониторинга и управления;
- интерактивные рабочие среды;
- серверные программы и приложения;
- графическая оболочка;
- командные интерпретаторы;
- прикладное программное обеспечение общего назначения;
- офисные приложения;
- программные средства виртуализации;
- программные средства контейнеризации;
- системы управления базами данных;
- программный комплекс Альт Домен.

Первичный и вторичный загрузчики ОС обращаются напрямую к ядру ОС, вызывая запуск системных процессов и приложений.

Взаимодействие и обмен информацией в ОС Альт СП контролируются КСЗ, предназначенным для защиты ОС от несанкционированного доступа к обрабатываемой (хранящейся) информации на ПЭВМ.

2.1. Ядро ОС Альт СП

Ядро ОС Альт СП управляет доступом к оперативной памяти, сети, дисковым и прочим внешним устройствам. Оно запускает и регистрирует процессы, управляет разделением времени между ними, реализует разграничение прав и определяет политику безопасности, обойти которую, не обращаясь к нему, нельзя.

Ядро работает в режиме «супервизора», позволяющем ему иметь доступ сразу ко всей оперативной памяти и аппаратной таблице задач. Процессы запускаются в

«режиме пользователя»: каждый жестко привязан ядром к одной записи таблицы задач, в которой, в числе прочих данных, указано, к какой именно части оперативной памяти этот процесс имеет доступ. Ядро постоянно находится в памяти, выполняя системные вызовы – запросы от процессов на выполнение этих подпрограмм.

2.2. КСЗ

КСЗ представляет собой набор специальных программных пакетов, в том числе из состава ядра ОС Альт СП, предназначенных для реализации механизмов безопасности и контроля функционирования ОС Альт СП в целом. Состав и версии пакетов КСЗ уточняйте в зависимости от архитектуры процессора.

* – группа пакетов.

КСЗ включает в себя следующие программные пакеты:

- acl – утилиты, предназначенные для администрирования списков контроля доступа Access Control Lists, которые используются для более точного задания прав доступа к файлам и директориям;
- alterator* – группа пакетов различных модулей системных настроек интерфейса Центра управления системой (ЦУС), предназначены для выполнения наиболее востребованных административных задач;
- apt – средства управления пакетами АРТ, установка, обновление, разрешение зависимостей RPM пакетов;
- audit – утилиты для хранения и поиска записей аудита, генерируемых подсистемой аудита;
- bash – командная оболочка Bourne-Again Shell;
- chrony – программа синхронизации времени;
- control – содержит общие интерфейсы управления системным оборудованием, предоставляемые другими пакетами;
- coreutils – набор утилит для управления файлами и изменения текстовых файлов;
- dm-secdel – утилита уничтожения информации, реализует безопасное удаление;

- icinga2 – система мониторинга служб и сетевой активности;
- ima-evm* – подсистема контроля целостности GNU/Linux, использует технологии IMA и EVM;
- iptables – используется для настройки, обслуживания и проверки находящихся в ядре Linux таблиц правил фильтрации пакетов IP;
- kernel-image* – ядро ОС Linux, управляет аппаратными ресурсами компьютера и обеспечивает взаимодействие между аппаратным обеспечением и программами. Отвечает за управление процессами, памятью, устройствами, системные вызовы;
- kernel-modules* – пакеты аппаратных драйверов и библиотек в ядре ОС;
- lightdm* – менеджер дисплеев, предоставляет графический интерфейс;
- mate-screensaver – хранитель и блокировщик экрана;
- mount – утилита для монтирования файловых систем;
- nagwad – сервис, генерирующий уведомления от icinga, основанные на записях из журнала аудита;
- ntpdate – устанавливает дату и время с помощью NTP. Используется для синхронизации времени компьютерного клиента или сервера с другим сервером или источником эталонного времени, обеспечивает временную точность работ;
- openvpn – VPN с использованием SSL, реализует подключение для удаленных пользователей, телекоммуникации для дома и офиса, безопасные подключения для беспроводных сетей;
- libpam0, pam*, pam0* – инструменты системы безопасности, позволяющие администраторам устанавливать политику аутентификации без необходимости повторной компиляции программ проверки подлинности;
- passwd – утилита для установки/смены паролей с использованием PAM;
- passwdqc – набор инструментов для контроля сложности паролей и парольных фраз, включающий PAM-модуль, программы и библиотеку;

- polkit – это набор инструментов для определения и обработки разрешений. Он используется для того, чтобы позволить непривилегированным процессам контактировать с привилегированными процессами;
- rpm – менеджер пакетов, используемый для сборки, установки, инспекции, проверки, обновления и удаления отдельных программных пакетов;
- rsync – утилита синхронизации файлов по сети, используется в качестве эффективного процесса зеркалирования, т. к. пересылает только различия между файлами, а не файлы целиком;
- secure_delete – набор утилит для безопасного удаления файлов, безопасной очистки от остатков данных неиспользуемого пространства дисков, безопасной очистки разделов подкачки и безопасной очистки неиспользуемой памяти;
- setup – начальный набор конфигурационных файлов;
- sh – командная оболочка Bourne shell;
- shadow – усиливает безопасность системных паролей;
- su – утилита запуска командного интерпретатора от имени другого пользователя;
- sudo – программа, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы;
- systemd*– менеджер системы и служб в ОС, реализует запуск демонов и отслеживает процессы;
- util-linux – коллекция основных системных утилит;
- vim-console – экранный редактор;
- vlock – программа блокировки сеансов в консоли.

2.3. Системные библиотеки

Системные библиотеки – наборы программ (пакетов программ), выполняющие различные функциональные задачи и предназначенные для динамического подключения к работающим программам, которым требуется выполнение этих задач.

2.4. Серверные программы и приложения

Серверные программы и приложения предоставляют пользователю специализированные услуги (почтовые службы, хранилище файлов, веб-сервер, система управления базой данных, обеспечение документооборота, хранилище данных пользователей и так далее) в локальной или глобальной сети и обеспечивают их выполнение.

В состав ОС Альт СП включены следующие серверные программы и приложения:

- приложения, обеспечивающие поддержку сетевого протокола DHCP (Dynamic Host Configuration Protocol);
- приложения, обеспечивающие поддержку протокола аутентификации LDAP (Lightweight Directory Access Protocol);
- приложения, обеспечивающие поддержку протоколов FTP, SFTP, SSHD;
- системы управления базами данных;
- программы, обеспечивающие работу SMB-сервера (сервер файлового обмена);
- программы почтового сервера postfix;
- программы прокси-сервера Squid;
- программы веб-сервера apache2;
- программы DNS-сервера.

2.5. Прочие системные приложения

Прочие системные приложения – приложения (программы), оказывающие пользователю дополнительные системные услуги при работе с ОС.

В состав ОС Альт СП включены следующие дополнительные системные приложения:

- архиваторы;
- для управления RPM-пакетами;
- резервного копирования;
- мониторинга системы;
- для работы с файлами;

- для настройки системы;
- для настройки параметров загрузки;
- для настройки оборудования;
- для настройки сети.

2.6. Программы веб-серверов

Программы веб-серверов участвуют в организации доступа пользователей к сети Интернет. Доступ организуется с помощью клиент-серверной архитектуры.

Клиент, которым обычно является веб-браузер, передает программе веб-сервера запросы на получение ресурсов. В качестве ресурсов могут выступать HTML-страницы, изображения, файлы, медиа-потoki или другие данные, которые требуются клиенту. В ответ веб-сервер передает клиенту запрошенные данные. Обмен происходит по протоколу HTTP.

В состав ОС Альт СП включены программы веб-сервера Apache.

2.7. Интерактивные рабочие среды

Интерактивные рабочие среды – программы (пакеты программ), предназначенные для работы пользователя в ОС Альт СП и предоставляющие ему удобный интерфейс для общения с ней.

2.8. Командные интерпретаторы

Командные интерпретаторы – специальные программы (терминалы), предназначенные для выполнения различных команд пользователей при работе с ОС Альт СП.

2.9. Графическая оболочка MATE

Графическая оболочка MATE – набор программ и технологий, предназначенных для управления ОС Альт СП и предоставляющих пользователю графический интерфейс для работы.

2.10. Системы управления базами данных

Системы управления базами данных (далее – СУБД) (см. раздел 13) – приложения, предназначенные для работы с данными, представленными в виде набора записей. СУБД осуществляет поиск, обработку и структурирование данных.

2.11. Электронные справочники

Электронные справочники – наборы внутрисистемных справочных страниц, описывающих работу команд и приложений, которые выполнены в виде примеров HOWTOs и справки man.

3. ПОДГОТОВИТЕЛЬНЫЕ ПРОЦЕДУРЫ

3.1. Настройка безопасной конфигурации компьютера

3.1.1. Процедура верификации

Проверка поставленного потребителю дистрибутива производится путем подсчета контрольной суммы с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2)/программы фиксации и контроля целостности информации «ФИКС-UNIX 1.0» по алгоритму «Уровень-3» (при наличии)¹ и сравнения ее с контрольной суммой, указанной в документе «Формуляр. ЛКНВ.11102-01 30 01» и на этикетке ПИ.

Администратор имеет возможность верифицировать версию ОС Альт СП, выполнив команду:

```
# cat /root/.install-log/diskinfo
```

3.1.2. Настройка среды функционирования

Для среды функционирования ОС Альт СП (средств вычислительной техники (СВТ)) сформулированы следующие рекомендации:

- обновление установленной системы до ОС Альт СП релиз 10 не допускается. Установка должна производиться с удалением всех предыдущих данных со всех разделов диска;
- не допускается использовать аппаратные платформы, базовые системы ввода-вывода, содержащие уязвимости, без применения патча, представленного разработчиком данной аппаратной платформы, версии базовой системы ввода-вывода;
- установка, конфигурирование и управление ОС Альт СП должны выполняться в соответствии с эксплуатационной документацией;

¹ Или с использованием аналогичного ПО, осуществляющего подсчет контрольных сумм по алгоритму ФИКС режим «Уровень-3».

- должна быть обеспечена защита от осуществления действий, направленных на нарушение физической целостности СВТ, на котором функционирует ОС Альт СП;
- 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 ресурсы для выполнения функциональных возможностей безопасности ОС, хранения резервных копий, создаваемых ОС, а также защищенное хранение данных ОС и защищаемой информации;
- должно быть обеспечено ограничение на установку ПО 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 ИС). В том числе 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 ОС;
- должно быть обеспечено выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;

- персонал, ответственный за функционирование ОС Альт СП, должен обеспечивать функционирование ОС Альт СП, в точности руководствуясь эксплуатационной документацией;
- лица, ответственные за эксплуатацию ОС Альт СП, должны обеспечить, чтобы аутентификационная информация для каждой учетной записи пользователя ОС содержалась в тайне и была недоступна лицам, не уполномоченным использовать данную учетную запись;
- должна обеспечиваться возможность генерации аутентификационной информации соответствующей метрике качества.

3.2. Настройка опций безопасности

Во время установки ОС Альт СП в соответствии с принятыми парольными ограничениями на объекте эксплуатации:

- задать пользователя с паролем, отвечающим требованиям безопасности;
- задать пароль администратора, отвечающий требованиям безопасности.

Перед началом эксплуатации ОС Альт СП рекомендуется администратору обеспечить выполнение следующих условий:

- 1) настроить параметры входа пользователя (порядок действий приведен в документе «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01» – далее Руководство по КСЗ):
 - время засыпания (блокирование сеанса доступа см. в п. 6.4);
- 2) настроить параметры пароля пользователя (порядок действий приведен в Руководстве по КСЗ подразделы «Настройка парольных ограничений», «Управление сроком действия пароля»):
 - сложность пароля;
 - время действия;
- 3) настроить средства контроля целостности (порядок действий приведен в Руководстве по КСЗ в подразделе «Средства контроля целостности»);
- 4) настроить параметры запрета удаления файлов (порядок действий приведен в п. 9.7 «Модуль AltNa»);

- 5) настроить сервисы в соответствии с функциональным назначением объекта автоматизации (управление сервисами см. в п. 14.1.1);
- 6) настроить аудит:
 - создать правила аудита (примеры использования аудита приведены в Руководстве по КСЗ подраздел «Использование аудита»);
 - настроить экспорт аудита на другой компьютер (порядок действий приведен в п. 7.6);
- 7) настроить подключение оповещений администратора (порядок действий приведен в п. 7.7);
- 8) механизм замкнутой программной среды должен быть настроен для работы в штатном режиме пользователя (порядок действий приведен в Руководстве по КСЗ в подразделе «Подсистема IMA/EVM»);
- 9) с использованием средств управления дискреционными правами разграничения доступа запретить пользователям, не обладающим привилегиями администратора:
 - доступ к библиотеке `libpcprofile.so`;
 - запуск (использование) средств создания символических ссылок;
- 10) с использованием средств управления запуском сервисов должна быть отключена служба `grm` для поддержки «мыши» в консольном режиме;
- 11) для защиты от атаки подбора пароля (brute force):
 - внести изменения в файл `/etc/pam.d/sshd` – добавить строку:
`auth required pam_faillock.so authfail deny=3 unlock_time=19`
- 12) для суперпользователя (root) заблокировать возможность его удаленного входа в ОС посредством включения PAM-модуля `pam_securetty` в файл сценария `/etc/pam.d/system-auth-common`. Для этого в «Primary block» в указанном файле первой строкой добавить:
`auth required pam_securetty.so`

3.3. Описание механизмов устранения идентифицированных скрытых каналов

Далее приведены дополнительные рекомендации по настройке механизмов защиты ОС Альт СП для устранения возможных скрытых каналов передачи информации.

Механизмы защиты направлены на ограничение, мониторинг, полное или частичное устранение идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них ОС Альт СП.

1) Исключить возможность работы с общими каталогами с правом записи для пользователей, имеющих разные полномочия доступа.

2) Для противодействия атакам на каналы передачи по времени и памяти администратору безопасности нужно исключить наличие в системе общих для пользователей файловых ресурсов, где размещаются файлы с разными правами дискреционного разграничения доступа, в частности, исключить размещение в каталогах файлов, доступ к которым полностью закрыт для конкретных пользователей данного каталога. Также можно монтировать файловую систему без учета времени доступа:

```
mount -noatime -nodiratime
```

3) На уровне ядра запретить процессам создавать слушающие сокеты, кроме тех, что им действительно нужны, в том числе запрещать слушать на фиксированном порту, а также контролировать частоту создания сокета.

4) Монтировать подсистему /proc с флагом hidepid=2 или 1. При этом имена процессов других пользователей и другие данные таких процессов будут недоступны вызывающему непривилегированному пользователю.

5) Организовать маскирующие процессы, имитирующие постоянную загрузку процессора. Использовать механизмы ограничения CPU для процессов, гарантирующих время выполнения, одинаковое для всех процессов, таких как cgroups.

6) Для предотвращения Timestamp Evaluation (вычисления временных меток) – отключить отметки времени TCP в ОС Альт СП. Для этого выполните команду:

```
# echo 0 > /proc/sys/net/ipv4/tcp_timestamps
```


и, чтобы изменения стали постоянными добавьте следующую строку в файл /etc/sysctl.conf:

```
net.ipv4.tcp_timestamps = 0
```

также можно настроить правила iptables:

```
iptables -A INPUT -p icmp --icmp-type timestamp-request -j DROP
iptables -A OUTPUT -p icmp --icmp-type timestamp-reply -j DROP
```

7) Для предотвращения ISN Evaluation (использование порядковых номеров для индексации передаваемых TCP-данных) – использовать TCP/IP прокси (socks).

8) Для предотвращения TCP URG Pointer (указателя TCP URG) – настроить правила iptables:

```
iptables -N BADFLAGS
iptables -A BADFLAGS -j LOG --log-prefix "BADFLAGS: "
iptables -A BADFLAGS -j DROP
iptables -N TCP_FLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,FIN FIN -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,PSH PSH -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ACK,URG URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags FIN,RST FIN,RST -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,FIN SYN,FIN -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags SYN,RST SYN,RST -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL ALL -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL NONE -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL FIN,PSH,URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j BADFLAGS
iptables -A TCP_FLAGS -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j BADFLAGS
```

9) Для предотвращения IP ToS Evaluation (оценки IP-ToS) – настроить способ обслуживания для telnet, ftp-control и ftp-data – выполнить команды:

```
# iptables -A PREROUTING -t mangle -p tcp --sport telnet \
-j TOS --set-tos Minimize-Delay
# iptables -A PREROUTING -t mangle -p tcp --sport ftp \
-j TOS --set-tos Minimize-Delay
# iptables -A PREROUTING -t mangle -p tcp --sport ftp-data \
-j TOS --set-tos Maximize-Throughput
```

Эти правила прописываются на удаленном хосте и воздействуют на входящие по отношению к компьютеру пакеты. Для пакетов, отправляемых в обратном направлении, эти флаги устанавливаются автоматически. Настроить их можно, прописав следующие правила:

```
# iptables -A OUTPUT -t mangle -p tcp --dport telnet \
-j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp \
-j TOS --set-tos Minimize-Delay
# iptables -A OUTPUT -t mangle -p tcp --dport ftp-data \
-j TOS --set-tos Maximize-Throughput
```

Для противодействия данной атаке нужно в командной строке прописать следующие правила:

```
# Разрешить главные типы протокола ICMP
iptables -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 3 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 4 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 11 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 12 -j ACCEPT
```

Типы ICMP-сообщений:

- 0 – echo reply (echo-ответ, пинг);
- 3 – destination unreachable (адресат недостижим);
- 4 – source quench (подавление источника, просьба посылать пакеты медленнее);
- 5 – redirect (редирект);
- 8 – echo request (echo-запрос, ping);
- 9 – router advertisement (объявление маршрутизатора);
- 10 – router solicitation (ходатайство маршрутизатора);
- 11 – time-to-live exceeded (истечение срока жизни пакета);
- 12 – IP header bad (неправильный IP заголовок пакета);
- 13 – timestamp request (запрос значения счетчика времени);
- 14 – timestamp reply (ответ на запрос значения счетчика времени);
- 15 – information request (запрос информации);
- 16 – information reply (ответ на запрос информации);
- 17 – address mask request (запрос маски сети);
- 18 – address mask reply (ответ на запрос маски сети).

10) Для предотвращения Initial Sequence Number hijacking and spoofing (перехвата и подмены изначальных порядковых номеров при индексации TCP-соединений) – настроить правила iptables:

```
# Защита от подмены
iptables -I INPUT -m conntrack --ctstate NEW,INVALID -p tcp \
  --tcp-flags SYN,ACK SYN,ACK -j REJECT --reject-with tcp-reset
# Защита от SYN-флуда
iptables -A INPUT -p tcp --syn -m limit --limit 10/s \
```

```

--limit-burst 50 -j ACCEPT
iptables -A INPUT -p udp -m limit --limit 10/s --limit-burst 50 -j \
ACCEPT
iptables -A INPUT -p icmp -m limit --limit 10/s --limit-burst 50 \
-j ACCEPT
iptables -A INPUT -j DROP
# Отбрасывать ошибочные пакеты
iptables -A INPUT -m state --state INVALID -j DROP
iptables -I INPUT -m conntrack --ctstate INVALID -j DROP
# Отбрасывать фрагментированные пакеты
iptables -A INPUT -f -j DROP
# Защита от попытки открыть входящее соединение TCP не через SYN
iptables -I INPUT -m conntrack --ctstate NEW -p tcp ! --syn -j DROP
# Защита от Ping of death
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit
10/s --limit-burst 50 -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
# Защита от некорректных ICMP
iptables -I INPUT -p icmp -f -j DROP
# Отбросить ошибочные пакеты
iptables -A FORWARD -m state --state INVALID -j DROP
iptables -I FORWARD -m conntrack --ctstate INVALID -j DROP
# Отбросить фрагментированные пакеты
iptables -A FORWARD -f -j DROP
# Сбрасывать фрагментированные пакеты
iptables -A OUTPUT -f -j DROP

```

Дополнительно требуется внести правки в /etc/sysctl.conf:

```

# vim /etc/sysctl.conf

# Отбросить ICMP-редиректы (против атак типа MITM)
net.ipv4.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_redirects=0
# Включить механизм TCP syncookies
net.ipv4.tcp_syncookies=1
# Различные улучшения (защита от подмены
# увеличение очереди «полуоткрытых» TCP-соединений и далее):
net.ipv4.tcp_timestamps=0
net.ipv4.conf.all.rp_filter=1
net.ipv4.tcp_max_syn_backlog=1280
kernel.core_uses_pid=1

```

4. ФУНКЦИИ И ЗАДАЧИ АДМИНИСТРИРОВАНИЯ ОС АЛЬТ СП

4.1. Функции администратора

Основными функциями администратора при эксплуатации ОС Альт СП являются:

- ввод в эксплуатацию и эксплуатация в соответствии с указаниями, приведенными в документе «Формуляр. ЛКНВ.11102-01 30 01»;
- соблюдение подготовительных процедур (см. раздел 3);
- установка и настройка ОС Альт СП;
- управление и поддержка функционирования ПЭВМ.

4.2. Задачи администрирования

В состав основных задач администрирования входят следующие:

- установка ОС Альт СП и назначение параметров системы;
- создание загрузочных носителей информации;
- конфигурирование параметров даты и времени, графической среды, средств ввода и вывода;
- настройка и управление системными сервисами и служебными программами;
- настройка и управление работой системы управления пакетами Advanced Packaging Tool (далее – АРТ);
- обновление ОС и прикладного ПО из ее состава;
- настройка и управление учетными записями и правами доступа пользователей;
- конфигурирование сети `/etc/net` и проверка ее работоспособности;
- настройка FTP-серверов;
- настройка служб DNS;
- настройка серверов электронной почты postfix;
- настройка и управление кэширующими прокси-серверами;
- настройка и управление печатью.

5. УСТАНОВКА ОС АЛЬТ СП

Обычно для установки дистрибутива используется установочный загрузочный компакт-диск дистрибутива. Если установка производится с компакт-диска, можно сразу перейти к п. 5.1 и п. 5.4.

Для начала процесса установки ОС Альт СП нужно:

- выбрать способ первоначальной загрузки компьютера;
- выбрать источник установки.

В случае загрузки с установочного компакт-диска эти две возможности предоставляются самим диском: он является загрузочным и содержит все требуемые для установки файлы. Однако вполне допустим и такой вариант: первоначальная загрузка происходит со специально подготовленного USB-flash-накопителя, а установочные файлы берутся с FTP-сервера сети.

Установка с загрузочного компакт-диска – это один из возможных способов установки системы. Он является самым распространенным способом установки системы, но не работает, например, в случае отсутствия на компьютере CD/DVD-привода. Для таких случаев поддерживаются альтернативные методы установки (см. п. 5.1).

5.1. Запись установочного образа на USB-flash-накопитель

⚠ Для загрузки вычислительного комплекса (ВК) «Эльбрус» требуется наличие на установочном носителе одного раздела в стиле MBR с файловой системой ext2/ext3; скрипт `write.sh` разбивку не меняет во избежание более тяжелых последствий ошибок.

Для создания загрузочного USB-flash-накопителя понадобится файл ISO-образа установочного компакт-диска с дистрибутивом. ISO-образы установочных компакт-дисков для семейства архитектуры Эльбрус **не являются** гибридными.

Примечание. Программа начального старта (ПНС) не декларирует возможность загрузки с ISO-образа на разделе, `mcst`.

В операционной системе Linux скопируйте полное содержимое ISO-образа, включая скрытый каталог `.disk`, на раздел USB-flash-накопителя с файловой системой `ext2` или `ext3`, и по желанию замените в файле конфигурации загрузчика `boot.conf` умолчание `default=install` на `default=install_flash`, чтобы не выбирать его вручную при загрузке.

Для упрощения этой процедуры на Linux-системах можно воспользоваться скриптом `write.sh`, который входит в состав ISO-образов или может быть найден рядом с ними:

- извлечение скрипта (требуется однократно):

```
# mount -o loop,ro <файл-образа.iso> /mnt
# cp -a /mnt/write.sh /usr/local/bin
# umount /mnt
```

- запись образа:

```
# sleep 1; write.sh <файл-образа.iso> /dev/sdX1
```

где `sdX` – устройство, соответствующее целевому flash-диску (см. вывод команды `lsblk`); при необходимости на указанном разделе, который должен уже существовать, будет создана файловая система `ext2`.

Примечание. Для выполнения скрипта на применяемой системе должна быть доступна команда `rsync`.

5.2. Способы первоначальной загрузки

Простейший способ запустить программу установки — загрузить компьютер с помощью загрузочного носителя, находящегося на установочном компакт-диске с дистрибутивом (при условии, что система поддерживает загрузку с устройства для чтения DVD).

Примечание. Для загрузки с USB-flash-накопителя выбирайте цель `install_flash` (достаточно нажать клавишу `<Enter>` в меню `boot#`).

5.3. Загрузка системы

После включения ВК «Эльбрус» происходит инициализация программы начальной загрузки, в процессе которой есть возможность вмешательства после вывода строки:

```
Autoboot in 03 sec. PRESS SPACE TO DISABLE IT.
```

Необходимо нажать пробел, после чего должны появиться следующие строки:

```
Key pressed. Autoboot canceled.
CPU#00: Starting menu.
```

```
BOOT SETUP
```

```
Press command letter, or press 'h' to get help
```

```
:
```

Можно запросить подсказку нажатием клавиши <h>, но необходимыми являются следующие пункты:

- **d** – show Disks and partitions (показать диски и разделы);
- **c** – Change boot parameters (изменить параметры загрузки);
- **u** – show cUrrent parameters (показать текущие параметры);
- **m** – save params to NVRAM (сохранить параметры в NVRAM);
- **b** – start Boot.conf menu (запустить меню Boot.conf).

При нажатии на клавишу <d> получим список дисков:

```
:d
CPU#00: Drive [2]: SATA - PCI BUS[1]:DEV[3]:FUNC[0], MCST SATA COMBINED Port
[0] - KINGSTON SMS200S3120G
CPU#00:      Partition [0]: Linux EXT2;
           U:246194e7-0512-4db3-a821-cbcbe3c92c38 L:""
CPU#00:      Partition [1]: Linux swap
CPU#00:      Partition [3]: Extended
CPU#00:      Partition [4]: Unknown file system type
CPU#00: Drive [10]: ATAPI device
```

В данном случае идентификатор 10 присвоен внешнему USB DVD-приводу, с которого и будет произведена установка ОС; следует выбрать его, указав идентификатор ответом на первый вопрос команды **c** и нажав клавишу <Esc> на остальные:

```
:c
```

```
CHANGE BOOT PARAMETERS
```

Current Settings:

```

drive_number:      '2'
drive_label:       '*'
partition_number:  '0'
file system id:    '07bde958-ec62-492e-933c-17334bb02da2'
command_string:    ''
filename:          ''
initrdfilename:    ''
autoboot in:       '10'

```

To advance to next setting press ENTER. To skip setting press ESC

```

Enter drive number      : 10
Enter partition number: < Skipped >
Enter command string   : < Skipped >
Enter filename         : < Skipped >
Enter initrd file name: < Skipped >
Enter autoboot value   : < Skipped >

```

Current Settings:

```

drive_number:      '10'
drive_label:       ''
partition_number:  '0'
file system id:    ''
command_string:    ''
filename:          ''
initrdfilename:    ''
autoboot in:       '10'

```

CPU#00: Search drive and partition by label or uuid succeed

Затем необходимо перейти к загрузке последовательным нажатием клавиш

 <Tab> <Enter>:

```

:b
boot# install
CPU#00: Label 'install' found, loading parameters
CPU#00: Search drive and partition by label or uuid succeed

```

Trying to load and start image with following parameters:

```

drive_number:      '10'
drive_label:       ''
partition_number:  '0'
file system id:    ''
command_string:    'hardreset fastboot live automatic=method:cdrom'
filename:          '/alt0/vmlinux.0'
initrdfilename:    '/alt0/full.cz'

```

Примечание. Мышь на этом этапе установки не поддерживается. Для выбора опций установки и различных вариантов необходимо использовать клавиатуру.

После загрузки инсталлятора установка продолжается штатным образом.

После установки системы, если установка производилась на диск, отличный от того, с которого ВК загружается по умолчанию – следует повторно зайти в конфигурацию программы начальной загрузки, определить загрузочный диск (d) и указать его в качестве загрузочного диска по умолчанию (c). После изменений параметров загрузки, следует воспользоваться командой m для записи изменений в NVRAM и их применения в дальнейшем.

5.4. Последовательность установки

До того как будет произведена установка базовой системы на жесткий диск, программа установки работает с образом системы, загруженным в оперативную память компьютера.

Если инициализация оборудования завершилась успешно, будет запущен графический интерфейс программы-установщика.

Процесс установки разделен на шаги; каждый шаг посвящен настройке или установке определенного свойства системы. Шаги нужно проходить последовательно, переход к следующему шагу происходит по нажатию кнопки «Далее». При помощи кнопки «Назад» можно вернуться к уже пройденному шагу и изменить настройки. Однако на этом этапе установки возможность перехода к предыдущему шагу ограничена теми шагами, где нет зависимости от данных, введенных ранее.

В случае необходимости отмены установки, следует нажать кнопку <Reset> на корпусе системного блока компьютера.

Примечание. Совершенно безопасно выполнить отмену установки только до шага «Подготовка диска» (см. п. 5.4.4), поскольку до этого момента не производится никаких изменений на жестком диске.

Технические сведения о ходе установки можно посмотреть, нажав клавиши <Ctrl>+<Alt>+<F1>, вернуться к программе установки – <Ctrl>+<Alt>+<F7>. По нажатию клавиш <Ctrl>+<Alt>+<F2> откроется отладочная виртуальная консоль.

Каждый шаг сопровождается краткой справкой, которую можно вызвать, нажав клавишу <F1>.

Во время установки системы выполняются следующие шаги:

- язык (см. п. 5.4.1);

- лицензионное соглашение (см. п. 5.4.2);
- дата и время (см. п. 5.4.3);
- подготовка диска (см. п. 5.4.4);
- перемонтирование (см. п. 5.4.5);
- установка системы (см. п. 5.4.6);
- сохранение настроек (см. 5.4.7);
- настройка сети (см. п. 5.4.8);
- администратор системы (см. п. 5.4.9);
- системный пользователь (см. п. 5.4.10);
- завершение установки (см. п. 5.4.11).

5.4.1. Язык

Установка начинается с выбора основного языка – языка интерфейса программы установки и устанавливаемой системы (рис. 2).

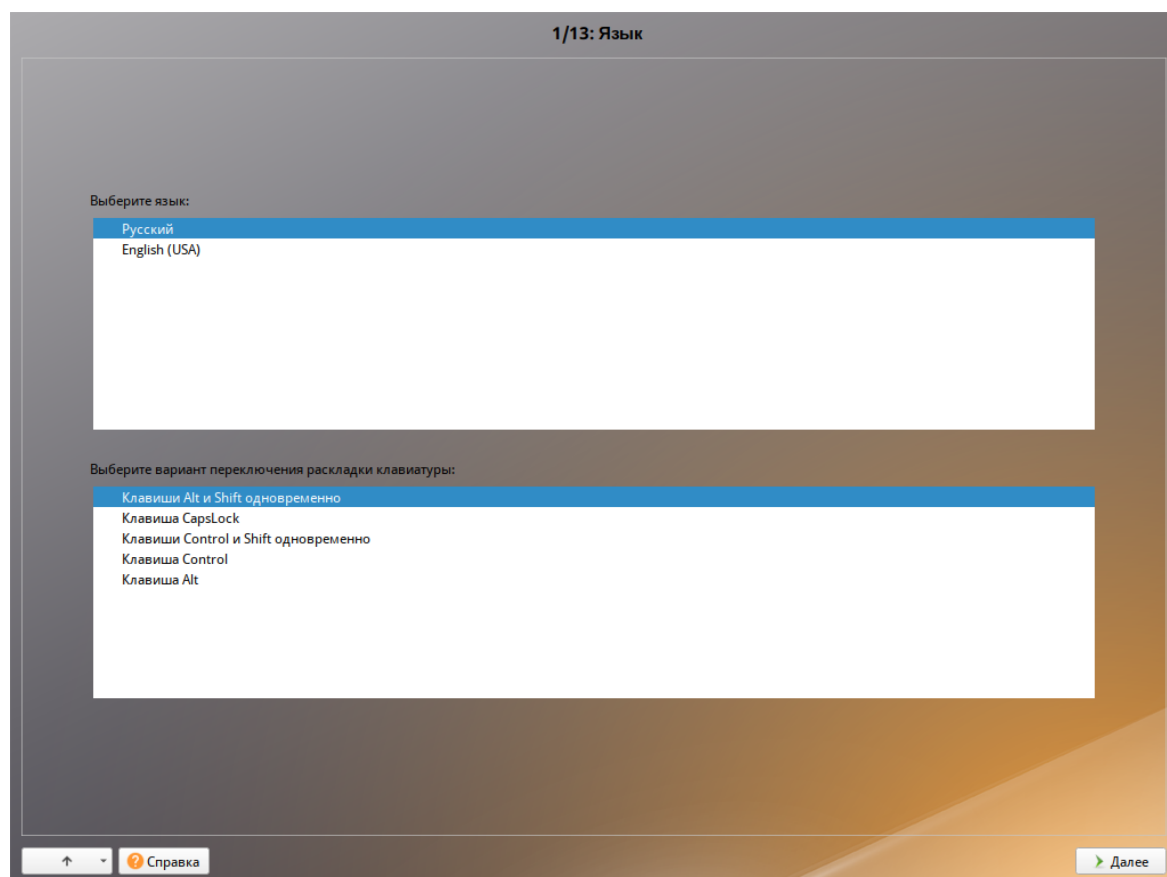


Рис. 2 – Установка. Выбор языка

На данном этапе также выбирается вариант переключения раскладки клавиатуры. Раскладка клавиатуры – это привязка букв, цифр и специальных символов к клавишам на клавиатуре. Переключение между раскладками осуществляется при помощи специально зарезервированных для этого клавиш.

Для настройки варианта переключения раскладки клавиатуры в пункте «Выберите вариант переключения раскладки клавиатуры» нужно установить одно из следующих значений (доступно при выборе русского языка, в качестве основного):

- клавиши <Alt> и <Shift> одновременно;
- клавиша <CapsLock>;
- клавиши <Control> и <Shift> одновременно;
- клавиша <Control>;
- клавиша <Alt>.

Если выбранный основной язык имеет всего одну раскладку (например, при выборе английского языка в качестве основного), эта единственная раскладка будет принята автоматически.

После завершения настройки основного языка и варианта переключения раскладки клавиатуры нужно нажать на кнопку «Далее».

5.4.2. Лицензионное соглашение

После окна выбора языковых параметров ОС Альт СП программа установки переходит к окну «Лицензионное соглашение» (рис. 3).

Перед продолжением установки следует внимательно прочитать условия, регулирующие права владельца экземпляра дистрибутива ОС Альт СП на использование дистрибутива, а также включенных в состав дистрибутива отдельных программ для ЭВМ в установленных условиях пределах.

Для подтверждения согласия следует отметить пункт «Да, я согласен с условиями» и нажать на кнопку «Далее».

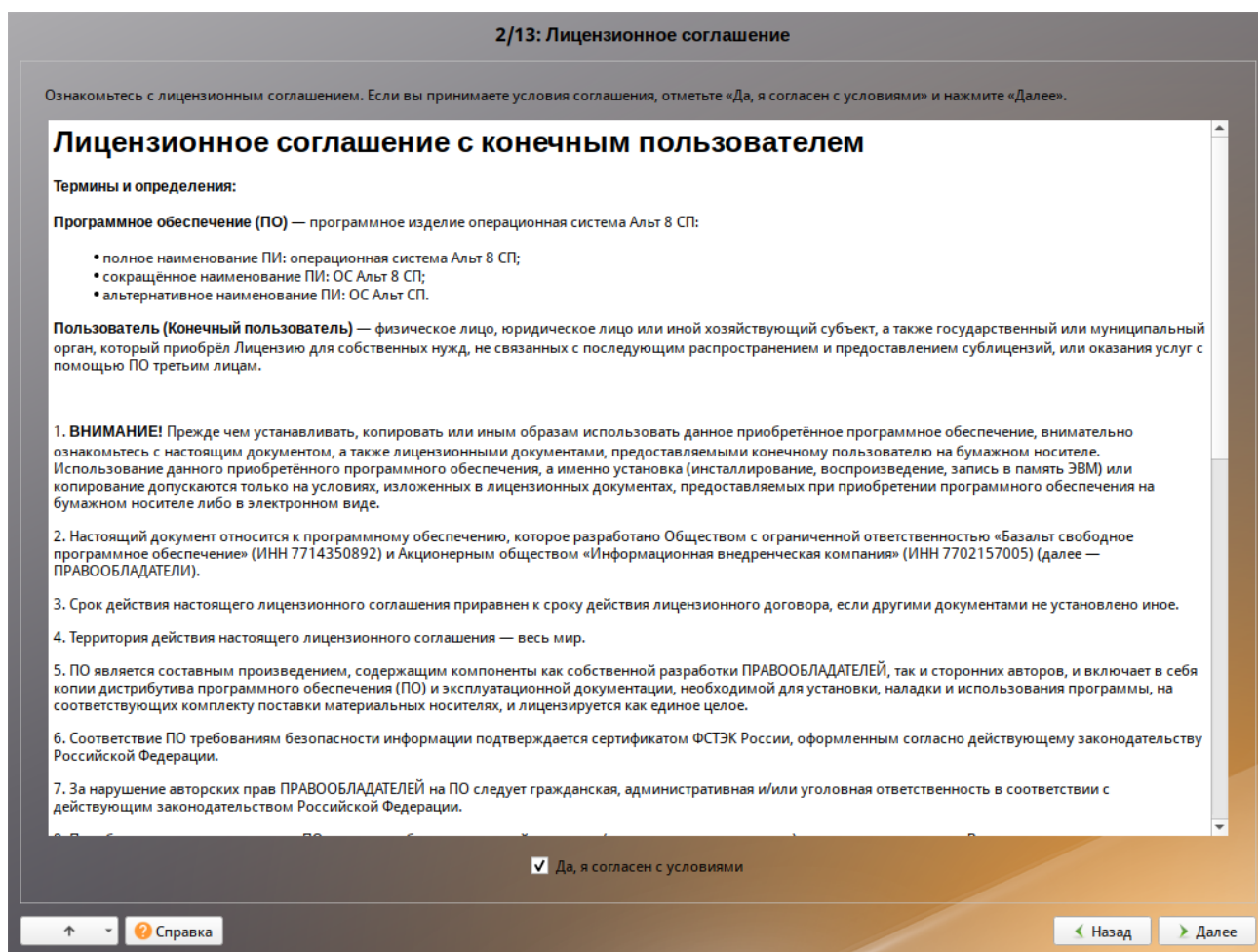


Рис. 3 – Установка. Лицензионное соглашение

5.4.3. Дата и время

После окна «Лицензионное соглашение» ОС Альт СП программа установки переходит к окну «Дата и время». На данном этапе выполняется выбор региона и города, по которым будет определен часовой пояс и установлены системные часы (рис. 4).

Для указания часового пояса в соответствующих списках выберите регион, а затем город. Поиск по списку можно ускорить, набирая на клавиатуре первые буквы искомого слова.

Пункт «Хранить время в BIOS по Гринвичу» выставляет настройки даты и времени в соответствии с часовыми поясами, установленными по Гринвичу, и добавляет к местному времени часовую поправку для выбранного региона.

После выбора часового пояса будут предложены системные дата и время по умолчанию.

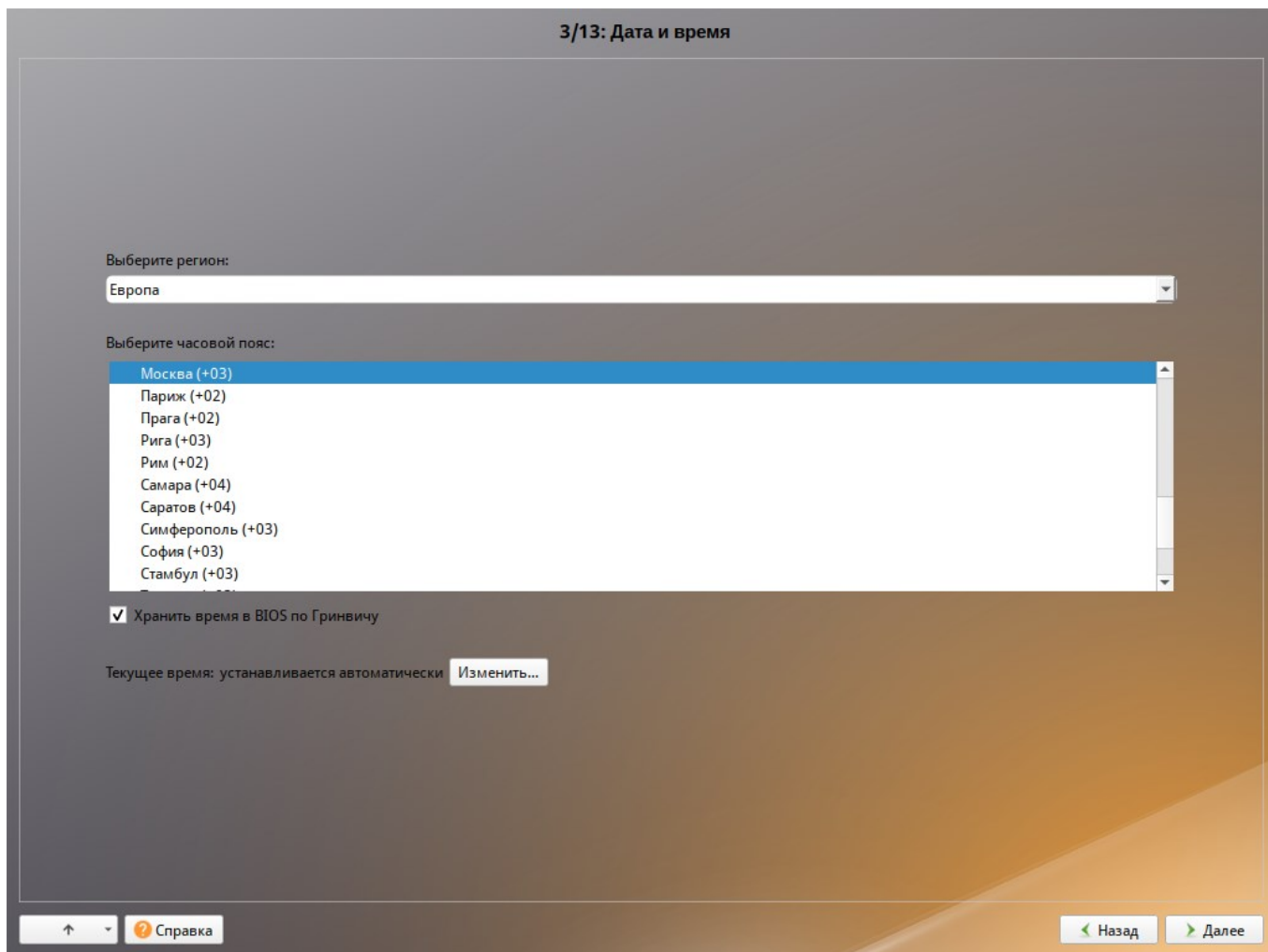


Рис. 4 – Установка. Выбор часового пояса

Для ручной установки текущих даты и времени нужно нажать на кнопку «Изменить...». Откроется окно ручной настройки системных параметров даты и времени (рис. 5).

По умолчанию для синхронизации системных часов (NTP) с удаленным сервером по сети Интернет отмечен пункт «Получать точное время с NTP-сервера» и указан NTP-сервер `pool.ntp.org`.

Если выбрана опция «Получать точное время с NTP-сервера», то компьютер может и сам быть сервером точного времени. Для работы компьютера в качестве сервера точного времени внутри локальной сети нужно отметить пункт «Работать как NTP-сервер».

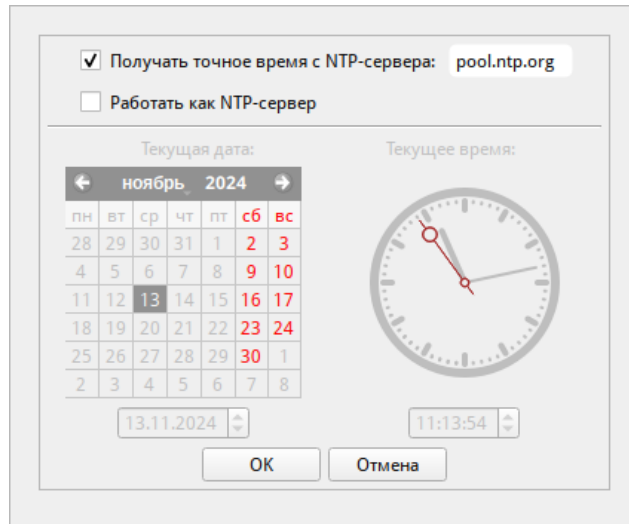


Рис. 5 – Установка. Настройка времени

Для сохранения настроек и продолжения установки системы в окне ручной установки даты и времени следует нажать на кнопку «ОК» и затем в окне «Дата и время» нажать на кнопку «Далее».

5.4.4. Подготовка диска

На этом этапе программа установки подготавливает площадку для установки ОС Альт СП, в первую очередь – выделяется свободное место на диске.

Переход к этому шагу может занять некоторое время – период ожидания может быть разным и зависит от производительности компьютера, объема жесткого диска, количества разделов на нем и других параметров.

5.4.4.1. Выбор профиля разбиения диска

После завершения первичной конфигурации загрузочного носителя откроется окно «Подготовка диска» (рис. 6). В списке разделов перечислены уже существующие на жестких дисках разделы (в том числе здесь могут оказаться съемные USB-носители, подключенные к компьютеру в момент установки).

В списке «Выберите профиль» перечислены доступные профили разбиения диска. Профиль – это шаблон распределения места на диске для установки ОС. Можно выбрать один из профилей:

- установка рабочей станции;
- ручную.

Первый профиль предполагает автоматическое разбиение диска.

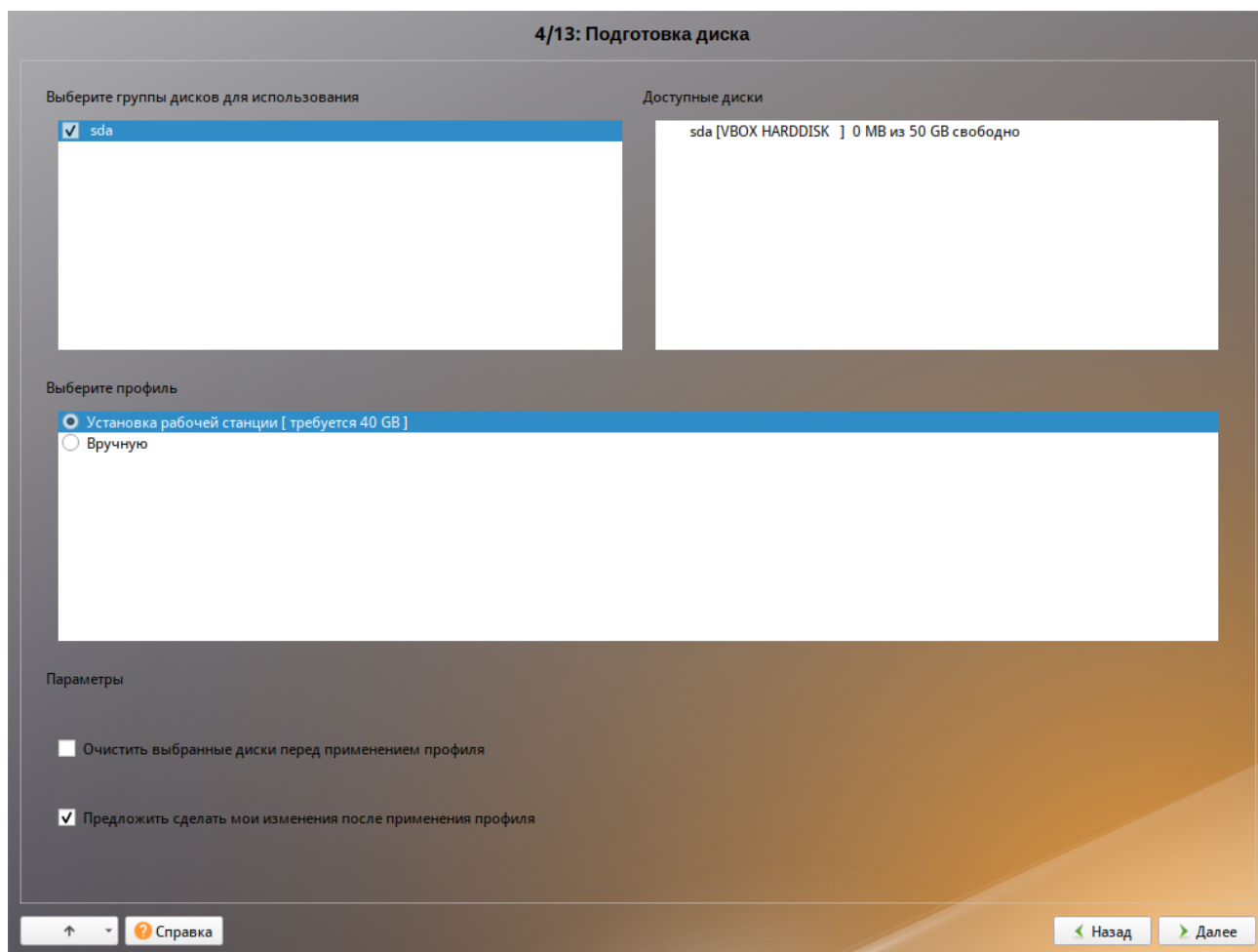


Рис. 6 – Установка. Установка рабочей станции

5.4.4.2. Автоматические профили разбиения диска

Если происходит установка рабочей станции, то при выборе профиля «Установка рабочей станции» будут выделены отдельные разделы для EFI, для корневой файловой системы и для /home (рис. 7).

Если результат разбиения дисков по каким-то причинам не устраивает, сейчас можно его отредактировать.

От возможности редактировать результат разбиения можно отказаться, сняв выделение с пункта «Предложить сделать мои изменения после применения профиля». В этом случае никакой информации о распределении дискового пространства на экране отображаться не будет. После осуществления физических изменений на жестком диске начнется установка базовой системы. Этот вариант подойдет для установки на чистый диск.

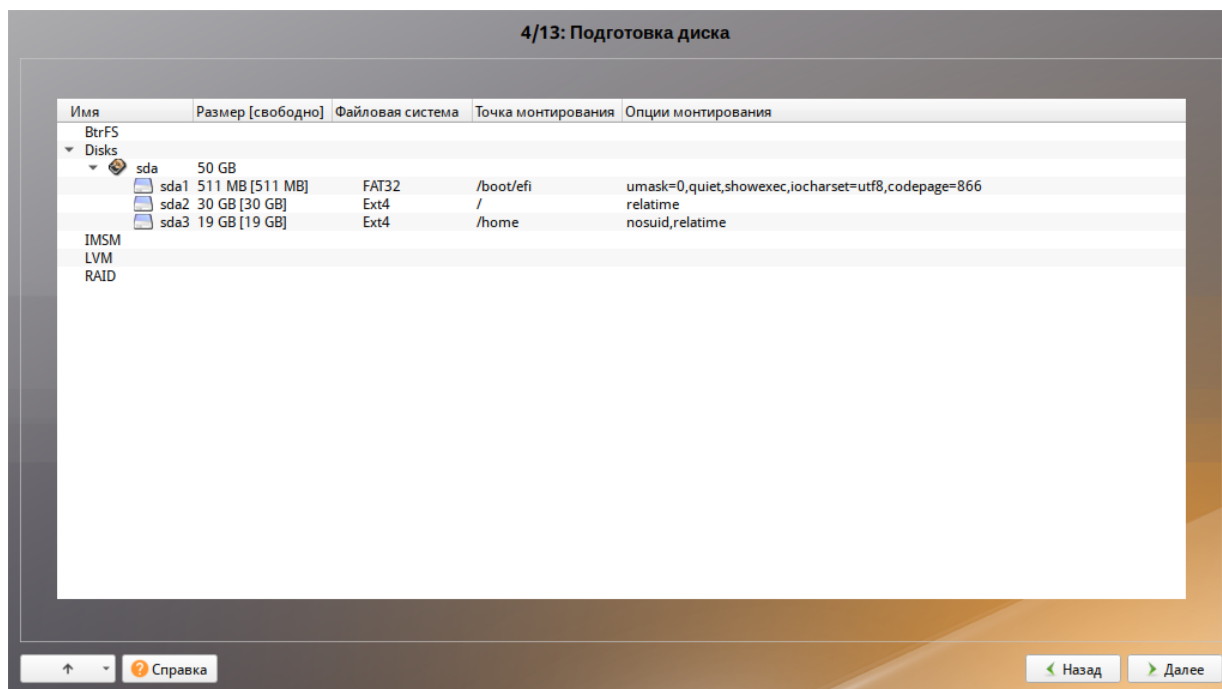


Рис. 7 – Установка. Профиль «Установка рабочей станции»

Рядом с названием профиля указан минимальный объем свободного места на диске, требуемый для установки в соответствии с данным профилем.

Примечание. Если при применении профиля автоматического разбиения диска доступного места на диске окажется недостаточно, то на монитор будет выведено сообщение об ошибке: «Невозможно применить профиль, недостаточно места на диске». Для решения этой проблемы можно полностью очистить место на диске, отметив пункт «Очистить выбранные диски» перед применением профиля и применить профиль повторно. Если сообщение о недостатке места на диске появляется и при отмеченном пункте «Очистить выбранные диски перед применением профиля», то это связано с недостаточным для использования автоматических методов разметки объемом выбранных дисков. В этом случае вы можете воспользоваться методом ручной разметки: профиль «Вручную».

⚠ При отмеченном пункте «Очистить выбранные диски перед применением профиля» будут удалены все данные с выбранных дисков (включая внешние USB-носители) без возможности восстановления. Рекомендуется использовать эту возможность при полной уверенности в том, что диски не содержат никаких ценных данных.

Для продолжения установки следует нажать кнопку «Далее». Появится окно со списком настроенных разделов и их точек монтирования. Подтвердите переход к следующему шагу нажатием на кнопку «ОК».

Примечание. Разбивка не затрагивает CF-диск, на котором может храниться система бинарной трансляции.

5.4.4.3. Ручной профиль разбиения диска

При необходимости освободить часть дискового пространства следует воспользоваться профилем разбиения «Вручную». В этом случае можно удалить некоторые из существующих разделов или содержащиеся в них файловые системы. После этого можно создать разделы самостоятельно или вернуться к шагу выбора профиля и применить автоматический профиль. Выбор этой возможности требует знаний об устройстве диска и технологиях его разбиения.

⚠ В случае ручной разбивки необходимо создать и подключить на первом разделе диска (не MD RAID) раздел для ядра `/boot` с файловой системой `ext2` (т. е. без `extents` и журнала).

По нажатию «Далее» будет произведена запись новой таблицы разделов на диск и форматирование разделов. Разделы, только что созданные на диске программой установки, пока не содержат данных и поэтому форматируются без предупреждения. Уже существовавшие, но измененные разделы, которые будут отформатированы, помечаются специальным значком в колонке «Файловая система» слева от названия. При уверенности в том, что подготовка диска завершена, подтвердите переход к следующему шагу нажатием кнопки «Далее».

Не следует форматировать разделы с теми данными, которые нужно сохранить, например, со старыми пользовательскими данными (`/home`). С другой стороны отформатировать можно любые разделы, которые нужно «очистить» (т. е. удалить все данные).

5.4.4.4. Дополнительные возможности разбиения диска

Ручной профиль разбиения диска позволяет установить ОС на программный RAID-массив, разместить разделы в томах LVM и использовать маскирование на разделах. Данные возможности требуют от пользователя понимания принципов функционирования указанных технологий.

5.4.4.4.1. Создание программного RAID-массива

Избыточный массив независимых дисков RAID (redundant array of independent disks) – технология виртуализации данных, которая объединяет несколько НЖМД в логический элемент для избыточности и повышения производительности.

Примечание. Для создания программного RAID-массива потребуется минимум два жестких диска.

Программа установки поддерживает создание программных RAID-массивов следующих типов:

- RAID 1;
- RAID 0;
- RAID 4/5/6;
- RAID 10.

Процесс подготовки к установке на RAID условно можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание RAID-массивов на разделах жесткого диска;
- создание файловых систем на RAID-массиве.

⚠ Для создания программного RAID-массива может потребоваться предварительно удалить существующую таблицу разделов с жесткого диска.

Для настройки параметров нового раздела из состава RAID-массива нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел».

Для создания программного массива на GPT-разделах в открывшемся окне (рис. 8) нужно настроить следующие параметры:

- «Размер» – в поле нужно указать размер будущего раздела в Мбайт;
- «Смещение» – в поле нужно указать смещение начала данных на диске в Мбайт;
- «Тип раздела» – в выпадающем поле нужно выбрать значение «Linux RAID» для последующего включения раздела в RAID-массивы.

На втором диске создать два раздела с типом «Linux RAID». При этом разделы на разных дисках должны совпадать по размеру.

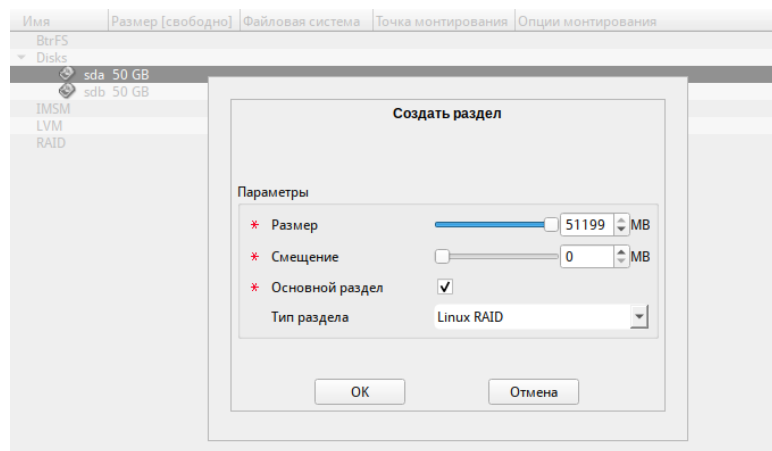


Рис. 8 – Создание раздела Linux RAID

Примечание. При создании разделов следует учесть, что объем результирующего массива может зависеть от размера, включенных в него разделов жесткого диска. Например, при создании RAID 1 результирующий размер массива будет равен размеру минимального участника.

После создания разделов на дисках можно переходить к организации самих RAID-массивов. Для этого в списке следует выбрать пункт «RAID», после чего нажать на кнопку «Создать RAID». Далее мастер предложит выбрать тип массива и указать его участников (рис. 9, рис. 10).

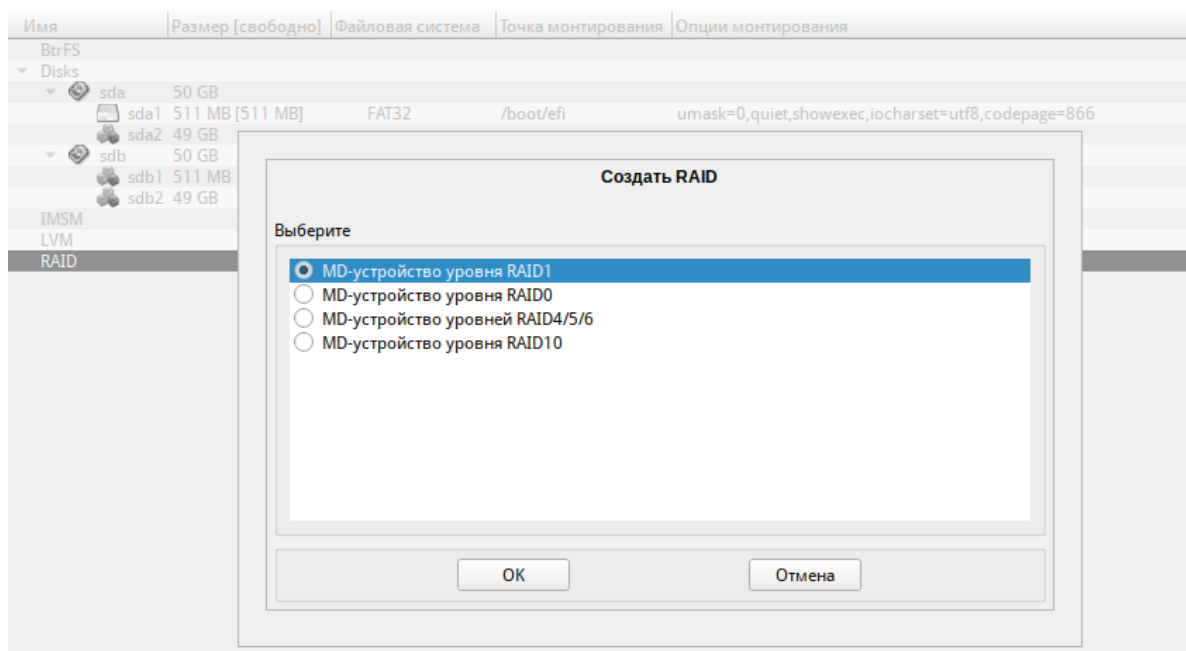


Рис. 9 – Установка. Выбор типа RAID-массива

Примечание. По умолчанию выбираются все разделы, поэтому необходимо снять отметку с раздела sdb1.

После того, как RAID-массив создан, его можно использовать как обычный раздел на жестких дисках, то есть на нем можно создавать файловые системы или же, например, включать в LVM-тома.

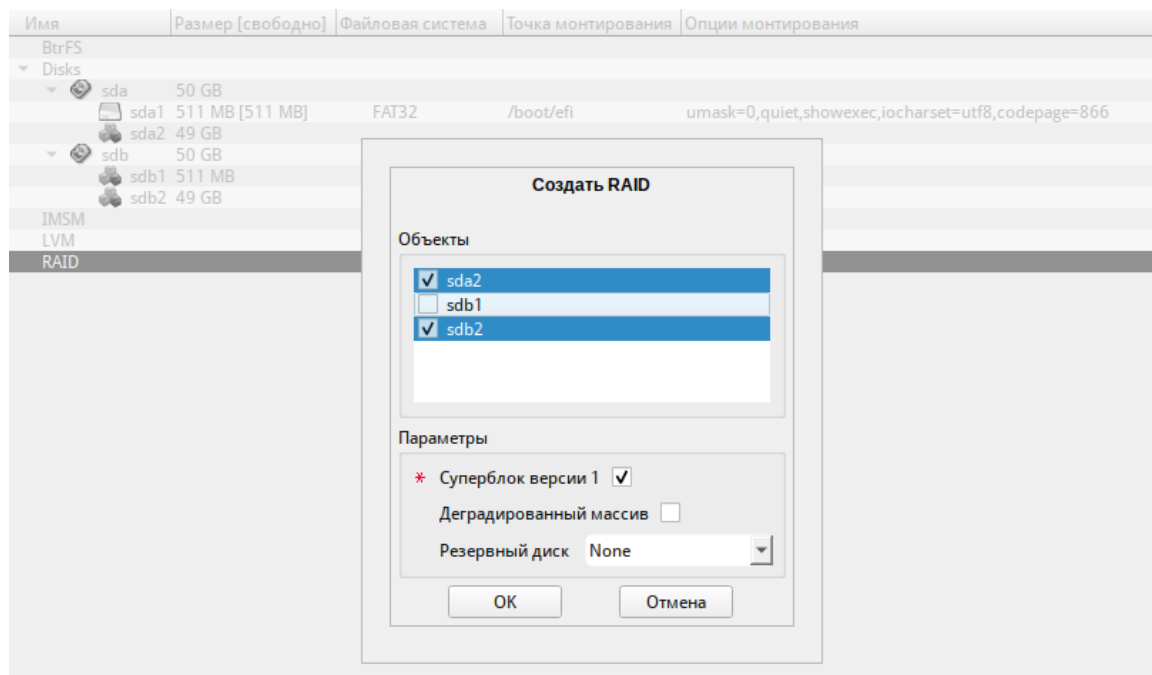


Рис. 10 – Установка. Выбор участников RAID-массива

5.4.4.4.2. Создание LVM-томов

Менеджер логических дисков LVM (Logical Volume Manager) – средство гибкого управления дисковым пространством, позволяющее создавать поверх физических разделов (либо неразбитых дисков) логические тома, которые в самой системе будут видны как обычные блочные устройства с данными (обычные разделы).

Процесс подготовки к установке на LVM можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание группы томов LVM;
- создание томов LVM;
- создание файловых систем на томах LVM.

Примечание. Для создания группы томов LVM может потребоваться предварительно удалить таблицу разделов с жесткого диска.

Для настройки параметров нового раздела нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать на кнопку «Создать раздел».

При создании разделов на жестких дисках для последующего включения их в LVM-тома следует указать «Тип раздела» для них, равным «Linux LVM» (рис. 11).

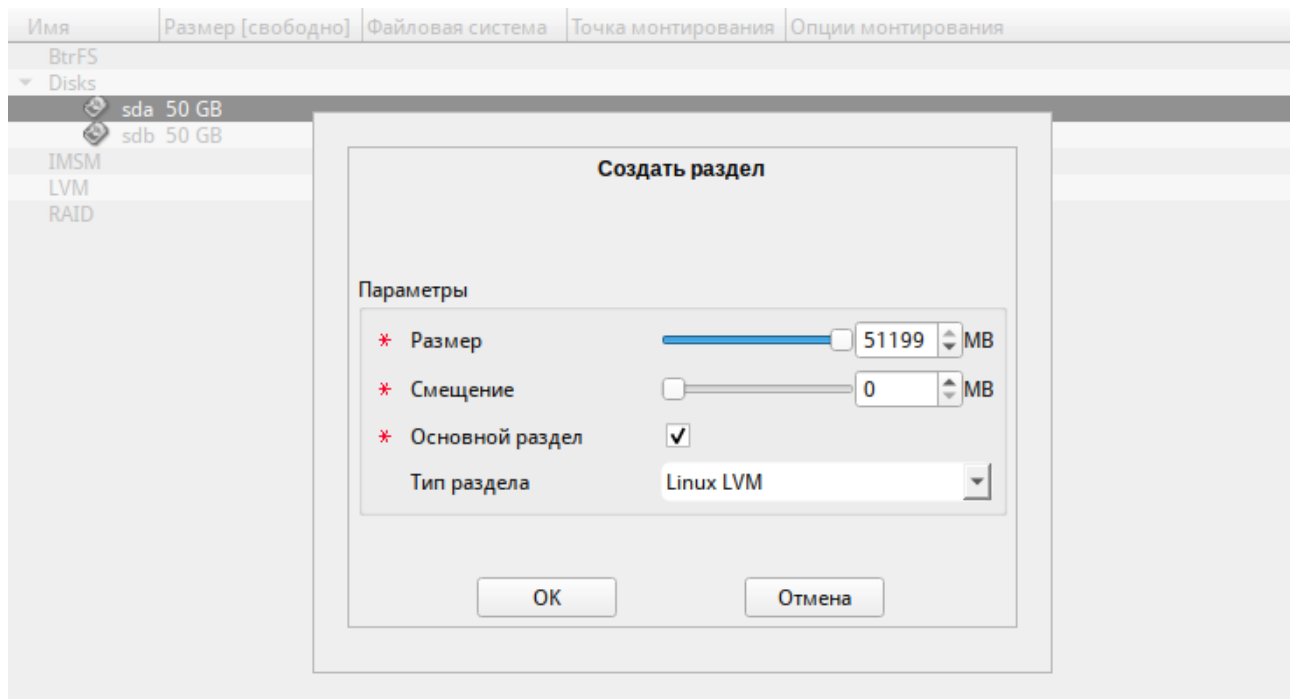


Рис. 11 – Создание раздела Linux LVM в режиме Legacy

После создания разделов на дисках можно переходить к созданию группы томов LVM. Для этого в списке следует выбрать «LVM», после чего нажать кнопку «Создать группу томов».

В открывшемся окне (рис. 12) необходимо выбрать физические разделы, которые будут входить в группу томов, указать название группы и выбрать размер экстенда.

Примечание. Размер экстенда представляет собой наименьший объем пространства, который может быть выделен тому. Размер экстенда по умолчанию 65536 (65536*512 байт = 32 Мбайт, где 512 байт – размер сектора).

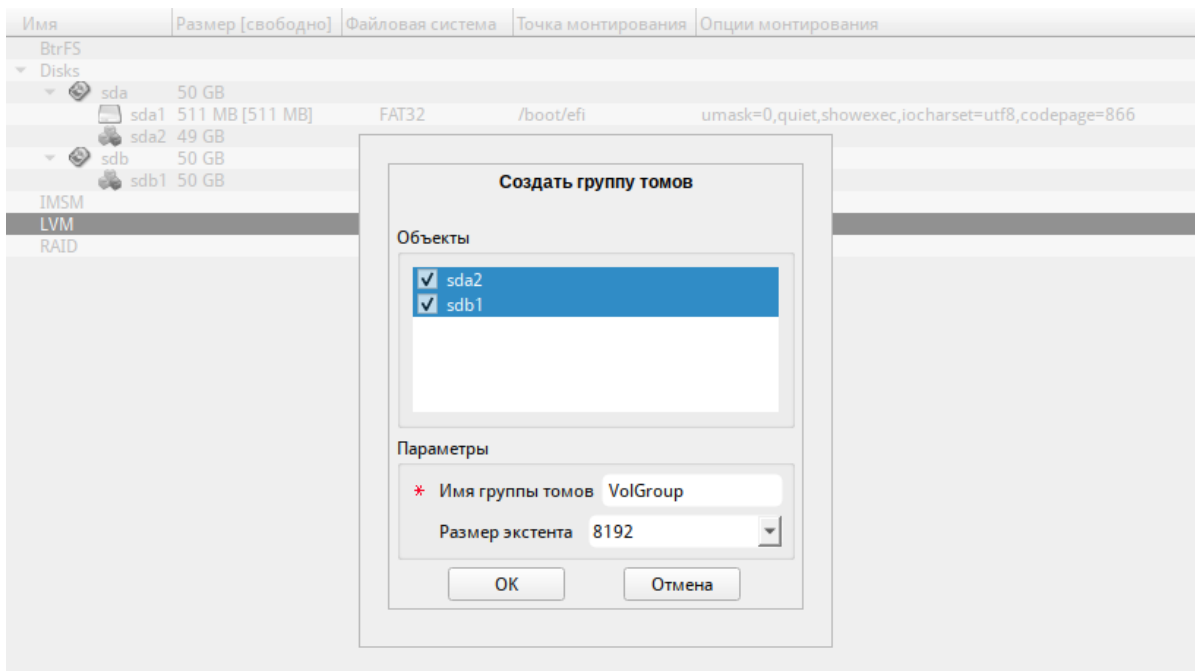


Рис. 12 – Установка. Подготовка диска. Создание группы томов LVM

После того, как группа томов LVM создана, ее можно использовать как обычный жесткий диск, то есть внутри группы томов можно создавать тома (аналог раздела на физическом жестком диске) и файловые системы внутри томов (рис. 13).

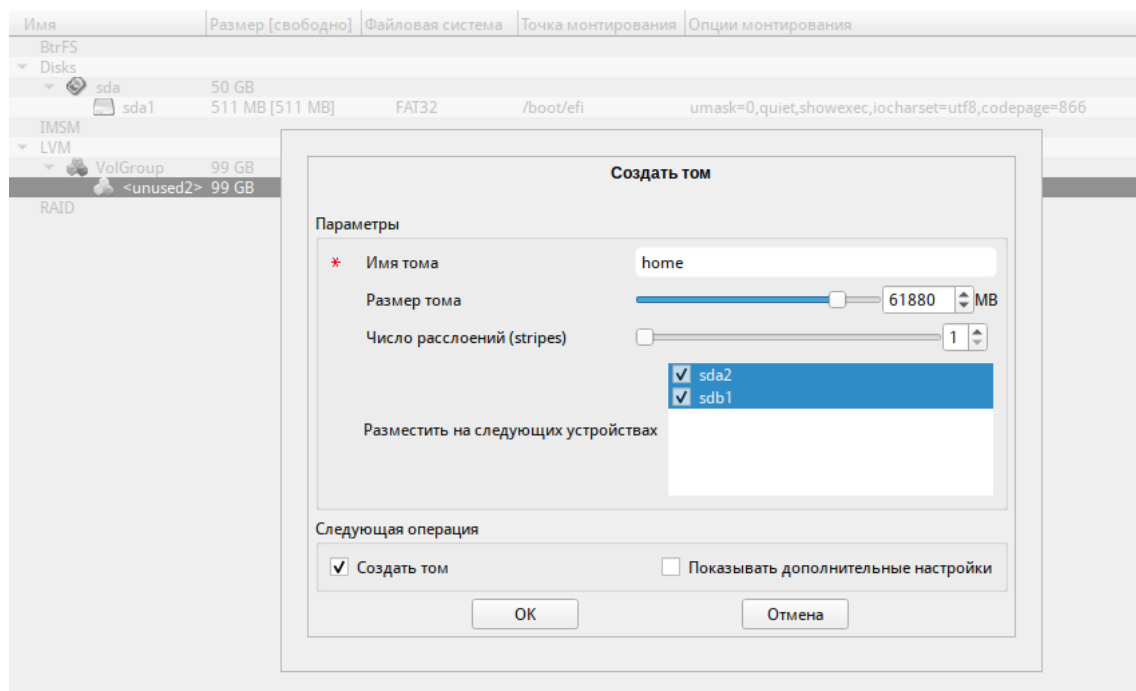


Рис. 13 – Установка. Подготовка диска. Создание тома

5.4.4.4.3. Создание подтомов Btrfs

Btrfs – файловая система, которая может работать с очень большими файлами, имеется поддержка снимков файловой системы (снапшотов), сжатие и подтома.

Подтом (subvolume) не является блочным устройством, но в каждом томе Btrfs создается один подтом верхнего уровня (subvol=5), в этом подтоме могут создаваться другие подтома и снапшоты. Подтома (подразделы, subvolumes) создаются ниже вершины дерева Btrfs по мере необходимости, например, для / и /home создаются подтома с именами @ и @home. Для монтирования подтомов нужны определенные параметры вместо корня системы Btrfs по умолчанию:

- подтом @ монтируется в / с помощью опции `subvol=@`;
- подтом @home (если он используется) монтируется с помощью параметра монтирования `subvol=@home`.

В данном разделе рассмотрен вариант подготовки раздела Btrfs с разбивкой на подтома @ и @home.

Программа установки позволяет создать подтома (subvolume), указав разные точки монтирования.

Процесс подготовки к установке на подтома условно можно разбить на следующие шаги:

- создание разделов на жестких дисках;
- создание подтомов на разделах жесткого диска.

Для настройки параметров нового раздела нужно выбрать неразмеченный диск в окне профиля разбивки пространства «Вручную» и нажать кнопку «Создать раздел».

При создании раздела на жестком диске следует указать «Тип раздела» равным «Linux» (рис. 14).

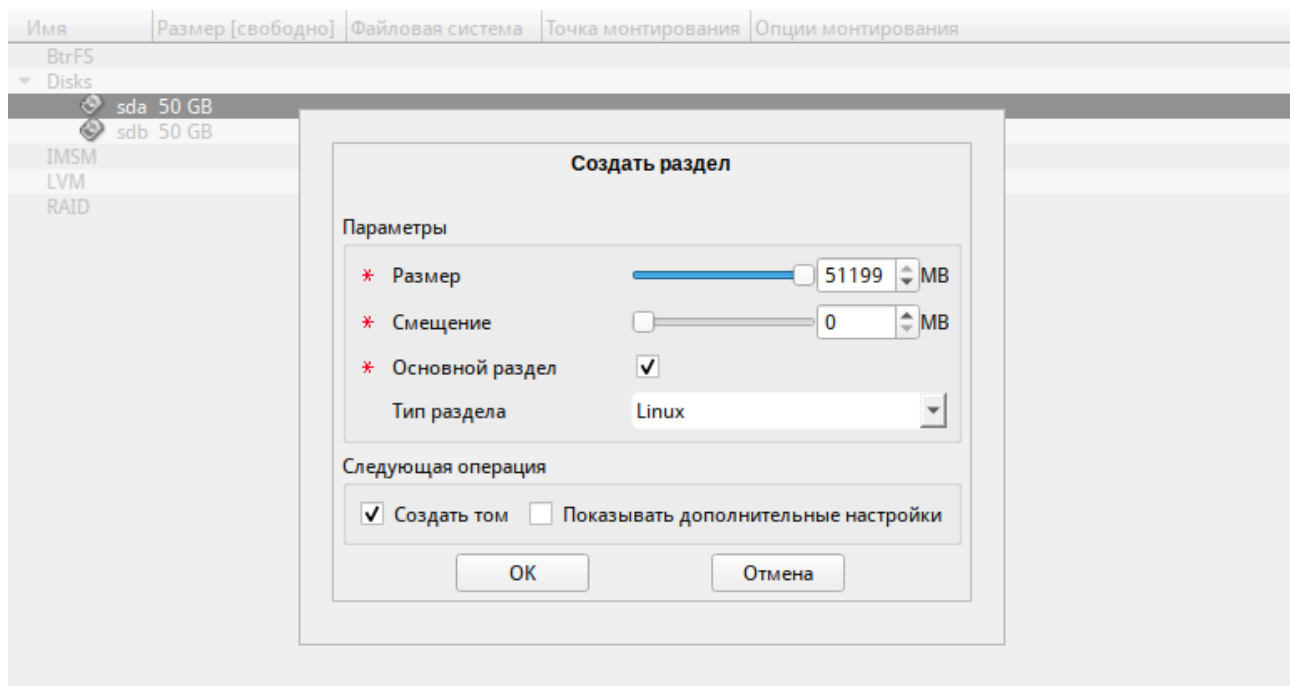


Рис. 14 – Создание раздела с ФС BtrFS

На следующем шаге выбрать файловую систему BtrFS (рис. 15).

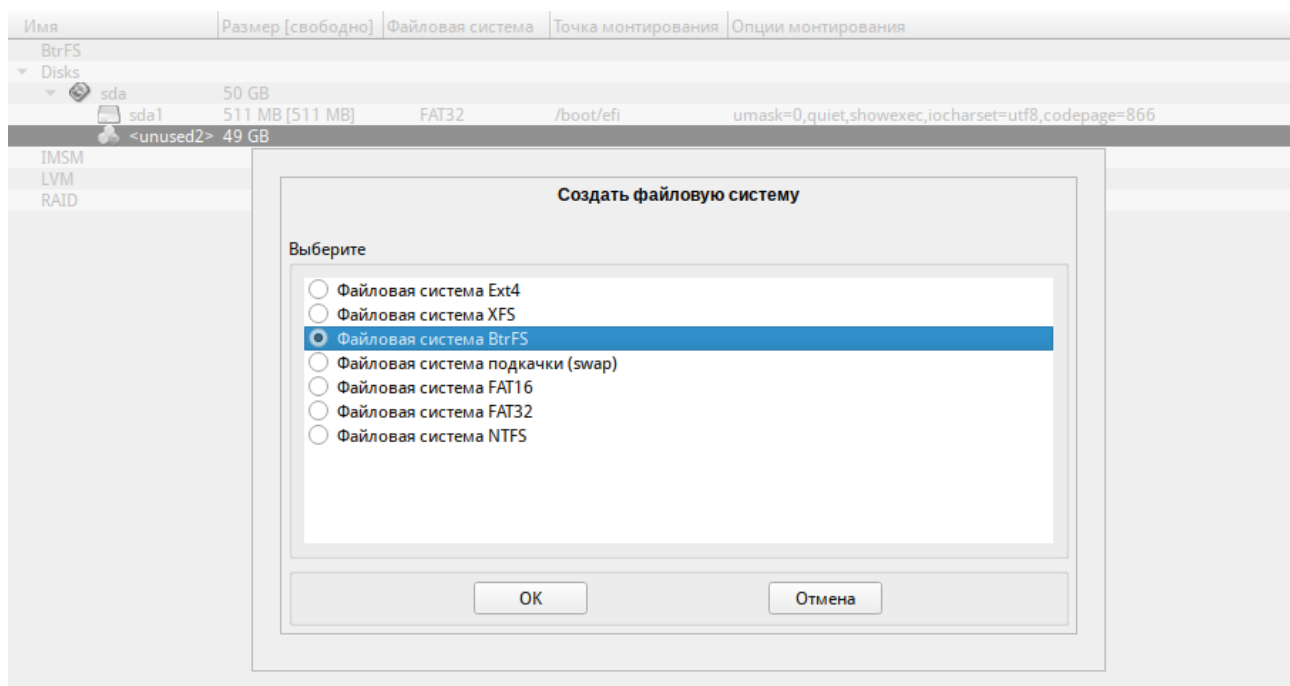


Рис. 15 – Создание раздела с ФС BtrFS

В окне «Изменить точку монтирования» (рис. 16) нажать кнопку «Отмена» (не указывать точку монтирования для раздела).

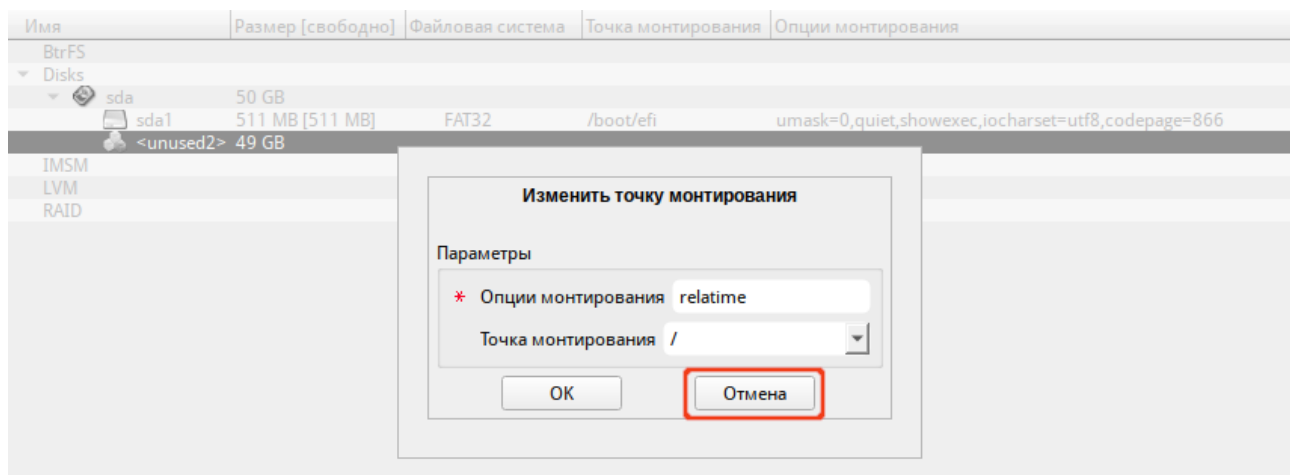


Рис. 16 – Окно «Изменить точку монтирования»

После создания раздела можно переходить к созданию подтомов. Для этого в списке следует выбрать раздел с файловой системой BtrFS, после чего нажать на кнопку «Создать подтом».

В открывшемся окне следует указать имя подтома или путь до него. На рис. 17 показано создание подтома @home. Данное действие следует повторить для создания подтома @.

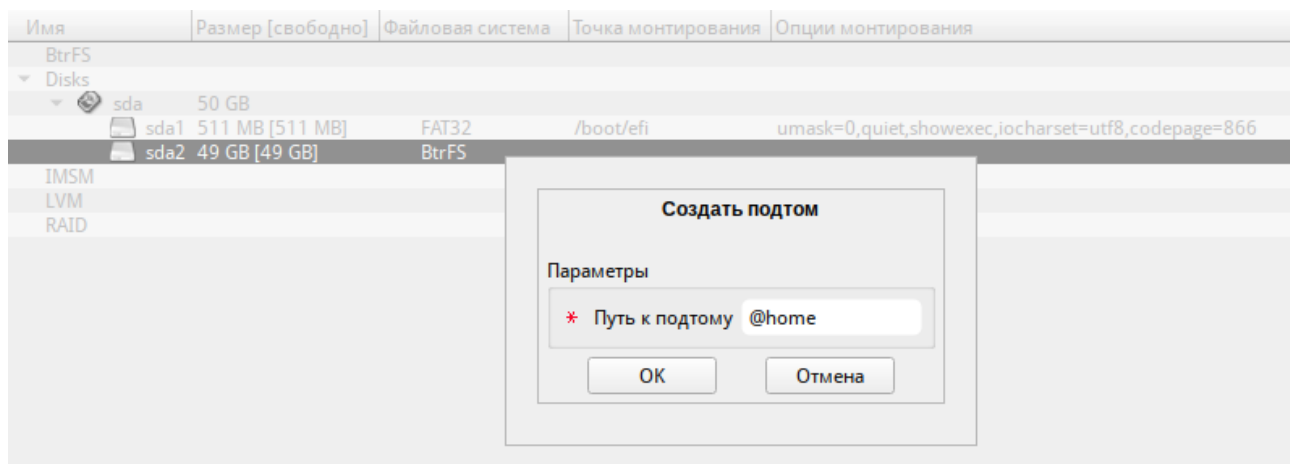


Рис. 17 – Создание подтома

После создания подтомов нужно указать точки монтирования для каждого тома. Для этого выбрать подтом и нажать на кнопку «Изменить точку монтирования» (рис. 18).

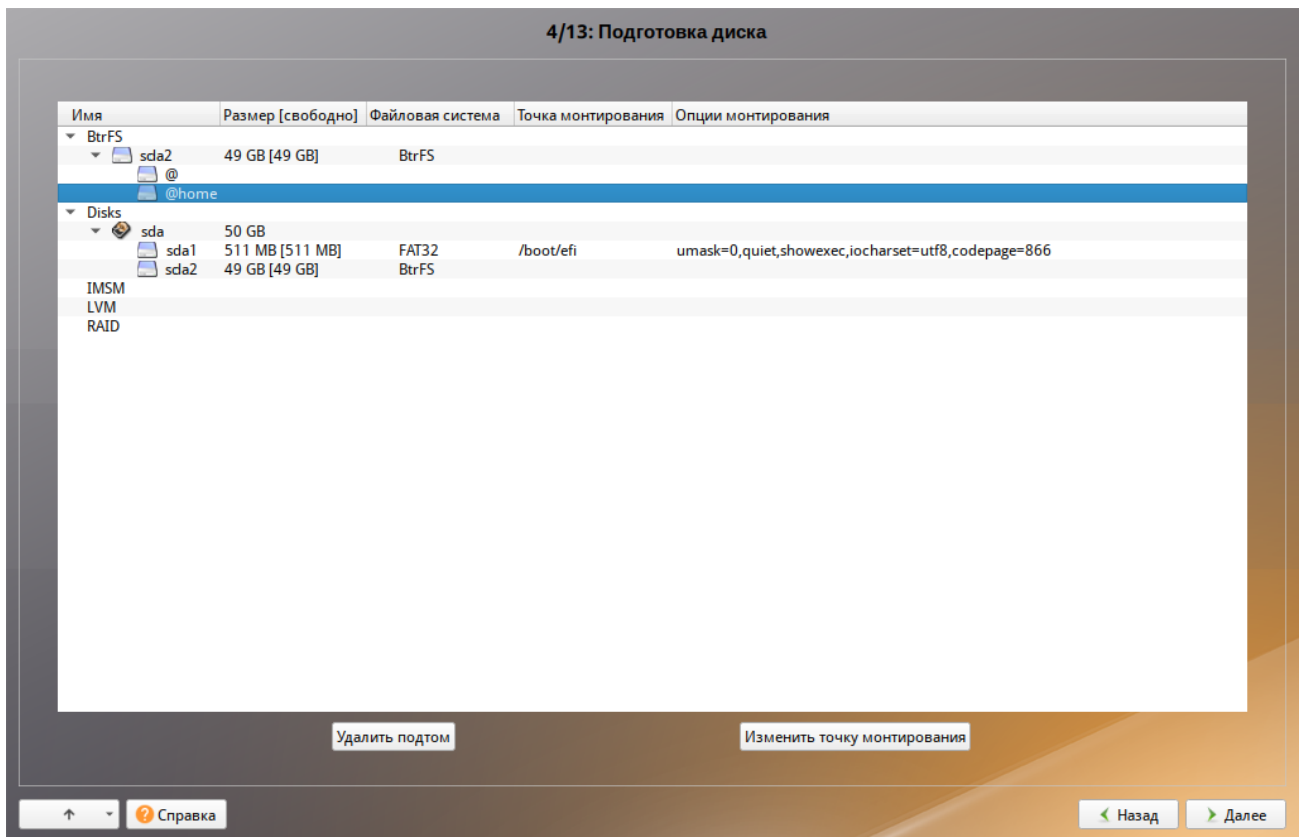


Рис. 18 – Созданные подтома

В открывшемся окне указать точку монтирования (рис. 19).

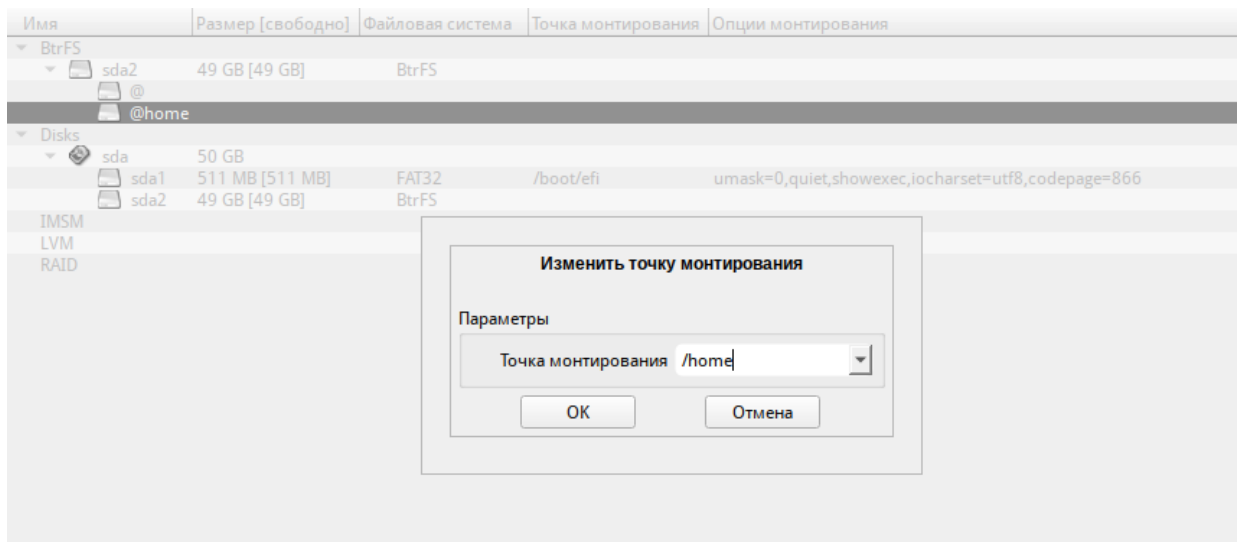


Рис. 19 – Точка монтирования для подтома @home

После указания точек монтирования для подтомов можно установить систему как обычно.

5.4.5. Перемонтирование

По завершении этапа подготовки диска начинается шаг перемонтирования. Он проходит автоматически и не требует вмешательства пользователя. На экране отображается индикатор выполнения (рис. 20).

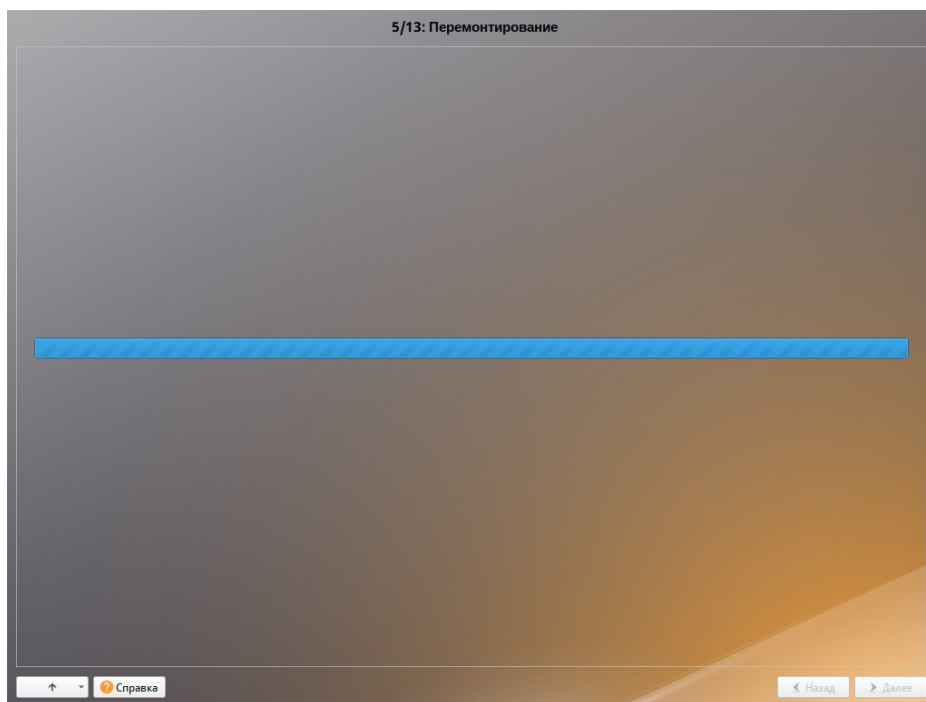


Рис. 20 – Перемонтирование

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.6. Установка системы

На данном этапе происходят распаковка ядра и установка набора программ, которые требуются для работы ОС Альт СП.

Программа установки предлагает выбрать дополнительные пакеты программ, которые будут включены в состав ОС Альт СП и установлены вместе с ней на диск (рис. 21).

Под списком групп на экране отображается информация об объеме дискового пространства, которое будет занято после установки пакетов, входящих в выбранные группы.

При выборе группы пакетов будет показан список программных пакетов, входящих в состав этой группы.

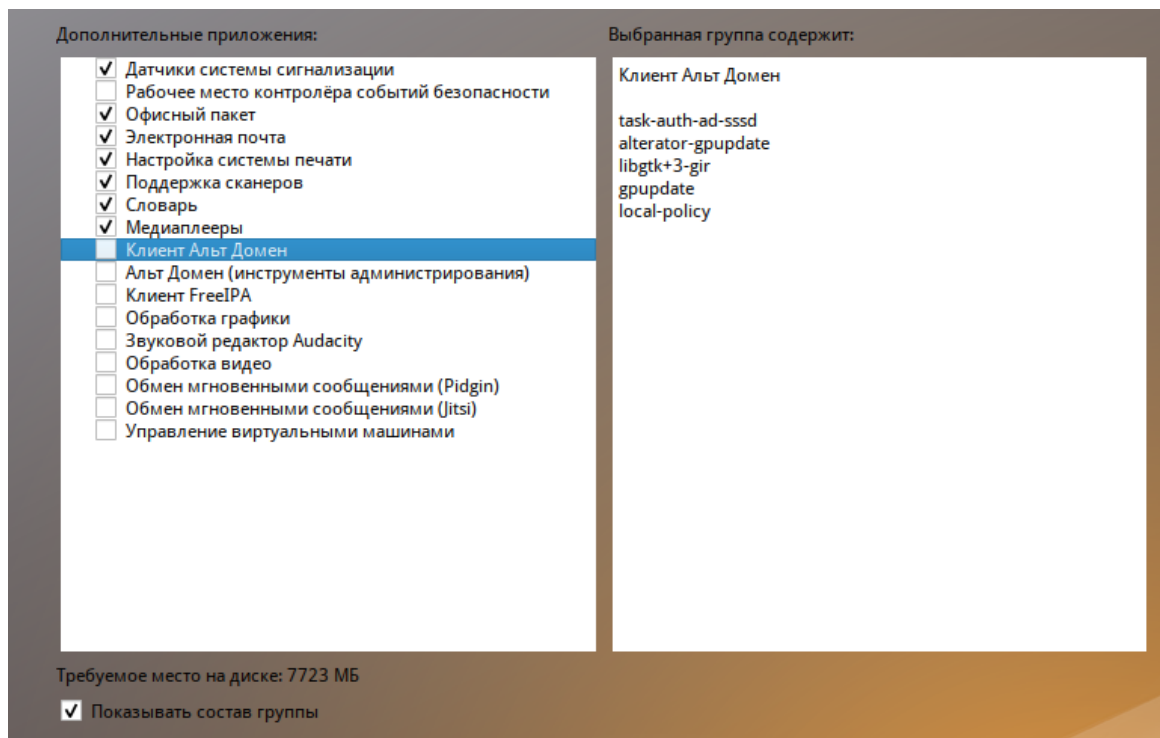


Рис. 21 – Установка рабочей станции. Выбор групп пакетов

Выбрав группы пакетов, следует нажать «Далее», после чего начнется установка пакетов (рис. 22).

Установка пакетов происходит автоматически в два этапа:

- получение пакетов;
- установка пакетов.

Получение пакетов осуществляется с источника, выбранного на этапе начальной загрузки. При сетевой установке (по протоколу FTP или HTTP) время выполнения этого шага будет зависеть от скорости соединения.



Рис. 22 – Установка. Установка пакетов

5.4.7. Сохранение настроек

Начиная с данного этапа, программа установки работает с файлами только что установленной базовой системы. Все последующие изменения можно будет совершить после завершения установки посредством редактирования соответствующих конфигурационных файлов или при помощи модулей управления, включенных в дистрибутив.

После завершения установки базовой системы выполняется шаг сохранения настроек (рис. 23). Он проходит автоматически и не требует вмешательства пользователя, на экране отображается индикатор выполнения.

На данном этапе производится перенос настроек, выполненных на первых шагах установки, в установленную базовую систему. Также производится запись информации о соответствии разделов жесткого диска смонтированным на них файловым системам (заполняется конфигурационный файл `/etc/fstab`).

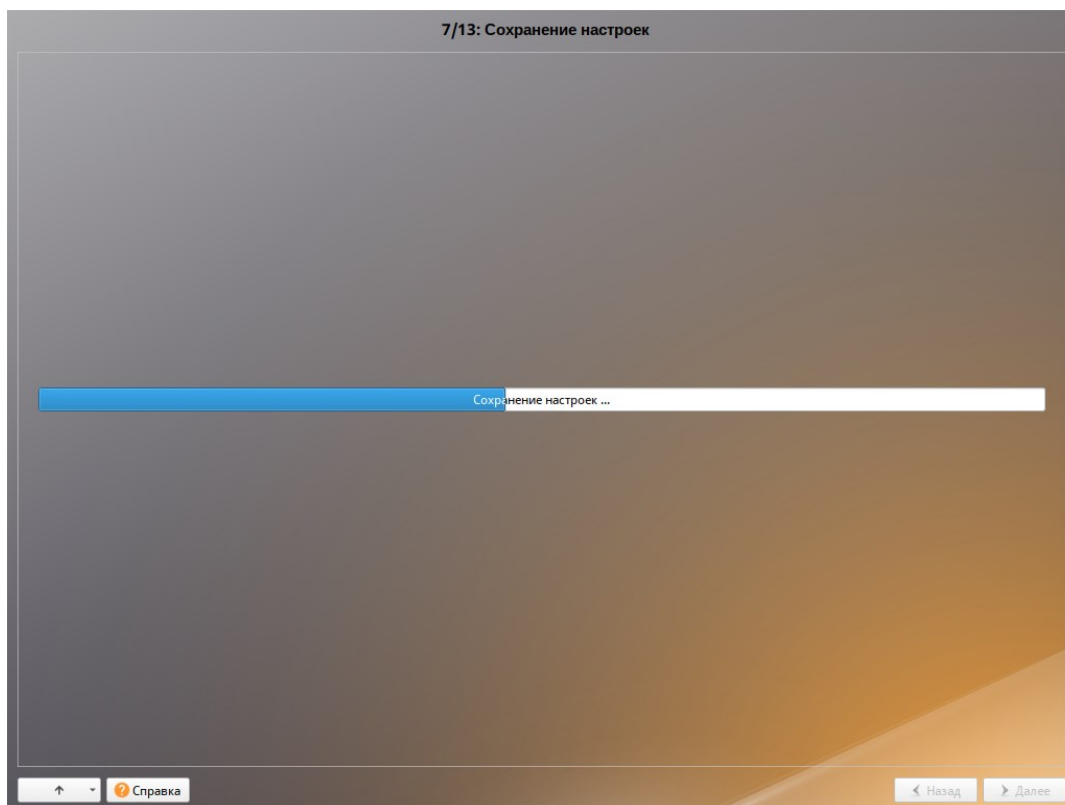


Рис. 23 – Установка. Сохранение настроек

В список доступных источников программных пакетов добавляется репозиторий, находящийся на установочном лазерном диске – выполняется команда `apt-cdrom add`, осуществляющая запись в конфигурационный файл `/etc/apt/sources.list`.

После сохранения настроек осуществляется автоматический переход к следующему шагу.

5.4.8. Настройка сети

На этом этапе в окне «Настройка сети» нужно задать параметры работы сетевой карты и настройки сети (рис. 24):

- «Имя компьютера» – сетевое имя компьютера (это общий сетевой параметр, не привязанный к какому-либо конкретному интерфейсу);
- «Интерфейсы» – список доступных сетевых интерфейсов;
- «Версия протокола IP» – версия используемого протокола IP (IPv4, IPv6);
- «Конфигурация» – способ назначения IP-адресов (службы DHCP, Zeroconf либо вручную);

- «IP-адреса» – пул назначенных IP-адресов из поля «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP» – позволяет ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети. Для переноса адреса в пул поля «IP-адреса» необходимо нажать кнопку «Добавить»;
- «Шлюз по умолчанию» – адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- «Домены поиска» – список предпочтительных доменов, по которым будет выполняться поиск.

Конкретные значения будут зависеть от используемого сетевого окружения. Ручного введения настроек можно избежать, если в сети уже есть настроенный DHCP-сервер. В этом случае все нужные сетевые настройки будут получены автоматически.

В окне (рис. 25), открываемом при нажатии кнопки «Дополнительно», можно выбрать сетевую подсистему (NetworkManager, Etcnet) для интерфейса, а также указать должен ли запускаться данный интерфейс при загрузке системы.

Для сохранения настроек сети и продолжения работы программы установки нужно нажать на кнопку «Далее».

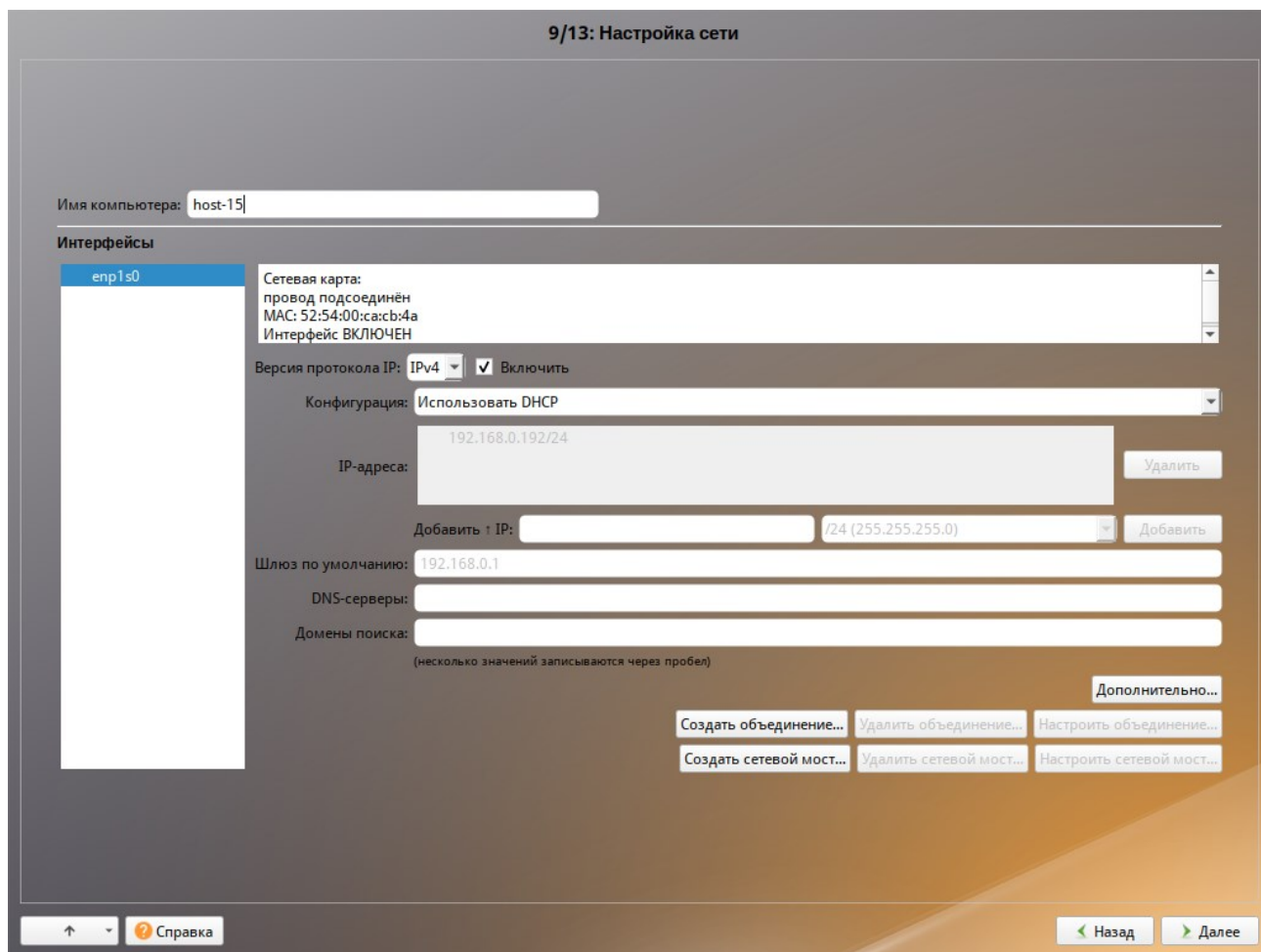


Рис. 24 – Установка. Настройка сети

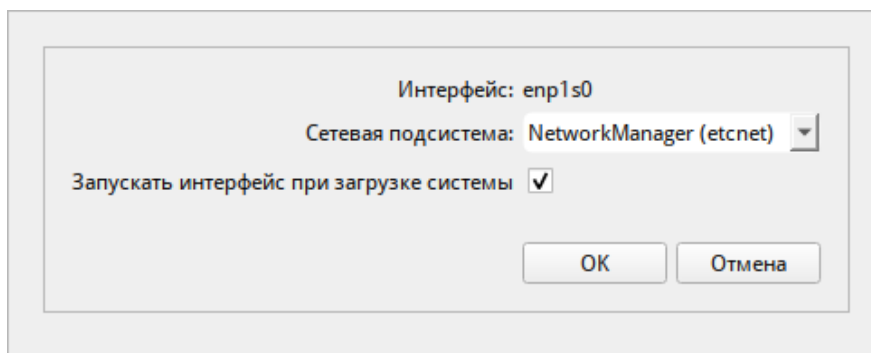


Рис. 25 – Установка. Настройка сетевой подсистемы

5.4.9. Администратор системы

На данном этапе загрузчик создает учетную запись администратора (рис. 26). В открывшемся окне нужно ввести пароль учетной записи администратора (root). Чтобы исключить опечатки при вводе пароля, пароль учетной записи вводится дважды.

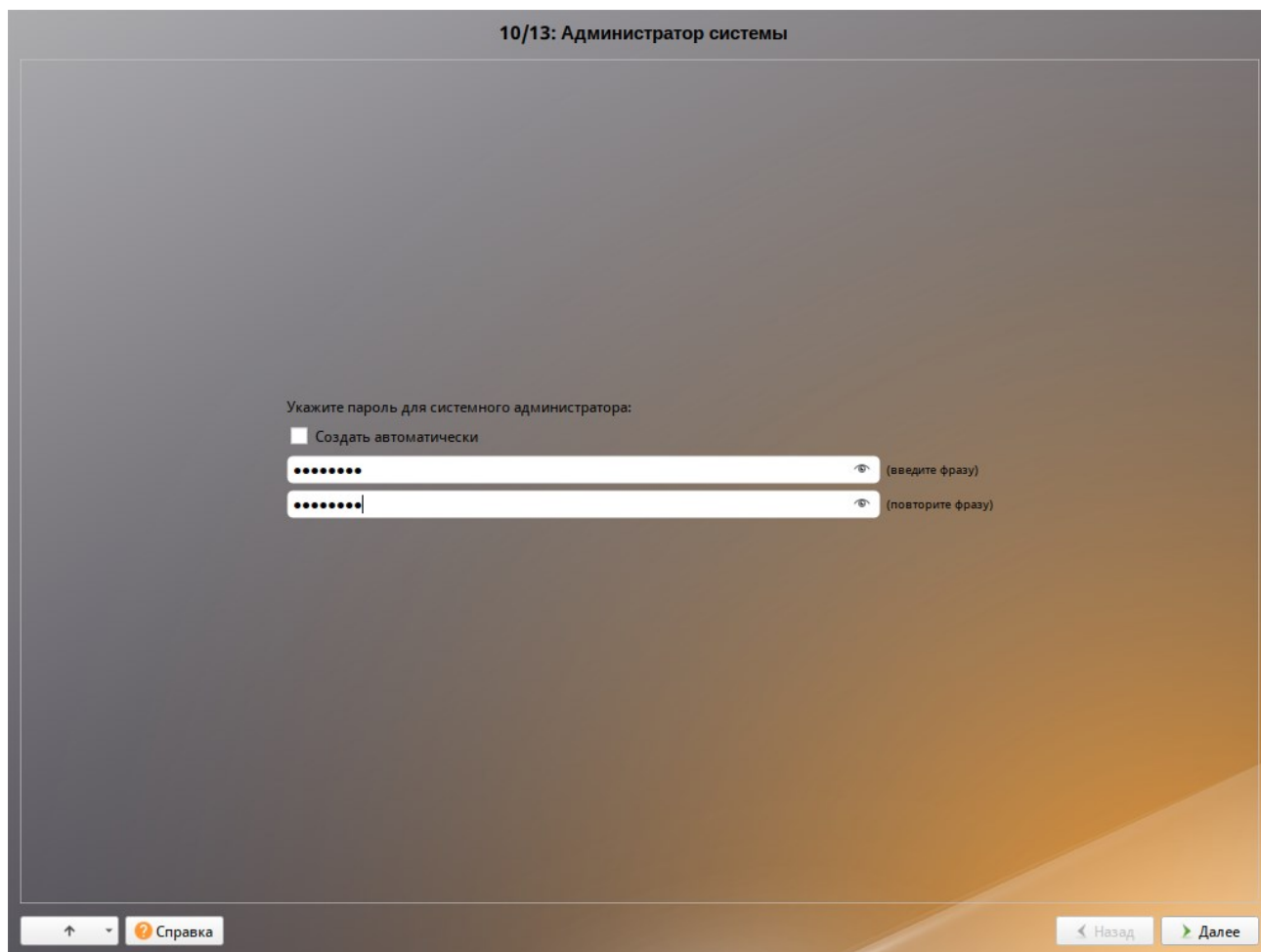


Рис. 26 – Установка. Задание пароля администратора

Для автоматической генерации пароля нужно отметить пункт «Создать автоматически». Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

В любой системе Linux всегда присутствует один специальный пользователь-администратор системы, он же суперпользователь. Для него зарезервировано стандартное системное имя – root.

Администратор системы отличается от всех прочих пользователей тем, что ему позволено производить любые, в том числе критичные изменения в системе. Поэтому выбор пароля администратора системы – очень важный момент для безопасности. Любой, кто сможет ввести его правильно (узнать или подобрать), получит неограниченный доступ к системе. Даже собственные неосторожные действия от имени root могут иметь катастрофические последствия для всей системы.

⚠ Запомните пароль root – его нужно будет вводить для получения права изменять настройки системы с помощью стандартных средств настройки ОС. Более подробную информацию о режиме суперпользователя см. в п. 17.2.

Подтверждение введенного (или сгенерированного) пароля учетной записи администратора (root) и продолжение работы программы установки выполняется нажатием кнопки «Далее».

5.4.10. Системный пользователь

На данном этапе программа установки создает учетную запись системного пользователя (пользователя) ОС Альт СП.

Помимо администратора (root) в систему нужно добавить, по меньшей мере, одного обычного системного пользователя. Работа от имени администратора системы считается опасной, поэтому повседневную работу в Linux следует выполнять от имени ограниченного в полномочиях системного пользователя.

При добавлении системного пользователя предлагается в окне «Системный пользователь» заполнить следующие поля (рис. 27):

- «Имя» – имя учетной записи пользователя ОС Альт СП (слово, состоящее только из строчных латинских букв, цифр и символа подчеркивания «_», причем цифра и символ «_» не могут стоять в начале слова, есть также возможность использовать «-»). Начинаться имя должно со строчной латинской буквы);
- «Комментарий» – комментарий к имени учетной записи (обычно тут указывается реальные имя и фамилия пользователя);
- «Пароль» – пароль учетной записи пользователя (чтобы исключить опечатки при вводе пароля, пароль пользователя вводится дважды).

Для автоматической генерации пароля нужно отметить пункт «Создать автоматически». Система предложит пароль, сгенерированный автоматическим образом в соответствии с требованиями по стойкости паролей.

11/13: Системный пользователь

Новая учётная запись пользователя

Имя: user

Комментарий:

Пароль: ☐ Создать автоматически

..... (введите фразу)

..... (повторите фразу)

☐ Автоматический вход в систему

↑ Справка

Назад Далее

Рис. 27 – Установка. Создание пользователя

В процессе установки предлагается создать только одну учетную запись пользователя – чтобы от его имени администратор мог выполнять задачи, которые не требуют привилегий администратора (root). Учетные записи для всех прочих пользователей системы можно будет создать в любой момент после ее установки.

Подтверждение введенного (или сгенерированного) пароля учетной записи системного пользователя и продолжение работы программы установки выполняется нажатием кнопки «Далее».

5.4.11. Завершение установки

На экране последнего этапа установки отображается информация о завершении установки ОС Альт СП (рис. 28).

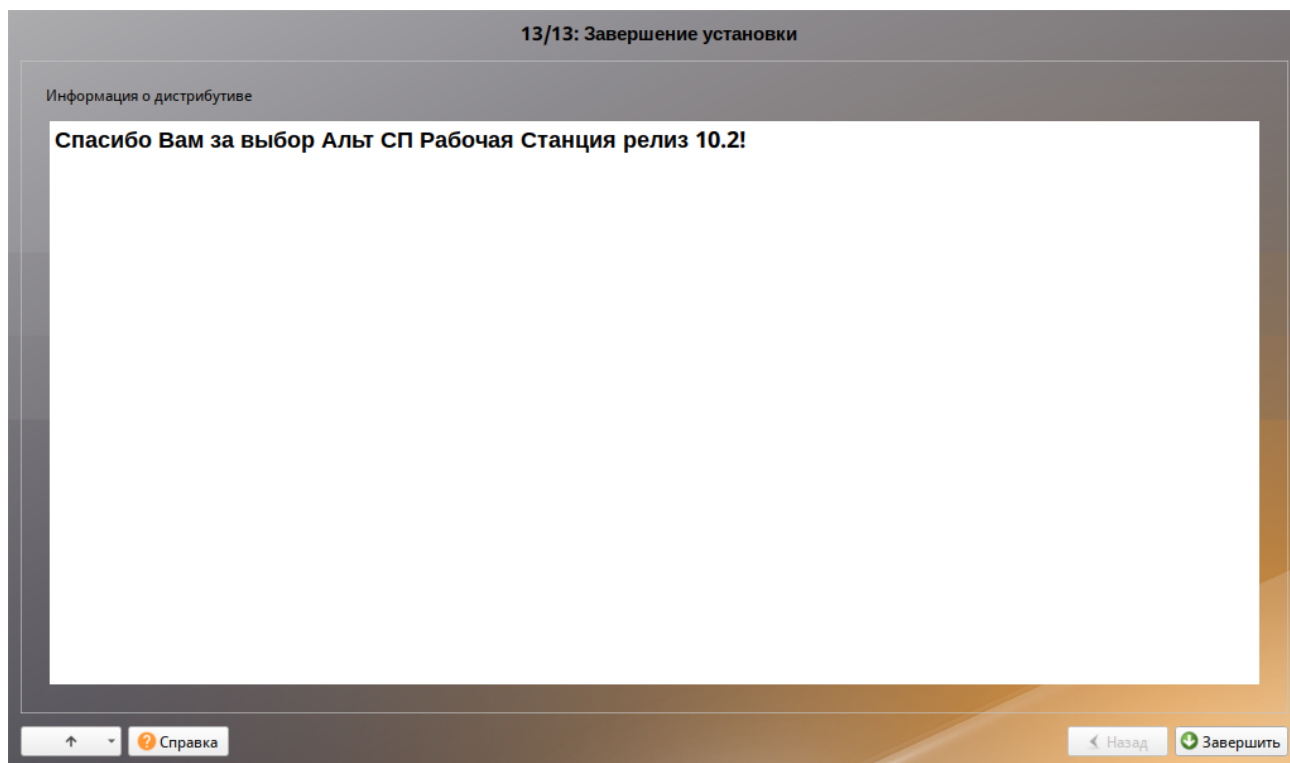


Рис. 28 – Установка. Завершение установки

После нажатия кнопки «Завершить» и перезагрузки компьютера выполняется штатная загрузка установленной ОС.

П р и м е ч а н и е . Если установка производилась на диск, отличный от того, с которого ВК загружается по умолчанию – следует повторно зайти в конфигурацию программы начальной загрузки, определить загрузочный диск (d) и указать его в качестве загрузочного диска по умолчанию (c). После изменений параметров загрузки, следует воспользоваться командой `m` для записи изменений в NVRAM и их применения в дальнейшем.

Не забудьте извлечь установочный компакт-диск (если это не происходит автоматически). Далее можно загружать установленную систему в обычном режиме.

5.5. Обновление системы до актуального состояния

После установки системы лучше сразу обновиться до актуального состояния. Можно не обновлять систему и сразу приступить к работе только в том случае, если не планируется подключение к сети или Интернету и нет необходимости устанавливать дополнительные программы.

Для обновления системы нужно выполнить команды (с правами администратора):

```
# apt-get update
# apt-get dist-upgrade
# update-kernel
# apt-get clean
# reboot
```

П р и м е ч а н и е . Получить права администратора (см. также п. 17.2) можно, выполнив в терминале команду:

```
$ su -
```

или зарегистрировавшись в системе (например, на второй консоли – нажать клавиши <Ctrl>+<Alt>+<F2>) под именем root.

Подробнее про обновление пакетов можно прочитать в п. 15.8, п. 15.9 и п. 15.11 «Обновление ядра».

5.6. Проблемы при установке системы

Если в системе не произошла настройка какого-либо компонента после стадии установки пакетов, доведите установку до конца, загрузитесь в систему и попытайтесь повторить настройку.

6. НАЧАЛО ИСПОЛЬЗОВАНИЯ ОС АЛЪТ СП

6.1. Использование кабеля RS232 (COM) для подключения к консоли

ПНС вычислительного комплекса Эльбрус является командно-строчной, что позволяет управлять ей через последовательный порт (порт RS232). Этот вариант подключения имеет ряд преимуществ – вывод диагностики начинается практически мгновенно после включения машины, ввод буферизуется (пробельный символ для перехода в меню можно отправить заранее, не дожидаясь подсказки), на принимающей стороне могут быть доступны средства копирования/вставки.

В случае терминала, подключенного к последовательному порту, ввод и вывод производится через оба имеющихся последовательных порта в полудуплексном режиме.

Для организации подключения используется кабель USB-COM «гнездо» («мама»), либо COM-COM («мама»/«мама»).

Примечание. При использовании кабеля COM-COM возможна ситуация, когда «общаться» начнут два экземпляра ПНС или, например, `agetty` – что может привести к неожиданным результатам; поэтому и предпочтителен асимметричный вариант USB-COM (ведомый компьютер – COM порт, ведущий – USB).

В качестве эмулятора последовательного терминала можно применять графические программы (`cutescom`), текстовые (`minicom`) или командно-строчные (`cu`, `miniterm.py`).

Параметры последовательного порта (115200 8N1):

- скорость – 115200 бит/сек;
- кадр – 8 бит;
- четность – нет;
- стоп-бит – 1;
- регулировка потока – нет.

Подключение к консоли на примере входящего в дистрибутив пакета `python-module-serial` и кабеля USB-COM:

```
miniterm.py /dev/ttyUSB0 115200
```

либо по кабелю COM-COM с применением команды `cu` из пакета `uusr`:

```
cu -l /dev/ttyS0 -s 115200
```

Далее можно вводить данные, которые хотите отправить в порт. Приходящие в порт данные от внешних устройств также будут выводиться.

Примечание. ПНС ожидает конец строки в форме «CR+LF», загруженная система – «LF». Может понадобиться соответственно настроить терминальную программу, либо передать дополнительные аргументы (в случае `miniterm.py` это может быть `--lf` или `--eol LF`).

6.2. Запуск ОС

После включения ВК «Эльбрус» происходит инициализация программы начального старта.

Загрузка ОС начинается автоматически после небольшого времени ожидания (обычно несколько секунд).

```
Autoboot in xx sec, PRESS SPACE TO DISABLE IT
```

Загрузка ОС может занять некоторое время, в зависимости от производительности компьютера. Основные этапы загрузки ОС – загрузка ядра, подключение (монтирование) файловых систем, запуск системных служб – периодически могут дополняться проверкой файловых систем на наличие ошибок. В этом случае время ожидания может занять больше времени, чем обычно.

Основной задачей программы начальной загрузки является загрузка ОС. Загрузку можно произвести по одной из четырех схем:

- 1) дождаться конца таймера обратного отсчета. В этом случае будет произведена загрузка заранее выбранной программы, с параметрами, хранящимися в энергонезависимой памяти либо в файле `boot.conf` (при его наличии) (метка, указанная как `default`;). Приоритетом обладает загрузка по параметрам, указанным в файле `boot.conf`. В этом случае из энергонезависимой памяти берется только значение номера устройства загрузки;
- 2) прервать таймер обратного отсчета и нажать клавишу `<s>`. В этом случае загрузка произойдет по параметрам, взятым из энергонезависимой памяти. Содержимое файла `a` приниматься в расчет не будет;

- 3) прервать таймер обратного отсчета и, нажав клавишу <c>, изменить параметры, взятые из энергонезависимой памяти. Потом, нажав клавишу <s>, загрузить программу;
- 4) прервать таймер обратного отсчета и, войдя в диалог загрузки с использованием конфигурационного файла `boot.conf` (b основного режима или #boot расширенного), загрузить одну из меток файла `boot.conf`.

П р и м е ч а н и е . Подробнее о работе с программой начального старта можно узнать из штатной документации ВК «Эльбрус».

6.3. Вход в систему

6.3.1. Идентификация и аутентификация в графической оболочке MATE

Стандартная установка ОС Альт СП Рабочая станция включает графическую оболочку MATE, которая состоит из набора различных программ и технологий, используемых для управления ОС и предоставляющих пользователю графический интерфейс для работы в виде оконных менеджеров.

При загрузке в графическом режиме работа загрузчика ОС заканчивается переходом к окну входа в систему (рис. 29).

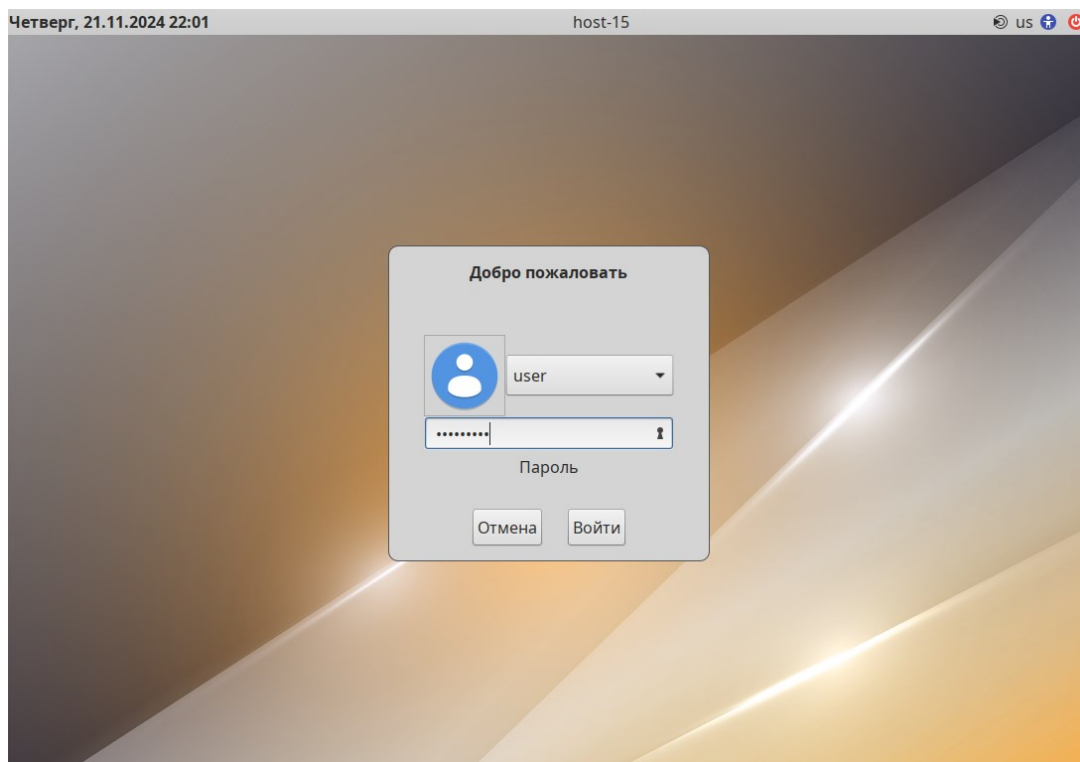


Рис. 29 – Окно входа в систему

Для продолжения работы и входа в ОС Альт СП в графическом режиме нужно выбрать одну из учетных записей, предлагаемых в окне аутентификации. Далее ввести пароль текущей учетной записи и нажать на кнопку «Войти».

Для выбора учетной записи, не показанной в списке выбора, нужно раскрыть выпадающий список со значением логина текущей учетной записи и выбрать пункт «Другие...» (рис. 30).

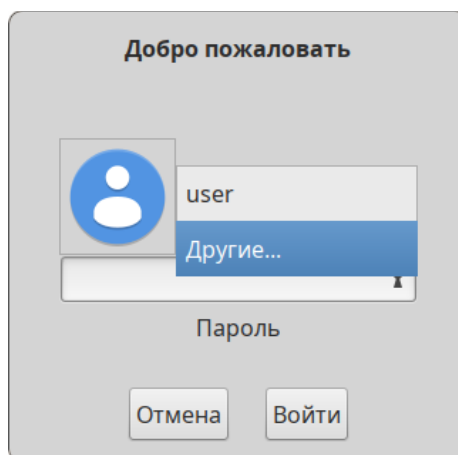


Рис. 30 – Выбор пользователя

После этого откроется окно ввода логина учетной записи (рис. 31), в котором нужно ввести логин учетной записи, и нажать кнопку «Войти». В следующем окне нужно ввести пароль учетной записи, и нажать кнопку «Войти».

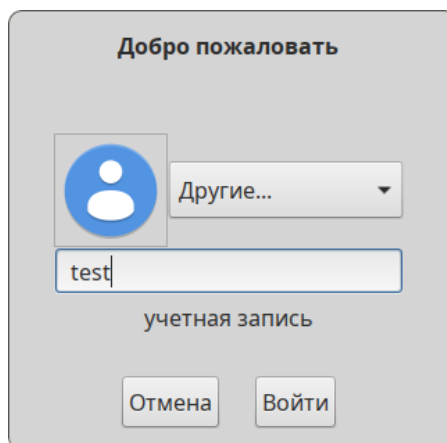


Рис. 31 – Ввод имени учетной записи

Чтобы запустить виртуальную клавиатуру на странице входа, следует нажать клавишу <F3> или щелкнуть на значок  на верхней панели, а затем отметить пункт «Экранная клавиатура» (рис. 32).

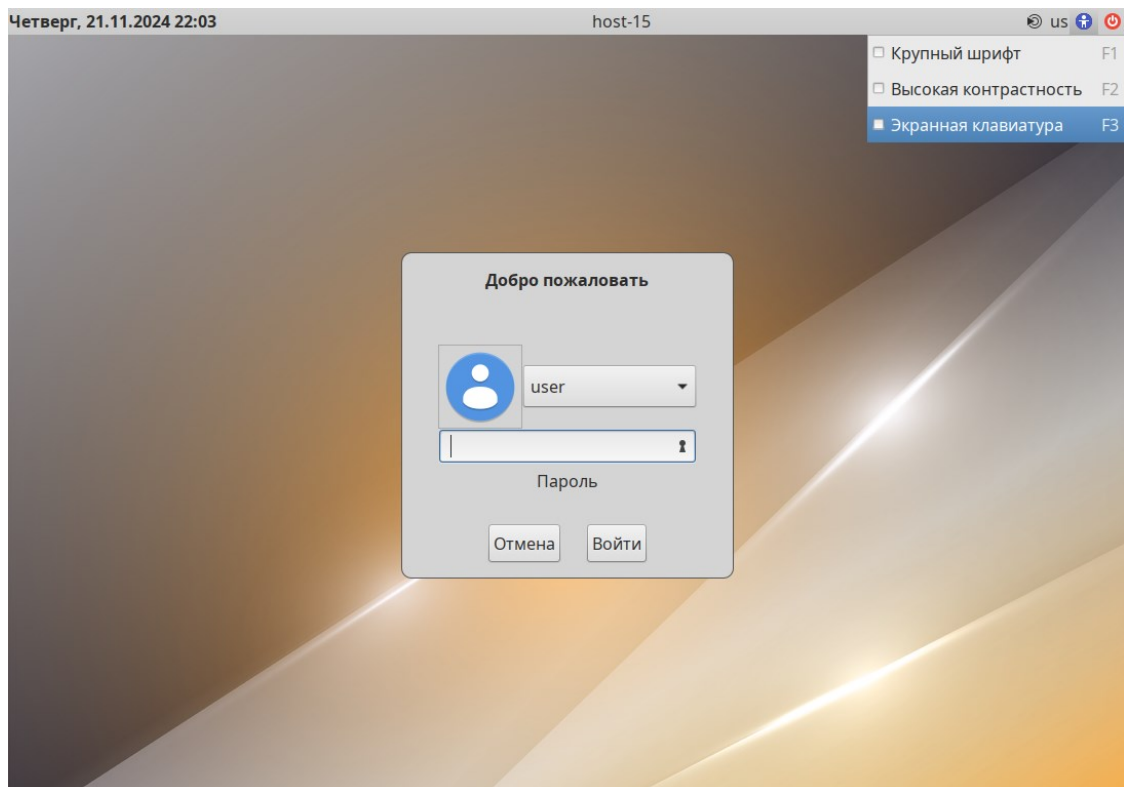


Рис. 32 – Страница входа в систему

На экране появится виртуальная клавиатура, ее можно использовать для ввода имени пользователя и пароля (рис. 33).

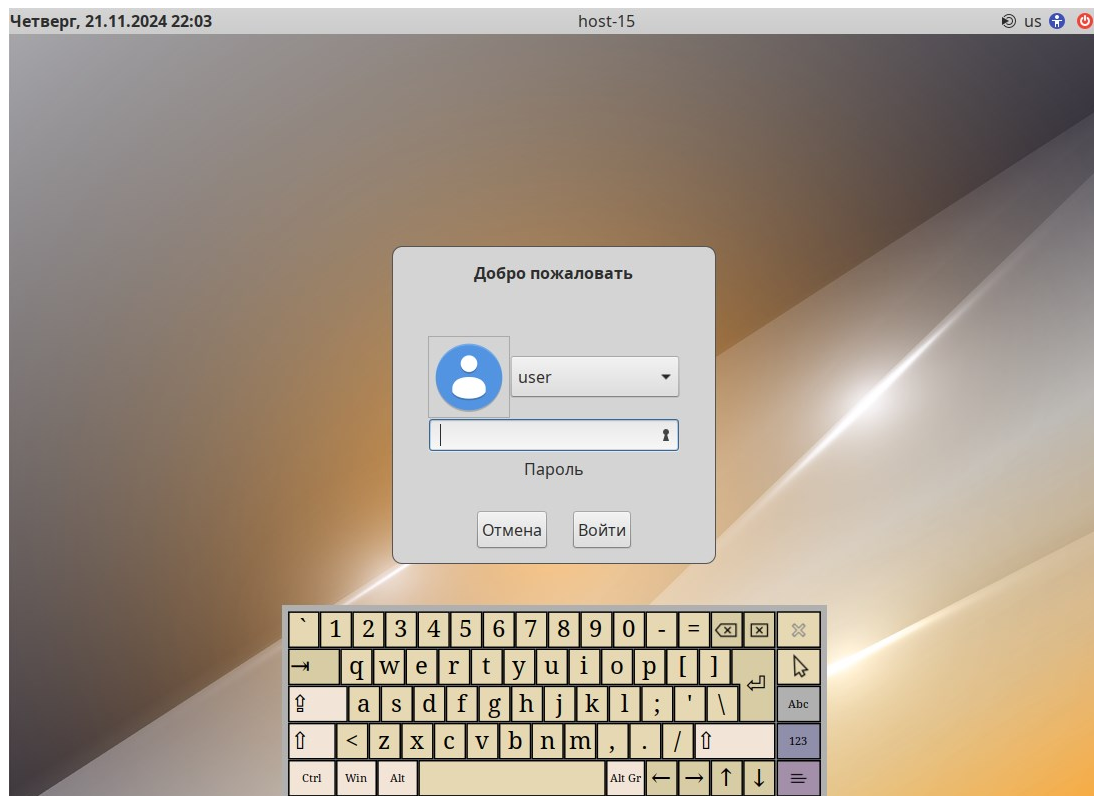


Рис. 33 – Виртуальная клавиатура при входе в систему

В результате успешного прохождения процедуры аутентификации и входа в систему запустится графическая оболочка ОС Альт СП (рис. 34).

Примечание. Работа в системе с использованием учетной записи администратора небезопасна, вследствие этого вход в систему в графическом режиме для администратора (root) запрещен. Попытка зарегистрироваться в системе будет прервана сообщением об ошибке.

В случае если графическая оболочка MATE была включена в состав ОС при установке, однако не стартовала автоматически, ее допускается вызвать вручную из консоли с помощью следующих команд:

```
~/ .xinitrc  
exec mate-session
```

Далее нужно использовать команду `startx` для запуска MATE.

Подробнее о пользовательских приложениях для ОС Альт СП Рабочая станция и рабочем столе MATE приведено в документе «Руководство пользователя. ЛКНВ.11102-01 91 01».

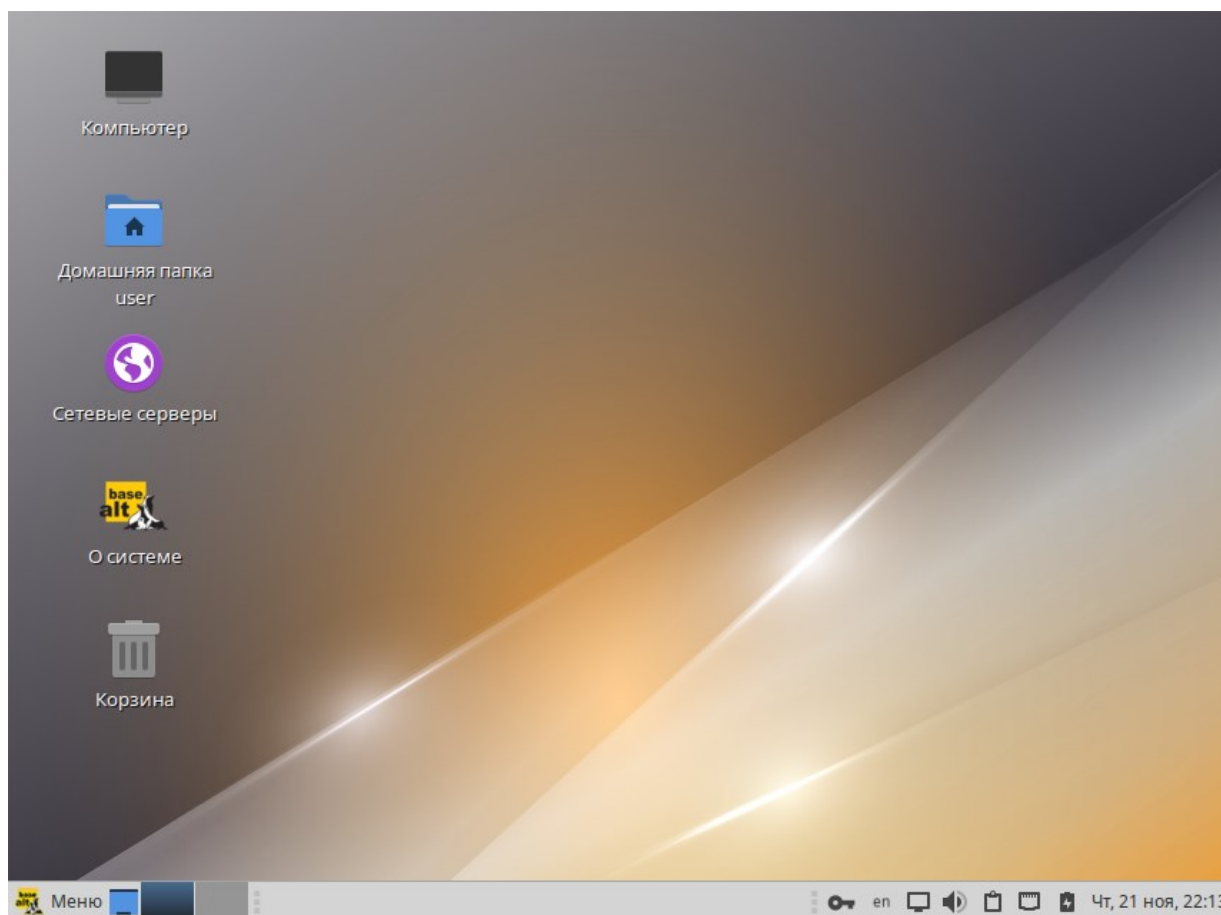


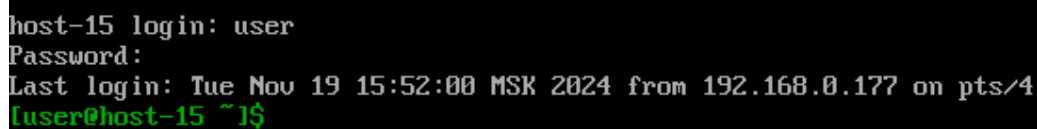
Рис. 34 – Рабочий стол MATE

6.3.2. Идентификация и аутентификация в консольном режиме

При загрузке в консольном режиме работа загрузчика завершается запросом на ввод логина и пароля учетной записи. В случае необходимости перехода на другую консоль нажмите клавиши <Ctrl>+<Alt>+<F2>.

Для продолжения работы в консольном режиме нужно ввести логин учетной записи пользователя и подтвердить его нажатием клавиши <Enter>. Затем ввести пароль и подтвердить его аналогичным образом.

В случае успешного прохождения процедуры аутентификации и входа в систему ОС перейдет к штатному режиму работы и предоставит дальнейший доступ к консоли (рис. 35).



```
host-15 login: user
Password:
Last login: Tue Nov 19 15:52:00 MSK 2024 from 192.168.0.177 on pts/4
[user@host-15 ~]$
```

Рис. 35 – Приглашение для ввода команд

6.3.3. Виртуальная консоль

В процессе работы ОС Альт СП активно несколько виртуальных консолей. Каждая виртуальная консоль доступна по одновременному нажатию клавиш <Ctrl>, <Alt> и функциональной клавиши с номером этой консоли от <F1> до <F6>.

На первых шести виртуальных консолях (от <Ctrl>+<Alt>+<F1> до <Ctrl>+<Alt>+<F6>) пользователь может зарегистрироваться и работать в текстовом режиме. Если была установлена графическая оболочка MATE, она будет загружаться в первой виртуальной консоли.

Двенадцатая виртуальная консоль (<Ctrl>+<Alt>+<F12>) выполняет функцию системной консоли – на нее выводятся сообщения о происходящих в системе событиях.

6.4. Блокирование сеанса доступа

6.4.1. Блокирование сеанса доступа после установленного времени бездействия (неактивности) пользователя или по его запросу

После авторизации и загрузки графической рабочей среды МАТЕ, пользователю предоставляется рабочий стол для работы с графическими приложениями.

Для безопасности данных компьютера и, чтобы другие пользователи не могли получить доступ к работающим приложениям, блокируйте свой экран, даже если оставляете компьютер на короткое время.

Заблокировать сеанс доступа можно по запросу пользователя: панель инструментов МАТЕ «Меню» → «Система» → «Заблокировать экран», или вызвать клавишами <Ctrl>+<Alt>+<L>.

При работе в графическом режиме блокирование сеанса доступа также происходит после установленного времени бездействия (по умолчанию 5 минут) посредством срабатывания программы – хранителя экрана (screensaver).

Время бездействия системы устанавливается: панель инструментов МАТЕ «Меню» → «Приложения» → «Параметры» → «Хранитель экрана».

При разблокировке экрана появляется виртуальная клавиатура (рис. 36), ее можно использовать для ввода пароля.

Для разблокировки требуется ввести пароль пользователя и нажать на кнопку «Разблокировать».

П р и м е ч а н и е . Если виртуальная клавиатура при разблокировке экрана не нужна, можно удалить пакет mate-screensaver-screenkeyboard.

При заблокированном экране другие пользователи могут входить в систему под своими учетными записями, нажав на экране ввода пароля кнопку «Переключить пользователя».

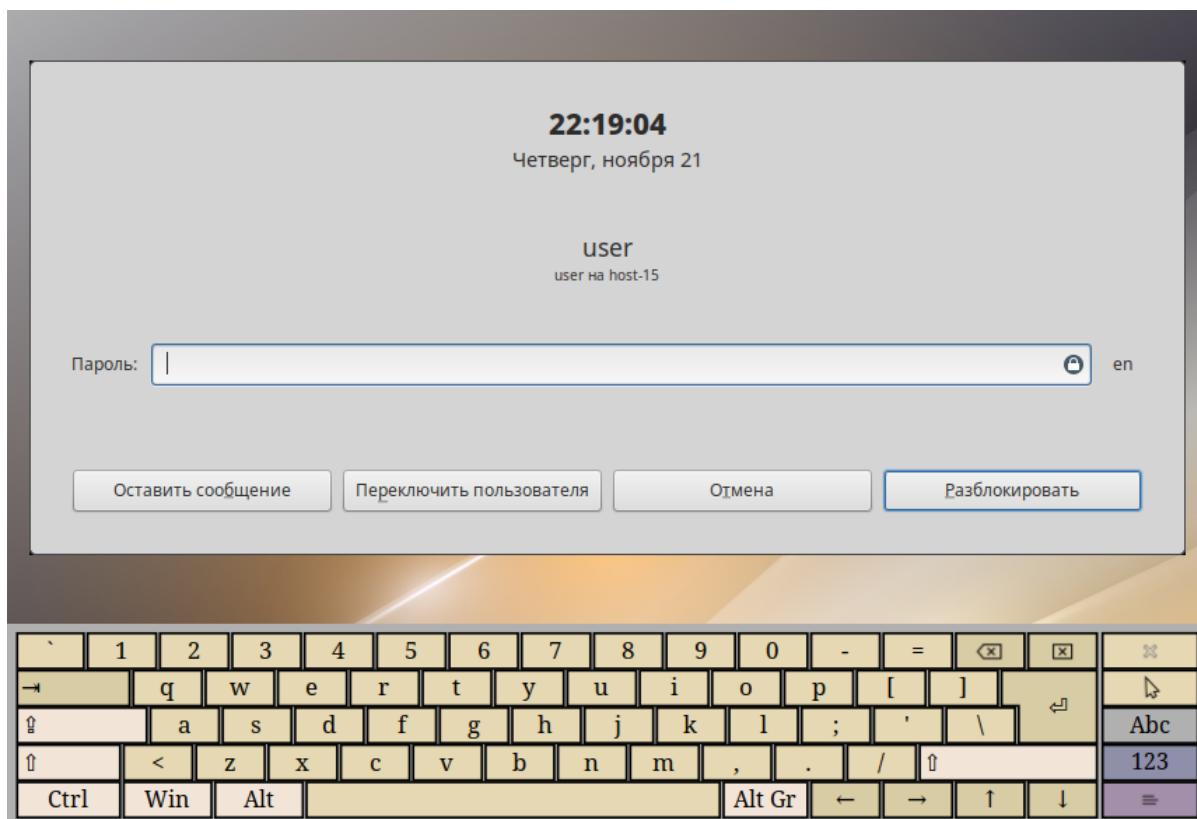


Рис. 36 – Разблокирование сеанса доступа

6.4.2. Блокировка виртуальных текстовых консолей

Программа `vlock` позволяет заблокировать сеанс при работе в консоли.

Выполнение команды `vlock` без дополнительных параметров заблокирует текущий сеанс виртуальной консоли, без прерывания доступа других пользователей:

```
$ vlock
```

Блокировка `tty2` установлена `user`.

Используйте `Alt`-функциональные клавиши для перехода в другие виртуальные консоли.

Пароль:

Чтобы предотвратить доступ ко всем виртуальным консолям машины, следует выполнить команду:

```
$ vlock -a
```

Теперь вывод на консоль полностью заблокирован `user`.

Пароль:

В этом случае `vlock` блокирует текущую активную консоль, а параметр `-a` предотвращает переключение в другие виртуальные консоли.

Примечание. Для разблокировки консоли необходимо ввести пароль пользователя.

6.4.3. Настройка блокировки возможности пользователя изменять настройки блокировки системы

Для блокировки возможности пользователя изменять настройки блокировки системы нужно выполнить следующие действия:

- 1) должен быть создан файл `/etc/dconf/profile/user` со следующим содержимым:

```
user-db:user
system-db:local
```

- 2) создать каталоги `/etc/dconf/db/local.d/` и `/etc/dconf/db/local.d/locks` (если их еще не существует):

```
# mkdir /etc/dconf/db/local.d/
# mkdir /etc/dconf/db/local.d/locks
```

- 3) создать файл `/etc/dconf/db/local.d/screensaver`, в который поместить текст:

```
[org/mate/screensaver]
idle-activation-enabled=true
lock-enabled=true
```

- 4) в файле `/etc/dconf/db/local.d/session` установить время бездействия в минутах:

```
[org/mate/session]
idle-delay=2
```

- 5) запретить пользователям изменять время бездействия, режим для этого создать файл `/etc/dconf/db/local.d/locks/00-screensaver` со следующим содержимым:

```
#prevent users from changing screensaver
/org/mate/screensaver/mode
/org/mate/desktop/session/idle-delay
```

- 6) выполнить обновление:

```
# dconf update
```

6.5. Завершение сеанса пользователя

6.5.1. Графический режим

Для завершения сеанса пользователя в графическом режиме следует выбрать на панели инструментов МАТЕ «Меню» → «Система» → «Завершить сеанс».

Далее откроется окно (рис. 37), в котором предоставляется выбор дальнейших действий:

- переключить пользователя – сеанс пользователя в графическом режиме блокируется, другой пользователь может войти в систему под своим именем;
- завершить сеанс – выполняется завершение сеанса пользователя в графическом режиме.

Если не производить никаких действий, то сеанс пользователя будет автоматически завершён через 1 минуту.

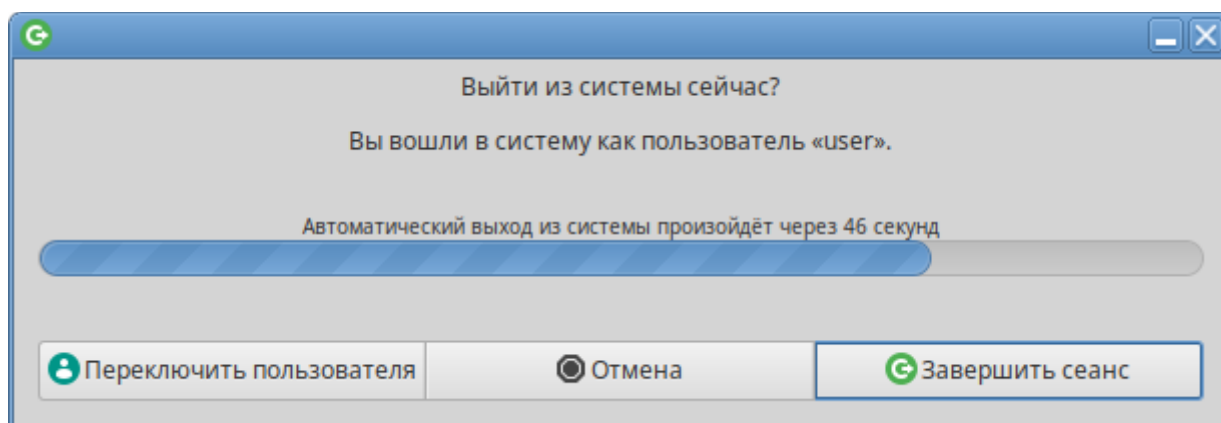


Рис. 37 – Окно выхода из системы

Примечание. Завершение сеанса произойдет до блокировки экрана, если установить время до завершения сеанса меньше, чем время, указанное для блокировки экрана (см. п. 6.4.3).

6.5.2. Консольный режим

Завершить сеанс пользователя в консольном режиме можно, выполнив команду `exit`.

6.5.3. Настройки завершения сеанса пользователя

Для каждого пользователя можно настроить автоматическое завершение сеанса после установленного времени бездействия (неактивности) пользователя.

Действия выполняются от администратора (root).

Для графического сеанса пользователя нужно создать файл `/etc/logout`, в который поместить допустимое время простоя (в секундах) для каждого пользователя, например:

```
user1 300  
user2 200
```

Формат файла `/etc/logout`:

<user> <время в секундах от момента последнего действия>

Для консольного режима добавить в конце файла `/home/пользователь/.bash_profile` строку с указанием допустимого времени простоя (в секундах):

```
TMOUT=300
```

Примечание. Для применения настроек необходимо перезагрузить ОС.

6.6. Выключение/перезагрузка компьютера

Для корректного завершения работы ОС (перезагрузки) во время ее работы запрещается выключать питание компьютера или перезагружать компьютер нажатием на кнопку «Reset», так как для корректного завершения работы требуется размонтирование файловой системы.

Перед окончанием работы с ОС нужно завершить все работающие программы.

6.6.1. Графический режим

Для выключения/перезагрузки компьютера следует выбрать на панели инструментов МАТЕ «Меню» → «Система» → «Выйти».

Далее откроется окно (рис. 38), в котором предоставляется выбор дальнейших действий:

- ждущий режим – компьютер переводится в режим экономии энергии;

- спящий режим – компьютер переводится в режим энергосбережения, позволяющий отключить питание компьютера, сохранив при этом текущее состояние ОС;
- перезагрузить – выполняется перезапуск ОС;
- выключить – выполняется выключение компьютера.

Если не производить никаких действий, то компьютер будет автоматически выключен через 1 минуту.

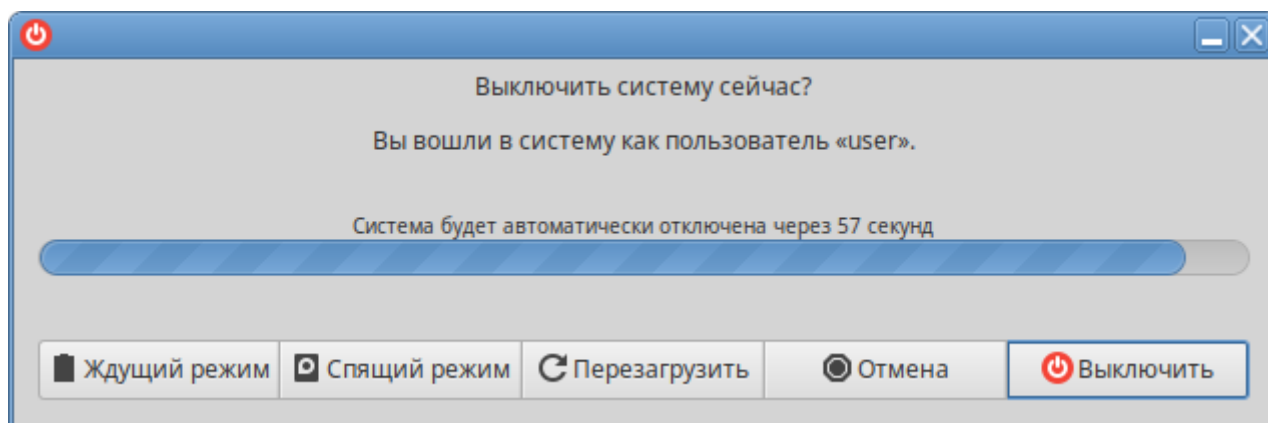


Рис. 38 – Окно выключения компьютера

6.6.2. Консольный режим

Перезагрузить систему в консольном режиме можно, выполнив команду:

```
$ systemctl reboot
```

Завершить работу и выключить компьютер (с отключением питания):

```
$ systemctl poweroff
```

Перевести систему в ждущий режим:

```
$ systemctl suspend
```

7. НАСТРОЙКИ СИСТЕМЫ

7.1. Центр управления системой

Для управления настройками установленной системы можно использовать ЦУС (также см. применение ЦУС в документе «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01»).

ЦУС состоит из нескольких независимых диалогов-модулей. Каждый модуль отвечает за настройку определенной функции или свойства системы. Модули настройки сгруппированы по задачам.

Список установленных модулей можно просмотреть, выполнив команду от администратора:

```
# alterator-standalone
```

ЦУС можно использовать для разных целей, например (в скобках указаны имена соответствующих модулей):

- просмотра системных журналов (logs) (п. 8.6.1);
- управления системными службами (services) (п. 8.6.2);
- конфигурирования сетевых интерфейсов (net-eth) (рис. 117);
- настройки межсетевого экрана (net-iptables) (п. 8.4.1);
- настройки ограничений на использование внешних носителей (usbguard) (см. Руководство по КСЗ);
- настройки ограничения доступа к файловой системе USB-устройства (usbmount) (см. Руководство по КСЗ);
- создания, удаления и редактирования учетных записей пользователей (users);
- изменения пароля администратора системы (root) (п. 8.6.6);
- настройки даты и времени (datetime) (п. 8.6.7);
- настройки ограничений выделяемых ресурсов памяти пользователям (квоты) (quota п. 8.6.9);
- конфигурирования групповых политик (grpupdate);
- управления выключением удаленного компьютера (ahttpd-power, доступно только в веб-интерфейсе).

Примечание. Соответствующие наименования пакетов ЦУС alterator-`<имя_модуля>`, например, alterator-net-eth.

Чтобы исключить возможность несанкционированного доступа к ЦУС, по окончании работы нужно завершить сеанс, нажав на кнопку «Выход».

7.1.1. Графический интерфейс

Графический интерфейс ЦУС можно запустить следующими способами:

- комбинацией клавиш `<ALT>+<F2>` открыть окно быстрого запуска приложений и ввести в поле название программы – асс;
- выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Администрирование» → «Центр управления системой»;
- при помощи консоли (приложение «Терминал»), в которой нужно ввести команду асс;
- зная имя модуля, запустить графический интерфейс для него, можно также выполнив команду:

```
$ alterator-standalone <имя-модуля>
```

Запуск ЦУС требует прав администратора – введите пароль root (рис. 39).

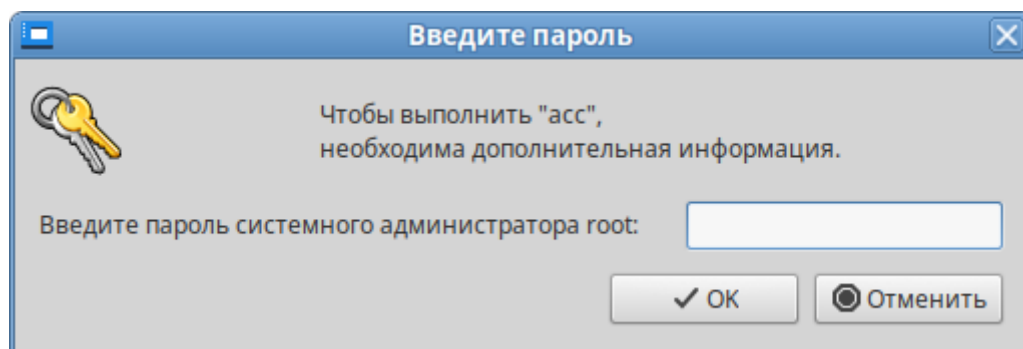


Рис. 39 – Запрос пароля для запуска «Центра управления системой»

После успешного входа откроется окно ЦУС (рис. 40).

Кнопка «Режим эксперта» (рис. 40) позволяет выбрать один из режимов:

- основной режим (кнопка отжата);
- режим эксперта (кнопка нажата).

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

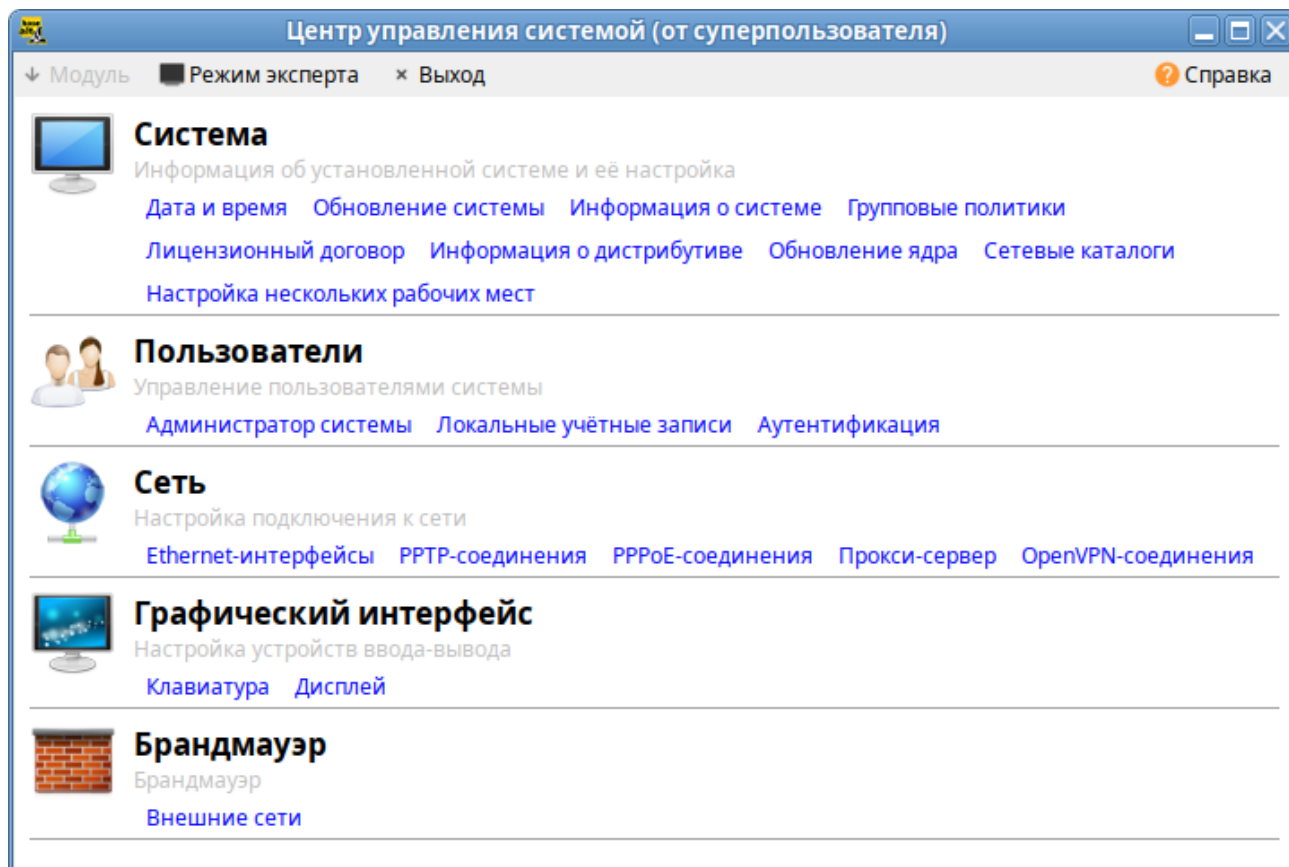


Рис. 40 – Окно «Центр управления системой»

7.1.2. Веб-интерфейс ЦУС

ЦУС имеет веб-ориентированный интерфейс, позволяющий управлять системой с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет `alterator-fbi`:

```
# apt-get install alterator-fbi
```

Должны быть запущены сервисы `ahttpd` и `alteratord`:

```
# systemctl enable --now ahttpd
```

```
# systemctl enable --now alteratord
```

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы нужно перейти по адресу `https://localhost:8080/` или `https://IP-адрес:8080/`.

IP-адрес можно узнать, выполнив команду:

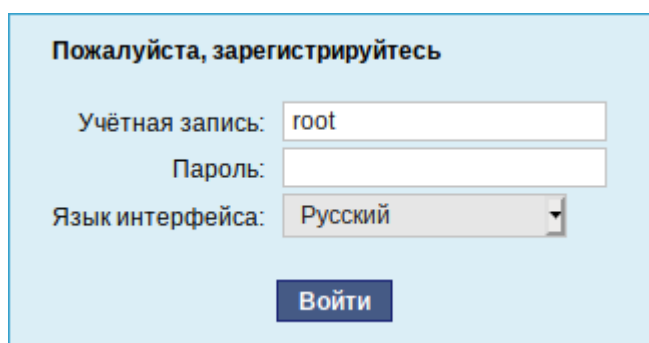
```
$ ip addr
```

П р и м е ч а н и е . IP-адрес будет указан после слова `inet`:

```
inet 192.168.0.147/24 brd 192.168.0.255 scope global eth0
```

где 192.168.0.147 – IP-адрес.

Для начала работы с ЦУС нужно зарегистрироваться. Запуск ЦУС требует прав администратора (ввести пароль `root`) (рис. 41). Дополнительно на этапе регистрации можно выбрать язык интерфейса. По умолчанию предлагается язык, определенный настройками веб-браузера.



Пожалуйста, зарегистрируйтесь

Учётная запись:

Пароль:

Язык интерфейса:

Рис. 41 – Запрос пароля администратора для запуска веб-интерфейса ЦУС

После успешного входа будут доступны все возможности ЦУС (рис. 42) на той машине, к которой было произведено подключение через веб-интерфейс.

Веб-интерфейс ЦУС можно настроить (кнопка «Настройка»), выбрав один из режимов:

- основной режим;
- режим эксперта.

Выбор режима влияет на количество отображаемых модулей. В режиме эксперта отображаются все модули, а в основном режиме только наиболее используемые.

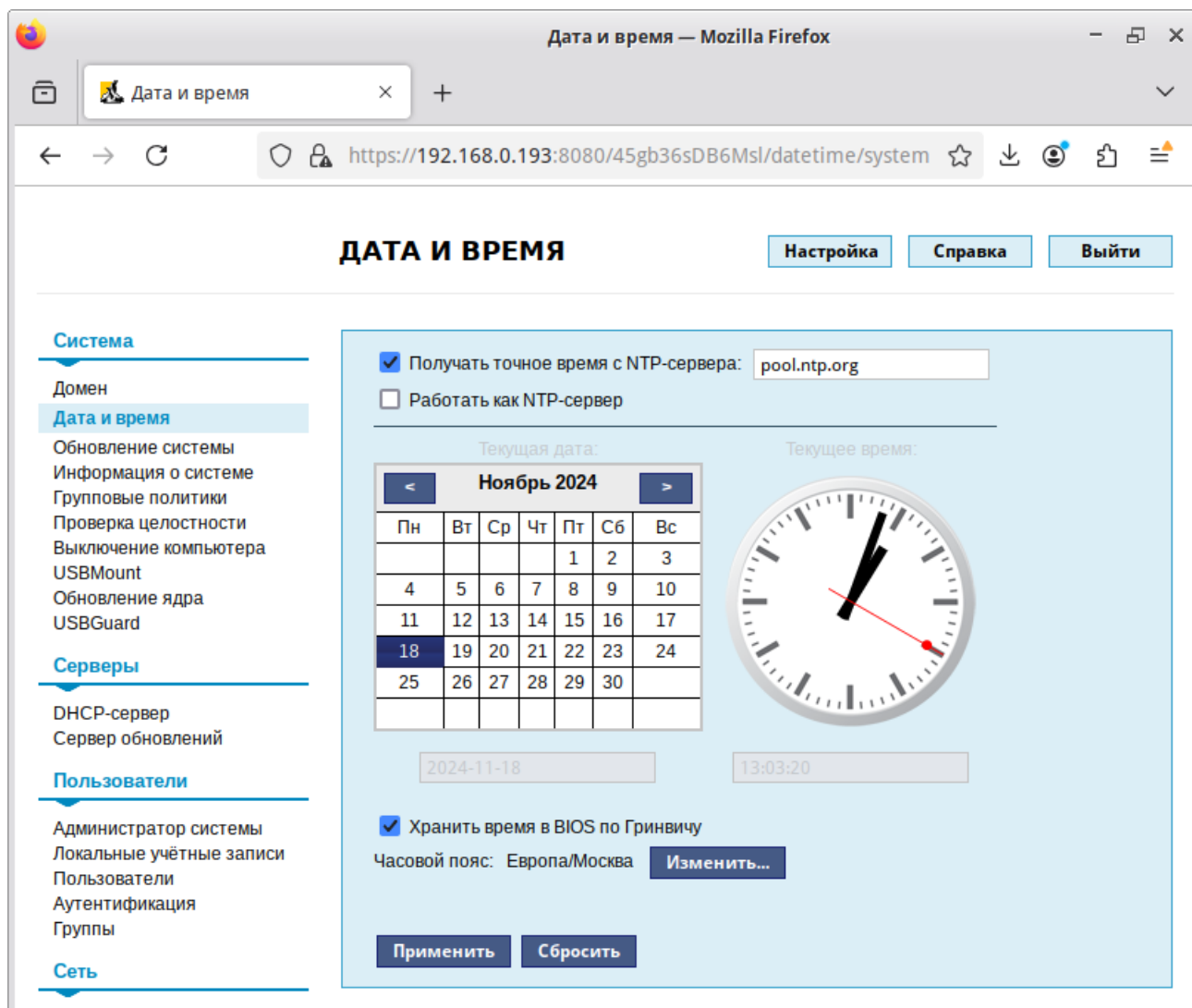


Рис. 42 – Окно веб-интерфейса «Центр управления системой»

ЦУС содержит справочную информацию по модулю, которую можно прочитать, нажав на кнопку «Справка» (см. п. 7.1.5).

⚠ После работы с ЦУС, в целях безопасности, не следует оставлять открытым веб-браузер. Необходимо обязательно выйти из сеанса работы с ЦУС, нажав на кнопку «Выйти».

7.1.3. Установка и удаление модулей ЦУС

Состав модулей, предоставляющих различные возможности для настройки системы в веб-интерфейсе, можно изменять.

Установленные пакеты, которые относятся к ЦУС, можно просмотреть, выполнив команду:

```
# rpm -qa | grep alterator
```

Для поиска прочих пакетов ЦУС выполните команду:

```
# apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
```

```
# apt-get remove alterator-net-openvpn
```

Примечание. После установки модуля, у которого есть веб-интерфейс, для того чтобы он отобразился в веб-интерфейсе, необходимо перезапустить службу ahttpd:

```
# systemctl restart ahttpd
```

7.1.4. Права доступа к модулям ЦУС

Администратор имеет доступ ко всем модулям, установленным в системе, и может назначать права доступа для пользователей к определенным модулям.

Для разрешения доступа пользователю к конкретному модулю, администратору в веб-интерфейсе ЦУС нужно выбрать нужный модуль и нажать ссылку «Параметры доступа к модулю», расположенную в нижней части окна модуля (рис. 43).

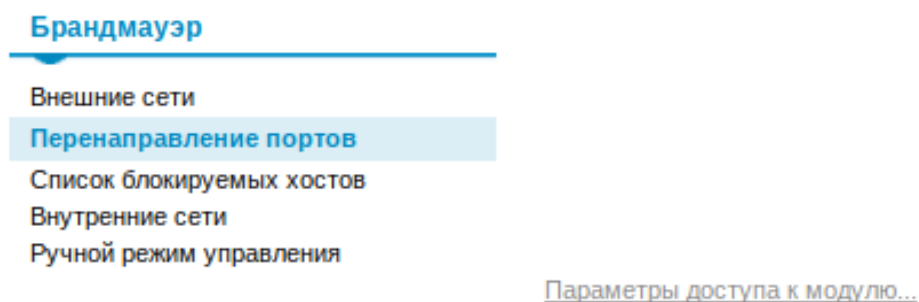
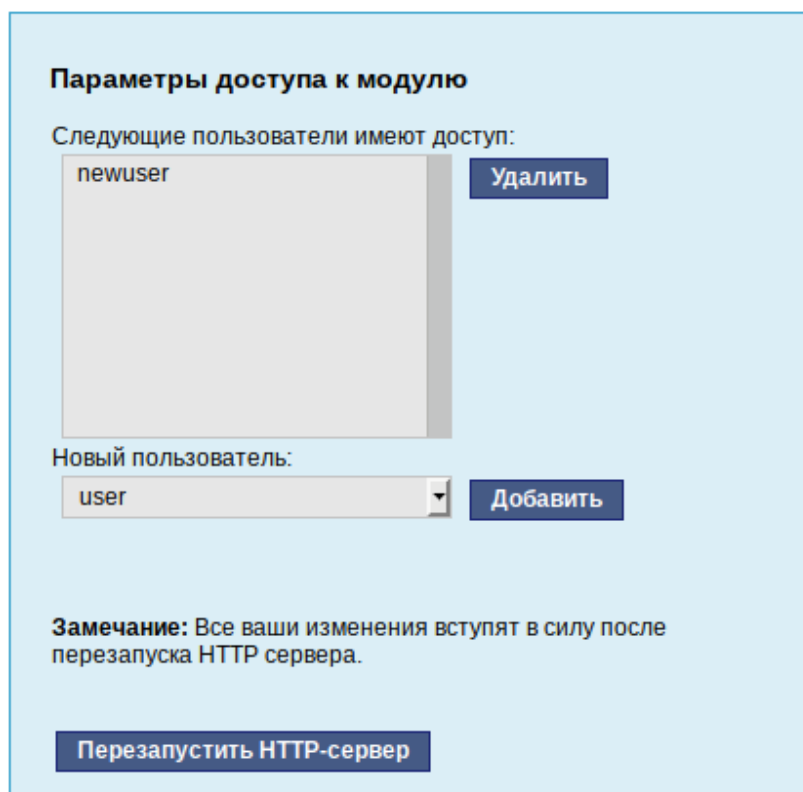


Рис. 43 – Ссылка «Параметры доступа к модулю»

В открывшемся окне, в списке «Новый пользователь», нужно выбрать пользователя, который получит доступ к данному модулю, и нажать на кнопку «Добавить». Для сохранения настроек нужно перезапустить НТТР-сервер, для этого достаточно нажать на кнопку «Перезапустить НТТР-сервер» (рис. 44).

Для удаления доступа пользователя к определенному модулю, администратору, в окне этого модуля нужно нажать ссылку «Параметры доступа к модулю», в открывшемся окне в списке пользователей, которым разрешен доступ, выбрать пользователя, нажать на кнопку «Удалить» (рис. 44) и нажать на кнопку «Перезапустить HTTP-сервер».



Параметры доступа к модулю

Следующие пользователи имеют доступ:

newuser	Удалить

Новый пользователь:

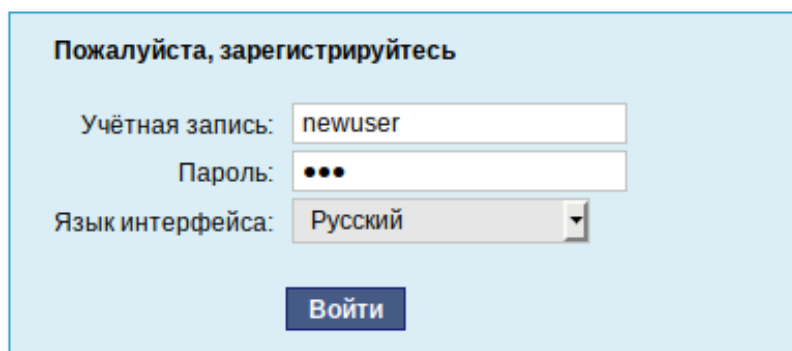
user	Добавить

Замечание: Все ваши изменения вступят в силу после перезапуска HTTP сервера.

Перезапустить HTTP-сервер

Рис. 44 – Параметры доступа к модулю

Системный пользователь, пройдя процедуру аутентификации (рис. 45), может просматривать и вызывать модули, к которым он имеет доступ (рис. 46).



Пожалуйста, зарегистрируйтесь

Учётная запись: newuser

Пароль: ●●●

Язык интерфейса: Русский

Войти

Рис. 45 – Запрос пароля учетной записи пользователя для запуска веб-интерфейса ЦУС

Настройка Справка Выйти

Система

Дата и время

Серверы

DHCP-сервер

Сеть

Ethernet-интерфейсы

Общие настройки

Версия IP: IPv4

☐ Включить службу DHCP

Интерфейс: enp0s3 (192.168.0.1 - 192.168.0.254)

(максимально допустимый диапазон адресов)

Начальный IP адрес:

Конечный IP адрес:

Срок действия адреса: 1 час

Информация, предоставляемая клиентам

DNS-сервер:

Домен поиска:

Шлюз по умолчанию:

Применить Сбросить

Рис. 46 – Веб-интерфейс ЦУС, запущенный от системного пользователя

7.1.5. Получение справочной информации

Модули ЦУС содержат встроенную справку (рис. 47), поясняющую назначение конкретного модуля. Справка вызывается кнопкой «Справка».

Настройка Справка Выйти

Ethernet-интерфейсы

IP (Internet Protocol) — основа стека протоколов TCP/IP. **IP-адрес и Маска сети** — обязательные параметры каждого узла IP-сети. Первый параметр — уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то не забудьте про параметр **Шлюз по умолчанию**.

В случае наличия *DHCP-сервера* можно все вышеперечисленные параметры получить автоматически — просто включите **Использовать DHCP**.

Если в компьютере имеется несколько сетевых карт, то возможна ситуация, когда при очередной загрузке ядро присвоит имена интерфейсов (eth0, eth1) в другом порядке. В результате интерфейсы получат не свои настройки. Чтобы этого не происходило, вы можете привязать интерфейс к имени по его аппаратному адресу (MAC) или по местоположению на системной шине.

Общие сетевые настройки

Существует ряд общих сетевых параметров, не привязанных к какому либо конкретному интерфейсу.

Имя компьютера — имя машины в локальной сети. Имя компьютера, в отличие от традиционного имени хоста в Unix (hostname), не содержит названия сетевого домена.

Рис. 47 – Получение справочной информации о модуле ЦУС

7.2. Выбор программ, запускаемых автоматически при входе в систему

Для более удобной работы с системой можно выбрать определенные программы, которые будут запущены автоматически при входе пользователя в систему. Автозапускаемые программы автоматически сохраняют свое состояние и безопасно завершаются сеансовым менеджером при выходе из системы и перезапускаются при входе.

Инструмент настройки сессии позволяет настроить, какие программы будут автоматически запущены при входе в систему. Для запуска инструмента настройки сессии, выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Параметры» → «Запускаемые приложения».

7.2.1. Вкладка автоматического запуска программ

Список автоматически запускаемых программ представлен на вкладке «Автоматически запускаемые программы» (рис. 48). Этот список содержит краткое описание каждой программы и отметку, указывающую запускать программу или нет.

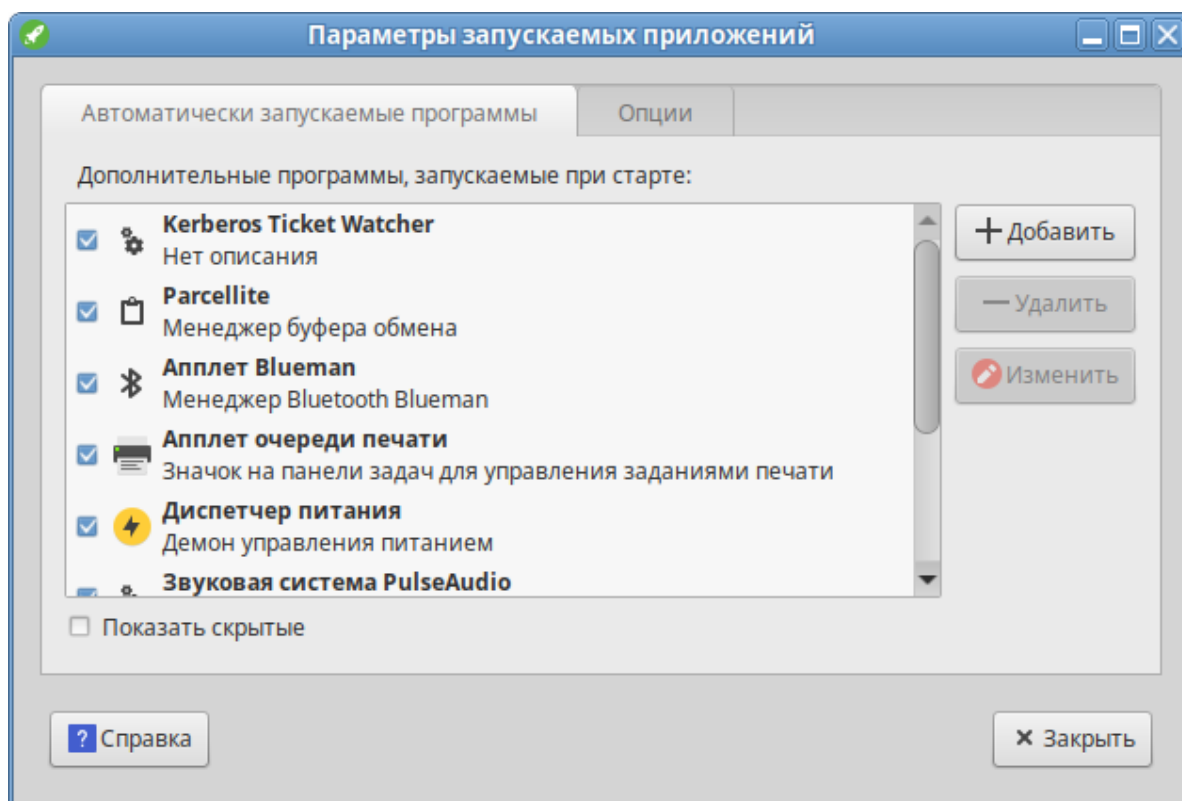


Рис. 48 – Автоматически запускаемые программы

На этой вкладке можно добавлять, удалять и изменять автозапускаемые приложения.

Для добавления новой автоматически запускаемой программы, следует выполнить следующие шаги:

- нажать на кнопку «Добавить». Откроется окно «Новая автоматически запускаемая программа»;
- указать имя программы и команду, которая запустит приложение (рис. 49);
- нажать на кнопку «Добавить».

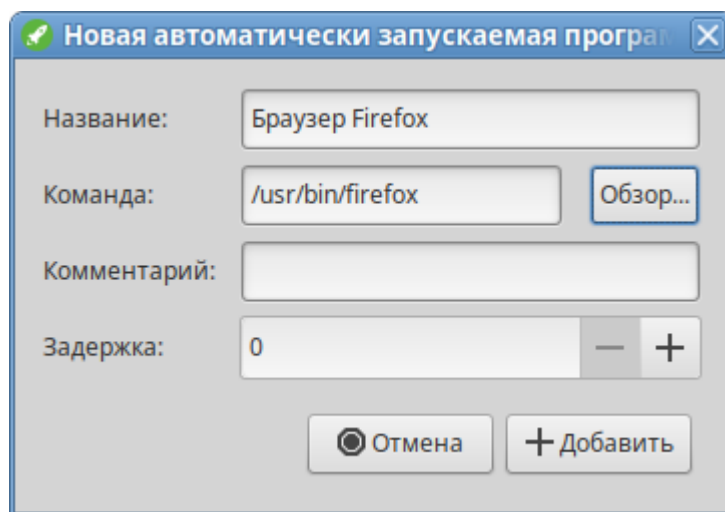


Рис. 49 – Добавление автоматически запускаемой программы

7.2.2. Вкладка настроек сессии

Менеджер сеанса может запомнить, какие приложения были запущены при выходе из системы, и автоматически запустить их при входе в систему. Для того чтобы это происходило каждый раз при выходе из системы, следует на вкладке «Опции» отметить пункт «Автоматически запоминать запущенные приложения при выходе из сеанса» (рис. 50).

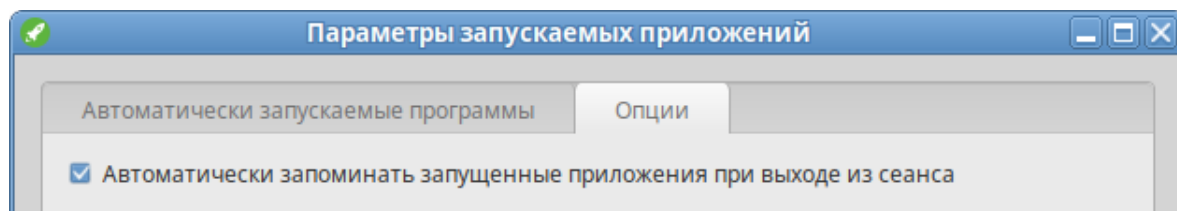


Рис. 50 – Запоминать запущенные приложения при выходе из сеанса

7.3. Режим киоск по ограничению запуска программ

В режиме киоск пользователь имеет право запускать программы только явно разрешенные администратором.

7.3.1. Настройка ограничения в ЦУС

Примечание. Для работы киоска должны быть установлены пакеты `alterator-kiosk` и `kiosk-mate-profiles`:

```
# apt-get install alterator-kiosk kiosk-mate-profiles
```

Для включения режима киоск необходимо в ЦУС перейти в раздел «Система» → «Настройка kiosk».

Для разрешения запуска определенных приложений, необходимо выбрать соответствующий профиль из списка «Профили», установить отметку в поле «Включен» (рис. 51).

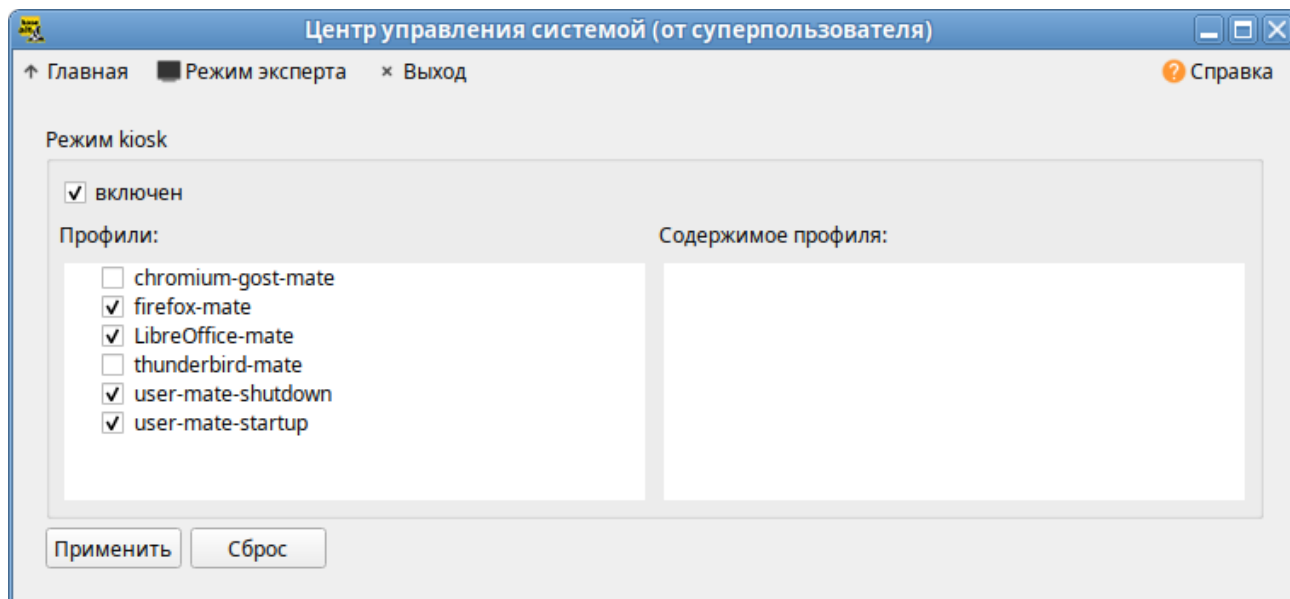


Рис. 51 – Настройка kiosk

Режим киоск будет применен после нажатия кнопки «Применить».

Список приложений, из которых состоит профиль, можно увидеть в окне «Содержимое профиля» (профиль выделяется щелчком любой кнопки мыши).

Примечание. Для создания нового профиля необходимо создать новый файл в каталоге `/etc/alterator/kiosk/profiles/` и вписать в него разрешенные к запуску программы. Например, для создания профиля `atril`, достаточно в файл `/etc/alterator/kiosk/profiles/` добавить строку:

```
U /usr/bin/atril
```

Для выключения режима киоск необходимо зарегистрироваться в системе под пользователем root (например, на второй консоли <Ctrl>+<Alt>+<F2>), выполнить команду:

```
# echo "0" > /etc/alterator/kiosk/mode
```

и перезагрузить систему.

7.3.2. Управление режимом киоск в консоли

Для управления режимом киоск, можно воспользоваться командой `kiosk`. Все команды выполняются с правами администратора.

Примечание. Утилита `kiosk` используется для временного включения/отключения режима киоск. После перезагрузки компьютера будет включен тот режим, который был установлен в модуле ЦУС «Настройка kiosk».

Примеры использования команды `kiosk`:

- просмотреть пути в белом списке:

```
# kiosk --user-list
/bin/basename
/bin/dbus-daemon
/bin/dbus-update-activation-environment
/bin/false
...
```

- добавить указанный путь в белый список:

```
# kiosk --user-list-append /путь
```

- удалить указанный путь из белого списка:

```
# kiosk --user-list-remove /путь
```

- активировать режим киоск:

```
# kiosk --set-mode 1
```

- деактивировать режим киоск:

```
# kiosk --set-mode 0
```

- просмотреть состояние режима:

```
# kiosk --get-mode
```

7.4. Задание хешей паролей

В ОС Альт СП реализована возможность хранения аутентификационной информации пользователей, полученной с использованием хеш-функций по ГОСТ Р 34.11–2012.

Примечание. Смена алгоритма хеширования происходит при изменении пароля пользователя, например, если истекает срок его действия, или пользователь сменил его. До этого момента алгоритм хеширования остается тем, с которым пароль был задан изначально. Поэтому, перед проверкой изменения алгоритма хеширования, измените пароль пользователя.

7.4.1. Смена алгоритма в консоли

Установить пакет tcb-hash-prefix-control:

```
# apt-get install tcb-hash-prefix-control
```

Список возможных хеш-функций можно вывести, выполнив команду:

```
# control tcb-hash-prefix help
bcrypt_2b: prefix=$2b$ count=8 (4 - 31 limit)
bcrypt_2y: prefix=$2y$ count=8 (4 - 31 limit)
bcrypt_2a: prefix=$2a$ count=8 (4 - 31 limit)
yescrypt: prefix=$y$ count=8 (0 - 11 limit)
scrypt: prefix=$7$ count=8 (0 - 11 limit)
gost_yescript: prefix=$gy$ count=8 (0 - 11 limit)
sha256: prefix=$5$ count=10000 (1000 - 100000 limit)
sha512: prefix=$6$ count=10000 (1000 - 100000 limit)
default: hash prefix managed by libcrypt
```

Просмотреть текущее значение хеш-функции:

```
# control tcb-hash-prefix
default
```

Изменить тип хеша по умолчанию на gost-yescript:

```
# control tcb-hash-prefix gost_yescript
```

Установить пароль пользователю:

```
# passwd user
```

Проверка:

```
# passwd -S user
Password set, gost-yescript encryption.
```

7.4.2. Смена алгоритма в ЦУС

Установить пакет alterator-secsetup:

```
# apt-get install alterator-secsetup
```

Для изменения типа хеша по умолчанию на ГОСТ Р 34.11–2012 необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности».

В открывшемся окне следует отметить пункт «Включить хеширование паролей пользователей по алгоритму ГОСТ Р 34.11-2012» и нажать кнопку «Применить» (рис. 52).

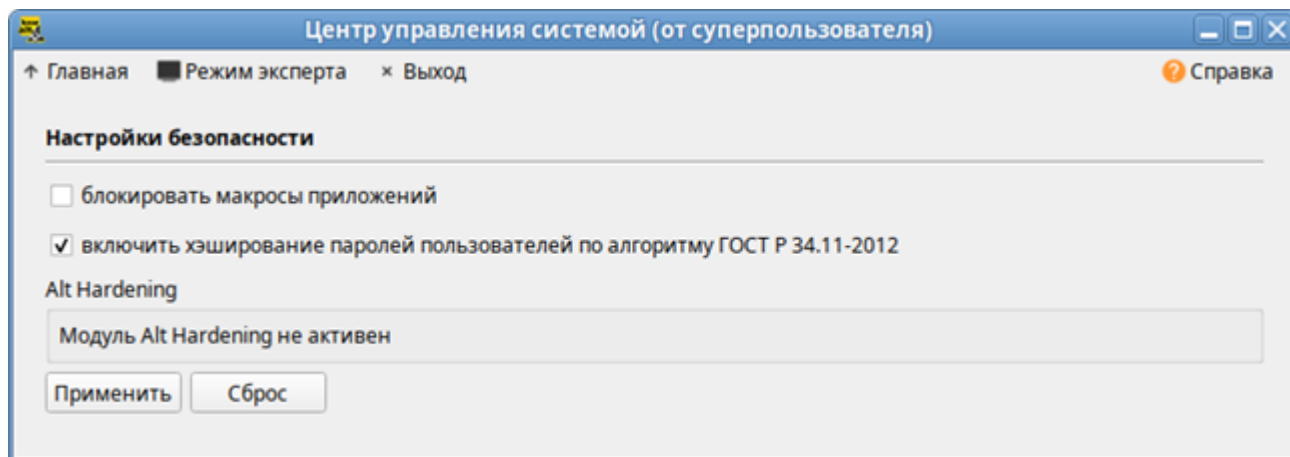


Рис. 52 – Задание хешей паролей в соответствии с ГОСТ Р 34.11–2012

Проверить настройку можно, установить пароль пользователю и выполнив команду:

```
# passwd user
# passwd -S user
Password set, gost-yescrypt encryption.
```

7.5. Настройка фильтрации пакетов с помощью утилиты iptables

Утилита iptables – стандартный интерфейс командной строки для управления фильтрацией сетевых пакетов и сбора статистики сетевого взаимодействия.

Утилита iptables позволяет фильтровать сетевые пакеты по следующим параметрам:

- на основе сетевых адресов отправителя и получателя (IP-адреса, MAC-адреса);
- по протоколам tcp, udp, icmp;
- с учетом входного и выходного сетевого интерфейса;
- на основе используемого порта;
- с учетом даты и времени.

Фильтры состоят из правил. Каждое правило – это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое нужно выполнить в случае удовлетворения критерия.

7.5.1. Устройство фильтра iptables

Для iptables в общем виде правила выглядят так:

```
iptables [-t table] command [match] [target/jump]
```

Если в правило не включается спецификатор `[-t table]`, то по умолчанию предполагается использование таблицы `filter`, если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы так же можно указывать в любом месте строки правила, однако для удобства чтения лучше указывать таблицу в начале правила.

Непосредственно за именем таблицы должна стоять команда управления фильтром. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables (вставить правило, добавить правило в конец цепочки, или удалить правило). Тело команды в общем виде выглядит так:

```
[команда] [цепочка]
```

Ключ команда указывает на то, что нужно сделать с правилом, например, команда `-A` указывает на то, что правило нужно добавить в конец указанной цепочки.

Цепочка указывает, в какую цепочку нужно добавить правило. Стандартные цепочки – `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING` и `POSTROUTING`. Они находятся в таблицах фильтра. Не все таблицы содержат все стандартные цепочки. Подробнее таблицы и цепочки описаны ниже.

Раздел `[match]` задает критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии – IP-адрес источника пакета или сети, сетевой интерфейс.

Раздел `[target]` указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно передать пакет в другую цепочку правил, «сбросить» пакет и забыть про него, выдать на источник сообщение об ошибке и т. д.

Когда пакет приходит на сетевое устройство, он обрабатывается соответствующим драйвером и далее передается в фильтр в ядре ОС. Далее пакет проходит ряд таблиц и затем передается либо локальному приложению, либо переправляется на другую машину (рис. 53).

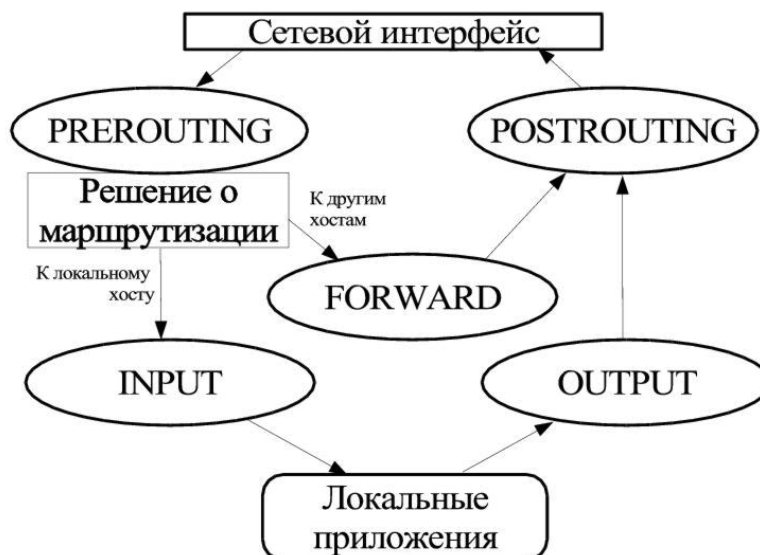


Рис. 53 – Схема движения пакетов в iptables

7.5.2. Встроенные таблицы фильтра iptables

По умолчанию используется таблица `filter`. Опция `-t` в правиле указывает на используемую таблицу. С ключом `-t` можно указывать следующие таблицы: `nat`, `mangle`, `filter`.

7.5.2.1. Таблица `nat`

Таблица `nat` используется главным образом для преобразования сетевых адресов Network Address Translation. Через эту таблицу проходит только первый пакет из потока. Преобразование адресов автоматически применяется ко всем последующим пакетам.

Таблица имеет три цепочки `PREROUTING`, `OUTPUT` и `POSTROUTING`:

- цепочка `PREROUTING` используется для внесения изменений в пакеты на входе в фильтр;
- цепочка `OUTPUT` используется для преобразования пакетов, созданных приложениями внутри компьютера, на котором установлен фильтр, перед принятием решения о маршрутизации;

- цепочка POSTROUTING используется для преобразования пакетов перед выдачей их в сеть.

7.5.2.2. Таблица mangle

Таблица mangle используется для внесения изменений в заголовки пакетов. Примером может служить изменение поля TTL, TOS или MARK. Таблица имеет две цепочки PREROUTING и OUTPUT:

- цепочка PREROUTING используется для внесения изменений на входе в фильтр перед принятием решения о маршрутизации;
- цепочка OUTPUT – для внесения изменений в пакеты, поступающие от внутренних приложений. Таблица mangle не должна использоваться для преобразования сетевых адресов (Network Address Translation) или маскардинга (masquerading), для этих целей используется таблица nat.

7.5.2.3. Таблица filter

Таблица filter используется, главным образом, для фильтрации пакетов.

Таблица имеет три цепочки – FORWARD, INPUT, OUTPUT:

- цепочка FORWARD используется для фильтрации пакетов, идущих транзитом через данный компьютер;
- цепочка INPUT предназначена для обработки входящих пакетов, направляемых локальным приложениям данного компьютера;
- цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных локальными приложениями данного компьютера.

7.5.3. Команды утилиты iptables

В таблице 1 приведены команды, которые используются в iptables.

Т а б л и ц а 1 – Команды утилиты iptables

Команда	Пример	Пояснения
-A, --append	iptables -A INPUT	Добавляет новое правило в конец заданной цепочки
-D, --delete	iptables -D INPUT -p tcp --dport 80 -j ACCEPT iptables -D INPUT 1	Удаление правила из цепочки. Команда имеет два формата записи, первый – когда задается критерий сравнения с опцией -D (см. первый пример), второй – порядковый номер правила. Если задается критерий сравнения, то удаляется правило, которое имеет в себе этот критерий, если задается номер правила, то будет удалено правило с заданным номером. Счет правил в цепочках начинается с 1
-R, --replace	iptables -R INPUT 1 -s 192.168.0.1 -j DROP	Данная команда заменяет одно правило другим. Используется в основном во время отладки новых правил
-I, --insert	iptables -I INPUT 1 -p tcp --dport 80 -j ACCEPT	Вставляет новое правило в цепочку. Число, следующее за именем цепочки, указывает номер правила, перед которым нужно вставить новое правило, другими словами число задает номер для вставляемого правила. В примере, указывается, что данное правило должно быть 1-м в цепочке INPUT
-L, --list	iptables -L INPUT	Вывод списка правил в заданной цепочке, в данном примере предполагается вывод правил из цепочки INPUT. Если имя цепочки не указывается, то выводится список правил для всех цепочек. Формат вывода зависит от наличия дополнительных ключей в команде, например, -n, -v, и пр.
-F, --flush	iptables -F INPUT	Удаление всех правил из заданной цепочки (таблицы). Если имя цепочки и таблицы не указывается, то удаляются все правила, во всех цепочках
-Z, --zero	iptables -Z INPUT	Обнуление всех счетчиков в заданной цепочке. Если имя цепочки не указывается, то подразумеваются все цепочки. При использовании ключа -v совместно с командой -L, на вывод будут поданы и состояния

Окончание таблицы 1

Команда	Пример	Пояснения
		счетчиков пакетов, попавших под действие каждого правила. Допускается совместное использование команд <code>-L</code> и <code>-Z</code> . В этом случае будет выдан сначала список правил со счетчиками, а затем произойдет обнуление счетчиков
<code>-N,</code> <code>--new-chain</code>	<code>iptables -N allowed</code>	Создается новая цепочка с заданным именем в заданной таблице. В приведенном выше примере создается новая цепочка с именем <code>allowed</code> . Имя цепочки должно быть уникальным и не должно совпадать с зарезервированными именами цепочек и действий (<code>DROP</code> , <code>REJECT</code> и т. п.)
<code>-X,</code> <code>--delete-chain</code>	<code>iptables -X allowed</code>	Удаление заданной цепочки из заданной таблицы. Удаляемая цепочка не должна иметь правил и не должно быть ссылок из других цепочек на удаляемую цепочку. Если имя цепочки не указано, то будут удалены все цепочки, определенные командой <code>-N</code> в заданной таблице
<code>-P, --policy</code>	<code>iptables -P INPUT DROP</code>	Определяет политику по умолчанию для заданной цепочки. Политика по умолчанию определяет действие, применяемое к пакетам, не попавшим под действие ни одного из правил в цепочке. В качестве политики по умолчанию допускается использовать <code>DROP</code> , <code>ACCEPT</code> и <code>REJECT</code>
<code>-E,</code> <code>--rename-chain</code>	<code>iptables -E allowed disallowed</code>	Команда <code>-E</code> выполняет переименование пользовательской цепочки. В примере цепочка <code>allowed</code> будет переименована в цепочку <code>disallowed</code> . Эти переименования не изменяют порядок работы, а носят только косметический характер

Команда должна быть указана всегда. Список доступных команд можно просмотреть с помощью команды `iptables -h` или, что то же самое, `iptables --help`. Некоторые команды могут использоваться совместно с дополнительными ключами.

7.5.4. Ключи утилиты iptables

В таблице 2 приводится список дополнительных ключей и описывается результат их действия.

Т а б л и ц а 2 – Ключи утилиты iptables

Ключ	Пример	Пояснения
<code>-v, --verbose</code>	<code>--list,</code> <code>--append,</code> <code>--insert,</code> <code>--delete,</code> <code>--replace</code>	Используется для повышения информативности вывода и, как правило, используется совместно с командой <code>--list</code> . В случае использования с командой <code>--list</code> , в вывод этой команды включаются: имя интерфейса, счетчики пакетов и байт для каждого правила. Формат вывода счетчиков предполагает вывод кроме цифр числа еще и символьные множители К (x1000), М (x1,000,000) и G (x1,000,000,000). Для того чтобы заставить команду <code>--list</code> выводить полное число (без употребления множителей) требуется применять ключ <code>-x</code> . Если ключ <code>-v, --verbose</code> используется с командами <code>--append</code> , <code>--insert</code> , <code>--delete</code> или <code>--replace</code> , то на вывод будет выдан подробный отчет о произведенной операции
<code>-x, --exact</code>	<code>--list</code>	Для всех чисел в выходных данных выводятся их точные значения без округления и без применения множителей К, М, G
<code>-n, --numeric</code>	<code>--list</code>	Iptables выводит IP-адреса и номера портов в числовом виде, предотвращая попытки преобразовать их в символические имена
<code>--line-numbers</code>	<code>--list</code>	Включает режим вывода номеров строк при отображении списка правил
<code>-c,</code> <code>--set-counters</code>	<code>--insert,</code> <code>--append,</code> <code>--replace</code>	Используется при создании нового правила для установки счетчиков пакетов и байт в заданное значение. Например, ключ <code>--set-counters 20 4000</code> установит счетчик пакетов = 20, а счетчик байт = 4000
<code>--modprobe</code>	Любая команда	Определяет команду загрузки модуля ядра

7.5.5. Основные действия над пакетами в фильтре iptables

В таблице 3 приведены доступные над пакетами действия.

Т а б л и ц а 3 – Действия над пакетами iptables

Действие	Пояснения
ACCEPT	Пакет прекращает движение по цепочке (и всем вызвавшим цепочкам, если текущая цепочка была вложенной) и считается принятым, тем не менее, пакет продолжит движение по цепочкам в других таблицах и может быть отвергнут там
DROP	Отбрасывает пакет и iptables «забывает» о его существовании. Отброшенные пакеты прекращают свое движение полностью
RETURN	Прекращает движение пакета по текущей цепочке правил и производит возврат в вызывающую цепочку, если текущая цепочка была вложенной, или, если текущая цепочка лежит на самом верхнем уровне (например, INPUT), то к пакету будет применена политика по умолчанию
LOG	Служит для журналирования отдельных пакетов и событий. В системный журнал могут заноситься заголовки IP-пакетов и другая интересующая информация
REJECT	Используется, как правило, в тех же самых ситуациях, что и DROP, но в отличие от DROP, команда REJECT выдает сообщение об ошибке на хост, передавший пакет
SNAT	Используется для преобразования сетевых адресов (Source Network Address Translation), т. е. изменение исходящего IP-адреса в IP-заголовке пакета
DNAT	Destination Network Address Translation используется для преобразования адреса места назначения в IP-заголовке пакета
MASQUERADE	В основе своей представляет то же самое, что и SNAT только не имеет ключа --to-source. Причиной тому то, что маскардинг может работать, например, с dialup подключением или DHCP, т. е. в тех случаях, когда IP-адрес присваивается устройству динамически. Если используется динамическое подключение, то нужно использовать маскардинг, если же используется статическое IP-подключение, то лучшим выходом будет использование действия SNAT
REDIRECT	Выполняет перенаправление пакетов и потоков на другой порт той же самой машины. К примеру, можно пакеты, поступающие на HTTP порт перенаправить на порт HTTP проху. Действие REDIRECT очень удобно для выполнения «прозрачного» проксирования (transparent проху), когда компьютеры в локальной сети даже не подозревают о существовании прокси
TTL	Используется для изменения содержимого поля «время жизни» (Time To Live) в IP-заголовке. Один из вариантов применения этого действия – это устанавливать значение поля «Time To Live» во всех исходящих пакетах в одно и то же значение. Если установить на все пакеты одно и то же значение TTL, то тем самым можно лишить провайдера одного из критериев определения того, что подключение к Интернету разделяется между несколькими компьютерами. Для примера можно привести число «TTL = 64», которое является стандартным для ядра Linux

7.5.6. Основные критерии пакетов в фильтре iptables

В таблице 4 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Т а б л и ц а 4 – Критерии пакетов в фильтре iptables

Критерий	Пояснения
-p, --protocol	Используется для указания типа протокола. Примерами протоколов могут быть TCP, UDP и ICMP. Список протоколов можно посмотреть в файле /etc/protocols. Прежде всего, в качестве имени протокола в данный критерий можно передавать три вышеупомянутых протокола, а также ключевое слово ALL. В качестве протокола допускается передавать число – номер протокола
-s, --src, --source	IP-адрес(а) источника пакета. Адрес источника может указываться без маски или префикса (например, 192.168.1.1), тогда подразумевается единственный IP-адрес. Можно указать адрес в виде address/mask, например, как 192.168.0.0/255.255.255.0, или более современным способом 192.168.0.0/24, т. е. фактически определяя диапазон адресов. Символ «!», установленный перед адресом, означает логическое отрицание, т. е. --source ! 192.168.0.0/24 означает любой адрес кроме адресов 192.168.0.x
-d, --dst, --destination	IP-адрес(а) получателя. Имеет синтаксис схожий с критерием --source, за исключением того, что подразумевает адрес места назначения. Точно так же может определять, как единственный IP-адрес, так и диапазон адресов. Символ «!» используется для логической инверсии критерия
-i, --in-interface	Интерфейс, с которого был получен пакет. Использование этого критерия допускается только в цепочках INPUT, FORWARD и PREROUTING, в любых других случаях будет вызывать сообщение об ошибке
-o, --out-interface	Задаёт имя выходного интерфейса. Этот критерий допускается использовать только в цепочках OUTPUT, FORWARD и POSTROUTING, в противном случае будет генерироваться сообщение об ошибке
-f, --fragment	Правило распространяется на все фрагменты фрагментированного пакета, кроме первого, сделано это потому, что нет возможности определить исходящий/входящий порт для фрагмента пакета, а для ICMP-пакетов определить их тип. С помощью фрагментированных пакетов могут производиться атаки на межсетевой экран, так как фрагменты пакетов могут не отслеживаться другими правилами
-sport, --source-port	Исходный порт, с которого был отправлен пакет. В качестве параметра может указываться номер порта или название сетевой службы. Соответствие имен сервисов и номеров портов можно найти в файле /etc/services. При указании номеров портов правила обрабатываются несколько быстрее
--dport, --destination-port	Порт, на который адресован пакет. Аргументы задаются в том же формате, что и для --source-port
--tcp-flags	SYN, ACK, FIN SYN определяет маску и флаги tcp-пакета. Пакет считается удовлетворяющим критерию, если из перечисленных флагов в первом списке в единичное состояние установлены флаги из второго списка. В качестве аргументов критерия могут выступать флаги SYN, ACK, FIN, RST, URG, PSH, а также зарезервированные идентификаторы ALL и NONE. ALL означает ВСЕ флаги, а NONE – НИ ОДИН флаг. Так, критерий --tcp-flags ALL NONE означает, что все флаги в пакете должны быть сброшены.

Окончание таблицы 4

Критерий	Пояснения
	Символ «!» означает инверсию критерия. Имена флагов в каждом списке должны разделяться запятыми, пробелы служат для разделения списков
--icmp-type	Тип сообщения ICMP определяется номером или именем. Числовые значения определяются в RFC 792. Чтобы получить список имен ICMP значений выполните команду <code>iptables --protocol icmp --help</code> . Символ «!» инвертирует критерий, например, <code>--icmp-type ! 8</code>
--state	Для использования данного критерия в правиле перед <code>--state</code> нужно явно указать <code>-m state</code> . Проверяется признак состояния соединения. Можно указывать 4 состояния: INVALID, ESTABLISHED, NEW и RELATED. INVALID подразумевает, что пакет связан с неизвестным потоком или соединением и возможно содержит ошибку в данных или в заголовке. ESTABLISHED указывает на то, что пакет принадлежит уже установленному соединению, через которое пакеты идут в обоих направлениях. NEW подразумевает, что пакет открывает новое соединение или пакет принадлежит однонаправленному потоку. RELATED указывает на то, что пакет принадлежит уже существующему соединению, но при этом он открывает новое соединение. Примером может служить передача данных по FTP, или выдача сообщения ICMP об ошибке, которое связано с существующим TCP или UDP соединением. Признак NEW – это не то же самое, что установленный бит SYN в пакетах TCP, посредством которых открывается новое соединение, и подобного рода пакеты могут быть потенциально опасны в случае, когда для защиты сети используется один сетевой экран

7.5.7. Модули iptables

Возможности фильтрации пакетов расширяются через модули. Модули подключаются автоматически при выборе протокола (`-p/--protocol`) или вручную опцией `-m/--match`, после которой следует имя подключаемого модуля и его опции.

Справку по опциям модуля можно получить с помощью ключа `-h/--help`. Допустимо указание нескольких модулей. Результаты фильтрации, выдаваемые модулем, можно инвертировать указав `!` перед его именем.

В таблице 5 приведены возможные критерии для фильтрации пакетов в фильтре iptables.

Т а б л и ц а 5 – Модули iptables

Модуль	Опции	Пояснение
connlimit	[!] --connlimit-above n – пакет подойдет под описание, если количество одновременных подключений на данный момент больше (меньше), чем n; --connlimit-mask bits – позволяет задать маску блока адресов	Позволяет задавать возможное количество одновременных подключений к машине от заданного IP или блока адресов. Пример. Допускать не больше 20 соединений на порт 80 с одного хоста iptables -A INPUT -p tcp --syn \ --dport 80 -m connlimit \ --connlimit-above 20 -j REJECT \ --reject-with tcp-reset
icmp	--icmp-type [!] тип – тип ICMP в виде числа или имени в соответствии с iptables -p icmp -h	Расширение загружается при указании --protocol icmp.
iprange	[!]--src-range ip-ip – диапазон IP-адресов отправителя; [!]--dst-range ip-ip – диапазон IP-адресов получателя	Выделяет не один адрес, как --src, а все адреса от ip1 до ip2
ipv4options (не подключен по умолчанию)	--flags [!]параметр[,...] – сопоставляет наличие/отсутствие(!) параметров (по имени или номеру); --any – хотя бы один --flags ipv4 или их комбинация. Примеры параметров: - ssrr – strict source routing – маршрутизация указывается источником; - lsrr – loose source routing – свободная маршрутизация; - rr – record-route – запись маршрута; - ra – оповещения маршрутизатора; - srr – source-routing – режим маршрутизации; ts – timestamp	Результат теста зависит от параметров заголовка IPv4, таких как параметры маршрутизации, запись маршрута, запрос времени, оповещение маршрутизатора. Примеры: - отбрасывать пакеты с флагом ssrr: iptables -A INPUT -m ipv4options \ --flags ssrr -j DROP - отбрасывать пакеты любые пакеты ipv4: iptables -A INPUT -m ipv4options \ --any -j DROP
length	--length [!] размер[:размер]	Позволяет проверять размеры пакетов (точно или по диапазону)
limit	--limit частота – максимальная средняя частота положительных результатов. После числа можно указывать единицы: '/second', '/minute', '/hour', '/day'; значение по умолчанию – 3/hour. --limit-burst number – ограничение на исходное число пропускаемых пакетов (по умолчанию – 5)	Выдает положительный результат с фиксированной частотой. Правило использующее этот модуль будет выполняться до момента достижения лимита (и наоборот, если указан «!»). Может использоваться вместе с целью LOG для получения ограниченного протоколирования

Окончание таблицы 5

Модуль	Опции	Пояснение
multiport	<pre>[!]<code>--source-ports</code> port1,port2,port3:port4 - исходный порт равен одному из указанных; [!]<code>--destination-ports</code> port1,port2,port3:port4 - порт назначения равен одному из указанных; [[!]<code>--ports</code> port1,port2,port3:port4 - исходный и порт назначения и равны одному из указанных</pre>	Позволяет указывать в тексте правила несколько (до 15) портов и диапазонов портов (порт:порт). Используется только вместе с <code>-p tcp</code> или <code>-p udp</code>
state	<code>--state</code> состояния – список фильтруемых состояний через запятую (см. таблицу)	Проверяется признак состояния соединения (state)
string	<pre><code>--algo</code> bm kmp – стратегия сравнения/поиска (bm = Boyer- Moore, kmp = Knuth-Pratt- Morris); <code>--from</code> позиция – позиция в данных, с которой следует начинать поиск. Значение по умолчанию – 0. <code>--to</code> позиция – позиция в данных, при достижении которой следует прекращать поиск. Значение по умолчанию – размер пакета; <code>--string</code> последовательность – последовательность символов, которую следует искать в пакете; <code>--hex-string</code> pattern – последовательность символов, которую следует искать в пакете (в шестнадцатеричном представлении)</pre>	Позволяет выполнять фильтрацию пакетов, основываясь на анализе содержимого области данных пакета
tcp	см. таблицу	Это расширение загружается при указании <code>--protocol tcp</code>
u32	<code>--u32</code> "Start&Mask=Range"	Позволяет извлекать из пакета данные размером до 4 байт, применять к ним операции логического И, сдвига, и проверять принадлежность получающихся данных определенным диапазонам. В простейшей форме, u32 вырезает блок из 4 байт начиная со Start, применяет к ним маску Mask и сравнивает результат с Range-m u32
udp	см. таблицу	Это расширение загружается при указании <code>--protocol udp</code>

Список доступных модулей можно просмотреть, выполнив команду:

```
# ls /lib/modules/$(uname -r)/kernel/net/netfilter/
```

Загруженные модули iptables можно найти в записи файловой системы proc

```
/proc/net/ip_tables_matches:
```

```
# cat /proc/net/ip_tables_matches
```

Загрузка модуля:

```
# modprobe <модуль>
```

Например:

```
# modprobe xt_limit
# modprobe xt_length
# modprobe xt_u32
```

7.5.8. Использование фильтра iptables

ОС Альт СП уже включает в себя предустановленный iptables. Для его настройки рекомендуется использовать возможности системы настройки сети /etc/net (см. п. 8.2.1).

7.5.9. Примеры команд iptables

Список текущих правил:

```
iptables -nvL --line-numbers
```

Очистка всех правил:

```
iptables -F
```

Очистка правил в цепочке:

```
iptables -F INPUT
```

Удаления пятого правила в цепочке INPUT:

```
iptables -D INPUT 5
```

7.5.9.1. Фильтрация по источнику пакета

Для фильтрации по источнику используется опция -s.

Например, запретить все входящие пакеты с узла 192.168.1.95:

```
iptables -A INPUT -s 192.168.1.95 -j DROP
```

Можно использовать доменное имя для указания адреса хоста:

```
iptables -A INPUT -s test.host.net -j DROP
```

Также можно указать целую подсеть:

```
iptables -A INPUT -s 192.168.1.0/24 -j DROP
```

Можно использовать отрицание (знак «!»). Например, все пакеты с хостов отличных от 192.168.1.96 будут уничтожаться:

```
iptables -A INPUT ! -s 192.168.1.96 -j DROP
```

Разрешить трафик по localhost:

```
iptables -A INPUT -i lo -j ACCEPT
```

Записывать в журнал попытки спуфинга с префиксом "IP_SPOOF A: " и запретить соединение:

```
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
```

7.5.9.2. Фильтрация по адресу назначения

Для фильтрации по адресу назначения используется опция `-d`.

Например, запретить все исходящие пакеты на хост 192.168.1.95:

```
iptables -A OUTPUT -d 192.168.156.156 -j DROP
```

Запретить доступ к ресурсу `vk.com`:

```
iptables -A OUTPUT -d vk.com -j REJECT
```

Как и в случае с источником пакета, можно использовать адреса подсети и доменные имена. Отрицание также работает.

7.5.9.3. Фильтрация по протоколу

Опция `-p` указывает на протокол. Можно использовать `all`, `icmp`, `tcp`, `udp` или номер протокола (из `/etc/protocols`).

Разрешить входящие эхо-запросы:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
```

7.5.9.4. Фильтрация по порту источника

Разрешить все исходящие пакеты с порта 80:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
```

Заблокировать все входящие запросы порта 80:

```
iptables -A INPUT -p tcp --dport 80 -j DROP
```

Для указания порта нужно указать протокол (`tcp` или `udp`). Можно использовать отрицание.

Открыть диапазон портов:

```
iptables -A INPUT -m state --state NEW -m tcp -p tcp \
--dport 7000:7010 -j ACCEPT
```

7.5.9.5. Фильтрация по порту назначения

Разрешить подключения по HTTP:

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Разрешить подключения по SSH:

```
iptables -A INPUT -p tcp -i eth0 --dport 22 -j ACCEPT
```

Разрешить получать данные от DHCP-сервера:

```
iptables -A INPUT -p UDP --dport 68 --sport 67 -j ACCEPT
```

Разрешить rsync с определенной сети:

```
iptables -A INPUT -i eth0 -p tcp -s 192.168.1.0/24 --dport 873 \
-m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 873 -m state \
--state ESTABLISHED -j ACCEPT
```

Разрешить IMAP/IMAP2 трафик:

```
iptables -A INPUT -i eth0 -p tcp --dport 143 -m state \
--state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 143 -m state \
--state ESTABLISHED -j ACCEPT
```

Разрешить исходящие HTTP, FTP, DNS, SSH, SMTP:

```
iptables -A OUTPUT -p TCP -o eth0 --dport 443 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 80 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p UDP -o eth0 --dport 53 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 25 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 22 -j ACCEPT
iptables -A OUTPUT -p TCP -o eth0 --dport 21 -j ACCEPT
```

Разрешить mysql для локальных пользователей:

```
iptables -I INPUT -p tcp --dport 3306 -j ACCEPT
```

Разрешить CUPS (сервер печати, порт 631) для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -p udp -m udp --dport 631 -j ACCEPT
iptables -A INPUT -s 192.168.1.0/24 -p tcp -m tcp --dport 631 -j ACCEPT
```

Разрешить синхронизацию времени NTP для пользователей внутри локальной сети:

```
iptables -A INPUT -s 192.168.1.0/24 -m state --state NEW -p \
udp --dport 123 -j ACCEPT
```

7.5.9.6. Перенаправление портов

Направим трафик с порта 442 на 22, это значит, что входящие ssh-соединения могут быть принятыми с порта 422 и 22:

```
iptables -t nat -A PREROUTING -p tcp -d 192.168.1.15 --dport 422 \
-j DNAT --to 192.168.1.15:22
```

Также надо разрешить входящие соединения с порта 422:

```
iptables -A INPUT -i eth0 -p tcp --dport 422 -m state \
--state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state \
--state ESTABLISHED -j ACCEPT
```

Как и в случае с портом источника, нужно указать протокол. Можно использовать отрицание.

7.5.9.7. Ограничение по локальным пользователям

Ограничение по локальным пользователям нельзя поручить внешнему межсетевому экрану, так как он не имеет этой информации.

Отбросить все пакеты, исходящие от процессов пользователя с UID=500:

```
# iptables -A OUTPUT -m owner --uid-owner 500 -j DROP
```

Попытка соединения с удаленным узлом, пользователя с UID=500:

```
# su - test
$ wget ya.ru
--2025-03-07 13:53:14-- http://ya.ru/
Распознается ya.ru (ya.ru)... ошибка: Имя или служба не известны.
wget: не удастся разрешить адрес «ya.ru»
```

Попытка соединения с локальным узлом, пользователя с UID=500:

```
# su - test
$ wget localhost
--2025-03-07 13:55:20-- http://localhost/
Распознается localhost (localhost)... 127.0.0.1
Подключение к localhost (localhost)|127.0.0.1|:80... ^C
```

7.5.9.8. Фильтрация по содержимому пакета

Отбросить все пакеты, данные в которых содержат подстроку virus:

```
# iptables -I INPUT -j DROP -p tcp -s 0.0.0.0/0 -m string \
--algo kmp --string "virus "
```

Записывать в журнал пакеты со строкой secret внутри:

```
# iptables -A INPUT -m string --algo kmp --string "secret" \
-j LOG --log-level info --log-prefix "SECRET "
```

Просмотр журнала:

```
# journalctl |grep SECRET
```

```
апр 03 16:47:18 host-15.localdomain kernel: SECRET IN=eth0 OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00 SRC=192.168.3.101 DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=30811 DF PROTO=TCP SPT=53878 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
апр 03 16:58:47 host-15.localdomain kernel: SECRET IN=eth0 OUT=
MAC=08:00:27:d5:f3:78:74:e5:0b:3e:2c:88:08:00 SRC=192.168.3.101 DST=192.168.3.104
LEN=47 TOS=0x00 PREC=0x00 TTL=64 ID=38640 DF PROTO=TCP SPT=54510 DPT=8080 WINDOW=229
RES=0x00 ACK PSH URGP=0
```

Статистика правил iptables и счетчики обработанных пакетов в цепочке

INPUT:

```
# iptables -nvL INPUT --line-numbers
Chain INPUT (policy ACCEPT 1711 packets, 1400K bytes)
num pkts bytes target prot opt in out source destination
1 47 49550 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "virus" ALGO name kmp TO 65535
2 0 0 DROP tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "virus " ALGO name kmp TO 65535
3 17 66141 LOG tcp -- * * 0.0.0.0/0 0.0.0.0/0
STRING match "secret" ALGO name kmp TO 65535 LOG flags 0 level 6 prefix "SECRET "
```

7.6. Настройка экспорта аудита на удаленный узел

Для настройки экспорта аудита на удаленный узел нужно настроить OpenVPN-соединение (см. подробнее п. 8.3) между принимающей и передающей стороной, настроить межсетевой экран и внести изменения в конфигурационные файлы аудита.

На принимающей стороне – сервер:

- 1) скопировать файл /usr/share/doc/openvpn-*/server.conf (* – версия openvpn) в директорию /etc/openvpn/ для его редактирования и последующего запуска сервера VPN;
- 2) в скопированном на предыдущем этапе файле server.conf, проверьте имена и пути файлов сертификата сервера (.crt), его ключа (.key), а также

сертификата CA (.crt) и DH (dh*.pem), а также закомментировать параметр `proto udp` и раскомментировать `proto tcp`;

3) установить утилиту `easy-rsa`:

```
# apt-get install easy-rsa
```

4) сгенерировать все ключи и сертификаты. Ввести для них пароли:

```
# easyrsa init-pki
# easyrsa build-ca
# easyrsa build-server-full server
# easyrsa build-client-full client1
# easyrsa gen-dh
# easyrsa sign-req client client1
# easyrsa sign-req server server
```

5) перенести полученные ключи и сертификаты в каталог

```
/etc/openvpn/keys/.
```

Настройка OpenVPN-клиента на передающей стороне:

1) скопировать из `/usr/share/doc/openvpn-*/client.conf` (* – версия `openvpn`) в директорию `/etc/openvpn/` для его редактирования и последующего запуска клиента VPN;

2) скопировать ранее сгенерированные ключи и сертификаты в директорию `/etc/openvpn/keys/` и указать их в `client.conf`;

3) открыть `client.conf` найти строку `remote` и изменить ее на:

```
remote 10.10.3.87 1194
```

где `10.10.3.87` – это IP-адрес сервера на внешнем интерфейсе принимающей стороны.

Также, закомментировать параметр `proto udp` и раскомментировать `proto tcp`.

Отредактировать конфигурационные файлы аудита:

- на принимающей стороне в файле `/etc/audit/auditd.conf` исправить параметр `tcp_listen_port=1060`;

- на передающей стороне в файле `/etc/audit/audisp-remote.conf` исправить параметры:

```
remote_server = 10.8.0.1
port = 1060
#queue_error_action
```

где 10.8.0.1 – IP-адрес сервера vpn на созданном интерфейсе-туннеле принимающей стороны;

- на передающей стороне изменить параметр: `active = yes` в файле `/etc/audit/plugins.d/au-remote.conf`;

- перезапустить систему на принимающей и передающей сторонах.

Запустить сервер на принимающей стороне:

```
# openvpn /etc/openvpn/server.conf
```

Запустить OpenVPN-клиент на передающей стороне:

```
# openvpn /etc/openvpn/client.conf
```

Команды установки правила пропуска tcp пакетов с портом назначения 1060 только через устройство vpn (например, tun0) на принимающей стороне:

```
# iptables -A INPUT -p tcp --dport 1060 -i tun0 -j ACCEPT
# iptables -A INPUT -p tcp --dport 1060 -j DROP
```

Для проверки аудита передающей стороны на принимающей стороне выполнить команду:

```
# ausearch -hn имя_передающей_стороны
```

Если ничего не отображается, то, возможно, было указано неверное имя передающей стороны. Для проверки, что лог приходит, можно, например, авторизоваться на передающей стороне, а затем проверить лог на принимающей стороне командой:

```
# ausearch -m USER_AUTH
```

Имя передающей стороны будет указано в параметре `hostname` лога.

7.7. Настройка системы сигнализации на основе icinga

Icinga2 – система мониторинга с открытым исходным кодом. Изначально была создана как ответвление от системы мониторинга Nagios.

С точки зрения клиент-серверной архитектуры в Icinga2 различается три роли (рис. 54):

- мастер (Master) – серверный экземпляр Icinga2 на верхнем уровне иерархии.

Мастер-узел в простых развертываниях один, в высоко-доступных развертываниях Мастер-узлов может быть несколько (кластер);

- спутник (Satellite) – вспомогательный узел, который способен выступать в качестве распространителя конфигурации Icinga для агентов и позволяет агентам не замечать недоступности основного Мастер-узла. Спутники могут быть полезны в больших развертываниях, где требуется децентрализация основной конфигурации, например, когда требования к мониторингу одних и тех же служб различаются на разных площадках;
- агент (Agent) – клиентский узел, который получает конфигурацию мониторинга с родительского узла (Мастер или Спутник).

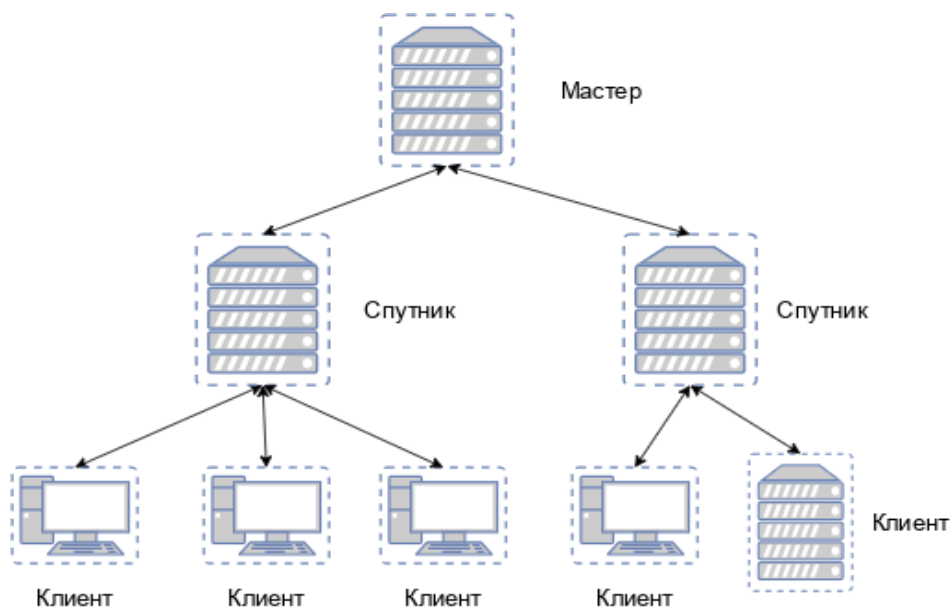


Рис. 54 – Роли Icinga2

В данном руководстве рассмотрена простая конфигурация с единственным мастер-узлом и некоторым количеством узлов агентов без участия узлов спутников.

Иерархия Icinga2 состоит из так называемых зон. Существуют определенные ограничения для дочерних зон, например, их участникам не разрешено отправлять команды конфигурации членам родительской зоны. И, наоборот, иерархия доверия позволяет главной зоне отправлять файлы конфигурации в вспомогательную зону.

Узлы агентов также имеют свою собственную уникальную зону. В качестве имени зоны необходимо использовать полное доменное имя. Узлы, являющиеся членами зоны, являются так называемыми объектами Endpoint (конечными точками).

Сервер Icinga2 – это главный сервер, который собирает все данные мониторинга и отображает их. Главный сервер состоит из процесса-демона (Icinga2), который работает в фоновом режиме, и веб-приложения (Icingaweb2), которое используется для отображения результатов из веб-браузера.

Примечание. Необходимо обеспечить взаимно однозначное прямое и обратное преобразование имен для всех узлов. Можно использовать DNS или обойтись соответствующими записями в локальных файлах `/etc/hosts`, например:

```
# echo "192.168.0.170 master1.test.alt" >> /etc/hosts
# echo "192.168.0.151 agent1.test.alt" >> /etc/hosts
# echo "192.168.0.152 agent2.test.alt" >> /etc/hosts
```

7.7.1. Настройка сервера мониторинга

7.7.1.1. Установка Icinga2

Установить пакеты:

```
# apt-get install icinga2 icingaweb2 icingaweb2-nginx icingaweb2-
cli icinga2-doc icingaweb2-php-fpm icingaweb2-style-altsp nagwad-
icinga-master
```

Примечание. Шаг установки пакетов `icinga2` можно пропустить, если при установке ОС на этапе «Установка системы» был выбран блок «Рабочее место контролера событий безопасности» (рис. 55).

Примечание. Все указанные пакеты доступны на ОС Альт СП Рабочая станция.

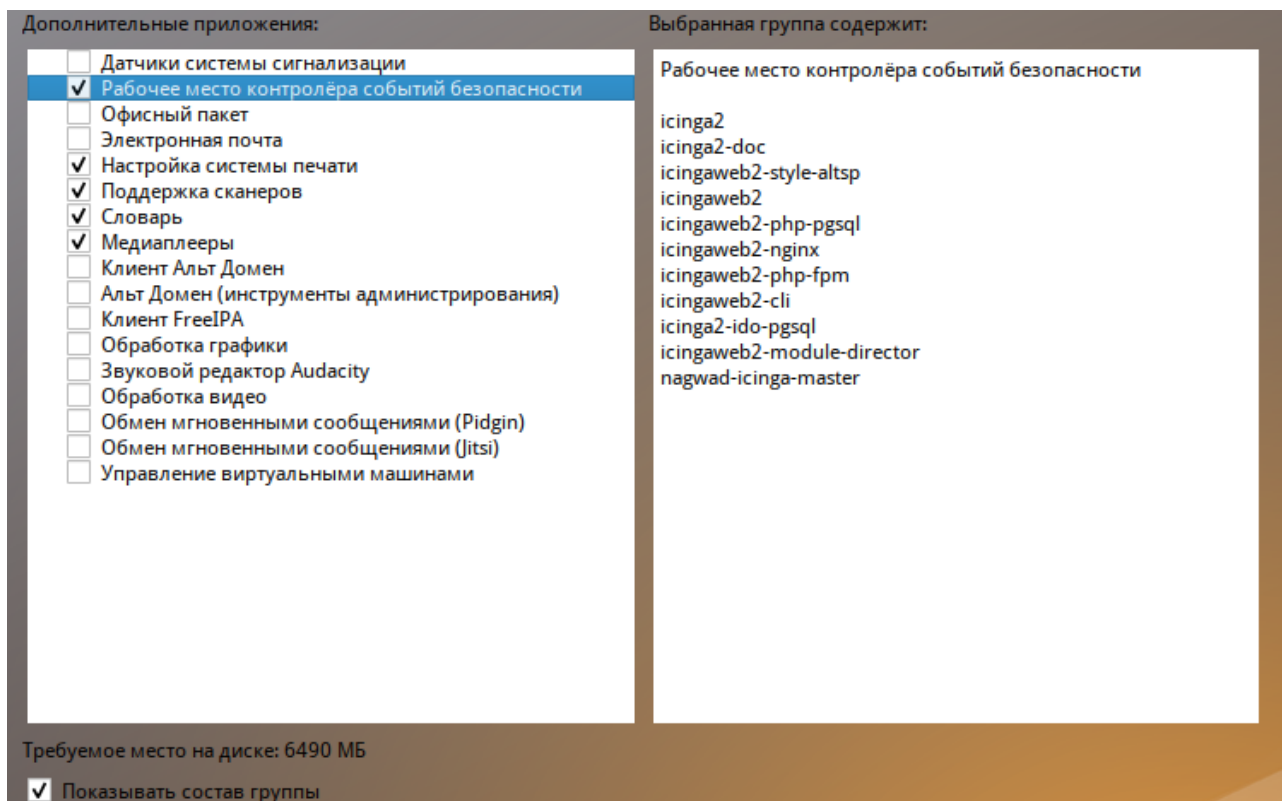


Рис. 55 – Блок «Рабочее место контролера событий безопасности»

Примечание. Начиная с версии php 8.0, пакеты модулей именуются следующим образом:

php<мажорная>.<минорная версии>-<имя модуля>.

В данной инструкции используется версия php8.3.

7.7.1.2. Установка и конфигурация БД

В процессе установки должна быть создана база данных для вывода данных icinga2 и для веб-интерфейса icinga2. Можно использовать базу данных MySQL или PostgreSQL.

⚠ В качестве сервера базы данных используется ПЭВМ 64 бит (x86_64)/ AArch64 (ARMv8) с установленной ОС Альт СП Рабочая станция/Сервер релиз 10. Далее настройки приводятся для указанной базы данных.

7.7.1.2.1. PostgreSQL

Установить PostgreSQL и IDO-модули для PostgreSQL:

```
# apt-get install postgresql16-server icinga2-ido-pgsql
icingaweb2-php-pgsql
```

Примечание. Пакет postgresql16-server доступен в репозитории или на компакт-диске дистрибутива ОС Альт СП Сервер релиз 10 64 бит (x86_64)/ AArch64 (ARMv8).

Подготовить к запуску и настроить службы PostgreSQL:

- создать системные базы данных (пароль пользователя PostgreSQL необходимо запомнить):

```
# /etc/init.d/postgresql initdb
Введите новый пароль суперпользователя:
Повторите его:
```

- включить по умолчанию и запустить службу:

```
# systemctl enable --now postgresql
```

Создать базы данных для icinga2:

- создать пользователя icinga (пароль необходимо запомнить) и базы данных icinga и icingaweb (при запросе «Пароль» следует ввести пароль пользователя postgresql, созданный при создании системных баз данных):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt icinga'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O icinga icinga'
```

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O icinga icingaweb'
```

Пароль:

- импортировать в базу icinga схему Icinga2 из IDO модуля:

```
# su - postgres -s /bin/sh -c 'psql -U icinga -f /usr/share/icinga2-ido-pgsql/schema/pgsql.sql icinga'
```

Пароль пользователя icinga:

Внести информацию о пользователе базы данных icinga в файл

/etc/icinga2/features-enabled/ido-pgsql.conf, например:

```
object IdoPgsqlConnection "ido-pgsql" {
    user = "icinga"
    password = "new_icinga"
    host = "IP-адрес_БД"
    database = "icinga"
}
```

7.7.1.2.2. MySQL/MariaDB

Установить сервер MariaDB и IDO-модули для MySQL:

```
# apt-get install mariadb-server icingaweb2-php-mysql icinga2-ido-mysql
```

Примечание. Пакет `mariadb-server` доступен в репозитории или на компакт-диске дистрибутива ОС Альт СП Сервер релиз 10 64 бит (x86_64)/ AArch64 (ARMv8).

Включить по умолчанию и запустить службу `mysqld`:

```
# systemctl enable --now mysqld
```

Создать базы данных `icinga` и `icingaweb` и пользователя `icinga` (пароль пользователя необходимо запомнить):

```
$ mysql -uroot -p
Enter password:
MariaDB [(none)]> create database icinga CHARACTER SET utf8
COLLATE utf8_general_ci;
MariaDB [(none)]> create database icingaweb CHARACTER SET utf8
COLLATE utf8_general_ci;
MariaDB [(none)]> grant all privileges on icinga.* to
icinga@localhost identified by '<пароль>';
MariaDB [(none)]> grant all privileges on icingaweb.* to
icinga@localhost identified by '<пароль>';
MariaDB [(none)]> quit;
```

Импортировать в базу `icinga` схему `Icinga2` из IDO модуля (по запросу ввести пароль пользователя `icinga`):

```
$ mysql -uicinga -p icinga < /usr/share/icinga2-ido-
mysql/schema/mysql.sql
Enter password:
```

Внести информацию о пользователе базы данных `icinga` в файл `/etc/icinga2/features-enabled/ido-mysql.conf`, например:

```
object IdomysqlConnection "ido-mysql" {
    user = "icinga"
    password = "new_icinga"
    host = "localhost"
    database = "icinga"
}
```

7.7.1.3. Запуск служб

Запустить и включить по умолчанию службы:

```
# systemctl enable --now php8.3-fpm.service
# systemctl enable --now nginx
# systemctl enable --now icinga2
```

7.7.1.4. Веб-интерфейс IcingaWeb2

Icinga Web 2 – веб-интерфейс панели наблюдения Icinga2.

Настроить Icinga Web 2 можно с помощью мастера настройки Icinga Web 2, который доступен при первом посещении Icinga Web 2 в веб-браузере.

7.7.1.4.1. Предварительная настройка

Создать каталог конфигурации:

```
# icingacli setup config directory --group icingaweb2
Successfully created configuration directory /etc/icingaweb2
```

При использовании веб-настройки потребуется пройти аутентификацию с использованием токена. Для генерации токена выполнить команду:

```
# icingacli setup token create
The newly generated setup token is: 5b24be3ace879072
```

Далее необходимо настроить REST API для связи Icinga и Icinga Web 2:

```
# icinga2 api setup
information/cli: Generating new CA.
information/base: Writing private key to
'/var/lib/icinga2/ca//ca.key'.
information/base: Writing X509 certificate to
'/var/lib/icinga2/ca//ca.crt'.
information/cli: Generating new CSR in
'/var/lib/icinga2/certs//master1.test.alt.csr'.
information/base: Writing private key to
'/var/lib/icinga2/certs//master1.test.alt.key'.
information/base: Writing certificate signing request to
'/var/lib/icinga2/certs//master1.test.alt.csr'.
information/cli: Signing CSR with CA and writing certificate to
'/var/lib/icinga2/certs//master1.test.alt.crt'.
information/pki: Writing certificate to file
'/var/lib/icinga2/certs//master1.test.alt.crt'.
information/cli: Copying CA certificate to
'/var/lib/icinga2/certs//ca.crt'.
information/cli: Adding new ApiUser 'root' in
'/etc/icinga2/conf.d/api-users.conf'.
information/cli: Reading '/etc/icinga2/icinga2.conf'.
```



```

information/cli: Enabling the 'api' feature.
Enabling feature api. Make sure to restart Icinga2 for these
changes to take effect.
information/cli: Updating 'NodeName' constant in
'/etc/icinga2/constants.conf'.
information/cli: Created backup file
'/etc/icinga2/constants.conf.orig'.
information/cli: Updating 'ZoneName' constant in
'/etc/icinga2/constants.conf'.
information/cli: Backup file '/etc/icinga2/constants.conf.orig'
already exists. Skipping backup.
Done.

```

Now restart your Icinga2 daemon to finish the installation!

Эта команда сгенерирует сертификаты, API-пользователя root с автогенерированным паролем (см. /etc/icinga2/conf.d/api-users.conf).

Для применения изменений перезагрузить icinga2:

```
# systemctl restart icinga2.service
```

7.7.1.4.2. Настройка Nginx

По умолчанию веб-интерфейс icinga2 доступен только с localhost. Для изменения этого поведения следует внести изменения в файл /etc/nginx/sites-available.d/icingaweb2.conf. Например, для возможности доступа к веб-интерфейсу по адресу http://192.168.0.170:81/icingaweb2 необходимо в раздел server добавить строку:

```
listen 192.168.0.170:81;
```

и перезагрузить Nginx:

```
# systemctl restart nginx
```

Примечание. Если обращение к веб-интерфейсу IcingaWeb2 происходит по IP-адресу, а не по имени, то для того чтобы Nginx при старте (например, после перезагрузки системы) не ругался на несуществующий IP, нужно разрешить поддержку нелокальных адресов. Для этого в файл /etc/sysctl.conf следует дописать строку:

```
net.ipv4.ip_nonlocal_bind = 1
```

и перезагрузить конфигурацию sysctl:

```
# sysctl -p /etc/sysctl.conf
```

Для настройки https можно создать файл `icingaweb2-ssl.conf` и дописать в него ранее сгенерированные сертификаты. Например:

1) создать новый файл конфигурации:

```
# cp /etc/nginx/sites-available.d/icingaweb2.conf
/etc/nginx/sites-available.d/icingaweb2-ssl.conf
```

2) внести изменения в файл:

```
server {
    listen 81;
    server_name master1.test.alt localhost localhost.localdomain;
    rewrite ^ https://$host$request_uri? permanent;
}
server {
    listen 443 ssl;
    server_name master1.test.alt localhost localhost.localdomain;
    ssl_certificate
/var/lib/icinga2/certs/master1.test.alt.crt;
    ssl_certificate_key
/var/lib/icinga2/certs/master1.test.alt.key;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;
    location ~ ^/icingaweb2/index\.php(.*?)$ {
        fastcgi_pass unix:/var/run/php8.3-fpm/icingaweb2.socket;
        fastcgi_index index.php;
        include fastcgi_params;
        fastcgi_param SCRIPT_FILENAME
/usr/share/icingaweb2/public/index.php;
        fastcgi_param ICINGAWEB_CONFIGDIR /etc/icingaweb2;
        fastcgi_param REMOTE_USER $remote_user;
    }
    location ~ ^/icingaweb2(.+)? {
        alias /usr/share/icingaweb2/public;
        index index.php;
        try_files $1 $uri $uri/ /icingaweb2/index.php$is_args$args;
    }
}
```

3) отключить старую конфигурацию и включить новую:

```
# rm -rf /etc/nginx/sites-enabled.d/icingaweb2.conf
# ln -s /etc/nginx/sites-available.d/icingaweb2-ssl.conf
/etc/nginx/sites-enabled.d/icingaweb2-ssl.conf
```

4) перезагрузить Nginx:

```
# systemctl restart nginx
```

В данном примере веб-интерфейс будет доступен по `https://master1.test.alt/icingaweb2/`.

7.7.1.4.3. Настройка рабочего места администратора безопасности

Под рабочим местом администратора безопасности подразумевается веб-интерфейс Icinga Web 2. Мастер первоначальной настройки будет предложен после перехода по адресу `http://localhost:81/icingaweb2/` (URL может быть иным в зависимости от изменений, сделанных при настройке Nginx).

На первом шаге настройки Icinga Web 2 необходимо ввести ранее полученный токен (рис. 56) и нажать кнопку «Далее».

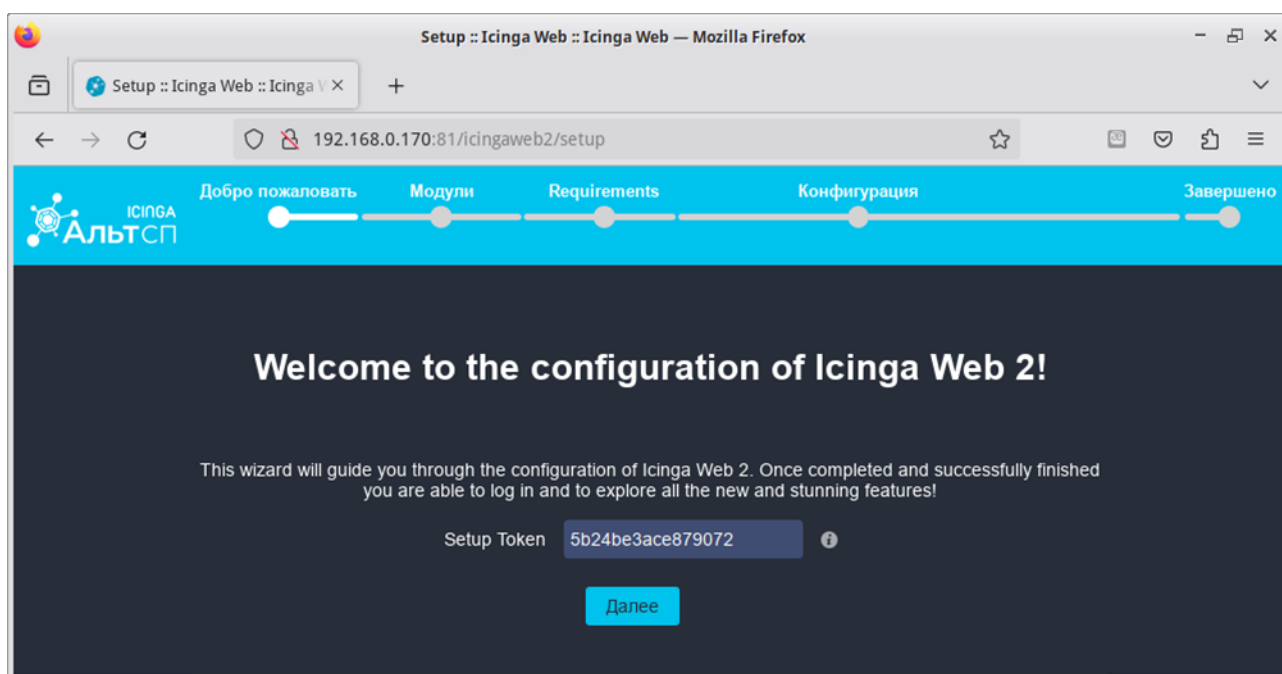


Рис. 56 – Конфигурирование Icinga Web 2

Примечание. Посмотреть текущий токен можно, выполнив команду:

```
# icingacli setup token show
5b24be3ace879072
```

На следующем шаге представлен набор модулей, которые обнаружила Icinga Web 2. Можно оставить значение по умолчанию (отмечен только модуль Monitoring) и нажать кнопку «Далее» (рис. 57).

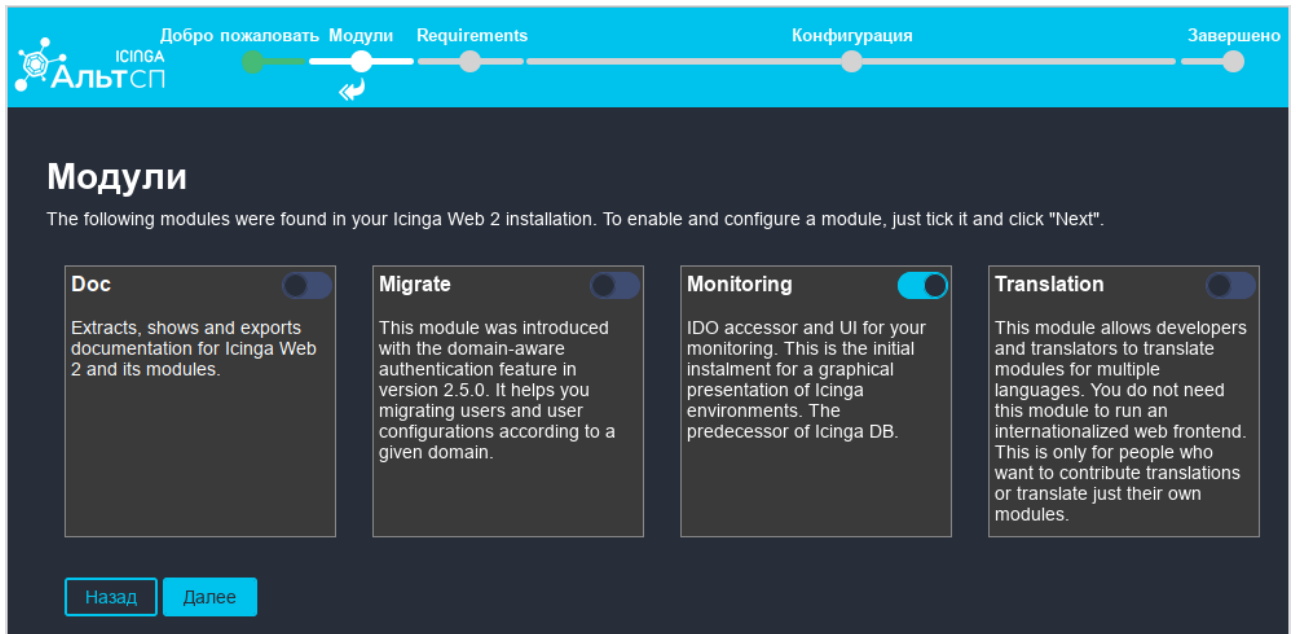


Рис. 57 – Icinga Web 2. Набор модулей

На следующей странице (рис. 58) показан набор предварительных требований. Если не все из них отмечены зеленым цветом, необходимо вернуться в консоль и обновить/установить соответствующий пакет.



Рис. 58 – Icinga Web 2. Набор предварительных требований

На следующем шаге необходимо выбрать тип аутентификации. Следует оставить, предложенную по умолчанию, аутентификацию с хранением учетных данных в БД – «База данных» (рис. 59).

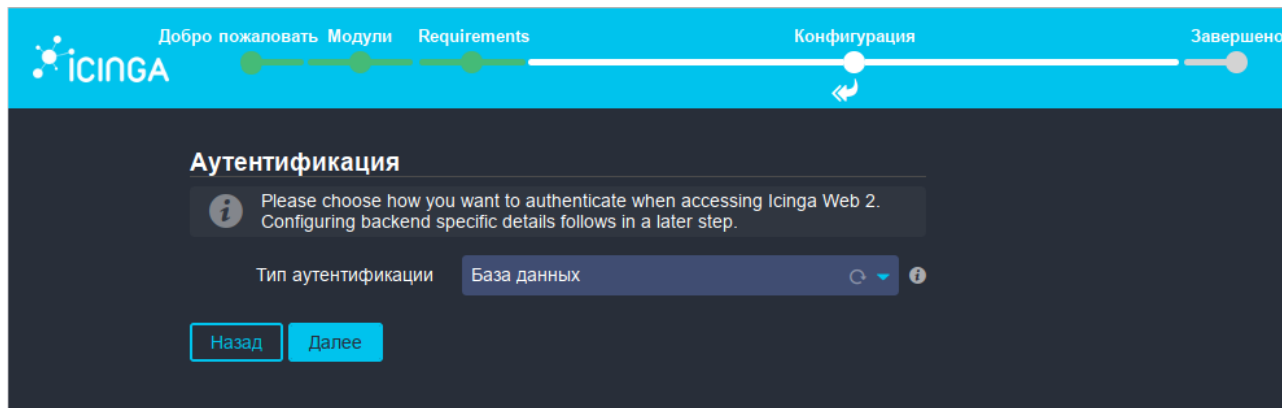


Рис. 59 – Icinga Web 2. Выбор типа аутентификации

Следующий шаг – настройка параметров подключения к базе данных для хранения учетных данных Icinga Web 2 (рис. 60, рис. 61):

- «Название ресурса» – имя ресурса данных;
- «Тип базы данных» – MySQL или PostgreSQL;
- «Узел» – узел, на котором расположена база данных;

⚠ В качестве сервера базы данных используется ПЭВМ 64 бит (x86_64)/ AArch64 (ARMv8) с установленной ОС Альт СП Рабочая станция/Сервер релиз 10, поэтому вместо localhost необходимо указывать IP-адрес ПЭВМ, на которой развернута база данных.

- «Порт» – порт для подключения к базе данных (при подключении к MySQL можно не указывать);
- «Название базы данных» – имя базы данных (icingaweb);
- «Имя пользователя» – имя пользователя для доступа к базе данных (icinga);
- «Пароль» – пароль пользователя.

Для проверки конфигурации следует нажать кнопку «Проверить конфигурацию». Если проверка прошла успешно, можно переходить к следующему шагу, нажав кнопку «Далее».

The screenshot shows the 'Источник базы данных' (Database Source) configuration step in the Icinga Web 2 wizard. The progress bar at the top indicates the current step is 'Конфигурация' (Configuration). The interface is in Russian. A message box states: 'Now please configure the database resource where to store users and user groups. Note that the database itself does not need to exist at this time as it is going to be created once the wizard is about to be finished.' Below this, a green status bar says 'Конфигурация была успешно проверена.' (Configuration was successfully checked). The configuration fields are as follows:

Field	Value
Название ресурса *	icingaweb_db
Тип базы данных *	MySQL
Узел *	localhost
Порт	
Название базы данных *	icingaweb
Имя пользователя *	icinga
Пароль *	
Набор символов	
Использовать SSL	☐

At the bottom, there are three buttons: 'Назад' (Back), 'Далее' (Next), and 'Проверить конфигурацию' (Check configuration). A note at the very bottom says 'Обязательное поле *' (Required field *).

Рис. 60 – Icinga Web 2. Параметры подключения к базе данных MySQL

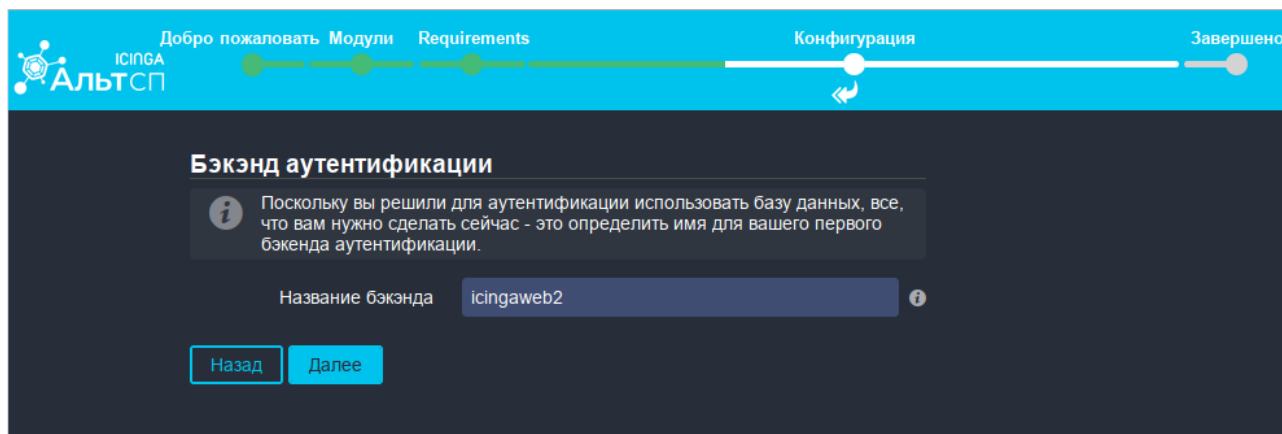
The screenshot shows the 'Источник базы данных' (Database Source) configuration step in the Icinga Web 2 wizard, but for PostgreSQL. The progress bar at the top indicates the current step is 'Конфигурация' (Configuration). The interface is in Russian. A message box states: 'Now please configure the database resource where to store users and user groups. Note that the database itself does not need to exist at this time as it is going to be created once the wizard is about to be finished.' Below this, a green status bar says 'Конфигурация была успешно проверена.' (Configuration was successfully checked). The configuration fields are as follows:

Field	Value
Название ресурса *	icingaweb_db
Тип базы данных *	PostgreSQL
Узел *	localhost
Порт *	5432
Название базы данных *	icingaweb
Имя пользователя *	icinga
Пароль *	
Набор символов	
Использовать SSL	☐

At the bottom, there are three buttons: 'Назад' (Back), 'Далее' (Next), and 'Проверить конфигурацию' (Check configuration). A note at the very bottom says 'Обязательное поле *' (Required field *).

Рис. 61 – Icinga Web 2. Параметры подключения к базе данных PostgreSQL

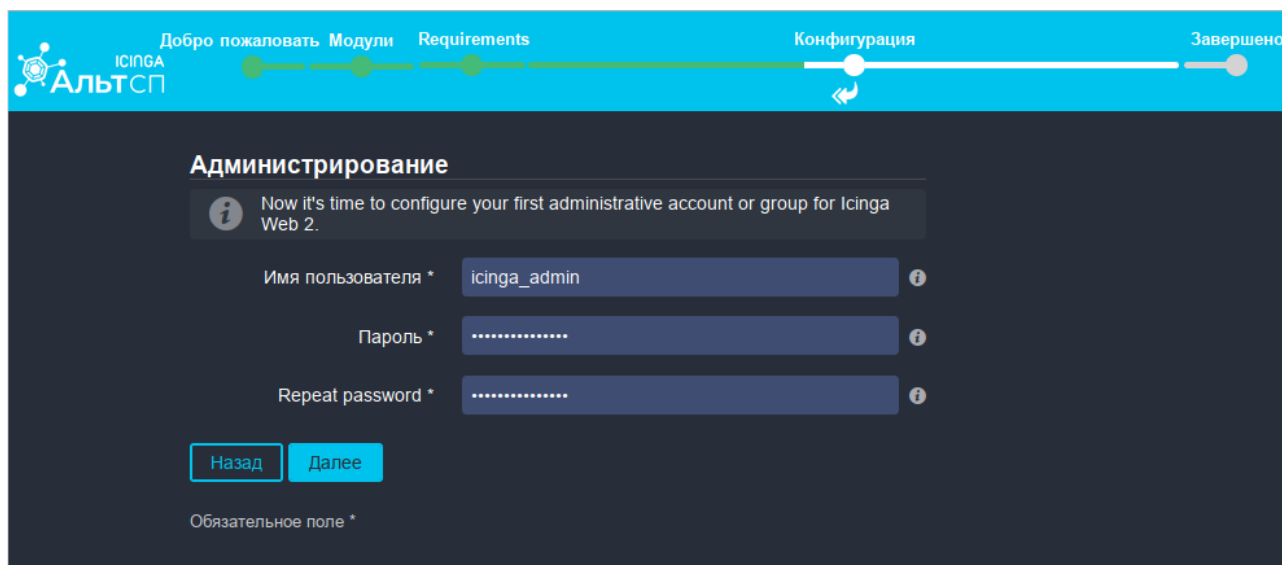
Далее нужно задать имя для бэкэнда (провайдера) аутентификации. Можно принять значение по умолчанию (рис. 62) и нажать кнопку «Далее».



The screenshot shows the Icinga Web 2 configuration wizard. At the top, a progress bar indicates the current step is 'Конфигурация' (Configuration), with previous steps being 'Добро пожаловать' (Welcome), 'Модули' (Modules), 'Requirements', and 'Завершено' (Completed). The main heading is 'Бэкэнд аутентификации' (Backend authentication). An information icon and text state: 'Поскольку вы решили для аутентификации использовать базу данных, все, что вам нужно сделать сейчас - это определить имя для вашего первого бэкэнда аутентификации.' (Since you decided to use a database for authentication, all you need to do now is determine the name for your first authentication backend). Below this, the 'Название бэкэнда' (Backend name) field is pre-filled with 'icingaweb2'. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next).

Рис. 62 – Icinga Web 2. Имя провайдера аутентификации

На следующем шаге (рис. 63) необходимо задать имя и пароль для учетной записи администратора для входа в веб-интерфейс Icinga Web 2.



The screenshot shows the next step in the Icinga Web 2 configuration wizard, titled 'Администрирование' (Administration). The progress bar remains at the 'Конфигурация' (Configuration) step. An information icon and text state: 'Now it's time to configure your first administrative account or group for Icinga Web 2.' Below this, there are three input fields: 'Имя пользователя *' (Username *) with the value 'icinga_admin', 'Пароль *' (Password *) with masked characters, and 'Repeat password *' with masked characters. Each field has an information icon to its right. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next). A note at the bottom left states 'Обязательное поле *' (Required field *).

Рис. 63 – Icinga Web 2. Учетная запись администратора веб-интерфейса

Параметры конфигурации веб-приложения Icinga Web 2, предложенные на следующем шаге (рис. 64), можно оставить по умолчанию.

Добро пожаловать Модули Requirements **Конфигурация** Завершено

Конфигурация приложения

Now please adjust all application and logging related configuration options to fit your needs.

Показать стеки ☒

Показывать сообщения о состоянии приложения ☒

Enable strict content security policy ☐

Тип журнала * Syslog

Уровень логирования * Ошибка

Префикс приложения * icingaweb2

Объект * user

Назад Далее

Обязательное поле *

Рис. 64 – Icinga Web 2. Конфигурация приложения

На следующем шаге будет выведено сообщение об успешной конфигурации Icinga Web 2 со сводной информацией по определенным ранее параметрам (рис. 65).

Добро пожаловать Модули Requirements **Конфигурация** Завершено

Настройка базы данных

The database user "icinga" will be used to setup the missing schema required by Icinga Web 2 in database "icingaweb".

Конфигурация приложения

Общее

- Стек трассировки исключений показывается каждому пользователю по умолчанию.
- Preferences will be stored using a database.

Логирование

Тип	Syslog
Уровень	Ошибка
Префикс приложения	icingaweb2

Аутентификация

Пользователи будут аутентифицироваться с помощью база данных.

Бэкэнд аутентификации

Название бэкэнда	icingaweb2

Администрирование

Административные права будут первоначально предоставлены новой учетной записи "icinga_admin".

Ресурс

База данных

Название ресурса	icingaweb_db
Тип базы данных	mysql
Узел	localhost
Порт	
Название базы данных	icingaweb
Имя пользователя	icinga
Пароль	*****

Назад Далее

Рис. 65 – Icinga Web 2. Сообщение об успешной конфигурации сервера

Следующие шаги – настройка модуля monitoring. Сначала настраиваются параметры подключения к базе данных мониторинга (рис. 66, рис. 67):

- «Название ресурса» – имя ресурса данных;
- «Тип базы данных» – MySQL или PostgreSQL;
- «Узел» – узел, на котором расположена база данных;

⚠ В качестве сервера базы данных используется ПЭВМ 64 бит (x86_64)/ AArch64 (ARMv8) с установленной ОС Альт СП Рабочая станция/Сервер релиз 10, поэтому вместо localhost необходимо указывать IP-адрес ПЭВМ, на которой развернута база данных.

- «Порт» – порт для подключения к базе данных (при подключении к MySQL можно не указывать);
- «Название базы данных» – имя базы данных (icinga);
- «Имя пользователя» – имя пользователя для доступа к базе данных (icinga);
- «Пароль» – пароль пользователя.

Добро пожаловать Модули Requirements Конфигурация Завершено

Monitoring IDO Resource

Please fill out the connection details below to access the IDO database of your monitoring environment.

Конфигурация была успешно проверена.

Журнал проверки

```
Connection to icinga as icinga on localhost: successful
have_ssl: DISABLED
protocol_version: 10
version: 10.6.16-MariaDB-alt1
version_compile_os: Linux
```

Название ресурса *

Тип базы данных *

Узел *

Порт

Название базы данных *

Имя пользователя *

Пароль *

Набор символов

Использовать SSL ☐

Обязательное поле *

Рис. 66 – Icinga Web 2. Настройка модуля monitoring (MySQL)

Добро пожаловать Модули Requirements Конфигурация Завершено

Monitoring IDO Resource

Please fill out the connection details below to access the IDO database of your monitoring environment.

Конфигурация была успешно проверена.

Журнал проверки

Connection to icinga as icinga on localhost:5432 successful
PostgreSQL 16.4 on x86_64-alt-linux-gnu, compiled by x86_64-alt-linux-gcc (GCC) 10.3.1 20210703 (ALT c10f2 10.3.1-alt2), 64-bit

Название ресурса * icinga_ido

Тип базы данных * PostgreSQL

Узел * localhost

Порт * 5432

Название базы данных * icinga

Имя пользователя * icinga

Пароль *

Набор символов

Использовать SSL ☐

Назад Далее Проверить конфигурацию

Обязательное поле *

Рис. 67 – Icinga Web 2. Настройка модуля monitoring (PostgreSQL)

Для проверки конфигурации следует нажать кнопку «Проверить конфигурацию». Если проверка прошла успешно, можно переходить к следующему шагу.

Далее настраивается способ управления Icinga через Icinga Web 2 (рис. 68). Необходимо указать следующие данные:

- «Имя транспорта» – имя транспорта;
- «Тип транспорта» – в данном руководстве используется API (Icinga2 API);
- «Узел» – узел Icinga (так как Icinga и Icinga Web 2 находятся на одном сервере, поэтому можно указать localhost);
- «Порт» – порт Icinga API по умолчанию (5665);
- «Имя пользователя API» – имя пользователя для подключения к API (root);
- «Пароль API» – пароль для подключения к API.

Примечание. Имя и пароль для подключения к API указаны в файле /etc/icinga2/conf.d/api-users.conf.

Добро пожаловать Модули Requirements Конфигурация Завершено

Транспорт команд

Please define below how you want to send commands to your monitoring instance.

Конфигурация была успешно проверена.

Имя транспорта * icinga2

Тип транспорта * API Icinga 2

Узел * localhost

Порт * 5665

Имя пользователя API * root

Пароль API *

Назад Далее Проверить конфигурацию

Обязательное поле *

Рис. 68 – Icinga Web 2. Настройка способа управления Icinga через Icinga Web 2

Проверить возможность подключения можно, нажав на кнопку «Проверить конфигурацию».

На следующем шаге (рис. 69) можно задать список названий переменных для полей в разных веб-формах, в которых может отображаться парольная информация. Значения в таких полях будут отображать в виде «звездочек».

Добро пожаловать Модули Requirements Конфигурация Завершено

Monitoring Security

Чтобы защитить вашу среду мониторинга от посторонних глаз, пожалуйста, заполните настройки ниже.

Защищенные пользовательские переменные *pw*,*pass*,community

Назад Далее

Рис. 69 – Icinga Web 2. Защищенные пользовательские переменные

На последнем шаге конфигурации (рис. 70) отображается суммарная информация о конфигурации модуля мониторинга.

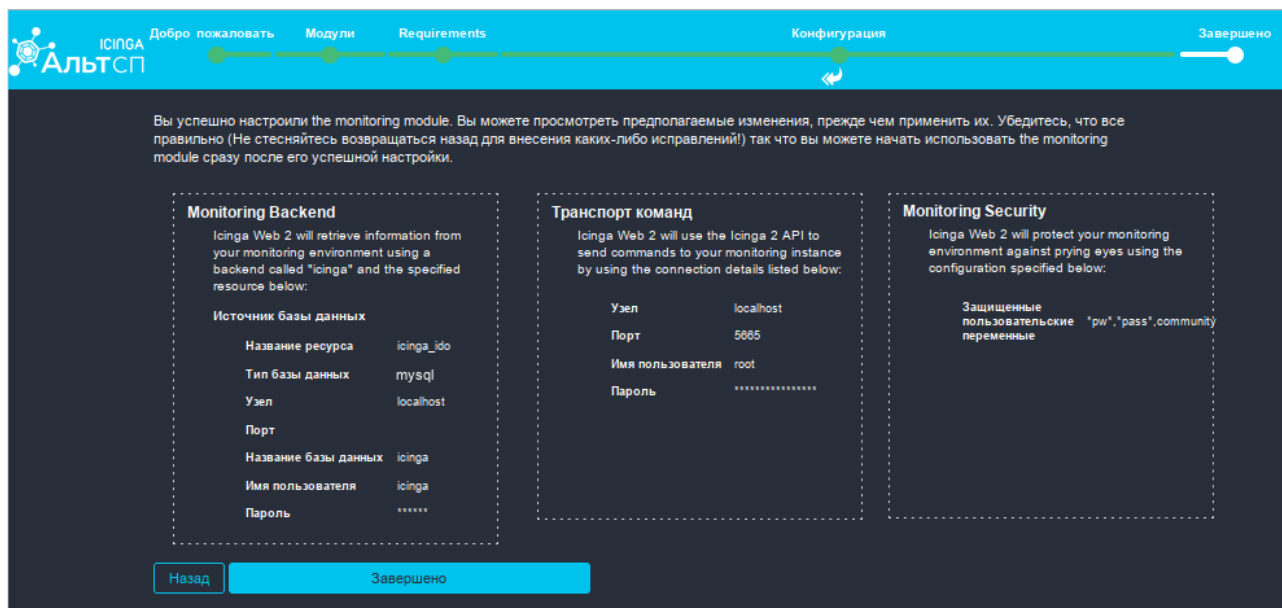


Рис. 70 – Icinga Web 2. Суммарная информация о конфигурации модуля мониторинга

После нажатия кнопки «Завершено» будет выведен краткий лог (рис. 71) и будет доступна кнопка перехода в веб-интерфейс («Login to Icinga Web 2»).

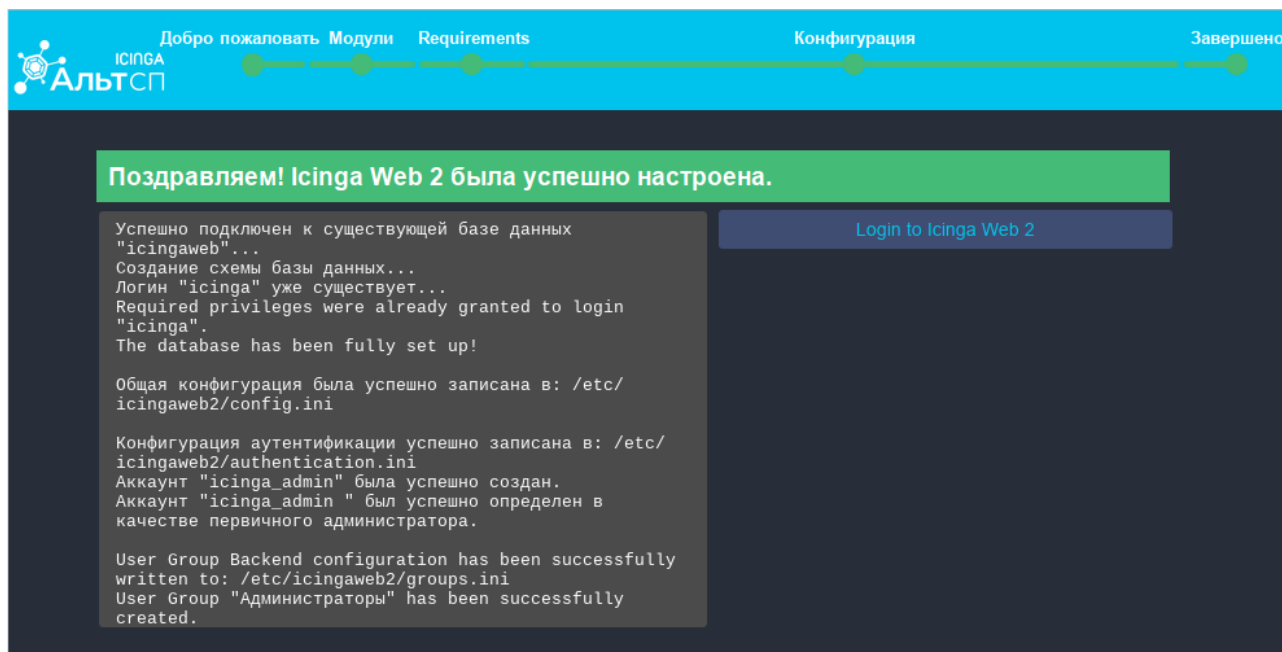


Рис. 71 – Icinga Web 2. Завершение настройки

Для входа в Icinga Web 2 (рис. 72) следует использовать учетные данные административного пользователя (в примере `icinga_admin`). В результате откроется сводная панель информации Icinga Web 2 (рис. 73) с информацией о состоянии базовых показателей мониторинга сервера.

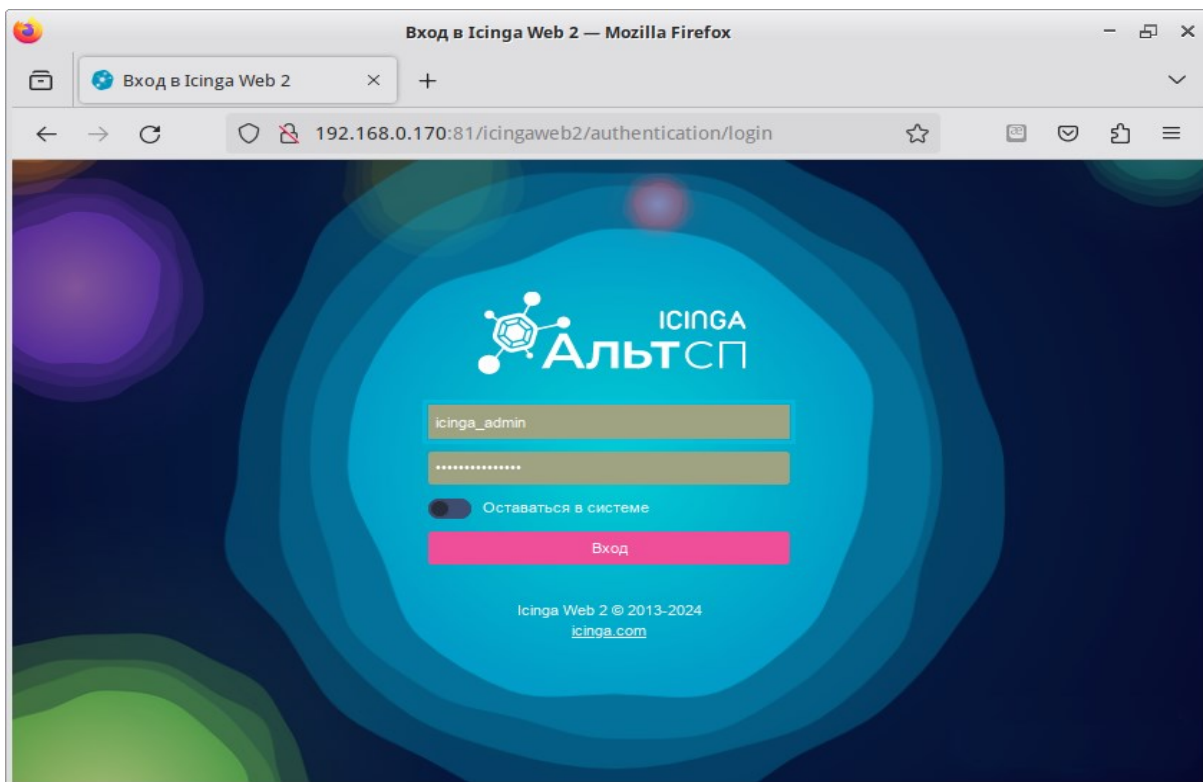


Рис. 72 – Вход в Icinga Web 2

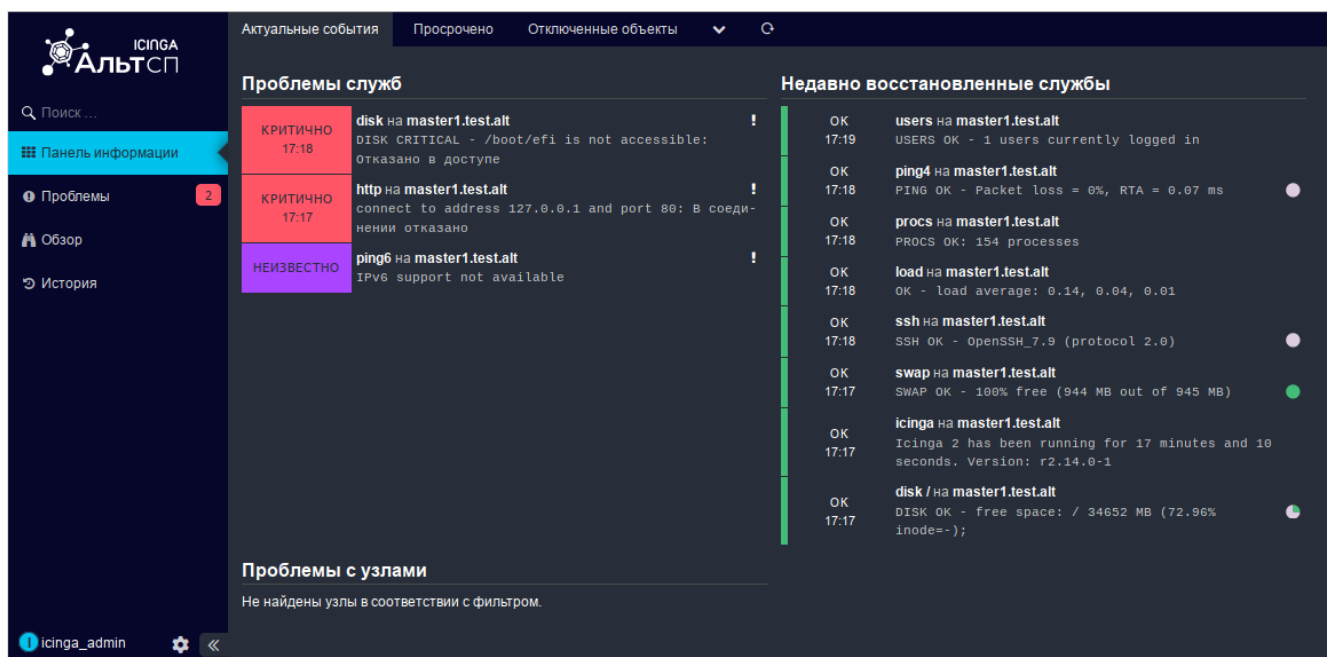


Рис. 73 – Панель информации Icinga Web 2

7.7.2. Настройка агентов

7.7.2.1. Установка пакетов

Установить пакеты `icinga2`, `nagwad-service`, `nagwad-audit` и `nagwad-icinga-agent`:

```
# apt-get install icinga2 nagwad-service nagwad-audit nagwad-icinga-agent
```

Включить в автозагрузку и запустить службу `nagwad.service`:

```
# systemctl enable --now nagwad.service
```

Включить в автозагрузку и запустить службу `icinga2.service`:

```
# systemctl enable --now icinga2.service
```

7.7.2.2. Настройка объектов наблюдения

Если для настройки объектов наблюдения используется Icinga Director (см. п. 7.7.3.2), то можно воспользоваться готовой корзиной (basket) шаблонов в формате JSON для наблюдения за событиями Nagwad из пакета `nagwad-icinga-master`.

Можно как добавлять конфигурацию каждого узла вручную, так и воспользоваться функцией API самообслуживания Icinga Director (см. п. 7.7.3.2.7).

В пакете `icinga2` также определены шаблоны конфигурации, пригодные для определения объектов наблюдения в конфигурационных файлах Icinga.

Шаблоны подготовлены для отслеживания следующих событий, фиксируемых `nagwad.service`:

- «Unauthorized file access» – несанкционированный доступ к файлам;
- «Unauthorized user or group change» – несанкционированное изменение файлов `/etc/passwd` и `/etc/group`;
- «Unauthorized device access» – несанкционированное подключение устройства;
- «Illegal login attempt» – неудачная попытка аутентификации;
- «System integrity violated» – нарушение целостности системы;
- «Printing policy violation attempt» – попытка нарушения политики печати.

7.7.2.2.1. Настройка политики печати

Поставляемый с пакетом nagwad фильтр событий печати `/etc/nagwad/print.regex` рассчитан на то, что служба печати cups будет:

- проверять права доступа при печати;
- записывать в журнал сообщения об отказе по причине нехватки прав.

Для этого службу печати необходимо настроить следующим образом:

- в конфигурационном файле `/etc/cups/cups-files.conf` установить:

```
AccessLog syslog
```

- в главном конфигурационном файле `/etc/cups/cupsd.conf` повысить уровень сообщений о нарушении доступа с `warn` до `info`:

```
LogLevel info
```

- в этом же файле ограничить доступ к операциям печати, например, разрешив их конкретному пользователю:

```
<Limit Create-Job Print-Job Print-URI Validate-Job>
  Require user имя-пользователя
  Order deny,allow
</Limit>
```

- перезапустить службу cups:

```
# systemctl restart cups
```

7.7.2.2.2. Сервис контроля целостности

Чтобы иметь возможность отслеживать нарушения целостности системных файлов должен быть установлен пакет `integalert`.

Выполнить настройку наблюдаемых файлов и каталогов, проинициализировать базу данных, выполнив команду:

```
# integalert fix
```

Включить и запустить службу:

```
# systemctl enable --now integalert.service
```

7.7.2.3. Служба наблюдения за системным журналом Nagwad

7.7.2.3.1. Состав

Основными компонентами пакета `nagwad` являются:

- системная служба `nagwad`, сканирующая системный журнал с помощью набора фильтров `/etc/nagwad/*.regex`, `/etc/nagwad/*.sed` (либо

простые регулярные выражения для `grep`, либо полнофункциональные скрипты `sed`);

- сценарии пост-фильтрации событий в `/etc/nagwad/filter-event.d`;
- сценарии пост-обработки событий в `/etc/nagwad/process-event.d`;
- NRPE-скрипт `check_nagwad`, который проверяет файлы сигналов событий в каталогах `/var/log/nagwad/<boot_id>/<filter>/`, где `boot_id` это текущий системный идентификатор загрузки (`/proc/sys/kernel/random/boot_id`);
- служебный скрипт `nagwad`, который позволяет запрашивать, проверять и управлять сигнальными файлами событий.

Дополнения для различных систем мониторинга включают в себя следующие компоненты:

- шаблоны конфигурации для агента мониторинга Icinga2;
- шаблоны конфигурации для агента мониторинга Nagios;
- скрипты для интерфейса мониторинга Nagstamon;
- оболочка оболочки `nscd-shell` с ведением журнала, которую можно использовать для удаленного доступа.

7.7.2.3.2. Принцип работы

Как только какой-либо из настроенных фильтров определяет сообщение из системного журнала, `nagwad` генерирует событие, которое затем передается сценариям в каталоге `filter-event.d`. Сценарии могут дать ответный сигнал `nagwad` о том, нужно ли пропустить или проигнорировать данное событие. Сценарии также могут добавить произвольный текст к сообщению о событии.

Если событие не игнорируется, то соответствующий сигнальный файл записывается в каталог `/var/log/nagwad/<boot_id>/<filter>/`.

Имя сигнального файла соответствует шаблону `<filter>.<HASH>.<LEVEL>`.

NRPE-совместимый агент мониторинга может проверить этот файл с помощью сценария `check_nagwad`.

При проверке сигнальных файлов скрипт игнорирует файлы со специальным суффиксом `.FIXED`. Это позволяет пометать зарегистрированные события как

разрешенные (либо с помощью команды `nagwad fix`, либо просто переименованием файла).

В дополнение к этому, данные о каждом событии передаются в скрипты в каталоге `process-event.d`.

7.7.2.3.3. Параметры конфигурации

Описание параметров конфигурации `nagwad` (файл `/etc/nagwad/nagwad.conf`) представлено в таблице 6.

Т а б л и ц а 6 – Описание конфигурационных параметров службы `nagwad`

Параметр	Описание	Значение по умолчанию
PIDFILE	Путь к PID-файлу, записываемому при запуске службы <code>nagwad</code>	<code>/run/nagwad.pid</code>
LOG_USER	Имя системного пользователя, которому принадлежат сигнальные файлы	<code>root</code>
LOG_GROUP	Имя системной группы, имеющей доступ на чтение для сигнальных файлов	<code>nagwad</code>
CONFDIR	Путь к каталогу конфигурации	<code>/etc/nagwad</code>
POSTFILTERS	Путь к каталогу для скриптов пост-фильтрации	<code>\$CONFDIR/filter-event.d</code>
POSTPROCESS	Путь к каталогу для скриптов пост-обработки	<code>\$CONFDIR/process-event.d</code>
LOGDIR	Путь к корневому каталогу журнала	<code>/var/log/nagwad</code>
MAXAGE	Количество дней, по истечении которых старые сигнальные файлы будут удалены	<code>30</code>
JOURNAL_TAIL	Количество сообщений, которые считываются из системного журнала при запуске и перезапуске <code>nagwad</code>	<code>5000</code>

Примечание. Если для параметра `MAXAGE` в файле `/etc/nagwad/nagwad.conf` установлено отличное от 0 значение, то при запуске `nagwad` удаляет все каталоги `/var/log/nagwad/*`, возраст которых превышает `MAXAGE`.

7.7.2.3.4. Команда `nagwad`

Синтаксис:

`nagwad` [опции] [команда]

Описание команд `nagwad` приведено в таблице 7.

Т а б л и ц а 7 – Описание команд nagwad

Команда	Описание
[list]	Просмотр списка зарегистрированных событий
[show] EVENT-ID	Просмотр информации о конкретном событии
fix EVENT-ID [EVENT-ID ...]	Пометить событие как исправленное
check [FILTER]	Проверить все события или события по определенному фильтру
status	Вывести статус службы nagwad
cleanup-old [DAYS]	Удалить события старше, указанного количества дней

Примеры использования команды nagwad:

- запуск в качестве системной службы:

```
# nagwad --service
```

- просмотр списка зарегистрированных событий:

```
# nagwad
```

```
2024-07-03+12:20:02.2161021330 login.c15459dac0fecba98fe27bfad170b3ba.WARNING
2024-07-03+12:20:35.7491051260
authdata.4d95e2fedcef82ca3e2dcbb062f3bd1c.CRITICAL
```

- просмотр информации о событии:

```
# nagwad show login.c15459dac0fecba98fe27bfad170b3ba.WARNING
WARNING: 2024-07-03T12:20:01+0200 agent4.test.alt audit[11506]:
USER_AUTH pid=11506 uid=0 auid=4294967295 ses=4294967295
msg='op=PAM:authentication grantors=? Acct="?" exe="/bin/login"
hostname=agent4.test.alt addr=? Terminal=/dev/tty2 res=failed'
```

- пометить событие как исправленное:

```
# nagwad fix authdata.4d95e2fedcef82ca3e2dcbb062f3bd1c.CRITICAL
```

- проверить события authdata:

```
# nagwad check authdata
```

```
CRITICAL: 2024-07-03T12:20:35+0200 agent4.test.alt audit[11815]:
SYSCALL arch=c000003e syscall=82 success=yes exit=0 a0=7fff2457ee60
a1=55873eafa900 a2=7fff2457edd0 a3=1f5 items=5 ppid=4114 pid=11815
auid=500 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
tty=pts0 ses=5 comm="useradd" exe="/usr/sbin/useradd" key="usergroup-
change"
```

- удалить события старше двух дней:

```
# nagwad cleanup-old 2
```

7.7.2.3.5. Некоторые скрипты пост-фильтрации

Скрипт фильтрации `/etc/nagwad/filter-event.d/10-eperm` используется для дополнительной фильтрации событий ошибочного доступа к файлам (EACCES

у процесса `systemd` при загрузке системы). Он использует файлы `.regex` из каталога `/etc/nagwad/filter-event.d/eperm-skip.d`, для определения того, какие события нужно пропустить. К событию, которое проходит пост-фильтр 10-`eperm`, добавляется строка:

```
PATH=<путь>
```

где `<путь>` – это фактический путь к файлу, в доступе к которому было отказано.

7.7.2.3.6. Добавление новых проверок

7.7.2.3.6.1. Добавление новых фильтров журнала событий

Начиная с версии 0.10.0 `nagwad` автоматически обрабатывает все `*.regex` и `*.sed` файлы в каталоге `/etc/nagwad`.

В файлах формата `*.regex` определяются регулярные выражения для отслеживания сообщений системного журнала. Файл может содержать сразу несколько регулярных выражений – по одному выражению на строке. Событие формируется если обнаруживается совпадение с любым из определенных выражений. Базовое имя записываемого `nagwad` сигнального файла определяется базовым именем файла с суффиксом `.regex`. Оно же определяет имя фильтра, которое используется для проверки сигнального файла из `Icinga2` или `Nagios`.

Файлы формата `*.sed` являются полноценными сценариями, предназначенными для программы `sed` (см. `man sed(1)` и `info sed`). В отличие от простого набора регулярных выражений, использование сценариев `sed` позволяет:

- модифицировать сообщения системного журнала;
- фиксировать различные «уровни критичности» события для различных сообщений.

Программа `sed` запускается из `nagwad` с аргументом `-n`, что позволяет использовать `sed` прежде всего как фильтр сообщений. Каждое отфильтрованное сценарием сообщение системного журнала должно после обработки принимать вид:

```
<имя_фильтра>:<ВАЖНОСТЬ>:<сообщение>
```

где «имя_фильтра» определяет базовое имя записываемого `nagwad` сигнального файла. Например, подстановку вида `s//myevent:CRITICAL:&/p`

удобно использовать после предварительной фильтрации сообщений системного журнала для того, чтобы транслировать отфильтрованное сообщение без изменений как критическое событие, которое будет записано в сигнальный файл `/var/log/nagwad/<boot_id>/<filter>/filterXXX.CRITICAL`. В Icinga2 это событие будет отражено как критичное.

При необходимости, вместо уровня `CRITICAL` можно использовать уровень `WARNING`, отображающийся в Icinga и Nagios как предупреждение. Другие уровни сообщений Icinga и Nagios не поддерживают.

7.7.2.3.6.2. Фильтры пост-обработки событий

Кроме фильтров для первичной обработки событий (то есть для их фильтрации из системного журнала), начиная с версии 0.10.1 nagwad поддерживает дополнительные фильтры для пост-обработки отфильтрованных событий. Сценарии для пост-обработки помещаются в каталог `/etc/nagwad/filter-event.d` и выполняются для каждого события в алфавитном порядке.

Каждый сценарий пост-обработки запускается с тремя аргументами:

```
<сценарий> FILTER STATUS MESSAGE
```

где:

- `FILTER` — имя фильтра, зафиксировавшего событие;
- `STATUS` — уровень критичности события (`CRITICAL` или `WARNING`);
- `MESSAGE` — сообщение.

На основе этих данных сценарий должен вынести решение пропустить данное событие дальше или «отбросить» его. Для этой цели используется код завершения работы сценария (exit code):

- 0 — означает, что событие можно пропускать дальше;
- `$NAGWAD_SKIP_EVENT` — означает, что событие должно быть отброшено (переменная `NAGWAD_SKIP_EVENT` передается из nagwad в окружение сценария);
- любое другое значение сигнализирует о сбое в работе сценария (однако событие пропускается дальше).

Если очередной сценарий из каталога `/etc/nagwad/filter-event.d` завершается со значением `$NAGWAD_SKIP_EVENT`, дальнейший вызов сценариев пост-обработки прекращается.

7.7.3. Управление конфигурацией

Управление конфигурацией клиентов Icinga может выполняться разными способами:

- с помощью веб-инструмента Icinga Director. Реализует управление всеми конфигурационными файлами через веб-интерфейс Icinga Web 2;
- ручная настройка посредством редактирования конфигурационных файлов (более гибкий способ).

Примечание. Настоятельно рекомендуется использовать файлы конфигурации или Director. Смещение вариантов может привести к конфликтам имен, труднообнаружимым проблемам или любому другому неожиданному поведению. Комбинирование данных способов возможно в некоторых нетривиальных сценариях, при этом необходимо учитывать:

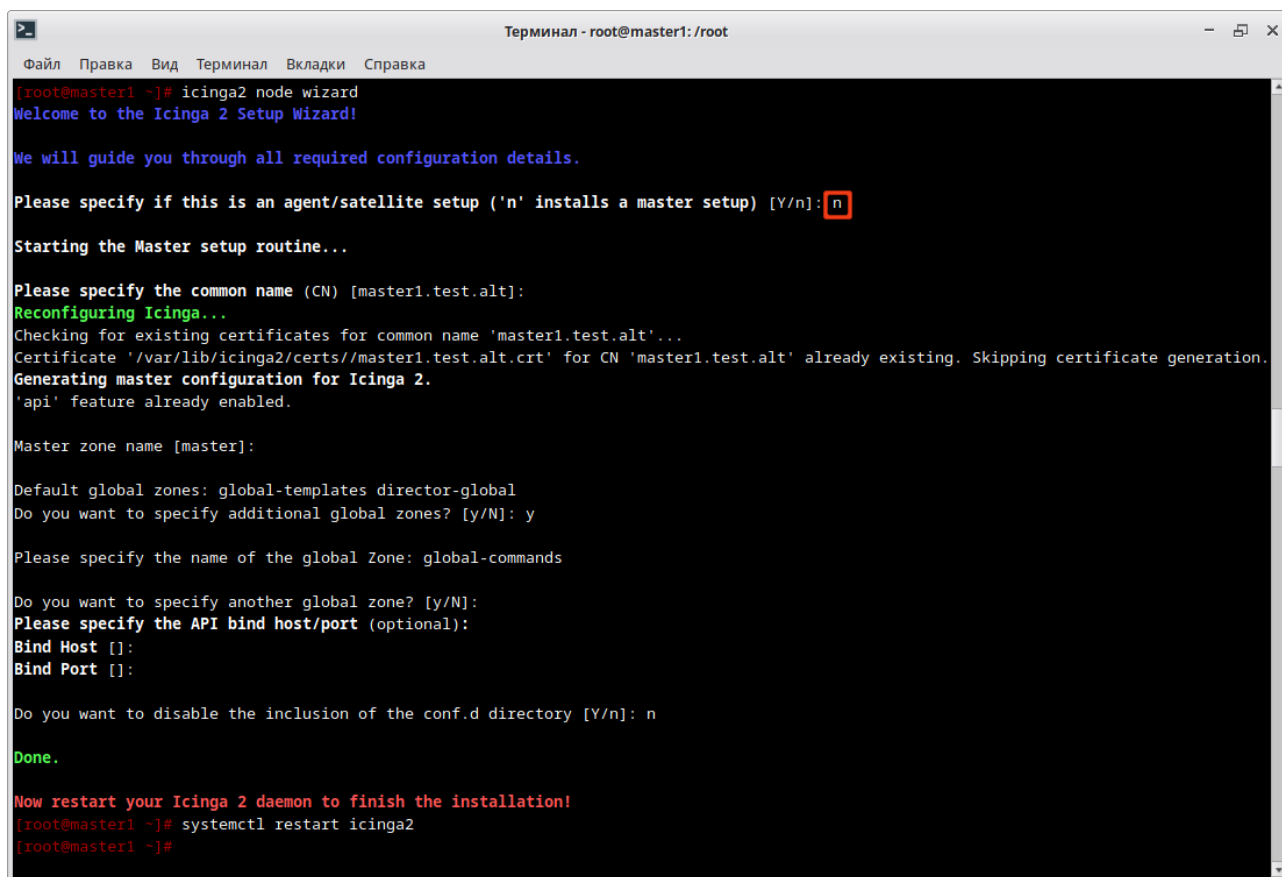
- объекты из файлов конфигурации не видны и не редактируются внутри Director;
- наименование объектов, которые предназначены для ручной настройки и объектов, которые предназначены для Icinga Director должны различаться;
- если что-то было добавлено/изменено в файлах конфигурации, перед развертыванием нужно проверить конфигурацию, выполнив команду `icinga2 daemon -C`
- при создании объектов с одинаковыми именами в файлах конфигурации, и Director не предупредит о наличии дубликата, до момента разворачивания конфигурации.

Далее будут рассмотрены оба способа.

7.7.3.1. Ручная конфигурация

7.7.3.1.1. Конфигурирование Мастер-узла

На сервере мониторинга, где развернуты Icinga2 и Icinga Web 2, необходимо запустить мастер конфигурирования узла, выполнив команду `icinga2 node wizard` (рис. 74).



```
Терминал - root@master1: /root
Файл  Правка  Вид  Терминал  Вкладки  Справка
[root@master1 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]: n

Starting the Master setup routine...

Please specify the common name (CN) [master1.test.alt]:
Reconfiguring Icinga...
Checking for existing certificates for common name 'master1.test.alt'...
Certificate '/var/lib/icinga2/certs/master1.test.alt.crt' for CN 'master1.test.alt' already existing. Skipping certificate generation.
Generating master configuration for Icinga 2.
'api' feature already enabled.

Master zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Do you want to disable the inclusion of the conf.d directory [Y/n]: n

Done.

Now restart your Icinga 2 daemon to finish the installation!
[root@master1 ~]# systemctl restart icinga2
[root@master1 ~]#
```

Рис. 74 – Настройка ведущего узла

В ответах можно принять значения по умолчанию (можно просто нажать клавишу Enter) или ввести свои ответы. Важно при ответе на первый вопрос ввести «n», чтобы перевести мастер настройки в режим настройки Мастер-узла. При ответе на вопрос Do you want to specify additional global zones? [y/N]: следует ответить «y» и при ответе на следующий вопрос Please specify the name of the global Zone: указать зону global-commands.

Описание остальных параметров приведено в таблице 8.

Примечание. Для возможности использования шаблонов generic-host нужно НЕ отключать чтение файлов из conf.d при первичной настройке узла (ответить «n» на вопрос «Do you want to disable the inclusion of the conf.d directory [Y/n]:»).

Т а б л и ц а 8 – Описание параметров

Параметр	Описание
Common name (CN)	Используется для генерации SSL-сертификата, который будет использоваться для защиты соединений между сервером и его клиентами. По умолчанию в качестве CN предлагается FQDN-имя сервера
Master zone name	Имя мастер-зоны. По умолчанию master
Global zones	Позволяет указать дополнительные глобальные зоны в дополнение к глобальным шаблонам и глобальному директору. По умолчанию N
API bind host	Адрес, к которому привязан ApiListener. Только для расширенного использования
API bind port	Порт, к которому привязан ApiListener. Только для расширенного использования
Disable conf.d	Позволяет отключить директиву include_recursive «conf.d», за исключением файла api-users.conf в файле icinga2.conf

Пример конфигурирования Мастер-узла:

```
# icinga2 node wizard
```

```
Welcome to the Icinga2 Setup Wizard!
```

```
We will guide you through all required configuration details.
```

```
Please specify if this is an agent/satellite setup ('n' installs
a master setup) [Y/n]: n
```

```
Starting the Master setup routine...
```

```
Please specify the common name (CN) [master1.test.alt]:
```

```
Reconfiguring Icinga...
```

```
Checking for existing certificates for common name
'master1.test.alt'...
```

```
Certificate '/var/lib/icinga2/certs//master1.test.alt.crt' for CN
'master1.test.alt' already existing. Skipping certificate generation.
```

```
Generating master configuration for Icinga2.
```

```
'api' feature already enabled.
```

```
Master zone name [master]:
```

```
Default global zones: global-templates director-global
```

```
Do you want to specify additional global zones? [y/N]: y
```

```
Please specify the name of the global Zone: global-commands
```

Please specify the API bind host/port (optional):

Bind Host []:

Bind Port []:

Do you want to disable the inclusion of the conf.d directory
[Y/n]: n

Done.

Now restart your Icinga2 daemon to finish the installation!

Примечание. Так как процедура активации Icinga API уже была запущена ранее (команда `icinga2 api setup`), то уже тогда был создан локальный центр сертификации (certificate authority) и сгенерирован SSL-сертификат для сервера (в каталоге `/var/lib/icinga2/certs/`). Поэтому в данном случае мастер конфигурирования узла обнаружит этот сертификат. Мастер также обнаружит, что поддержка API в Icinga уже включена.

После окончания конфигурации необходимо перезапустить сервис Icinga2:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле будет добавлена в файл
`/etc/icinga2/zones.conf`:

```
object Endpoint "master1.test.alt" {
}

object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}

object Zone "global-templates" {
    global = true
}

object Zone "director-global" {
    global = true
}

object Zone "global-commands" {
    global = true
}
```

7.7.3.1.2. Конфигурирование агента

Все сертификаты агентов должны быть подписаны одним и тем же центром сертификации (CA). Это гарантирует, что все узлы доверяют друг другу в распределенной среде мониторинга.

Избежать подписания и развертывания сертификатов вручную можно, используя встроенные методы автоматического подписания запросов на подпись сертификатов (CSR):

- автоматическое подписание CSR – использует билет клиента (агента или спутника), сгенерированный на мастер-узле, в качестве идентификатора доверия;
- подписание CSR по требованию – позволяет подписывать ожидающие запросы сертификатов на мастер-узле.

7.7.3.1.2.1. Автоматическое подписание CSR

В этом сценарии агент отправляет запрос на подпись сертификата (CSR) и должен пройти аутентификацию доверенным способом. Мастер генерирует билет клиента, который включается в этот запрос. Таким образом, мастер может проверить, что запрос соответствует ранее доверенному билету, и подписать запрос.

Получить билет можно двумя способами:

- выполнить команду на мастер-узле;
- выполнить запрос REST API к мастер-узлу.

Пример генерации билета на мастер-узле:

```
# icinga2 pki ticket --cn 'agent1.test.alt'
84bffc6d33eccbbbd9b2ec6130031cef1d68ac01
```

где agent1.test.alt – FQDN добавляемого агента.

Пример генерации билета с выполнением запроса REST API:

```
# curl -k -s -u root:df0a9ffdbb104326 -H 'Accept: application/json' \
-X POST 'https://localhost:5665/v1/actions/generate-ticket' \
-d '{ "cn": "agent1.test.alt" }'
{"results":[{"code":200,"status":"Generated          PKI          ticket
'526ac5033f52716feddf1271eca8a18df2cd7584'          for          common          name
'agent1.test.alt'.", "ticket": "526ac5033f52716feddf1271eca8a18df2cd7584"}]}
```

где:

- root – имя пользователя для подключения к API;
- df0a9ffdbb104326 – пароль для подключения к API;
- agent1.test.alt – FQDN добавляемого агента.

Примечание. Для запроса API Icinga2 на мастер-узле требуется объект API User как минимум с разрешением на создание билета (actions/generate-ticket). Создать данное разрешение можно, добавив следующие строки в файл /etc/icinga2/conf.d/api-users.conf:

```
object ApiUser "client-pki-ticket" {  
    password = "333beabb8fd23e6e9" //change this  
    permissions = [ "actions/generate-ticket" ]  
}
```

После внесения изменений в файл /etc/icinga2/conf.d/api-users.conf необходимо перезапустить службу:

```
# systemctl restart icinga2
```

Сгенерированный на мастер-узле билет необходимо будет использовать на агенте во время установки.

Запустить мастер конфигурирования узла на агенте можно, выполнив команду (рис. 75):

```
# icinga2 node wizard
```

В ответах можно принять значения по умолчанию (можно нажать клавишу <Enter>) или ввести свои ответы. При ответе на первый вопрос можно нажать клавишу <Enter>, чтобы перевести мастер настройки в режим настройки агента. При ответе на вопрос Do you want to specify additional global zones? [y/N]: следует ответить «у» и при ответе на следующий вопрос Please specify the name of the global Zone: указать зону global-commands. Описание остальных параметров приведено в таблице 9.

```

Терминал - root@agent1: /root
Файл  Правка  Вид  Терминал  Вкладки  Справка
[root@agent1 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent1.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:
Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:
Please specify the master/satellite connection information:
Master/Satellite endpoint host (IP address or FQDN): master1.test.alt
Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:
Parent certificate information:

Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul  1 07:11:38 2024 GMT
Valid Until:      Aug  2 07:11:38 2025 GMT
Serial:           c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a

Signature Algorithm: sha256WithRSAEncryption
Subject Alt Names:  master1.test.alt
Fingerprint:       19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90 52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga 2 master (optional).
(Hint: # icinga2 pki ticket --cn 'agent1.test.alt': 84bffc6d33ecb9b2ec6130031cef1d68ac01
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Accept config from parent node? [y/N]: y
Accept commands from parent node? [y/N]: y

Reconfiguring Icinga...
Disabling feature notification. Make sure to restart Icinga 2 for these changes to take effect.
Enabling feature api. Make sure to restart Icinga 2 for these changes to take effect.

Local zone name [agent1.test.alt]:
Parent zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Do you want to disable the inclusion of the conf.d directory [Y/n]:
Disabling the inclusion of the conf.d directory...

Done.

Now restart your Icinga 2 daemon to finish the installation!
[root@agent1 ~]#

```

Рис. 75 – Регистрация агента

Примечание. Для возможности использования шаблонов generic-host и nagwad-host с мастер-узла (см. п. 7.7.3.1.4), нужно отключить чтение файлов из conf.d (нажать Enter на вопрос Do you want to disable the inclusion of the conf.d directory [Y/n]:). Если же планируется использование шаблонов с агента, нужно НЕ отключать чтение файлов из conf.d при первичной настройке узла (ответить «n» на вопрос Do you want to disable the inclusion of the conf.d directory [Y/n]:). Данное значение можно будет изменить и после настройки узла.

Т а б л и ц а 9 – Описание параметров команды конфигурации агента

Параметр	Описание
Common name (CN)	Используется для генерации SSL-сертификата. По умолчанию используется FQDN-имя агента
Master/Satellite Common Name	Имя мастер-зоны. Необходимо указать имя, заданное на Мастер-узле
Establish connection to the parent node	Должен ли узел пытаться подключиться к родительскому узлу или нет. По умолчанию <code>y</code>
Master/Satellite endpoint host	Требуется, если агенту необходимо подключиться к главному/спутнику. IP-адрес или полное доменное имя родительской конечной точки. Эта информация будет включена в конфигурацию объекта Endpoint в файле <code>Zones.conf</code>
Master/Satellite endpoint port	Необязательно, если агенту необходимо подключиться к главному/спутнику. Порт прослушивания родительских конечных точек. Эта информация включена в конфигурацию объекта Endpoint
Add more master/satellite endpoints	Если настроено несколько Мастер-узлов, необходимо указать их здесь
Parent Certificate information	Информация о Мастер-узле. Следует убедиться, что подключающийся хост действительно является запрошенным главным узлом. Отпечаток ключа мастер-узла можно узнать, выполнив на Мастер-узле команду: # openssl x509 -noout -fingerprint -sha256 -in \ "/var/lib/icinga2/certs/\$(hostname --fqdn).crt"
Request ticket	Билет, сгенерированный на мастере
API bind host	Адрес, к которому привязан ApiListener. Только для расширенного использования
API bind port	Порт, к которому привязан ApiListener. Только для расширенного использования
Accept config from parent node?	Принимает ли этот узел синхронизацию конфигурации от главного узла (требуется для режима синхронизации конфигурации). По соображениям безопасности по умолчанию установлено значение <code>n</code> .
Accept commands from parent node?	Принимает ли этот узел сообщения о выполнении команд от главного узла (требуется для режима конечной точки команды). По соображениям безопасности по умолчанию установлено значение <code>n</code>
Local zone name	Позволяет указать имя локальной зоны, когда этот экземпляр является спутником, а не агентом. По умолчанию используется FQDN-имя
Parent zone name	Позволяет указать имя родительской зоны. Это важно, если у агента родительским экземпляром является вспомогательный, а не главный. По умолчанию <code>master</code>
Global zones	Позволяет указать дополнительные глобальные зоны в дополнение к глобальным шаблонам и глобальному директору. По умолчанию <code>N</code>
Disable conf.d	Позволяет отключить включение каталога <code>conf.d</code> , в котором хранится локальный пример конфигурации. Клиенты должны получать свою конфигурацию от родительского узла или действовать как мост выполнения командной конечной точки. По умолчанию <code>y</code>

Пример конфигурации агента:

```
# icinga2 node wizard
Welcome to the Icinga2 Setup Wizard!
```

```
We will guide you through all required configuration details.
```

```
Please specify if this is an agent/satellite setup ('n' installs
a master setup) [Y/n]:
```

```
Starting the Agent/Satellite setup routine...
```

```
Please specify the common name (CN) [agent1.test.alt]:
```

```
Please specify the parent endpoint(s) (master or satellite) where
this node should connect to:
```

```
Master/Satellite Common Name (CN from your master/satellite
node): master1.test.alt
```

```
Do you want to establish a connection to the parent node from
this node? [Y/n]:
```

```
Please specify the master/satellite connection information:
```

```
Master/Satellite endpoint host (IP address or FQDN):
master1.test.alt
```

```
Master/Satellite endpoint port [5665]:
```

```
Add more master/satellite endpoints? [y/N]:
```

```
Parent certificate information:
```

```
Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul 1 07:11:38 2024 GMT
Valid Until:      Aug 1 07:11:38 2025 GMT
Serial:
c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a
```

```
Signature Algorithm: sha256WithRSAEncryption
Subject Alt Names:  master1.test.alt
Fingerprint:       19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90
52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98
```

```
Is this information correct? [y/N]: y
```

```
Please specify the request ticket generated on your Icinga2
master (optional).
```

ЛКНВ.11102-01 90 01

```
(Hint: # icinga2 pki ticket --cn 'agent1.test.alt'):
84bffc6d33eccbbbd9b2ec6130031cef1d68ac01
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:
```

```
Accept config from parent node? [y/N]: Y
Accept commands from parent node? [y/N]: Y
```

```
Reconfiguring Icinga...
```

```
Disabling feature notification. Make sure to restart Icinga2 for
these changes to take effect.
```

```
Enabling feature api. Make sure to restart Icinga2 for these
changes to take effect.
```

```
Local zone name [agent1.test.alt]:
Parent zone name [master]: master1.test.alt
```

```
Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y
```

```
Please specify the name of the global Zone: global-commands
```

```
Do you want to disable the inclusion of the conf.d directory
[Y/n]:
```

```
Disabling the inclusion of the conf.d directory...
```

```
Done.
```

```
Now restart your Icinga2 daemon to finish the installation!
```

После окончания конфигурации необходимо перезапустить сервис Icinga2:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле и об агенте будет добавлена в файл
/etc/icinga2/zones.conf:

```
object Endpoint "master1.test.alt" {
    host = "master1.test.alt"
    port = "5665"
}

object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}

object Endpoint "agent1.test.alt" {
```

```

}

object Zone "agent1.test.alt" {
    endpoints = [ "agent1.test.alt" ]
    parent = "master"
}

object Zone "global-templates" {
    global = true
}

object Zone "director-global" {
    global = true
}

object Zone "global-commands" {
    global = true
}

```

7.7.3.1.2.2. Подписание CSR по требованию (sign on demand)

В данном разделе рассмотрен вариант с подписыванием сертификата агента на мастере (sign on demand).

В этом сценарии не требуется предварительное получение билета на мастере. Агент отправляет запрос на подпись сертификата указанному родительскому узлу (это может быть либо непосредственно мастер, либо спутник, который пересылает запрос подписывающему мастеру). Администратор основного мастера отвечает за проверку и подписание запросов с помощью закрытого ключа СА.

Для регистрации агента в режиме sign on demand после запуска мастера конфигурирования узла (команда `icinga2 node wizard`) следует пропустить вопрос с указанием билета (рис. 76) и подписать запрос позже на мастере. Описание остальных параметров приведено в таблице 9.

Примечание. Для возможности использования шаблонов `generic-host` и `nagwad-host` с мастер-узла с мастер-узла (см. п. 7.7.3.1.4), нужно отключить чтение файлов из `conf.d` (нажать клавишу Enter на вопрос `Do you want to disable the inclusion of the conf.d directory [Y/n]:`). Если же планируется использование шаблонов с агента, нужно НЕ отключать чтение файлов из `conf.d` при первичной настройке узла (ответить «n» на вопрос `Do you want to disable the inclusion of the conf.d directory [Y/n]`). Данное значение можно будет изменить и после настройки узла.

```

Терминал - root@agent3: /root
Файл  Правка  Вид  Терминал  Вкладки  Справка
[root@agent3 ~]# icinga2 node wizard
Welcome to the Icinga 2 Setup Wizard!

We will guide you through all required configuration details.

Please specify if this is an agent/satellite setup ('n' installs a master setup) [Y/n]:

Starting the Agent/Satellite setup routine...

Please specify the common name (CN) [agent3.test.alt]:

Please specify the parent endpoint(s) (master or satellite) where this node should connect to:
Master/Satellite Common Name (CN from your master/satellite node): master1.test.alt

Do you want to establish a connection to the parent node from this node? [Y/n]:
Please specify the master/satellite connection information:
Master/Satellite endpoint host (IP address or FQDN): 192.168.0.194
Master/Satellite endpoint port [5665]:

Add more master/satellite endpoints? [y/N]:
Parent certificate information:

Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul  1 07:11:38 2024 GMT
Valid Until:      Aug  2 07:11:38 2025 GMT
Serial:           c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a

Signature Algorithm: sha256WithRSAEncryption
Subject Alt Names:   master1.test.alt
Fingerprint:        19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90 52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98

Is this information correct? [y/N]: y

Please specify the request ticket generated on your Icinga 2 master (optional).
(Hint: # icinga2 pki ticket --cn 'agent3.test.alt'):

No ticket was specified. Please approve the certificate signing request manually
on the master (see 'icinga2 ca list' and 'icinga2 ca sign --help' for details).
Please specify the API bind host/port (optional):
Bind Host []:
Bind Port []:

Accept config from parent node? [y/N]: y
Accept commands from parent node? [y/N]: y

Reconfiguring Icinga...
Disabling feature notification. Make sure to restart Icinga 2 for these changes to take effect.
Enabling feature api. Make sure to restart Icinga 2 for these changes to take effect.

Local zone name [agent3.test.alt]:
Parent zone name [master]:

Default global zones: global-templates director-global
Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to specify another global zone? [y/N]:
Do you want to disable the inclusion of the conf.d directory [Y/n]:
Disabling the inclusion of the conf.d directory...

Done.
Now restart your Icinga 2 daemon to finish the installation!
[root@agent3 ~]#

```

Рис. 76 – Регистрация агента в режиме sign on demand

Пример конфигурации агента в режиме sign on demand:

```
# icinga2 node wizard
Welcome to the Icinga2 Setup Wizard!
```

```
We will guide you through all required configuration details.
```

```
Please specify if this is an agent/satellite setup ('n' installs
a master setup) [Y/n]:
```

```
Starting the Agent/Satellite setup routine...
```

```
Please specify the common name (CN) [agent3.test.alt]:
```

```
Please specify the parent endpoint(s) (master or satellite) where
this node should connect to:
```

```
Master/Satellite Common Name (CN from your master/satellite
node): master1.test.alt
```

```
Do you want to establish a connection to the parent node from
this node? [Y/n]:
```

```
Please specify the master/satellite connection information:
```

```
Master/Satellite endpoint host (IP address or FQDN):
master1.test.alt
```

```
Master/Satellite endpoint port [5665]:
```

```
Add more master/satellite endpoints? [y/N]:
```

```
Parent certificate information:
```

```
Version:          3
Subject:          CN = master1.test.alt
Issuer:           CN = Icinga CA
Valid From:       Jul 1 07:11:38 2024 GMT
Valid Until:      Aug 1 07:11:38 2025 GMT
Serial:
```

```
c8:74:1e:c2:8f:6a:8b:bf:bc:61:97:3d:64:90:5a:bc:5d:54:62:9a
```

```
Signature Algorithm: sha256WithRSAEncryption
```

```
Subject Alt Names:  master1.test.alt
```

```
Fingerprint:      19 07 D1 40 51 7B EE 74 6C C0 57 21 8C 90
52 73 7E F8 65 C6 3B 60 B0 46 4D B4 4C DC B5 C4 82 98
```

```
Is this information correct? [y/N]: y
```

```
Please specify the request ticket generated on your Icinga2
master (optional).
```

```
(Hint: # icinga2 pki ticket --cn 'agent3.test.alt'):
```

```
No ticket was specified. Please approve the certificate signing
request manually
```

```
on the master (see `icinga2 ca list` and `icinga2 ca sign -help`
for details).
```

Please specify the API bind host/port (optional):

Bind Host []:

Bind Port []:

Accept config from parent node? [y/N]: Y

Accept commands from parent node? [y/N]: Y

Reconfiguring Icinga...

Disabling feature notification. Make sure to restart Icinga2 for these changes to take effect.

Enabling feature api. Make sure to restart Icinga2 for these changes to take effect.

Local zone name [agent3.test.alt]:

Parent zone name [master]: master

Default global zones: global-templates director-global

Do you want to specify additional global zones? [y/N]: y

Please specify the name of the global Zone: global-commands

Do you want to disable the inclusion of the conf.d directory [Y/n]:

Disabling the inclusion of the conf.d directory...

Done.

Now restart your Icinga2 daemon to finish the installation!

После окончания конфигурации необходимо перезапустить сервис:

```
# systemctl restart icinga2.service
```

Информация о мастер-узле и об агенте будет добавлена в файл
/etc/icinga2/zones.conf:

```
object Endpoint "master1.test.alt" {
    host = "master1.test.alt"
    port = "5665"
}
```

```
object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}
```

```
object Endpoint "agent3.test.alt" {
}
```

```
object Zone "agent3.test.alt" {
    endpoints = [ "agent3.test.alt" ]
}
```

```

        parent = "master"
    }

    object Zone "global-templates" {
        global = true
    }

    object Zone "director-global" {
        global = true
    }

    object Zone "global-commands" {
        global = true
    }

```

Созданный запрос необходимо подписать на мастер-узле.

На мастер-узле посмотреть запросы, ожидающие подпись сертификата, можно с помощью команды:

```

# icinga2 ca list
Fingerprint          | Timestamp          | Signed | Subject
-----|-----|-----|-----
77a930d263ed2...8067| Jul 02 09:03:51 2024 GMT|        | CN = agent3.test.alt

```

Чтобы отобразить все запросы, используется параметр `all`:

```
# icinga2 ca list --all
```

Примечание. Запросы на подпись сертификата старше 1 недели автоматически удаляются.

Примечание. Чтобы получить подробную информацию о запросе в формате JSON необходимо добавить в команду параметр `json`.

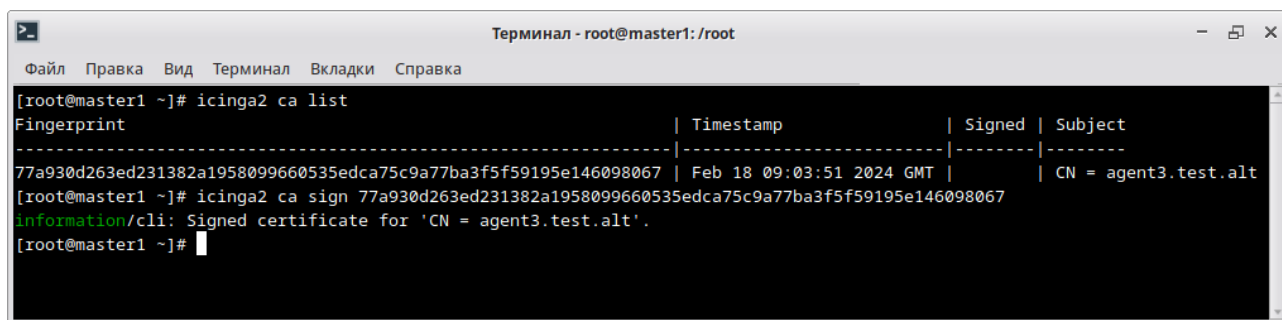
Для подписания запроса, используется команда `icinga2 ca sign` с отпечатком запроса (`fingerprint`) в качестве аргумента (рис. 77):

```
# icinga2 ca sign 77a930d263ed2...8067
```

Для удаления нежелательного запроса используется команда `icinga2 ca remove`:

```
# icinga2 ca remove 77a930d263ed2...9195e146098067
```

Восстановить удаленный сертификат, можно с помощью команды `icinga2 ca restore`.



```

Терминал - root@master1: /root
Файл  Правка  Вид  Терминал  Вкладки  Справка
[root@master1 ~]# icinga2 ca list
Fingerprint                                     | Timestamp                               | Signed | Subject
-----|-----|-----|-----
77a930d263ed231382a1958099660535edca75c9a77ba3f5f59195e146098067 | Feb 18 09:03:51 2024 GMT |         | CN = agent3.test.alt
[root@master1 ~]# icinga2 ca sign 77a930d263ed231382a1958099660535edca75c9a77ba3f5f59195e146098067
information/cli: Signed certificate for 'CN = agent3.test.alt'.
[root@master1 ~]#

```

Рис. 77 – Список запросов и подпись запроса на сертификат

7.7.3.1.3. Настройка взаимодействия мастера с агентами

Существуют разные способы гарантировать, что узлы кластера Icinga2 выполняют проверки, отправляют уведомления и т. д.

Предпочтительный метод – настроить объекты мониторинга на мастере и распространить конфигурацию на спутники и агенты.

В режиме Top Down Command Endpoint узел Icinga2 удаленно выполняет команды на указанной конечной точке. Конфигурация объекта host/service находится на мастере/спутнике, и агенту нужны только доступные определения объекта CheckCommand (см. п. 7.7.3.1.4).

Примечание. Не требуется никакой локальной настройки агента, за исключением определений CheckCommand, которые можно синхронизировать с помощью глобальной зоны. Поэтому следует закомментировать строку `include_recursive conf.d в /etc/icinga2/icinga2.conf` на агенте.

В примере, рассматриваемом ниже:

- master1.test.alt – мастер конфигурации;
- agent1.test.alt, agent2.test.alt – агенты.

Примечание. Конфигурация зон и Endpoint (конечных точек) на агенте выполняется при конфигурировании узла.

Примечание. Каждому агенту требуется собственная конфигурация зоны и конечной точки (Endpoint). Лучше всего использовать FQDN имя агента для всех имен объектов.

На Мастер-узле необходимо выполнить следующие действия:

- 1) включить конфигурации конечной точки и определить две зоны. Для этого в файл `/etc/icinga2/zones.conf` добавить информацию об агенте (в поле `host` должен быть указан адрес клиентского узла, зона `master` является родительской для зон клиентских узлов):

```
object Endpoint "master1.test.alt" {
    host = "192.168.0.170"
}
object Endpoint "agent1.test.alt" {
    host = "192.168.0.151"
    log_duration = 0 // Отключить ротацию журнала
}
object Endpoint "agent2.test.alt" {
    host = "192.168.0.152"
    log_duration = 0 // Отключить ротацию журнала
}
object Zone "master" {
    endpoints = [ "master1.test.alt" ]
}
object Zone "agent1.test.alt" {
    endpoints = [ "agent1.test.alt" ]
    parent = "master"
}
object Zone "agent2.test.alt" {
    endpoints = [ "agent2.test.alt" ]
    parent = "master"
}
object Zone "global-templates" {
    global = true
}

object Zone "director-global" {
    global = true
}

object Zone "global-commands" {
    global = true
}
```

- 2) создать файл конфигурации для мониторинга машин, входящих в зону `master`. Для этого создать каталог `/etc/icinga2/zones.d/master`:

```
# mkdir -p /etc/icinga2/zones.d/master
```

В этом каталоге создать файл `hosts.conf`, в который добавить информацию об агентах:

```
object Host "agent1.test.alt" {
    import "generic-host"
    import "nagwad-host"
    address = "192.168.0.151"
    vars.agent_endpoint = name //follows the convention that host
name == endpoint name
}
object Host "agent2.test.alt" {
    import "generic-host"
    import "nagwad-host"
    address = "192.168.0.152"
    vars.agent_endpoint = name //follows the convention that host
name == endpoint name
}
```

где:

- `import "generic-host"` – импорт стандартной конфигурации из шаблона `generic-host`;
- `import "nagwad-host"` – импорт конфигурации `nagwad` из шаблона `nagwad-host`;
- `address` – IP-адрес клиентского узла;
- `agent_endpoint` – пользовательская переменная, которая служит двум целям:

а) ей могут соответствовать правила применения службы;

б) правила применения могут получать его значение и присваивать его атрибуту `command_endpoint`;

3) проверить целостность конфигурации Icinga2, выполнив команду:

```
# icinga2 daemon -C
```

4) перезапустить сервис Icinga2 на мастер-узле:

```
# systemctl restart icinga2
```

В веб-интерфейсе Icinga2 (раздел «Обзор» → «Узлы») агент сначала появится в статусе «Рассматриваемый» (рис. 78), а затем, если все настроено правильно, перейдет в статус «Включен» (рис. 79).



Рис. 78 – Статус узла «Рассматриваемый»

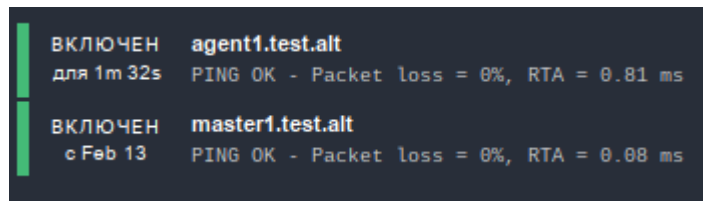


Рис. 79 – Статус узла «Включен»

После окончания настройки мониторинга клиентов, они будут отображаться в веб-интерфейсе Icinga2 (Рис. 80).

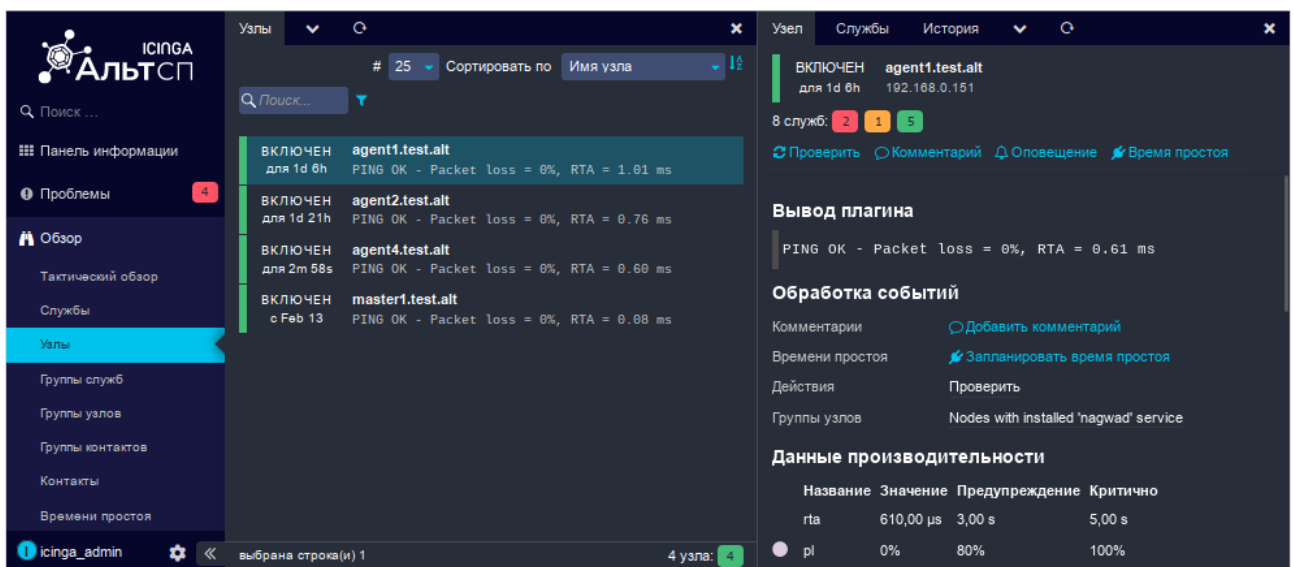


Рис. 80 – Клиенты мониторинга

7.7.3.1.4. Глобальные зоны

Глобальные зоны можно использовать для синхронизации универсальных объектов конфигурации со всеми зависящими от них узлами.

Примечание. Проверяемые объекты (хосты и службы) нельзя поместить в глобальную зону.

Конфигурация объекта зоны должна быть развернута на всех узлах, которые должны получать файлы глобальной конфигурации.

Примечание. Глобальные зоны по умолчанию, созданные мастерами установки, называются `global-templates` и `director-global`. Зона `director-global` зарезервирована для использования Icinga Director, в этой зоне нельзя размещать какие-либо конфигурации вручную.

Глобальная зона `global-commands`, в которой определен объект `CheckCommand` `check_nagwad` должна быть добавлена на этапе конфигурирования узлов (см. выше). Если это не сделано на мастере и на агентах в файл `/etc/icinga2/zones.conf` необходимо добавить информацию о глобальной зоне `global-commands`:

```
object Zone "global-commands" {  
    global = true  
}
```

7.7.3.2. Веб-интерфейс Icinga Director

Icinga Director предоставляет веб-интерфейс для управления конфигурацией Icinga2. Данный модуль позволяет описывать объекты Icinga (Services, Commands, Hosts) в веб-интерфейсе, используя гибкое и понятное меню.

Icinga Director не вносит никаких правок в классические конфигурационные файлы Icinga (в каталоге `/etc/icinga2`), а имеет свою независимую конфигурацию. Конфигурация хранится в БД и выгружается в текстовый вид, для чтения серверной частью Icinga, по требованию (при развертывании). Director ведет журнал всех изменений и предоставляет возможность отката на предыдущие версии конфигурации.

В файловой системе текущую и последнюю конфигурации можно найти в каталоге `/var/lib/icinga2/api/packages/director`. В веб-интерфейсе Director для просмотра выгруженных файлов конфигурации (рис. 81) необходимо перейти в раздел «Управление Icinga» → «Развертывания» и нажать кнопку «Render Config».

Примечание. Не следует напрямую редактировать выгруженные файлы конфигурации в файловой системе. Для работы нужно использовать только графический интерфейс или API.

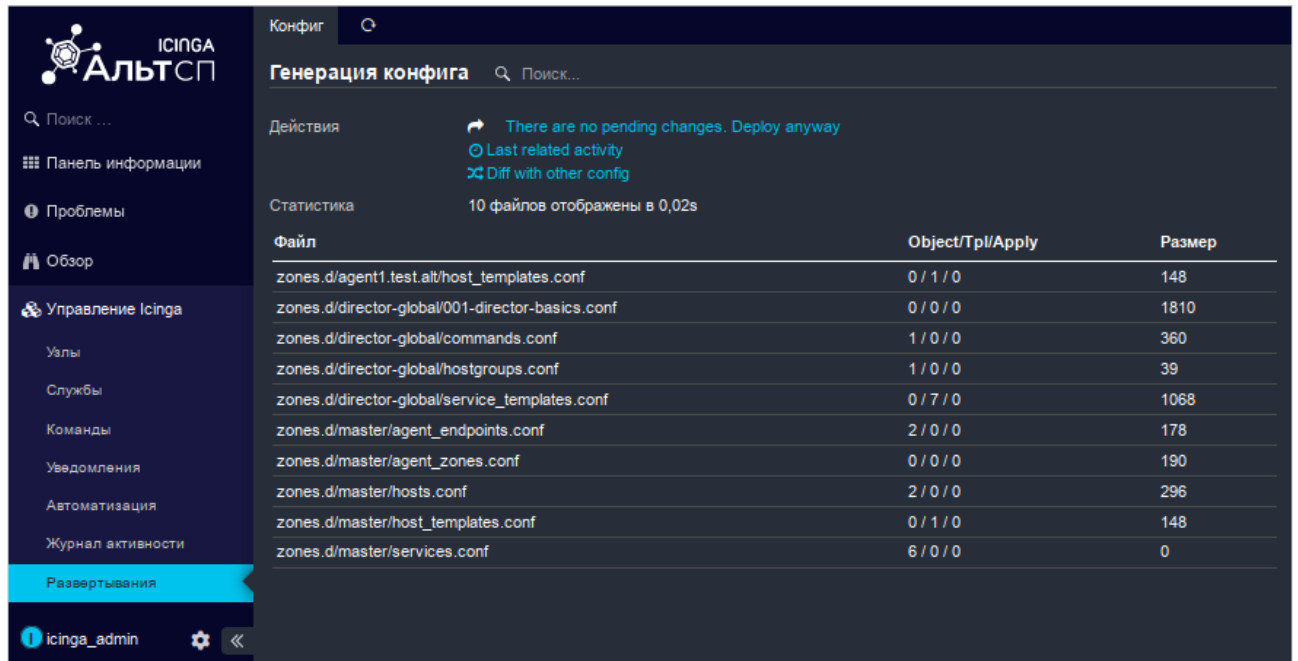


Рис. 81 – Файлы конфигурации Icinga Director

7.7.3.2.1. Установка Icinga Director на мастер-узле

7.7.3.2.1.1. Установка пакетов

Для управления конфигурацией посредством веб-интерфейса, необходимо на мастер-узле установить пакет:

```
# apt-get install icingaweb2-module-director
```

7.7.3.2.1.2. Создание базы данных

⚠ В качестве сервера базы данных используется ПЭВМ 64 бит (x86_64)/AArch64 (ARMv8) с установленной ОС Альт СП Рабочая станция/Сервер релиз 10. Создание базы данных выполняется на указанной ПЭВМ.

MySQL/MariaDB

Создать пользователя director и базу данных director (пароль необходимо запомнить):

```
$ mysql -uroot -p
Enter password:
MariaDB [(none)]> create database director character set 'utf8'
collate utf8_general_ci;
MariaDB [(none)]> grant all privileges on director.* to
director@localhost identified by '<пароль>';
MariaDB [(none)]> quit;
```

PostgreSQL

Установить пакет:

```
# apt-get install postgresql16-contrib
```

Создать пользователя director и базу данных director (потребуется также ввести пароль пользователя postgres):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt director'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -E utf8 -O director director'
```

Пароль:

Включить расширение pgcrypto:

```
# psql -U postgres
```

Пароль пользователя postgres:

psql (16.3)

Введите "help", чтобы получить справку.

```
postgres=# create extension pgcrypto;
```

```
CREATE EXTENSION
```

```
postgres=# \q
```

7.7.3.2.1.3. Подключение базы данных для Icinga Director

В Icinga необходимо создать запись о новом ресурсе с типом «База данных SQL», который будет ссылаться на базу данных director. Для этого в веб-интерфейсе Icinga Web 2 следует выбрать пункт «Настройки» → «Приложение», перейти на вкладку «Ресурсы» (рис. 82) и нажать кнопку «Создание нового ресурса».

В открывшемся окне введите данные подключения к базе данных director (рис. 83).

Примечание. Вместо localhost (рис. 83) необходимо указывать IP-адрес ПЭВМ, на которой развернута база данных.

Проверить конфигурацию, нажав кнопку «Проверить конфигурацию», и, если проверка прошла успешно, сохранить новый ресурс, нажав кнопку «Сохранить изменения».

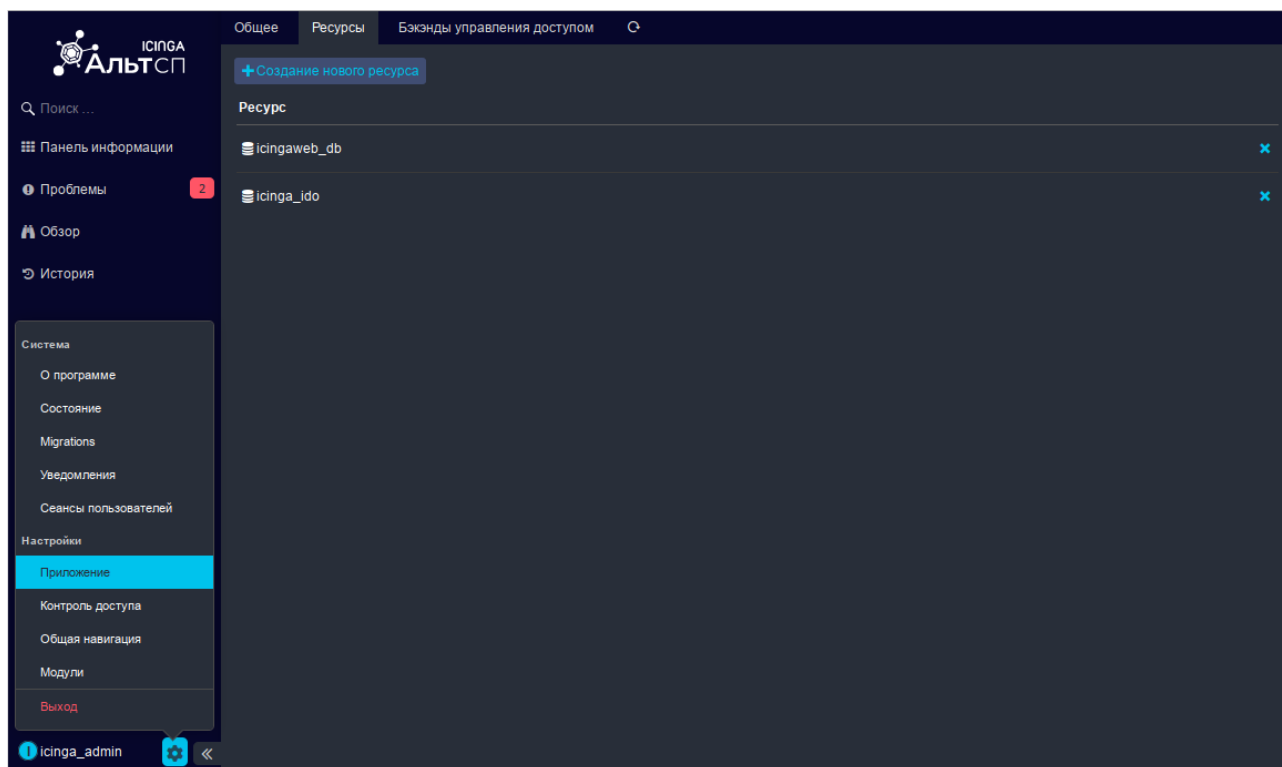


Рис. 82 – Список ресурсов

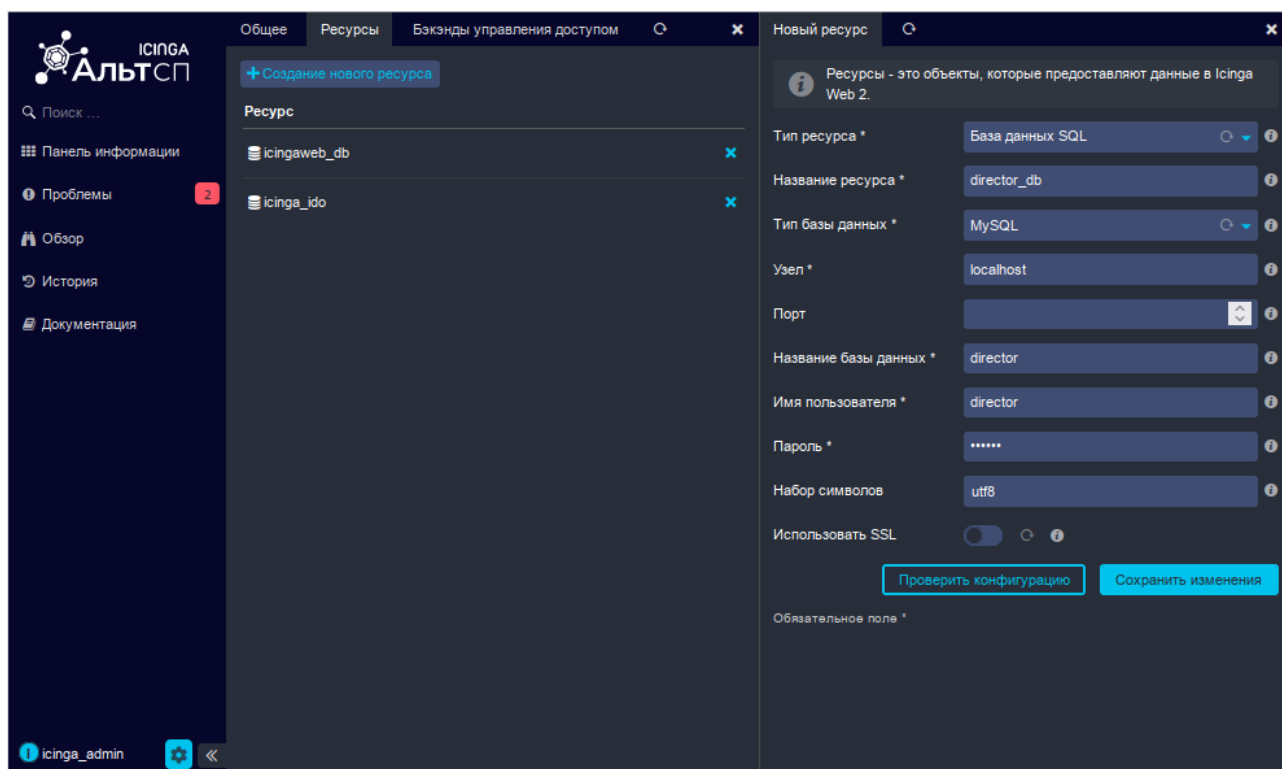


Рис. 83 – Создание нового ресурса

7.7.3.2.1.4. Включение модуля Icinga Director

Для просмотра списка модулей перейти в раздел «Настройки» → «Модули» (рис. 84).

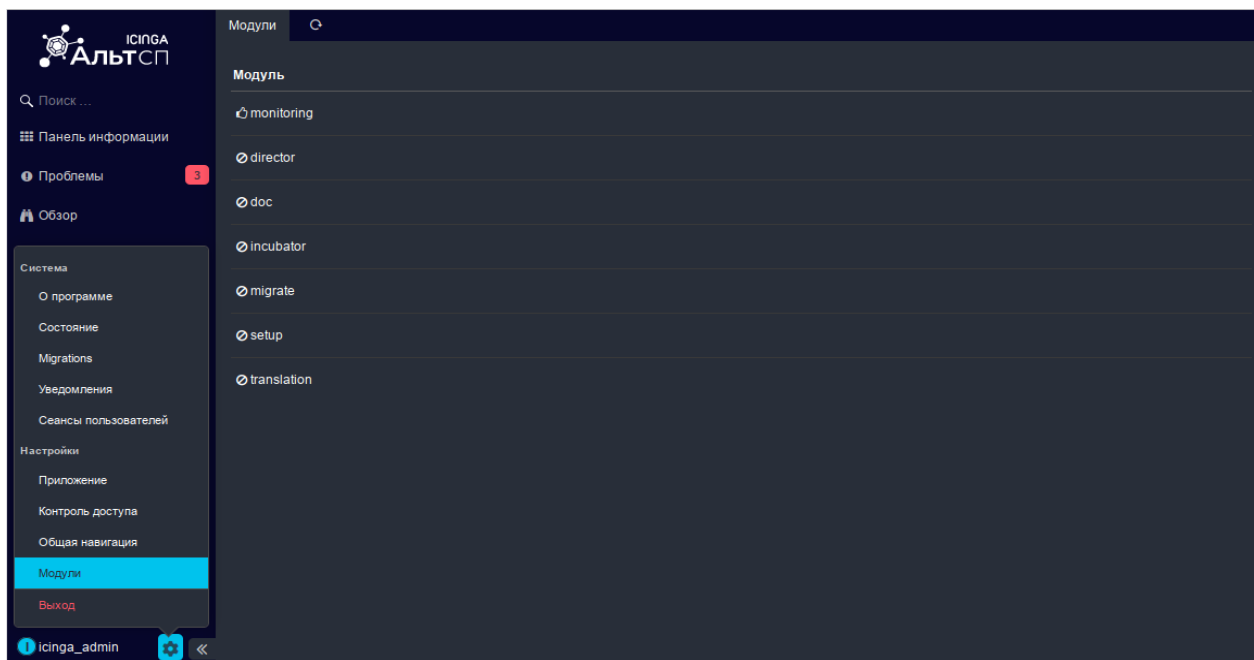


Рис. 84 – Список модулей

Предварительно необходимо включить модуль incubator. Для этого следует выбрать данный модуль в списке модулей, и, в открывшейся справа форме, нажать на значок «Обновить» справа от слова «disabled» в строке «Состояние» (рис. 85).

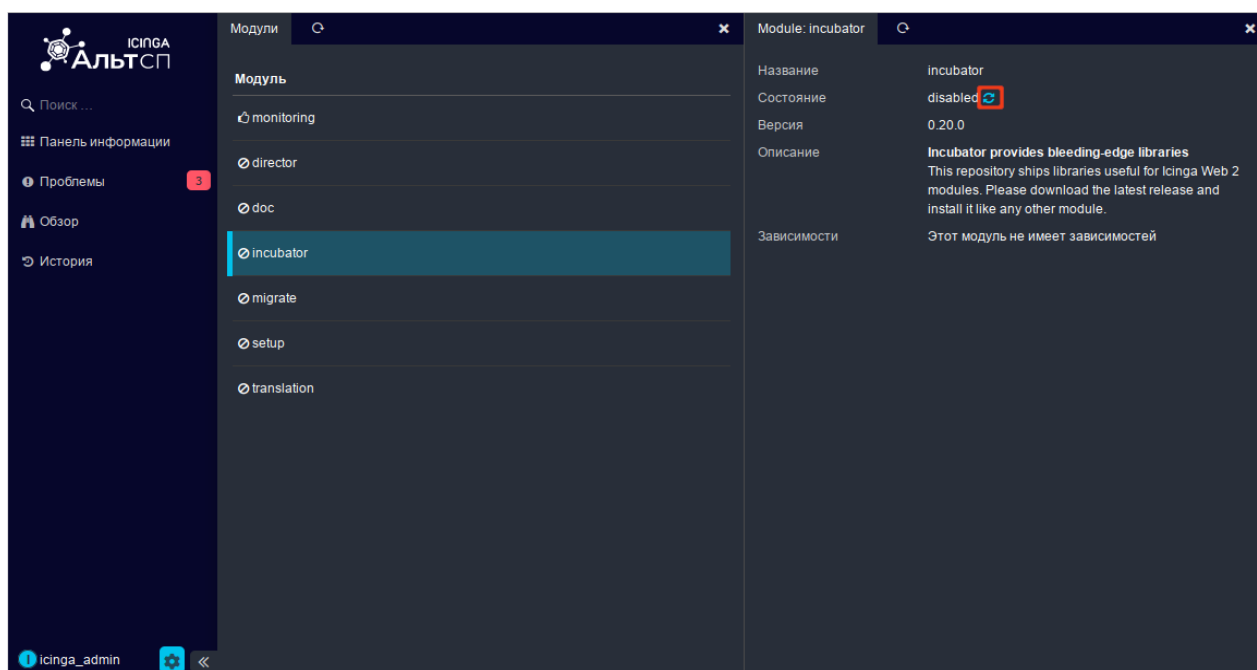


Рис. 85 – Модуль incubator

Состояние модуля должно измениться с disabled на enabled. Далее нужно повторить эти действия для модуля director (рис. 86).

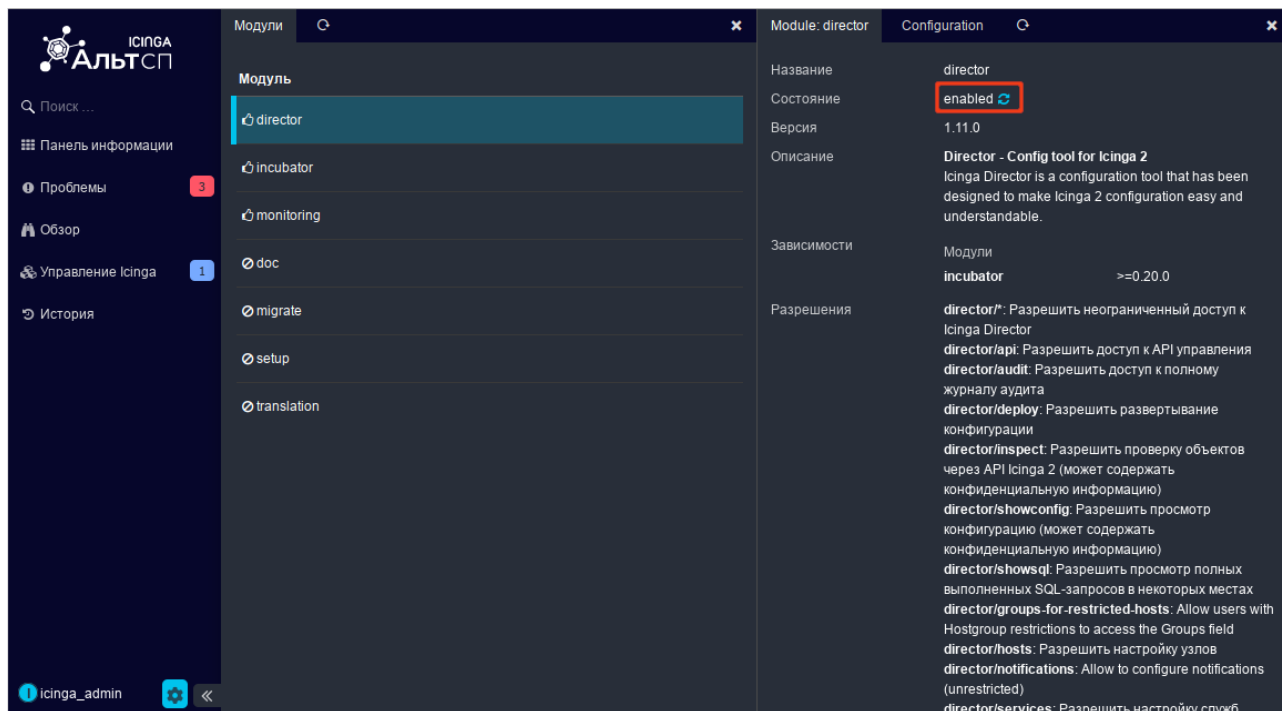


Рис. 86 – Модуль director

После того как модуль director включен, необходимо перейти на вкладку «Configuration» (рис. 87) и выполнить настройку модуля. Для этого выбрать из выпадающего списка «Источник БД» ресурс director_db. Будет выведено сообщение о том, что ассоциированная база данных пуста и не имеет схемы (рис. 88). Для создания схемы необходимо нажать кнопку «Создание схемы базы данных».

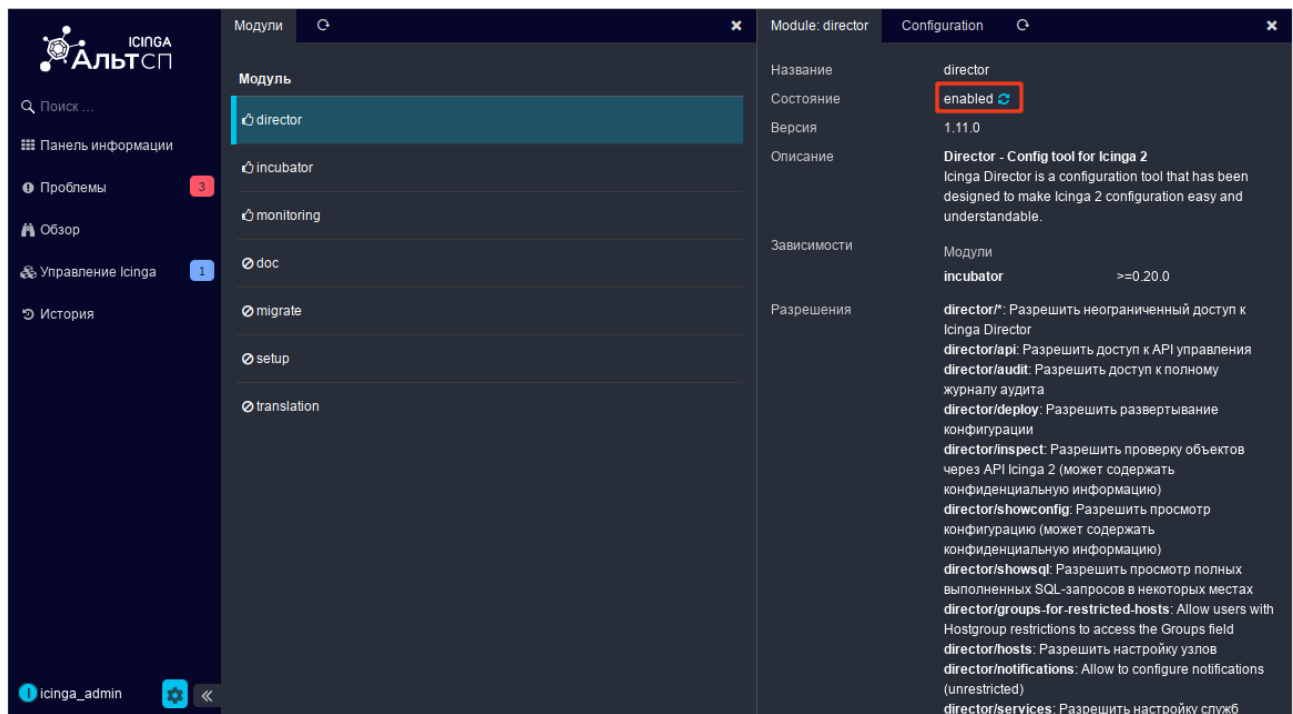


Рис. 87 – Модуль director вкладка «Configuration»

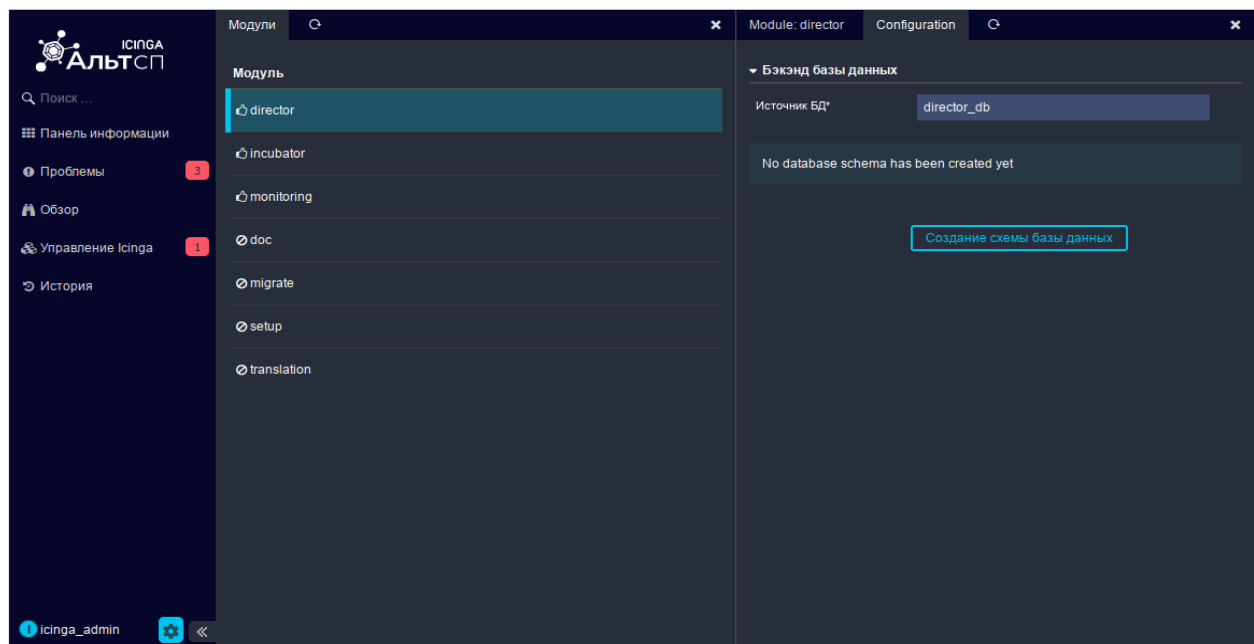


Рис. 88 – Ассоциированная база данных пуста и не имеет схемы

В открывшейся форме необходимо настроить параметры подключения модуля Director к серверу Icinga (рис. 89):

- «Имя конечной точки» – имя Common Name (CN) из SSL-сертификата, который был сгенерирован в процессе включения Icinga API. По умолчанию

в качестве CN для SSL-сертификата используется FQDN-имя сервера, на котором выполняется включение Icinga API;

- «Icinga Host» – имя сервера Icinga;
- «Порт» – порт Icinga API по умолчанию (5665);
- «Имя пользователя API» – имя пользователя для подключения к API (root);
- «Пароль API» – пароль для подключения к API.

Примечание. Имя и пароль пользователя для подключения к API указаны в файле `/etc/icinga2/conf.d/api-users.conf`.

Примечание. Если в дальнейшем планируется делегирование прав доступа к API можно создать отдельного пользователя API Icinga2 для Director с полным доступом к API, добавив следующие строки в файл `/etc/icinga2/conf.d/api-users.conf`:

```
object ApiUser "director" {
    password = "aaabea888fd23e777" //change this
    permissions = [ "*" ]
}
```

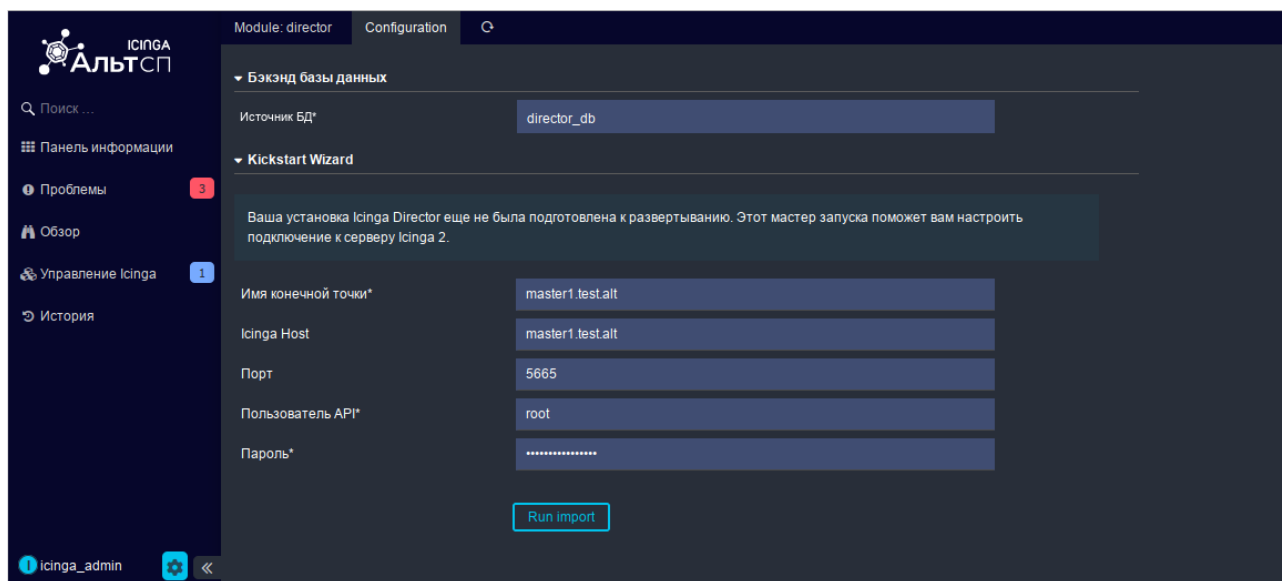


Рис. 89 – Настройка подключения к серверу Icinga

После внесения изменений в файл `/etc/icinga2/conf.d/api-users.conf` необходимо перезапустить службу `icinga2`:

```
# systemctl restart icinga2
```

Запустить подключение, нажав на кнопку «Run Import». В случае успешного подключения будет выведено сообщение «Ваша база данных выглядит хорошо» (рис. 90).

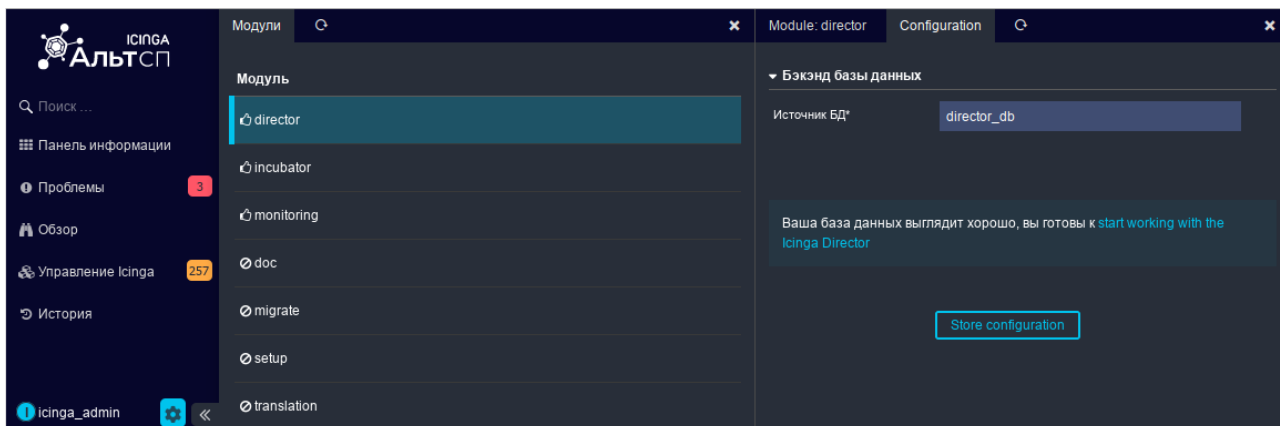


Рис. 90 – Подключение к Icinga

Включить и добавить в автозагрузку службу icinga-director:

```
# systemctl enable --now icinga-director.service
```

Для доступа к функциям подключенного модуля в главном меню навигации Icinga Web 2 используется пункт «Управление Icinga» (рис. 91).

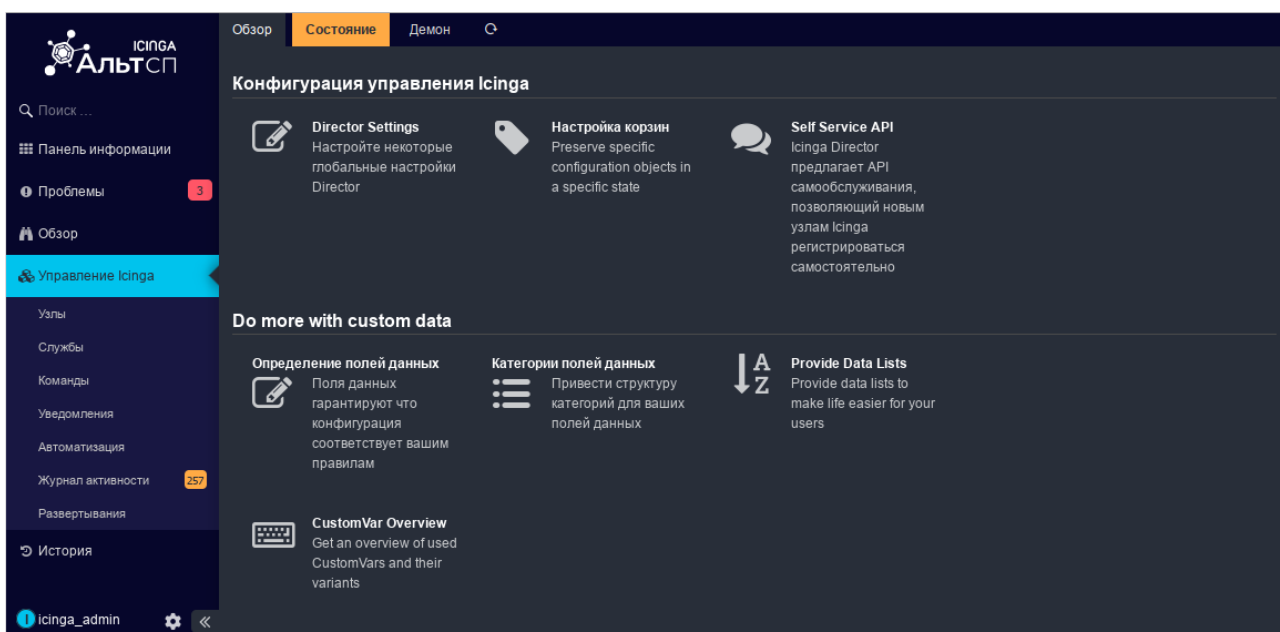


Рис. 91 – Управление Icinga

Примечание. В файле `/etc/icinga2/zones.conf` должна присутствовать запись о глобальной зоне `director-global`. Эта зона нужна для хранения общих объектов конфигурации, которые Icinga Director будет распространять на клиентов. Если записи о зоне нет, ее необходимо добавить, добавив в файл строки:

```
object Zone "director-global" {
    global = true
}
```


и перезапустить службу icinga2:

```
# systemctl restart icinga2
```

Для возможности запрашивания билетов для агента необходимо сгенерировать секретный ключ и записать его в файл `/etc/icinga2/constants.conf`:

- сгенерировать TicketSalt:

```
# openssl rand -base64 30
FbatRmRfzLccmuXQKQbZOapCoNLkYSEWs9eQkl0c
```

- записать полученный TicketSalt в файл `/etc/icinga2/constants.conf` в строку `const TicketSalt = ""`:

```
const TicketSalt = "FbatRmRfzLccmuXQKQbZOapCoNLkYSEWs9eQkl0c"
```

- и перезапустить службу icinga2:

```
# systemctl restart icinga2
```

7.7.3.2.2. Основные объекты конфигурации

Одним из основных принципов взаимосвязей объектов в Icinga2 является то, что сначала создаются шаблоны того или иного вида объекта, а потом создаются сами объекты с привязкой к этим шаблонам. Шаблоны описывают одно или несколько схожих для некоего множества объектов значений свойств. Для объекта может быть создано любое необходимое количество шаблонов. Основное назначение шаблона – это определить параметры, характерные для некоторого массива объектов, чтобы в дальнейшем можно было применить эти параметры к этому массиву объектов.

Основные объекты конфигурации:

1) Команды (Command) и шаблоны команд (Command Templates). Команда – это предопределенное действие, которое выполняется на проверяемой системе или удаленно проверяет систему.

Атрибуты команды:

- описание базовых параметров и пути запуска скрипта или утилиты, выполняющих проверку (например, скрипты удаленной и локальной проверки);

- аргументы команды, то есть сопоставление ключей запуска или с переменными среды Icinga, например, \$address\$ (адрес хоста, к которому применяется проверка), или с вычисляемыми значениями;
- переменные команды, то есть определенные пользователем переменные, задающие значение переменных.

Основные типы команд:

- Check command – команды проверок;
- Notification command – команды отсылки уведомлений (e-mail, SMS, службы сообщений);
- Event command – команды действий по отношению к узлу или сервису (перезагрузка, запуск дополнительных утилит и т. д.).

Шаблоны команд используются в том случае, когда необходимо задать некие общие параметры проверок или переменные для группы команд.

2) Служба (Service) – это сущность, описывающая проверку того или иного параметра системы указанной командой с некоторым набором параметров, определяющих среду вызова и исполнения этой команды. В частности, в свойствах службы задается то, где выполняется команда – на стороне сервера или на стороне агента. Также в свойствах службы может быть задано количество попыток выполнения команды, интервалы между попытками и другие параметры. Здесь можно выделить такие сущности, как:

- шаблоны служб (Service Templates) используются чтобы задать общие групповые характеристики. Это может быть частота проверок, общие переменные или назначение определенной функциональности (агент Icinga);
- правила применений служб (Service Apply Rules) – применение определенной службы к узлу или группе узлов на основе набора признаков. Это могут быть, как свойства узла (имя, адрес, принадлежность к группе), так и набор пользовательских переменных;
- группа служб (Service Groups) – может применяться для визуализации однотипных сервисов, определения прав пользователей Служб, или упрощения управления ими через API;

- наборы служб (Service Sets) – используются для назначения группы команд к группе хостов.

3) Узлы (Host) – это конечные компьютеры или сетевые устройства, однозначно идентифицируемые при помощи адреса, которые добавляются в систему мониторинга. Вспомогательные сущности:

- шаблоны узла (Host Templates) – представляют собой те или иные параметры настройки, которые могут быть применимы к одному или множеству узлов, а также могут содержать в себе привязку служб;
- группы узлов (Host Groups) – применяются для группировки узлов, настройки разграничения доступа или управлению через API.

7.7.3.2.3. Пример настройки конфигурации Icinga

В данном разделе рассмотрен пример создания шаблона служб, набора служб на его основе и шаблона узла.

Этот раздел можно пропустить и развернуть готовую конфигурацию из корзины (см. п. 7.7.3.2.4).

7.7.3.2.3.1. Создание шаблона служб (Service Templates)

В первую очередь необходимо настроить шаблон службы, который будет использоваться для мониторинга систем и служб. В шаблоне определяется служба и часть системы, которая будет отслеживаться.

В данном примере создадим шаблон, который отслеживает доступность системы по ssh и использование диска.

Для создания шаблона служб перейти в веб-интерфейсе «Управление Icinga» в раздел «Службы», выбрать «Шаблоны служб» и на вкладке «Шаблоны» нажать ссылку «Добавить» (рис. 92).

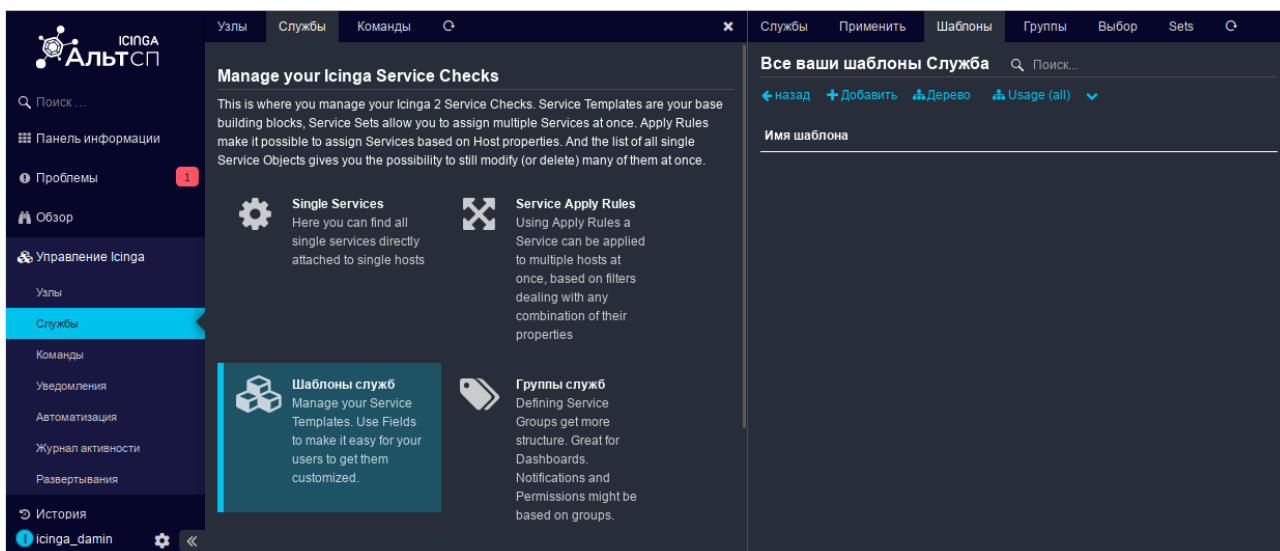


Рис. 92 – Раздел «Шаблоны служб»

В открывшейся справа форме создания шаблона службы (рис. 93) указать следующие данные:

- «Название» – произвольное имя службы;
- «Команда проверки» – команда, которая будет использоваться для проверки мониторинга, например, ssh, ping (можно начать вводить символы и выбрать из предложенного списка);
- «Run on Agent» – разрешить запуск команды проверки на стороне клиента.

Нажать кнопку «Добавить», чтобы сохранить шаблон службы.

Аналогичным способом создать шаблон службы проверки диска.

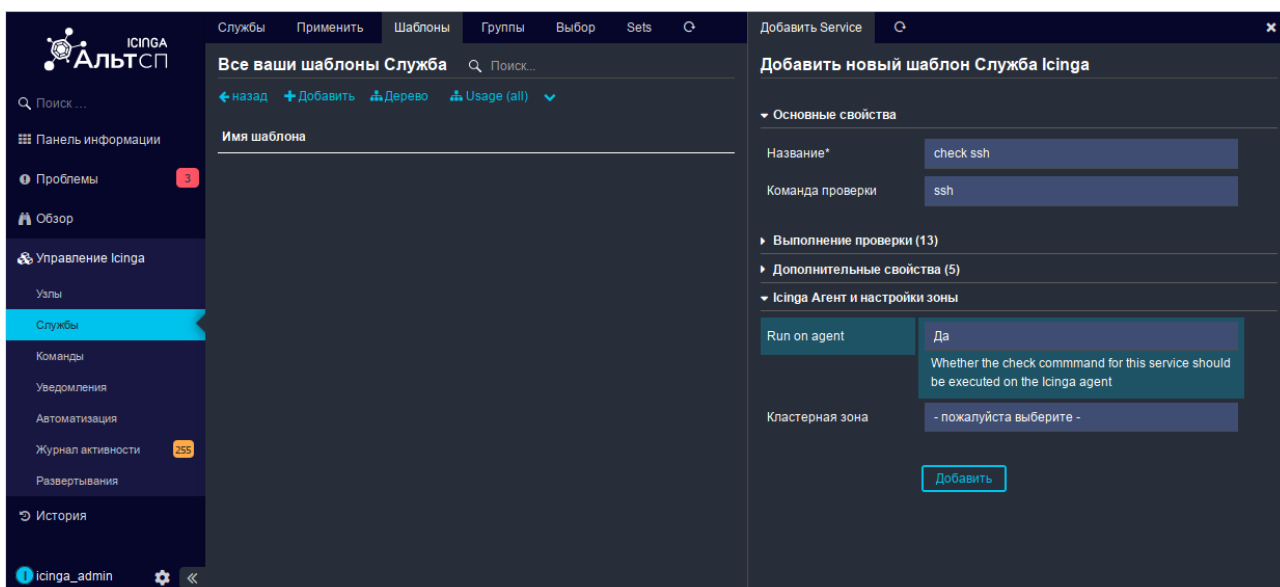


Рис. 93 – Создание шаблона службы

7.7.3.2.3.2. Создание набора служб (Service Set)

Следующий шаг – создание набор служб и добавление в него шаблонов служб. Для этого перейти в веб-интерфейсе «Управление Icinga» в раздел «Службы», выбрать «Наборы служб» и на вкладке «Sets» нажать ссылку «Добавить» (рис. 94).

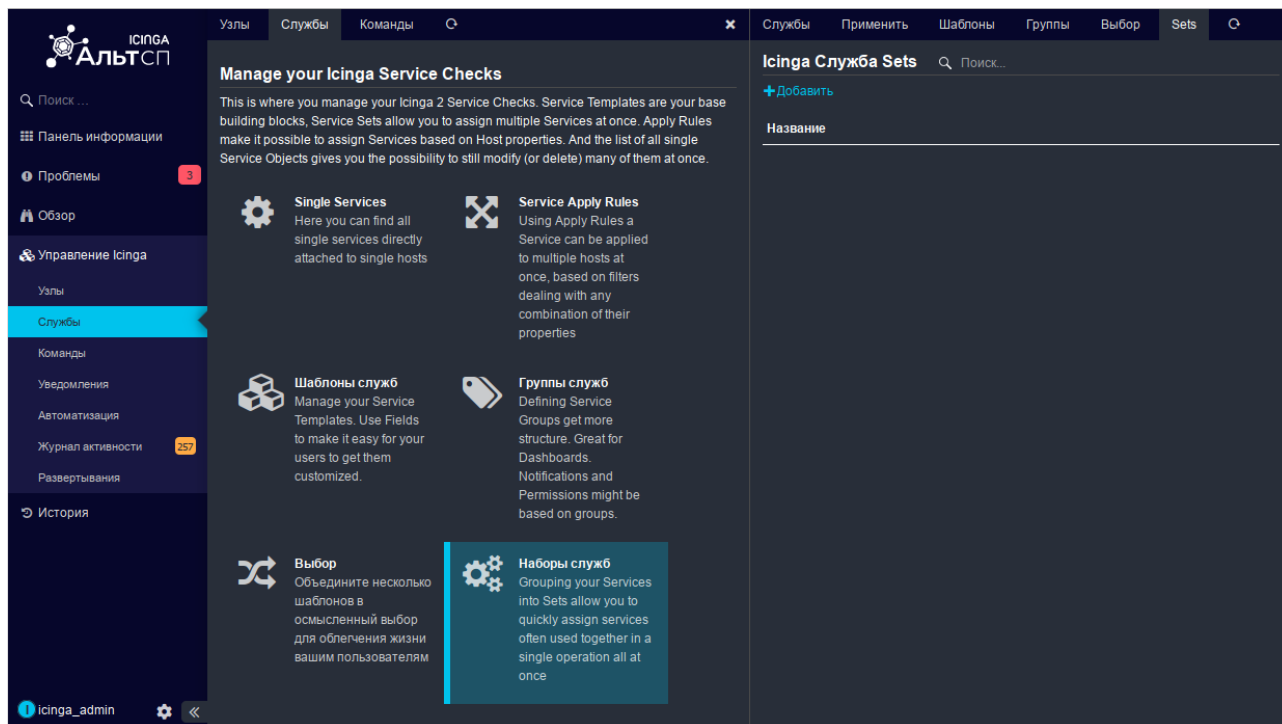


Рис. 94 – Раздел «Наборы служб»

В открывшейся справа форме создания шаблона службы (рис. 95) указать параметры:

- «Service set name» – краткое название, идентифицирующее этот набор служб;
- «Описание» – содержательное описание, объясняющее пользователям чего следует ожидать при назначении этого набора служб.

Нажать кнопку «Добавить», чтобы сохранить набор служб.

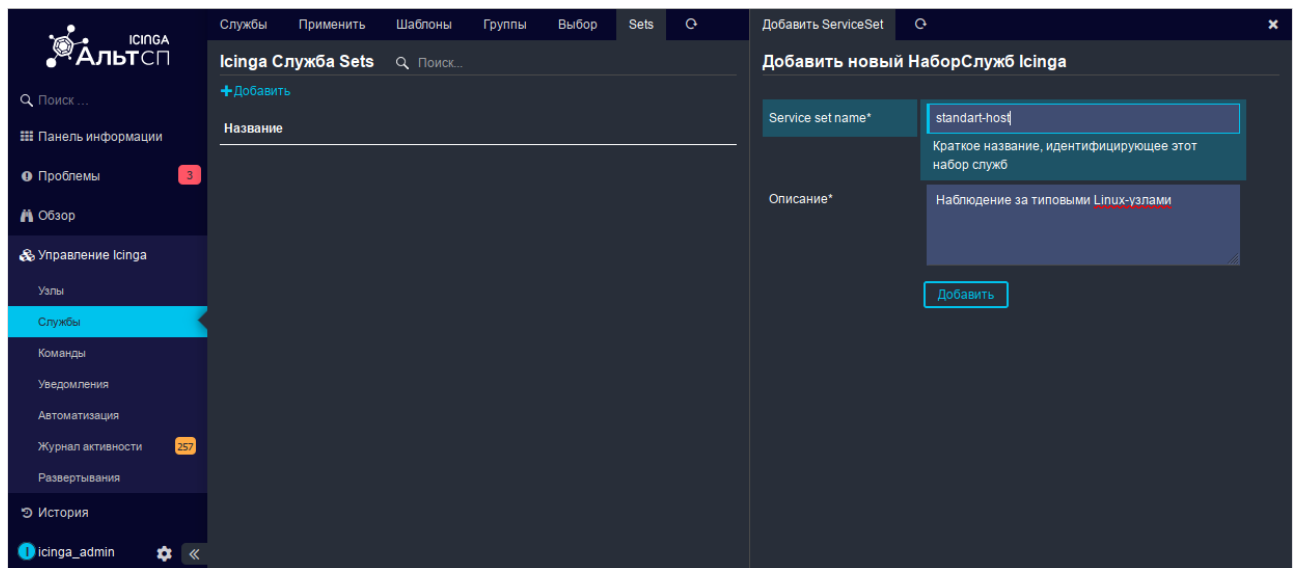


Рис. 95 – Новый набор служб

Далее следует добавить шаблоны служб в созданный набор сервисов. Для этого выбрать набор служб в списке на левой панели, перейти на вкладку «Services» на правой панели (рис. 96) и нажать ссылку «Добавить службу».

Выбрать имя службы в раскрывающемся списке «Imports» и нажать кнопку «Добавить» (рис. 97).

Повторить это действие для второго шаблона.

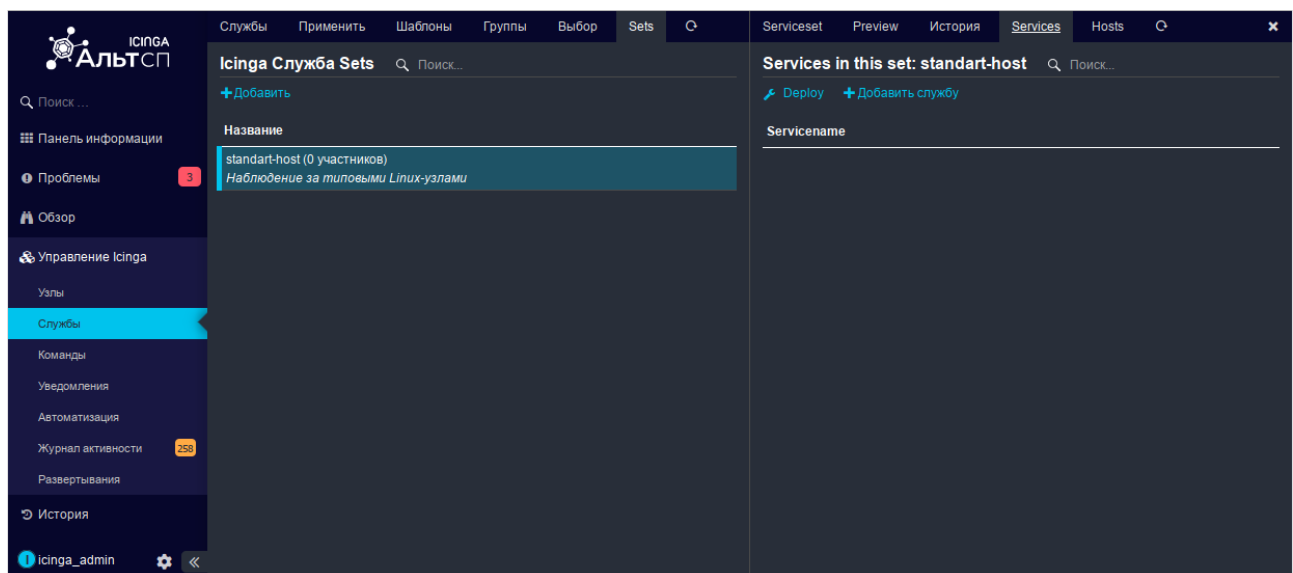


Рис. 96 – Список шаблонов в наборе служб

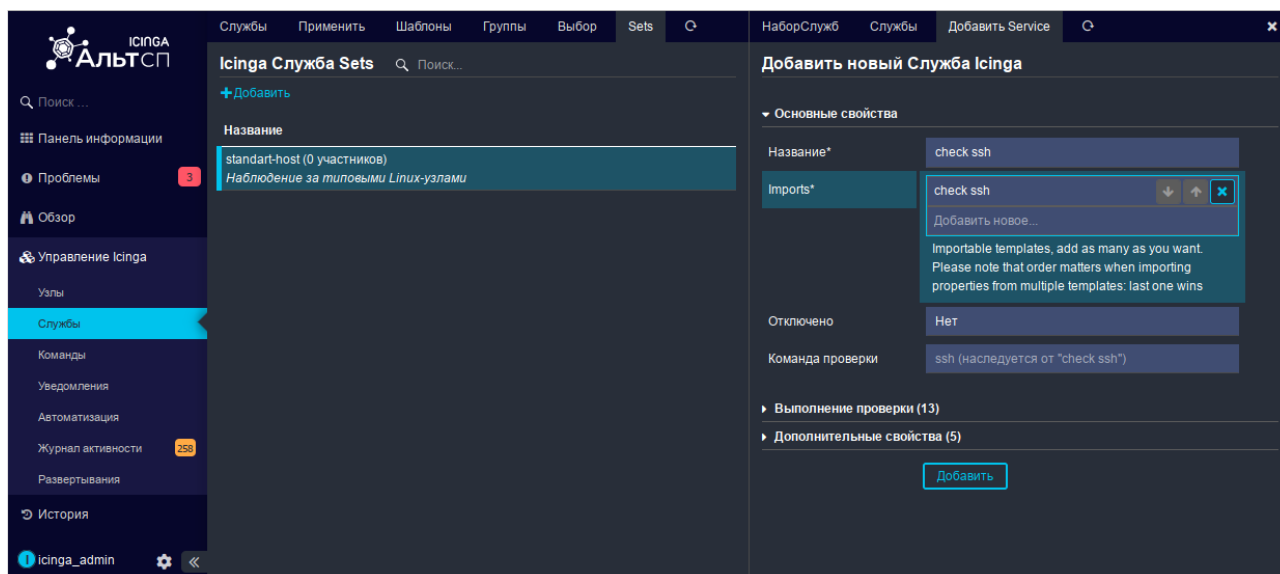


Рис. 97 – Добавление шаблона в набор служб

7.7.3.2.3.3. Создание шаблона узла (Host Templates)

На этом шаге необходимо создать шаблон узла и подключить к нему созданный выше набор служб.

Перейти в веб-интерфейсе «Управление Icinga» в раздел «Узлы», выбрать «Шаблоны узла» и на вкладке «Шаблоны» нажать ссылку «Добавить» (рис. 98).

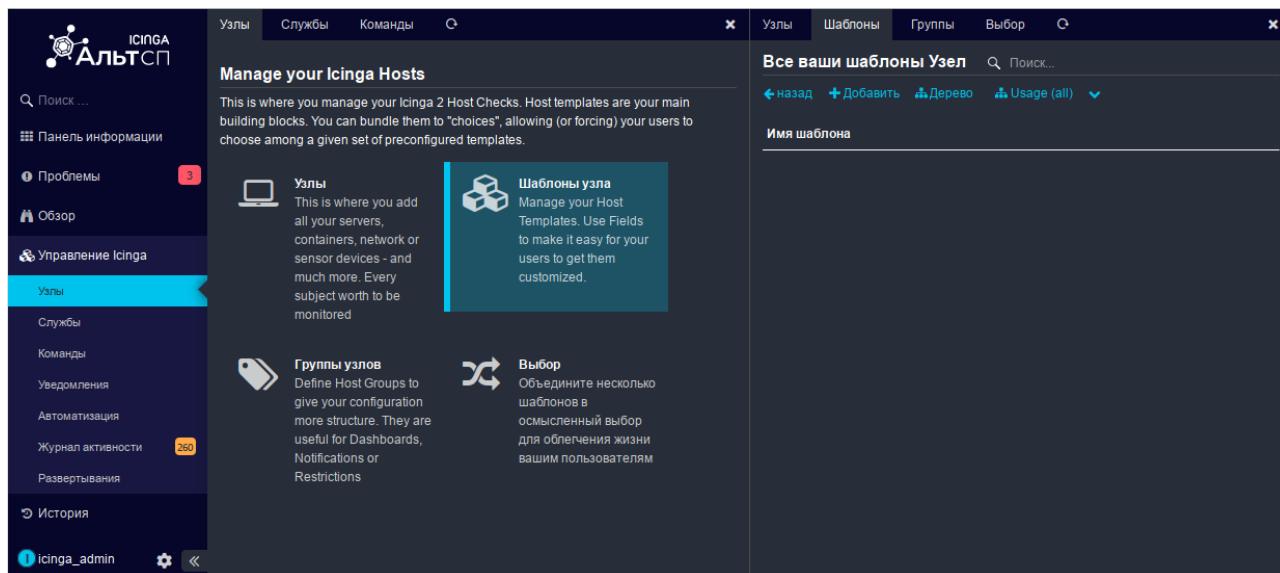


Рис. 98 – Вкладка «Шаблоны узла»

В открывшейся форме (рис. 99) необходимо заполнить следующие поля:

- «Название» – описательное имя шаблона узла (рекомендуется использовать значимые имена для шаблонов);

- «Команда проверки» – определение команды проверки (hostalive);
 - «Icinga2 Агент» – установлен ли на этом узле агент Icinga2 (да);
 - «Establish connection» – должен ли мастер активно пытаться подключиться к этому агенту (да);
 - «Принять конфигурацию» – настроен ли агент на прием конфигурации (да).
- Нажать кнопку «Добавить», чтобы сохранить шаблон узла.

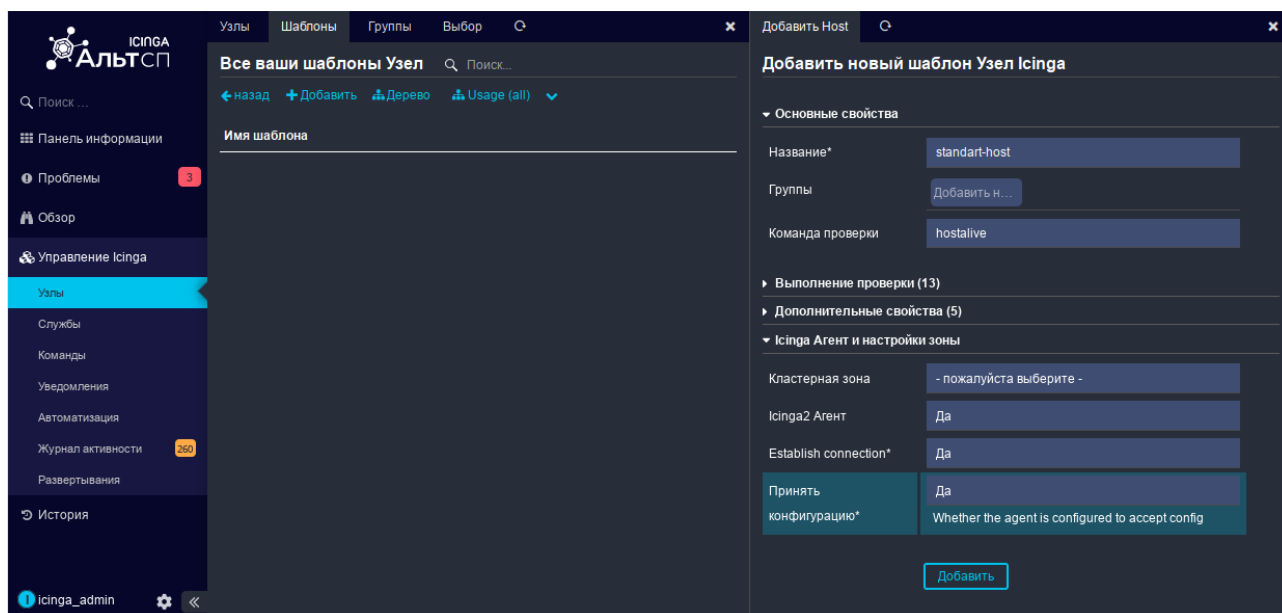


Рис. 99 – Создание шаблона узла

Для добавления набора служб в шаблон следует выделить созданный шаблон узла, затем на вкладке «Службы» нажать ссылку «Добавить набор служб» (рис. 100).

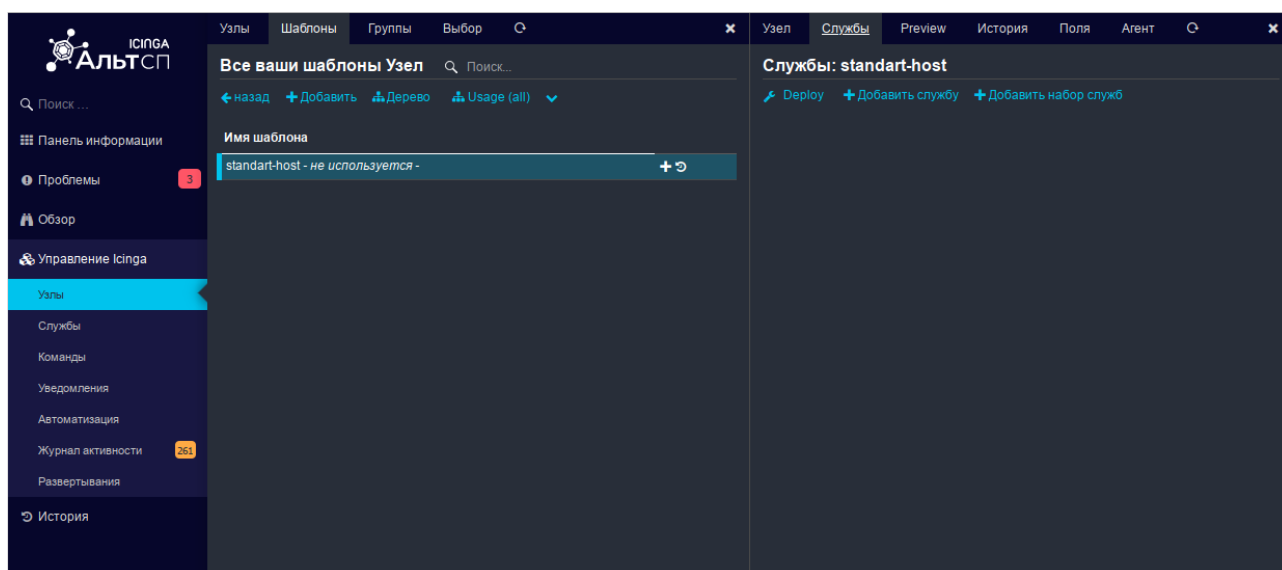


Рис. 100 – Ссылка «Добавить набор служб»

В открывшейся форме (рис. 101) необходимо выбрать созданный ранее набор услуг (standart-host) и нажать кнопку «Добавить».

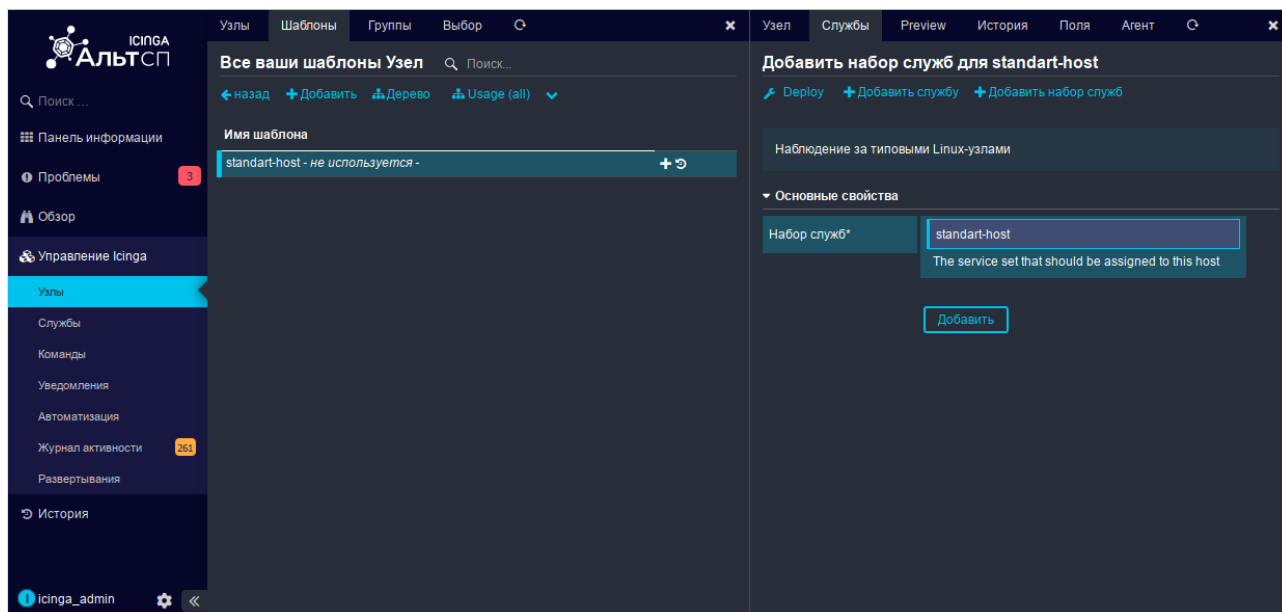


Рис. 101 – Добавление набора служб шаблону узла

На этом этапе шаблон узла создан и к нему добавлен набор служб. Теперь можно переходить к добавлению узла (агента) к Icinga2, с помощью Icinga Director (см. п. 7.7.3.2.5).

7.7.3.2.4. Импорт конфигурации Director из корзины

Корзины конфигурации позволяют экспортировать, импортировать, восстанавливать всю или часть конфигурации Icinga.

В пакете nagwad-icinga в каталоге /usr/share/doc/nagwad-icinga-master*/ есть готовая корзина (basket) шаблонов в формате JSON для наблюдения за событиями Nagwad. Шаблон для добавления узла называется d-nagwad-node.

Для импорта конфигурации необходимо перейти в раздел «Управление Icinga», выбрать ссылку «Настройка корзин» и в открывшейся справа форме нажать ссылку «Загрузка» (рис. 102). Указать имя корзины, выбрать файл шаблонов в формате JSON, нажав кнопку «Обзор» (рис. 103) и нажать кнопку «Загрузка».

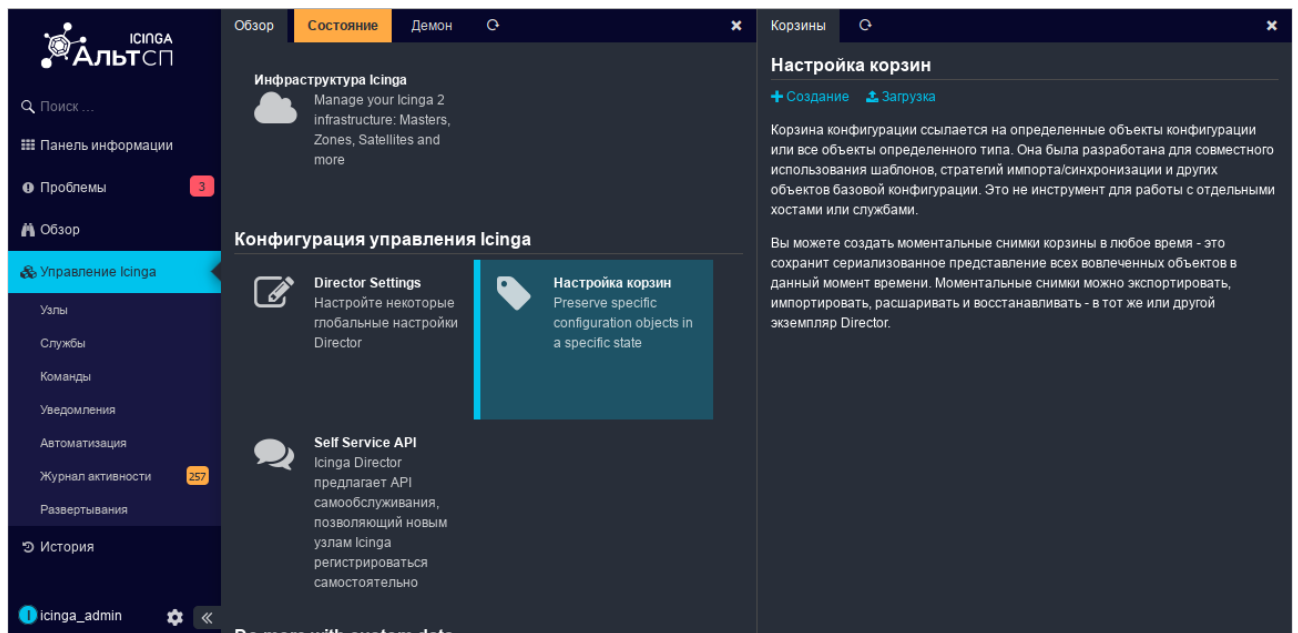


Рис. 102 – Настройка корзин

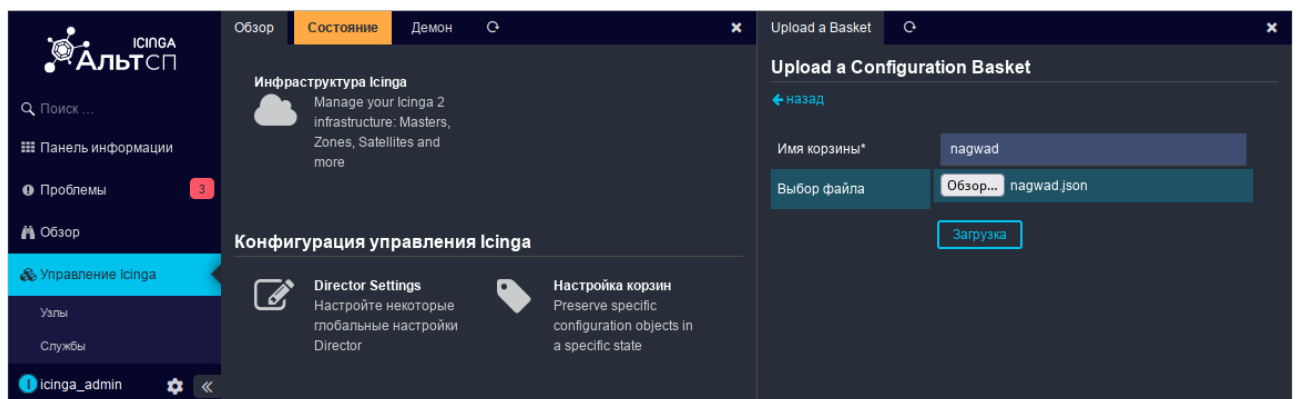


Рис. 103 – Загрузка корзины

Далее следует выбрать, должен ли каждый из элементов конфигурации отображаться в снимках этой корзины. Для каждого типа элемента доступны следующие варианты (рис. 104):

- «Все из них» – помещать все элементы этого типа в снимки (например, все шаблоны хостов);
- «Игнорировать» («Ignore») – не помещать этот элемент в снимки (например, не включать правила синхронизации);
- «Настраиваемый выбор» – помещать в снимок только указанные элементы этого типа. В этом случае нужно вручную отмечать каждый элемент.

Например, если отмечены шаблоны хостов, то нужно перейти к каждому из нужных шаблонов хостов и выбрать действие «Добавить в корзину». Это приведет к тому, что эти конкретные шаблоны хостов будут включены в следующий снимок.

Оставить значения по умолчанию и нажать кнопку «Принять». Будет создана корзина (рис. 105).

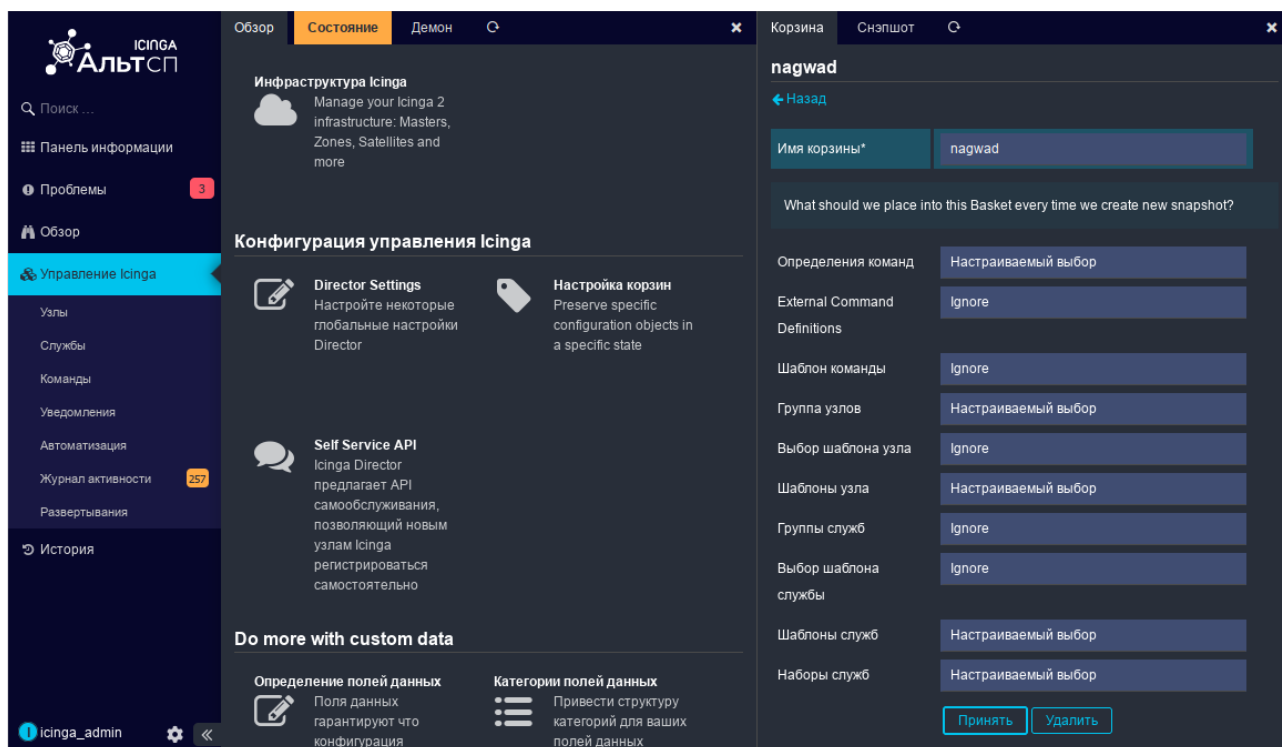


Рис. 104 – Выбор элементов конфигурации для корзины

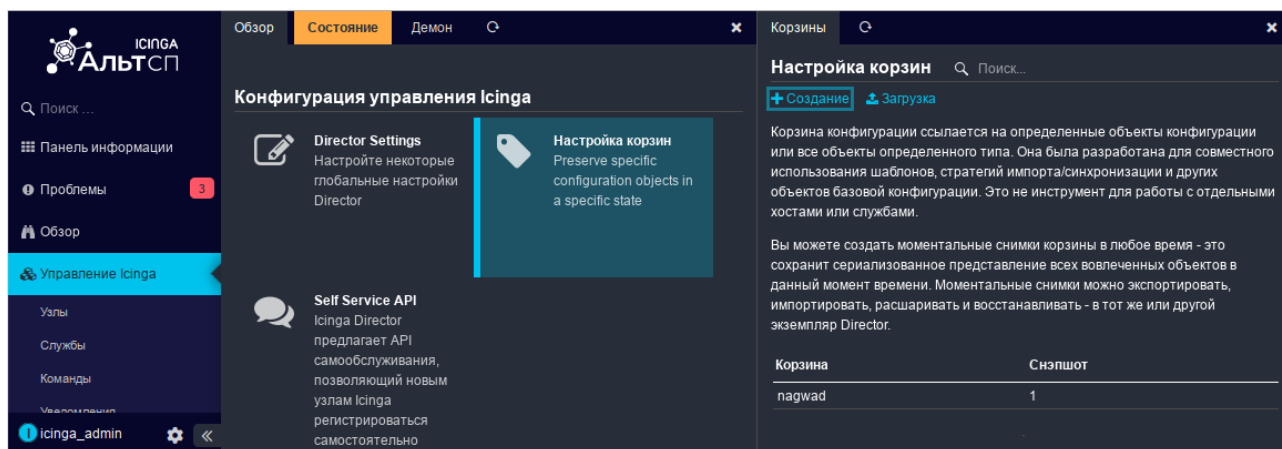


Рис. 105 – Корзина nagwad

Выбрать корзину из списка, перейти на вкладку «Снэпшот» (рис. 106) и выбрать снимок. В открывшейся справа форме нажать ссылку «Восстановление» (рис. 107), выбрать целевую базу данных и нажать кнопку «Восстановление». В результате будут созданы:

- команда (d_check_nagwad);
- шаблон группы (d-check-nodes);
- шаблон узла (d-nagwad-host);
- шаблоны служб (d-nagwad-service, d-nagwad-eperm, d-nagwad-login, d-nagwad-integralert, d-nagwad-print, d-nagwad-device, d-nagwad-authdata, d-nagwad-status);
- набор служб (d-nagwad-service-set).

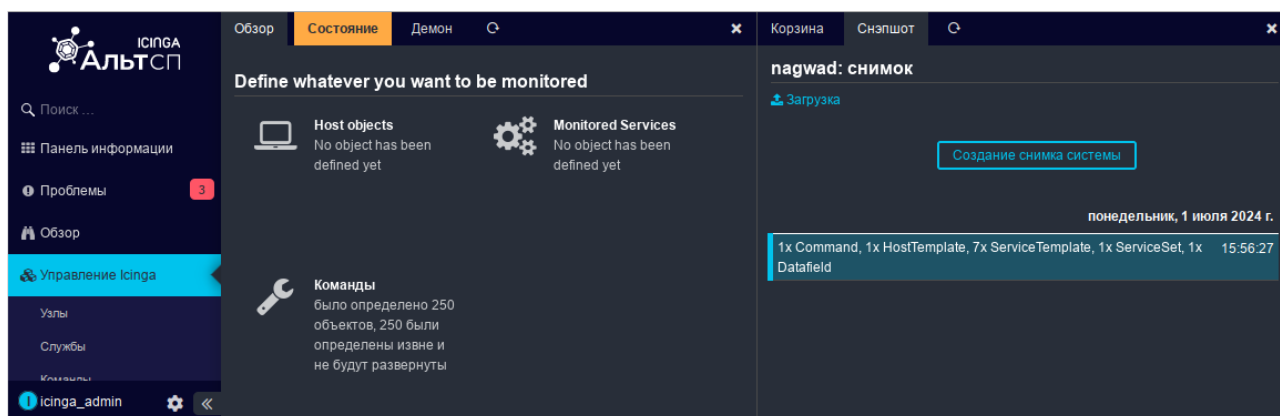


Рис. 106 – Вкладка «Снэпшот»

Далее необходимо убедиться, что шаблону узла добавлен набор служб. Для этого в разделе «Управление Icinga» → «Узлы» → «Шаблоны узла» выбрать шаблон d-nagwad-host, перейти на вкладку «Службы». Шаблону узла должны быть добавлены 7 служб из набора d-nagwad-service-set (рис. 108).

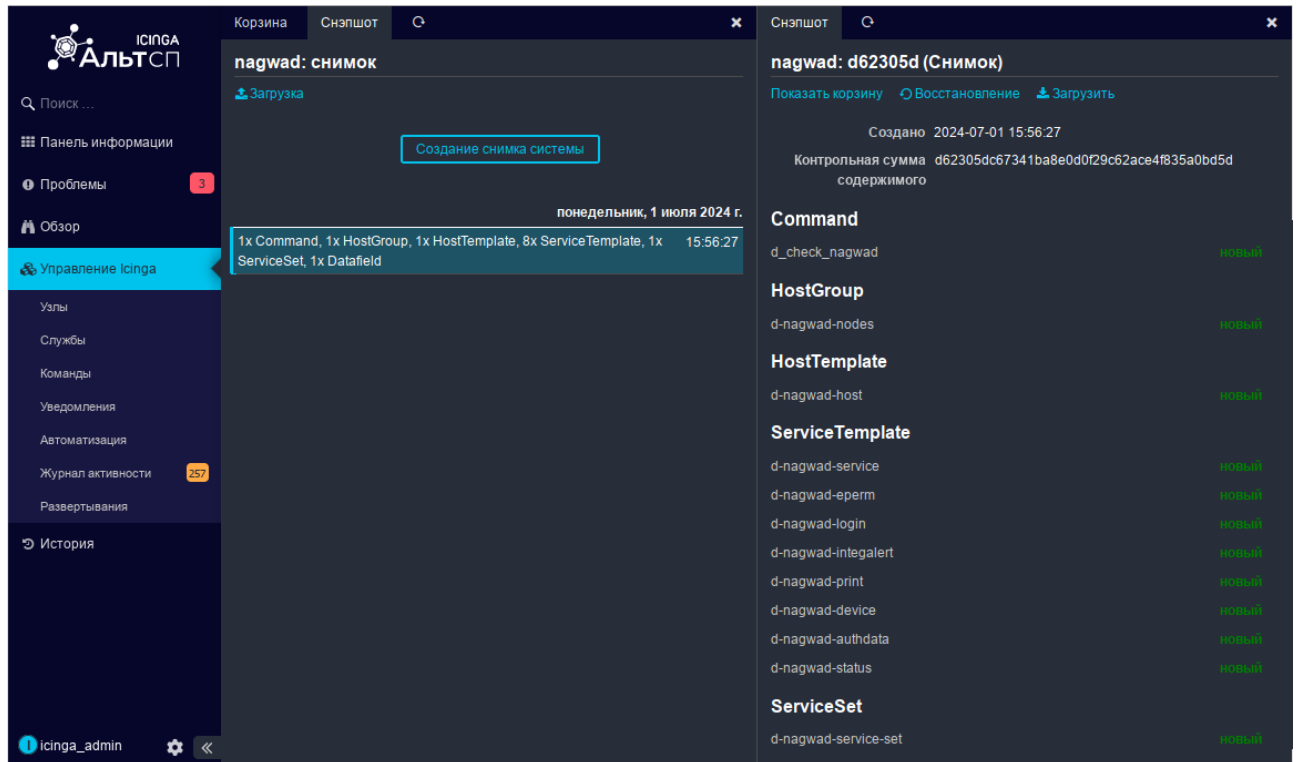


Рис. 107 – Просмотр снимка

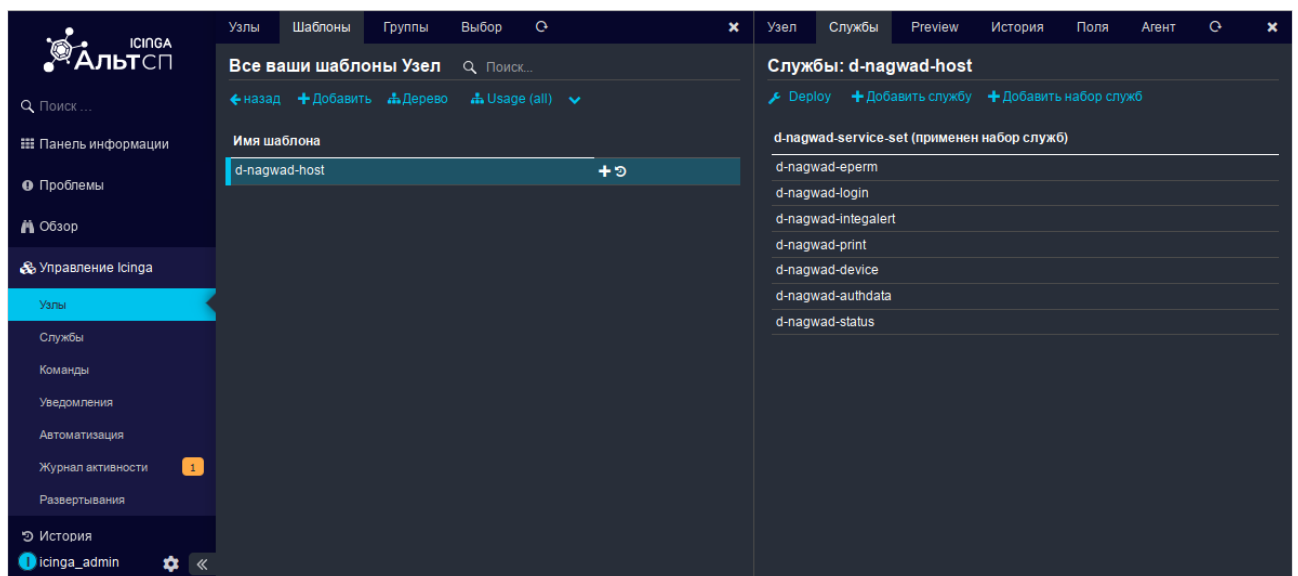


Рис. 108 – Службы, назначенные шаблону узла

7.7.3.2.5. Создание записи об агенте

Для создания записи о агенте с помощью Icinga Director перейти в раздел «Управление Icinga» → «Узлы» и на вкладке «Узлы» нажать ссылку «Добавить». В открывшейся справа форме добавления узла (рис. 109) заполнить следующие поля:

- «Host Template» – выбрать шаблон узла (можно выбрать несколько шаблонов, при этом если в разных шаблонах имеются одни и те же конфликтующие параметры, то к агенту будет применен тот параметр, который находится самым последним в этом списке шаблонов);
- «Имя узла» – FQDN-имя добавляемого узла;
- «Отображаемое имя» – имя имя агента, так как оно будет отображаться на веб-консоли;
- «Адрес узла» – IPv4-адрес добавляемого узла;
- «Группы» – группа, в которую будет добавлен узел.

Рис. 109 – Добавление нового агента

После создания новой записи о агенте, как и после прочих операций по созданию и изменению объектов в Icinga Director, необходимо применить сделанные изменения в действующую конфигурацию Icinga, то есть выполнить развертывание (Deploy) обновленной конфигурации. Для этого необходимо нажать ссылку «Deploy» (рис. 110). После добавления новый агент перейдет сначала в состояние «Рассматриваемый» (PENDING), а после проверки его сетевой доступности, в состояние «Включен» (UP). Службы же этого агента будут иметь статус UNKNOWN с сообщением об отсутствии настроенного соединения клиента с сервером.

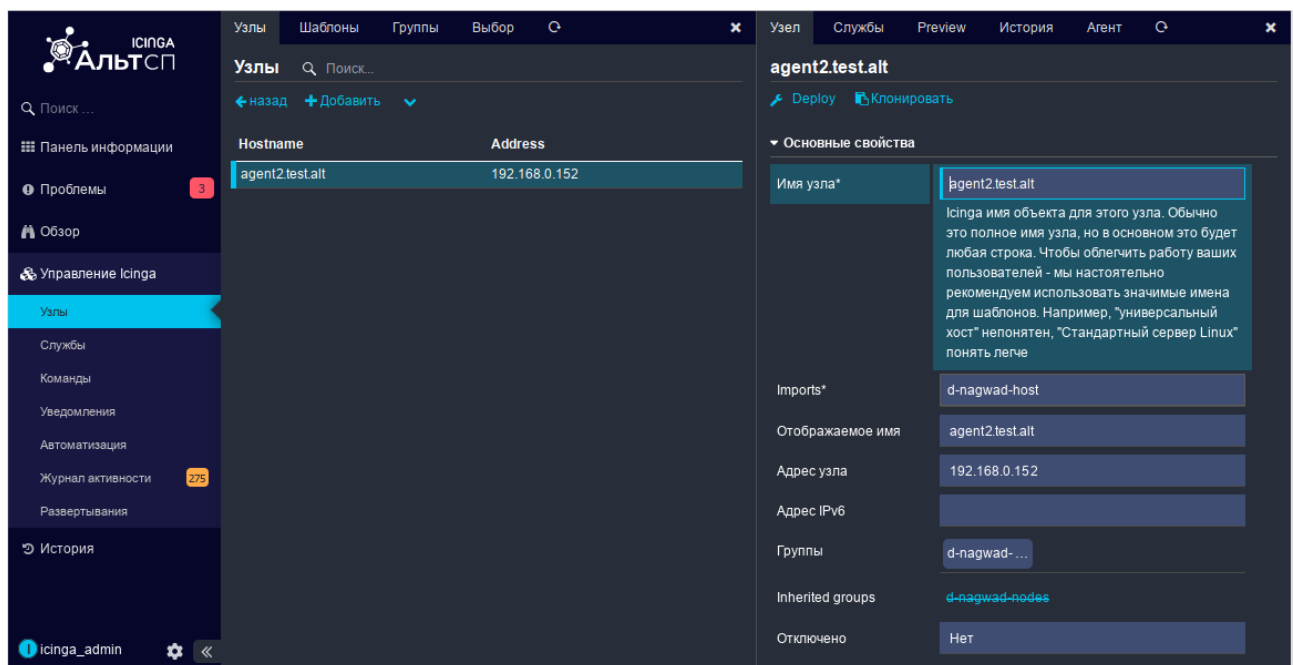


Рис. 110 – Созданный агент

Переключиться на вкладку «Агент» (рис. 111). Здесь можно найти билет (ticket) для настройки агента.

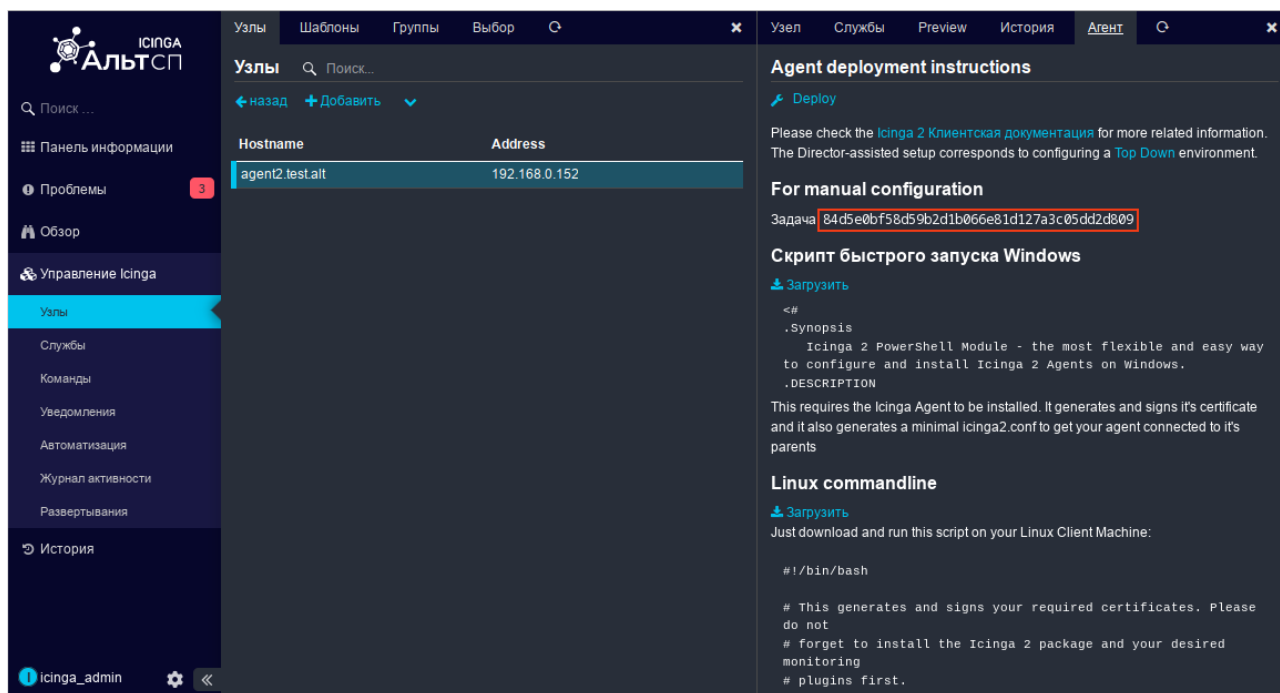


Рис. 111 – Вкладка «Агент»

7.7.3.2.6. Регистрация агента

Для регистрации агента может использоваться команда `icinga2-register-host`.

Синтаксис:

```
icinga2-register-host [options] [<Icinga Web 2 URL> <host-template-key>]
```

Возможные опции:

- `--name` – имя добавляемого узла (по умолчанию `hostname`);
- `--zone` – имя зоны (по умолчанию имя узла);
- `--address` – адрес добавляемого узла (по умолчанию `hostname`);
- `--remote` – адрес удаленной конечной точки в формате `CN[,HOST[,PORT]]` (по умолчанию адрес извлекается из указанного URL-адреса Icinga Web 2);
- `--parent-zone` – имя родительской зоны (по умолчанию `master`);
- `--trustedcert` – файл доверенного сертификата для проверки родительского узла (по умолчанию загрузка и проверка в интерактивном режиме);
- `--ticket` – билет Icinga2 для настройки узла (если этот параметр указан, то URL-адрес Icinga Web 2 не используется);

- --web-ca – файл CA для проверки URL-адреса Icinga Web 2;
- --no-web-ca – пропустить проверку URL-адреса Icinga Web 2.

Для настройки наблюдаемого узла с помощью билета следует запустить скрипт регистрации, на агенте, выполнив команду:

```
# icinga2-register-host --name agent2.test.alt --remote
master1.test.alt --ticket 84d5e0bf58d59b2d1b066e81d127a3c05dd2d809
```

где 84d5e0bf58d59b2d1b066e81d127a3c05dd2d809 – билет для настройки агента.

7.7.3.2.7. Регистрация агента через API самообслуживания Icinga Director (Self Service API)

Icinga Director предлагает API самообслуживания, позволяющий новым хостам, на которых работает агент Icinga, безопасно регистрироваться.

7.7.3.2.7.1. Конфигурация Icinga Director

Для настройки API самообслуживания необходимо перейти в раздел «Управление Icinga» и выбрать ссылку «Self Service API». Справа появится форма настроек API самообслуживания (рис. 112).

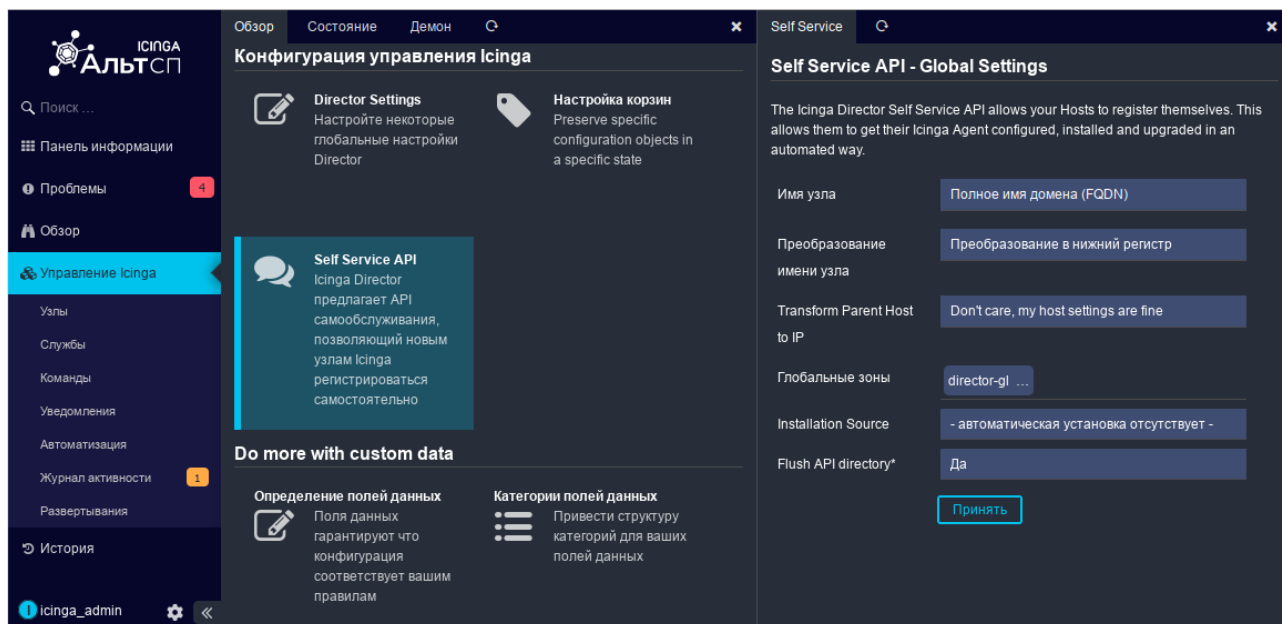


Рис. 112 – Настройка автоподключения

Для создания API ключа самообслуживания необходимо перейти в раздел «Управление Icinga» → «Узлы» → «Шаблоны узла», выбрать шаблон и в

открывшейся справа форме перейти на вкладку «Агент» и нажать кнопку «Создание API ключа самообслуживания» (рис. 113). В результате будет создан API ключ самообслуживания (рис. 114).

В шаблоне можно определить все виды пользовательских переменных, которые будут применяться автоматически.

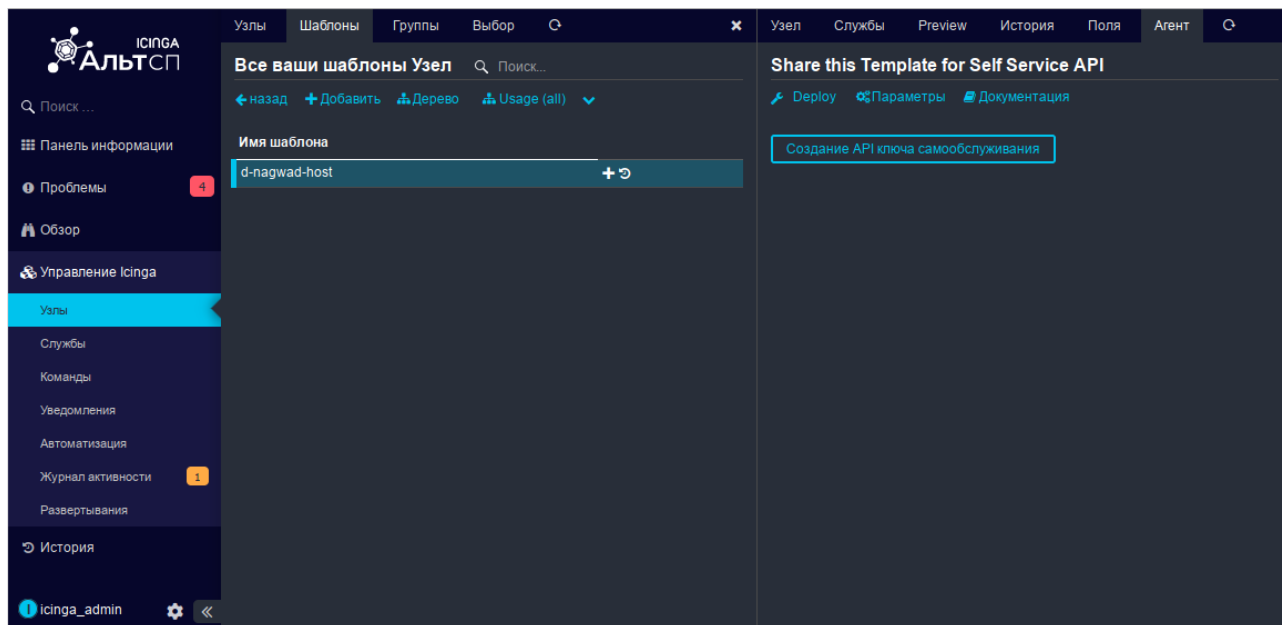


Рис. 113 – Создание API ключа самообслуживания

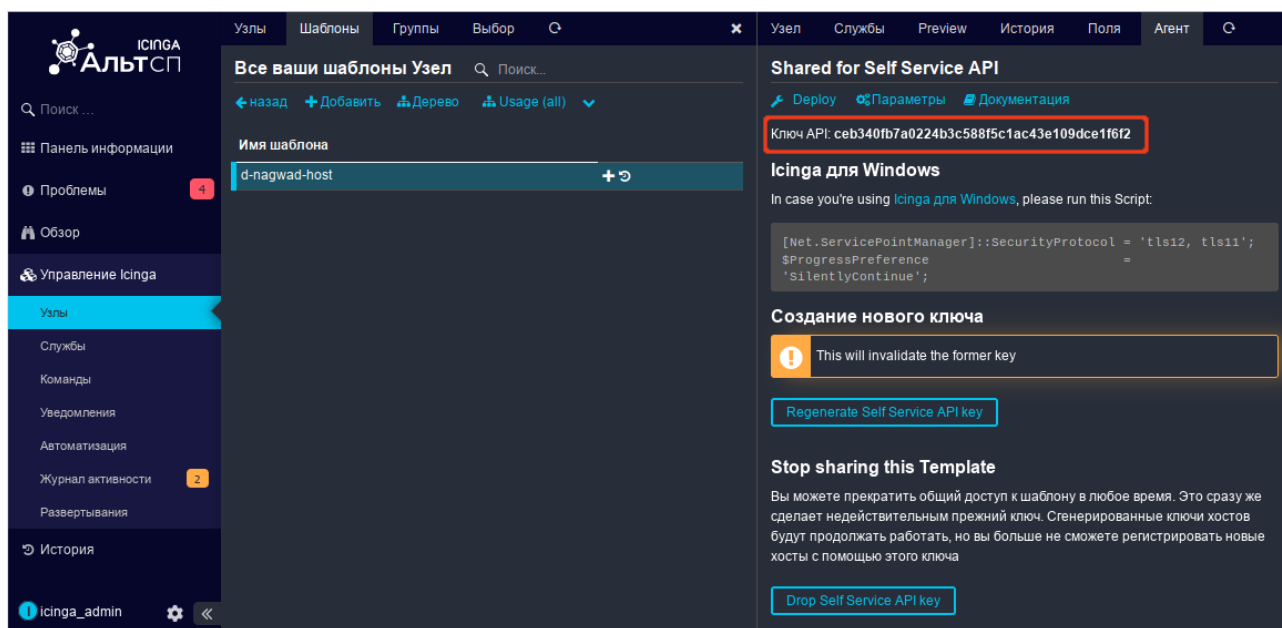


Рис. 114 – API ключ самообслуживания

7.7.3.2.7.2. Регистрация агента

Для регистрации агента может использоваться команда `icinga2-register-host`.

Для авторегистрации наблюдаемого узла следует запустить скрипт регистрации, на агенте, выполнив команду:

```
#      icinga2-register-host      --name      agent3.test.alt
http://192.168.0.170:81/icingaweb2 60ac7b9a9fc13a32196909ae4e93e438558a93f9
```

где `60ac7b9a9fc13a32196909ae4e93e438558a93f9` – API ключ самообслуживания.

В результате выполнения данного скрипта агент будет зарегистрирован через API самообслуживания Icinga Director.

7.7.3.2.8. Настройка службы синхронизации пользователей API

Для того, чтобы сценарий `10-push-icinga` (см. п. 7.7.3.2.9) мог нормально передавать данные с наблюдаемых узлов, необходимо обеспечить доступ с соответствующими правами к Icinga2 REST API. В целях обеспечения безопасности имеет смысл предоставлять такие права отдельно для каждого наблюдаемого узла, ограничивая сферу возможных действий данными, относящимися к этому узлу. Для этой цели можно использовать службу `icinga2-usersyncd`.

`icinga2-usersyncd` – служба синхронизации наблюдаемых узлов (объектов типа Host) с доступом по REST API (объектов типа `ApiUser`).

Настройка службы автоматической синхронизации (все команды выполняются на мастере):

- установить пакет:

```
# apt-get install icinga2-usersyncd
```

- сгенерировать клиентский сертификат для пользователя API `icinga2-usersyncd`:

```
# icinga2-usersyncd -setup
information/base:      Writing      private      key      to
'/var/lib/icinga2/certs/icinga2-usersyncd.key'.
information/base:  Writing  certificate  signing  request  to
'/var/lib/icinga2/certs/icinga2-usersyncd.req'.
information/pki:      Writing      certificate      to      file
'/var/lib/icinga2/certs/icinga2-usersyncd.crt'
```

- перезапустить сервис icinga2:

```
# systemctl restart icinga2
```

- запустить и добавить в автозагрузку службу icinga2-usersyncd:

```
# systemctl enable --now icinga2-usersyncd
```

Примечание. Конфигурационный файл службы icinga2-usersyncd /etc/sysconfig/icinga2-usersyncd. По умолчанию предполагается доступ к мастер-ноде через `https://localhost:5665/`.

Синтаксис команды icinga2-usersyncd:

```
icinga2-usersyncd [-v] [-q] [-c CONFIG] [--no-config] [-L URL] [-u USERNAME] [-p PASSWORD] [-C CERT] [-K KEY] [-A CA_CERT] [-Q QUEUE] [-P PREFIX] [-T TEMPLATES] [-f FILTER] [-t DELAY]
```

```
icinga2-usersyncd --setup
```

Возможные опции:

- -v, --verbose – подробный вывод сообщений;
- -q, --quiet – подавлять вывод сообщений;
- -c CONFIG, --config CONFIG – указать файл конфигурации (по умолчанию /etc/sysconfig/icinga2-usersyncd);
- --no-config – не использовать конфигурационный файл;
- -L URL, --url URL – Icinga2 API URL;
- -u USERNAME, --username USERNAME – пользователь для аутентификации в Icinga2 API;
- -p PASSWORD, --password PASSWORD – пароль пользователя для аутентификации в Icinga2 API;
- -C CERT, --cert CERT – сертификат для аутентификации в API Icinga2;
- -K KEY, --key KEY – ключ для аутентификации в API Icinga2;
- -A CA_CERT, --ca CA_CERT – сертификат API Icinga2 (CA);
- -Q QUEUE, --queue QUEUE – имя используемой очереди событий (по умолчанию либо из конфигурации, либо icinga2-usersyncd, если опущено);
- -P PREFIX, --prefix PREFIX – префикс для имен ApiUser (по умолчанию – либо из конфигурации, либо «host-», если он опущен);

- -T TEMPLATES, --templates TEMPLATES – набор шаблонов, которые должен импортировать каждый созданный ApiUser (по умолчанию – либо из конфигурации, либо [usersync], если опущено);
- -f FILTER, --filter FILTER – фильтр узла;
- -t DELAY, --delay DELAY – количество секунд ожидания между попытками подключения (по умолчанию – либо из конфигурации, либо 1, если опущено);
- --setup – сгенерировать сертификат для CN icinga2-usersyncd (сертификат будет создан в каталоге /var/lib/icinga2/certs/).

7.7.3.2.9. Настройка работы «пассивных» проверок

Скрипт пост-обработки событий 10-push-icinga (пакет nagwad-icinga-push) предназначен для отправки зарегистрированных событий на сервер Icinga2 через REST API не дожидаясь опроса со стороны мастер-узла. Одним из преимуществ использования этого скрипта является то, что он может снимать флаг подтверждения для события каждый раз, когда регистрируется новое событие того же типа.

Для возможности работы «пассивных» проверок на агенте необходимо установить пакет:

```
# apt-get install nagwad-icinga-push
```

Скрипт 10-push-icinga считывает свою конфигурацию из файла /etc/nagwad/process-event.d/push-icinga.conf и не требует настроек при условии, что узел правильно настроен как агент/спутник Icinga2 (если для регистрации агента использовалась команда icinga2-register-host). Скрипт использует SSL-сертификаты из каталога /var/lib/icinga2/certs).

Однако для использования Icinga2 REST API на сервере должен быть настроен ApiUser с соответствующим набором прав. Для этой цели удобно использовать демон icinga2-usersyncd (см. п. 7.7.3.2.8).

7.7.4. Работа с Icinga

7.7.4.1. Проверка сигнальных файлов

Проверка сигнальных файлов Nagwad производится средствами Icinga и Nagios с помощью сценария `check_nagwad`, которому в качестве аргумента требуется передать имя фильтра:

```
/usr/lib/nagios/plugins/check_nagwad <имя_фильтра>
```

Если сигнальный файл отсутствует, сценарий завершается с кодом 0 и выводит строку `OK: Nothing detected for <имя_фильтра>` (рис. 115). Если же сигнальный файл присутствует, выводится содержащаяся в нем информация (за исключением имени фильтра) (рис. 116), а код завершения сценария соответствует уровню критичности события.

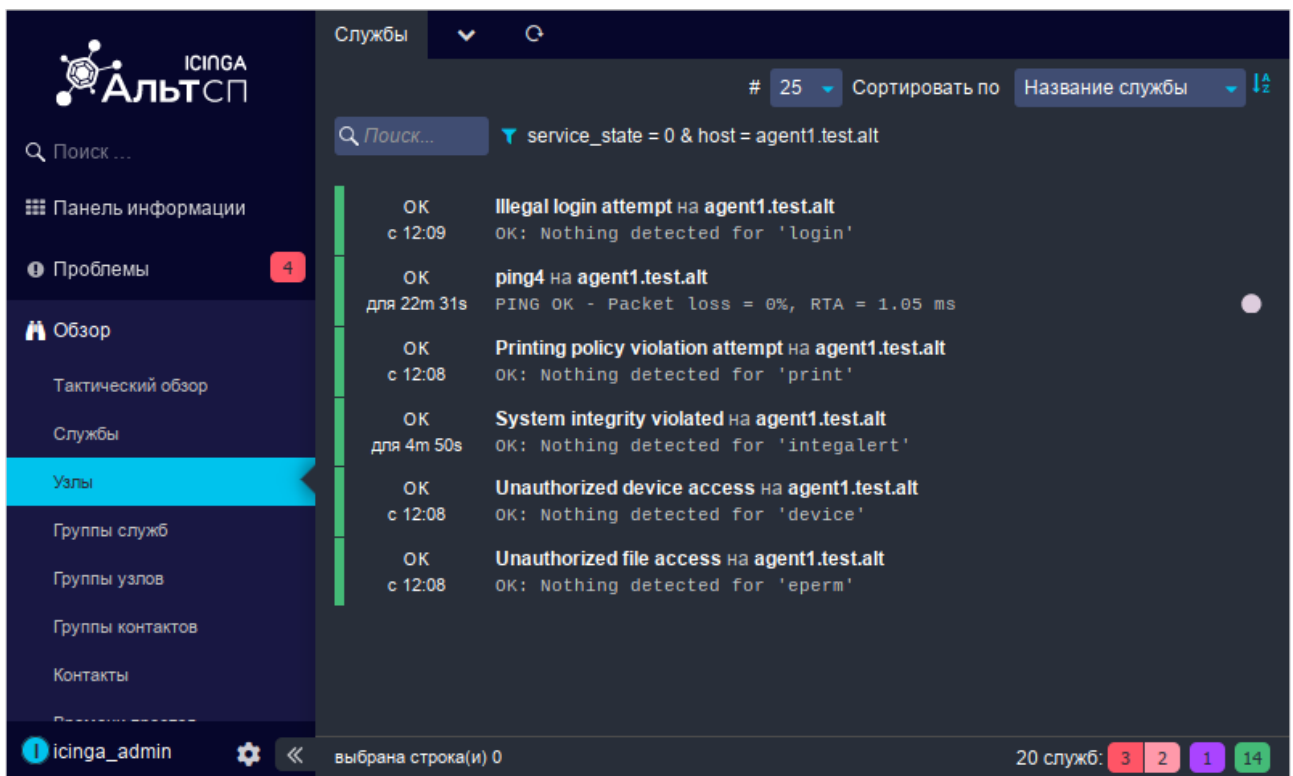


Рис. 115 – Сценарии, завершившиеся с кодом 0



Рис. 116 – Информация из сигнального файла

При наличии нескольких сигнальных файлов, связанных с событием одного и того же типа, сперва обрабатываются сигнальные файлы уровня CRITICAL.

7.7.4.2. Пометка проблем (событий) как разрешенных

После того как событие зафиксировано и обработано, администратор безопасности может пометить сигнальный файл на управляемой машине как решенный. Для этого можно переименовать файл (в каталоге `/var/log/nagwad/<boot_id>/<имя_фильтра>`), изменив суффикс файла на `FIXED` или использовать команду `nagwad fix`.

Пример использования команды `nagwad fix` для пометки проблемы, как разрешенной:

- просмотреть список зарегистрированных событий:

```
# nagwad
2024-07-01+16:35:10.5837078000 integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
2024-07-01+16:35:10.5837078000 integralert.62476f6497eaf88fe1f46d1f5382e.CRITICAL
```

- просмотреть конкретное событие:

```
# nagwad show integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
CRITICAL:          integralert:CRITICAL:2024-07-01T16:35:10+0200          agent3.test.alt
integralert[2371]: System integrity check (chg=3,add=55,del=0)
```

- пометить событие как исправленное:

```
# nagwad fix integralert.e30128170ee5b3871821adaf5ad75.CRITICAL
```

7.8. ГОСТ в OpenSSL

7.8.1. Поддержка шифрования по ГОСТ в OpenSSL

Для включения поддержки шифрования ГОСТ в OpenSSL нужно выполнить следующие действия:

1) установить пакет:

```
# apt-get install openssl-gost-engine
```

2) изменить конфигурационный файл OpenSSL, выполнив команду:

```
# control openssl-gost enabled
```

3) проверить, доступны ли шифры ГОСТ для OpenSSL:

```
$ openssl ciphers|tr ':' '\n'|grep GOST
GOST2012-GOST8912-GOST8912
GOST2001-GOST89-GOST89
```

7.8.2. Создание ключей

Пример генерации закрытого ключа с алгоритмом ГОСТ-2012:

```
$ openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCA \
-out ca.key
```

Пример создания сертификата на 365 дней (ca.cer):

```
$ openssl req -new -x509 -md_gost12_256 -days 365 -key ca.key -out ca.cer \
-subj "/C=RU/ST=Russia/L=Moscow/O=SuperPlat/OU=SuperPlat CA/CN=SuperPlat CA Root"
```

Проверка сертификата (ca.cer):

```
$ openssl x509 -in ca.cer -text --noout
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

0c:dc:50:10:4b:de:a8:0f:ed:3f:0c:81:5c:7d:d3:15:55:87:52:69

Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)

Issuer: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat

CA, CN = SuperPlat CA Root

Validity

Not Before: Nov 22 10:24:23 2024 GMT

Not After : Nov 22 10:24:23 2025 GMT

Subject: C = RU, ST = Russia, L = Moscow, O = SuperPlat, OU = SuperPlat

CA, CN = SuperPlat CA Root

Subject Public Key Info:

Public Key Algorithm: GOST R 34.10-2012 with 256 bit modulus

Public key:

```
X:AC949E79BCDC65E4808635A069DB5078F555EBD5E8C25B72426B701FDF6E68D5
```


Y:AF06E27ABC4D92CAD091F857CEB54A85738A5193ABE50E25025F9D129272683A

Parameter set: GOST R 34.10-2012 (256 bit) ParamSet A

X509v3 extensions:

X509v3 Subject Key Identifier:

61:EC:DB:51:A6:A0:5F:79:C3:4C:A1:0B:E9:7B:7B:47:D5:AD:E6:DF

X509v3 Authority Key Identifier:

keyid:61:EC:DB:51:A6:A0:5F:79:C3:4C:A1:0B:E9:7B:7B:47:D5:AD:E6:DF

X509v3 Basic Constraints:

CA:TRUE

Signature Algorithm: GOST R 34.10-2012 with GOST R 34.11-2012 (256 bit)

1c:12:59:e5:c0:2d:db:ec:c2:db:6a:4b:38:d9:e7:4c:09:9e:

d0:9b:78:33:6b:1f:ba:39:db:55:4a:0b:9e:1a:11:9c:cd:00:

b2:59:50:88:bc:61:a0:27:94:c7:e9:35:24:de:42:dc:08:d3:

fd:32:27:35:d3:7c:1a:4b:3c:19

7.9. Утилита уничтожения информации при удалении – dm-secdel

Операции удаления обычно ограничиваются пометкой блоков данных как «неиспользуемых» в файловой системе. Утилита dm-secdel так же помечает блоки как неиспользуемые, но заменяет очищение записью случайных данных в освобождаемые блоки. Таким образом, данные удаляются надежно.

В силу своего абстрактного характера dm-secdel поддерживает множество файловых систем, которые поддерживают опцию discard (например, ext3, ext4, xfs, btrfs).

⚠ Следует создать сопоставленное устройство с помощью инструмента secdelsetup. Убедиться, что файловая система (ФС) смонтирована на это, а не основное устройство. Убедиться, что ФС установлена с опцией `-o discard`.

Проверить, смонтирована ли ФС в данный момент с этой опцией, можно посмотрев вывод команды mount:

```
/dev/sdd1 on / type ext4 (rw,discard,errors=remount-ro)
```

Не следует включать ведение журнала данных. Обратите внимание, что при удалении файлов командой `rm` удаление будет выполняться асинхронно, поэтому, чтобы убедиться, что данные уже удалены, следует использовать команду `sync` или опцию монтирования файловой системы `-o sync` до использования команды `rm`.

Если нужно, чтобы имена файлов также были уничтожены, во-первых, следует убедиться, что файловая система создана полностью без ведения журнала

(например, `mkfs.ext4 -O ^has_journal`), а во-вторых, удалите сам каталог, тогда его блоки освободятся и будут стерты.

При использовании команды `fstrim` все свободные блоки файловой системы будут отброшены (`discarded`) и, следовательно, также стерты (файловая система должна быть примонтирована с опцией `-o discard`).

Применение:

```
secdelsetup <источник-устройство> [маппинг]
```

Опции:

- 1) `-d|--detach <устройство>` – отсоединить устройство;
- 2) `-D|--detach-all|--stop` – отключить все устройства;
- 3) `-l|--list` – список активных карт устройства;
- 4) `-a|--all` – список в другом формате;
- 5) `--lsblk` – вывод в формате `lsblk`;
- 6) `--start` – запускать устройства из `secdeltab`;
- 7) `--save` – сохранение активных устройств в `secdeltab`.

Пример: пусть `/home` находится на устройстве `/dev/sda5`, закомментировать строку с разделом `/home` в файле `/etc/fstab` и выполнить перезагрузку системы.

Проверить наличие журналирования на устройстве, выполнить команду:

```
dumpe2fs /dev/sda5 | grep has_journal
```

Если параметры журналирования найдены, отключить их с помощью команды:

```
tune2fs -O ^has_journal /dev/sda5
```

Создадим для `/dev/sda5` сопоставленное устройство (карта) (по умолчанию задается один проход со случайными битами):

```
# secdelsetup /dev/sda5
```

Пример ожидаемого вывода команды:

```
/dev/mapper/secdel0 is attached to /dev/sda5
```

где `/dev/mapper/secdel0` имя созданного сопоставленного устройства.

В файл `/etc/fstab` добавить новую строку, указывающую на точку монтирования `/home`:

```
/dev/mapper/secdel0 /home ext4 noexec,nosuid,relatime,discard 1 2
```

Затем `/dev/mapper/secdel0` должно быть смонтировано с параметром `-o discard`, выполнить команды:

```
# mkdir /mnt/test/  
# mount /dev/mapper/secdel0 /mnt/test/ -o discard
```

Команда просмотра текущих (существующих) карт:

```
# secdelsetup -all  
/dev/mapper/secdel0 /dev/sda5
```

Для хранения конфигурации карт используется файл `/etc/secdeltab`, который будет автоматически активирован после перезагрузки (системной службой `secdeltab.service`). Для сохранения текущих карт в файл выполнить команду:

```
# secdelsetup --save
```

Для изменения перезаписи, например, с тремя проходами (первый проход – 1, второй проход случайные биты – R, третий проход – 0) выполнить команду:

```
# secdelsetup /dev/sda5 /dev/mapper/secdel0 1R0
```

Перед отсоединением отмонтировать устройство:

```
# umount /mnt/test/
```

Команда отсоединения всех активных карт:

```
# secdelsetup --detach-all
```

Пример ожидаемого вывода команды:

```
detach /dev/mapper/secdel0
```

8. СРЕДСТВА УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Дальнейшие разделы описывают некоторые возможности использования ОС, настраиваемые в ЦУС.

⚠ Последующие пункты рекомендуются к прочтению опытным пользователям и системным администраторам.

8.1. Вход в систему

Для начала работы по настройке системы сразу после ее установки, нужно использовать веб-ориентированный интерфейс ЦУС (см. п. 7.1.2), позволяющий управлять выбранным компьютером с любого другого в сети.

8.2. Настройка подключения к Интернету

Помимо множества различных служб, которые ОС Альт СП может предоставлять компьютерам сети, важно определить, будет ли сервер предоставлять общий доступ в Интернет для компьютеров домена или нет. В зависимости от этого сервер можно рассматривать как:

- сервер без подключения к сети Интернет – это сервер с одним сетевым интерфейсом (одной сетевой картой), который и связывает его с компьютерами локальной сети. Такой сервер называется также сервер рабочей группы;
- шлюз – в этом случае сервер обычно имеет два сетевых интерфейса (например, две сетевые карты), одна из которых служит для подключения к локальной сети, а другая – для подключения к сети Интернет.

Как для обеспечения доступа в сеть Интернет самого сервера, так и для настройки общего выхода в Интернет для компьютеров сети нужно настроить подключение к Интернету на самом сервере.

Для настройки подключения к сети Интернет можно воспользоваться одним из разделов ЦУС «Сеть»:

- Ethernet-интерфейсы (см. п. 8.2.1);
- PPTP-соединения;

- PPPoE-соединения;
- OpenVPN-соединения (см. п. 8.3).

8.2.1. Конфигурирование сетевых интерфейсов

Конфигурирование сетевых интерфейсов осуществляется в модуле ЦУС «Ethernet-интерфейсы» (пакет alterator-net-eth) из раздела «Сеть» (рис. 117).

Имя компьютера: server

Интерфейсы

enp0s3

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:f1:99:3a

Версия протокола IP: IPv4 ☒ Включить

Конфигурация: Вручную

IP-адреса:

192.168.0.191/24 Удалить

Добавить + IP: /24 (255.255.255.0) Добавить

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 192.168.0.2

Домены поиска:
(несколько значений записываются через пробел)

Дополнительно...

Создать объединение... Удалить объединение... Настроить объединение...

Создать сетевой мост... Удалить сетевой мост... Настроить сетевой мост...

Применить Сбросить

Рис. 117 – Настройка модуля «Ethernet-интерфейсы»

В модуле «Ethernet-интерфейсы» можно заполнить следующие поля:

- «Имя компьютера» – указать сетевое имя ПЭВМ в поле для ввода имени компьютера (это общий сетевой параметр, не привязанный к какому-либо конкретному интерфейсу);
- «Интерфейсы» – выбрать доступный сетевой интерфейс, для которого будут выполняться настройки;
- «Версия протокола IP» – указать в выпадающем списке версию используемого протокола IP (IPv4, IPv6) и убедиться, что пункт «Включить», обеспечивающий поддержку работы протокола, отмечен;

- «Конфигурация» – выбрать способ назначения IP-адресов (службы DHCP, Zeroconf, вручную);
- «IP-адреса» – пул назначенных IP-адресов из поля «Добавить ↑ IP», выбранные адреса можно удалить нажатием кнопки «Удалить»;
- «Добавить ↑ IP» – ввести IP-адрес вручную и выбрать в выпадающем поле предпочтительную маску сети. Для переноса адреса в пул поля «IP-адреса» необходимо нажать кнопку «Добавить»;
- «Шлюз по умолчанию» – в поле для ввода нужно ввести адрес шлюза, который будет использоваться сетью по умолчанию;
- «DNS-серверы» – в поле для ввода нужно ввести список предпочтительных DNS-серверов, которые будут получать информацию о доменах, выполнять маршрутизацию почты и управлять обслуживающими узлами для протоколов в домене;
- «Домены поиска» – в поле для ввода нужно ввести список предпочтительных доменов, по которым будет выполняться поиск. Если в поле «Домены поиска» перечислить наиболее часто используемые домены (например, domain), то можно пользоваться неполными именами машин (computer вместо computer.domain).

«IP-адрес» и «Маска сети» – обязательные параметры каждого узла IP-сети.

Первый параметр – уникальный идентификатор машины, от второго напрямую зависит, к каким машинам локальной сети данная машина будет иметь доступ. Если требуется выход во внешнюю сеть, то нужно указать параметр «Шлюз по умолчанию».

В случае наличия DHCP-сервера можно все вышеперечисленные параметры получить автоматически – выбрав в списке «Конфигурация» пункт «Использовать DHCP».

Имя компьютера: server

Интерфейсы

enp0s3

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:f1:99:3a

Версия протокола IP: IPv4 ☒ Включить

Конфигурация: Использовать DHCP

IP-адреса: 192.168.0.191/24 Удалить

Добавить + IP: /24 (255.255.255.0) Добавить

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 192.168.0.2

Домены поиска:
(несколько значений записываются через пробел)

Дополнительно...

Создать объединение... Удалить объединение... Настроить объединение...

Создать сетевой мост... Удалить сетевой мост... Настроить сетевой мост...

Применить Сбросить

Рис. 118 – Автоматическое получение настроек от DHCP-сервера

Дополнительно для каждого интерфейса можно настроить сетевую подсистему (NetworkManager, Etcnet), а также должен ли запускаться данный интерфейс при загрузке системы (рис. 119).

Интерфейс: enp0s3

Сетевая подсистема: Etcnet

Запускать интерфейс при загрузке системы ☒

OK Отмена

Рис. 119 – Выбор сетевой подсистемы

В списке «Сетевая подсистема» можно выбрать следующие режимы:

- «Etcnet» — в этом режиме настройки берутся исключительно из файлов, находящихся в каталоге настраиваемого интерфейса `/etc/net/ifaces/<интерфейс>`. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`;

- «NetworkManager (etcnet)» – в этом режиме NetworkManager сам иницирует сеть, используя в качестве параметров – настройки из файлов Etcnet. Настройки сети могут изменяться либо в ЦУС в данном модуле, либо напрямую через редактирование файлов `/etc/net/ifaces/<интерфейс>`. В этом режиме можно просмотреть настройки сети, например полученный по DHCP IP-адрес, через графический интерфейс NetworkManager;
- «NetworkManager (native)» – в данном режиме управление настройками интерфейса передается NetworkManager и не зависит от файлов Etcnet. Управлять настройками можно через графический интерфейс NetworkManager. Файлы с настройками находятся в директории `/etc/NetworkManager/system-connections`. Этот режим особенно актуален для задач настройки сети на клиенте, когда IP-адрес нужно получать динамически с помощью DHCP, а DNS-сервер указать явно. Через ЦУС так настроить невозможно, так как при включении DHCP отключаются настройки, которые можно задавать вручную;
- «Не контролируется» – в этом режиме интерфейс находится в состоянии DOWN (выключен).

8.2.2. Объединение сетевых интерфейсов

Модуль «Объединение интерфейсов» (пакет `alterator-net-bond`) позволяет объединить несколько физических сетевых интерфейсов в один логический. Это позволяет достичь отказоустойчивости, увеличения скорости и балансировки нагрузки.

Для создания объединения интерфейсов необходимо выполнить следующие действия:

- 1) нажать на кнопку «Создать объединение...» (рис. 120);

Имя компьютера: server

Интерфейсы

enp0s3
enp0s8

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:87:a2:24

Версия протокола IP: IPv4 ☒ Включить

Конфигурация: Вручную

IP-адреса: 192.168.0.185/24 Удалить

Добавить IP: /24 (255.255.255.0) Добавить

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 8.8.8.8

Домены поиска:
(несколько значений записываются через пробел)

Дополнительно...

Создать объединение... Удалить объединение... Настроить объединение...

Создать сетевой мост... Удалить сетевой мост... Настроить сетевой мост...

Применить Сбросить

Рис. 120

- 2) переместить сетевые интерфейсы, которые будут входить в объединение, из списка «Доступные интерфейсы» в список «Используемые интерфейсы» (рис. 121);
- 3) выбрать режим объединения:
 - «Round-robin» – режим циклического выбора активного интерфейса для исходящего трафика;
 - «Активный-резервный» – активен только один интерфейс, остальные находятся в режиме горячей замены;
 - «XOR» – один и тот же интерфейс работает с определенным получателем, передача пакетов распределяется между интерфейсами на основе формулы $((\text{MAC-адрес источника}) \text{ XOR } (\text{MAC-адрес получателя})) \% \text{ число интерфейсов}$;

- «Широковещательная» – трафик идет через все интерфейсы одновременно;
 - «Агрегирование каналов по стандарту IEEE 802.3ad» – в группу объединяются одинаковые по скорости и режиму интерфейсы, все физические интерфейсы используются одновременно в соответствии со спецификацией IEEE 802.3ad. Для реализации этого режима необходима поддержка на уровне драйверов сетевых карт и коммутатор, поддерживающий стандарт IEEE 802.3ad (коммутатор требует отдельной настройки);
 - «Адаптивная балансировка нагрузки передачи» – исходящий трафик распределяется в соответствии с текущей нагрузкой (с учетом скорости) на интерфейсах (для данного режима необходима его поддержка в драйверах сетевых карт). Входящие пакеты принимаются только активным сетевым интерфейсом;
 - «Адаптивная балансировка нагрузки» – включает в себя балансировку исходящего трафика и балансировку на прием (rlb) для IPv4 трафика и не требует применения специальных коммутаторов. Балансировка на прием достигается на уровне протокола ARP путем перехвата ARP ответов локальной системы и перезаписи физического адреса на адрес одного из сетевых интерфейсов (в зависимости от загрузки);
- 4) указать, если это необходимо, параметры объединения в поле «Параметры объединения»;
 - 5) нажать на кнопку «Назад»;
 - 6) в результате будет создан агрегированный интерфейс bond0. Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (рис. 122);
 - 7) нажать на кнопку «Применить».

Объединенный интерфейс bond0

Используемые интерфейсы: enp0s3, enp0s8

Доступные интерфейсы:

Политика:

- ☐ Round-robin
- ☐ Активный-резервный
- ☐ XOR
- ☐ Широковещательная
- ☒ Агрегирование каналов по стандарту IEEE 802.3ad
- ☐ Адаптивная балансировка нагрузки передачи
- ☐ Адаптивная балансировка нагрузки

Параметры объединения: miimon=100 lacp_rate=1 xmit_hash_policy=2

[Назад](#)

Рис. 121 – Выбор сетевых интерфейсов для объединения

Имя компьютера: server

Интерфейсы

bond0

Объединение: enp0s3 enp0s8
Интерфейс ВЫКЛЮЧЕН

Версия протокола IP: IPv4 ☒ Включить

Конфигурация: Вручную

IP-адреса: 192.168.0.185/24 [Удалить](#)

Добавить IP: /24 (255.255.255.0) [Добавить](#)

Шлюз по умолчанию: 192.168.0.1

DNS-серверы: 8.8.8.8

Домены поиска:
(несколько значений записываются через пробел)

[Дополнительно...](#)

[Создать объединение...](#) [Удалить объединение...](#) [Настроить объединение...](#)

[Создать сетевой мост...](#) [Удалить сетевой мост...](#) [Настроить сетевой мост...](#)

[Применить](#) [Сбросить](#)

Рис. 122 – Настройки интерфейса bond0

Информацию о получившемся агрегированном интерфейсе можно посмотреть в `/proc/net/bonding/bond0`.

Для удаления агрегированного интерфейса необходимо выбрать его в списке «Интерфейсы» и нажать на кнопку «Удалить объединение...».

8.2.3. Сетевые мосты

Модуль «Сетевые мосты» (пакет `alterator-net-bridge`) позволяет организовать виртуальный сетевой мост.

⚠ Если интерфейсы, входящие в состав моста, являются единственными физически подключенными и настройка моста происходит с удаленного узла через эти интерфейсы, то требуется соблюдать осторожность, так как эти интерфейсы перестанут быть доступны.

Для создания Ethernet-моста необходимо выполнить следующие действия:

- 1) у интерфейсов, которые будут входить в мост, удалить IP-адреса и шлюз по умолчанию (если они были установлены);
- 2) нажать на кнопку «Создать сетевой мост...»(рис. 123);

Имя компьютера:

Интерфейсы

enp0s3
enp0s8

Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller
провод подсоединён
MAC: 08:00:27:33:68:99

Версия протокола IP: ☒ Включить
Конфигурация:

IP-адреса:

Добавить + IP:

Шлюз по умолчанию:

DNS-серверы:

Домены поиска:
(несколько значений записываются через пробел)

Рис. 123 – Настройка сети в веб-интерфейсе

- 3) в окне «Сетевые мосты» в поле «Интерфейс-мост» ввести имя моста;
- 4) в выпадающем списке «Тип моста» выбрать тип моста: «Linux Bridge» (по умолчанию) или «Open vSwitch»;
- 5) переместить сетевые интерфейсы, которые будут входить в мост, из списка «Доступные интерфейсы» в список «Члены»;
- 6) нажать на кнопку «Ок» (рис. 124);

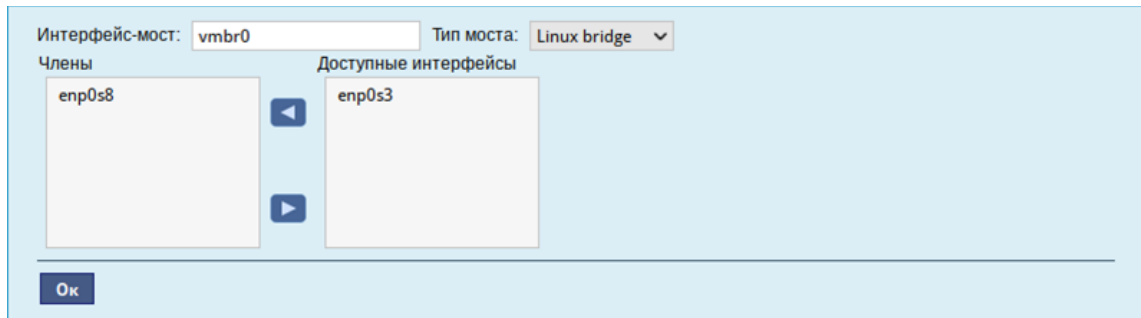


Рис. 124 – Выбор сетевых интерфейсов для моста

- 7) в результате будет создан сетевой интерфейс моста (в примере vmbr0). Для данного интерфейса можно задать IP-адрес и, если необходимо, дополнительные параметры (рис. 125);

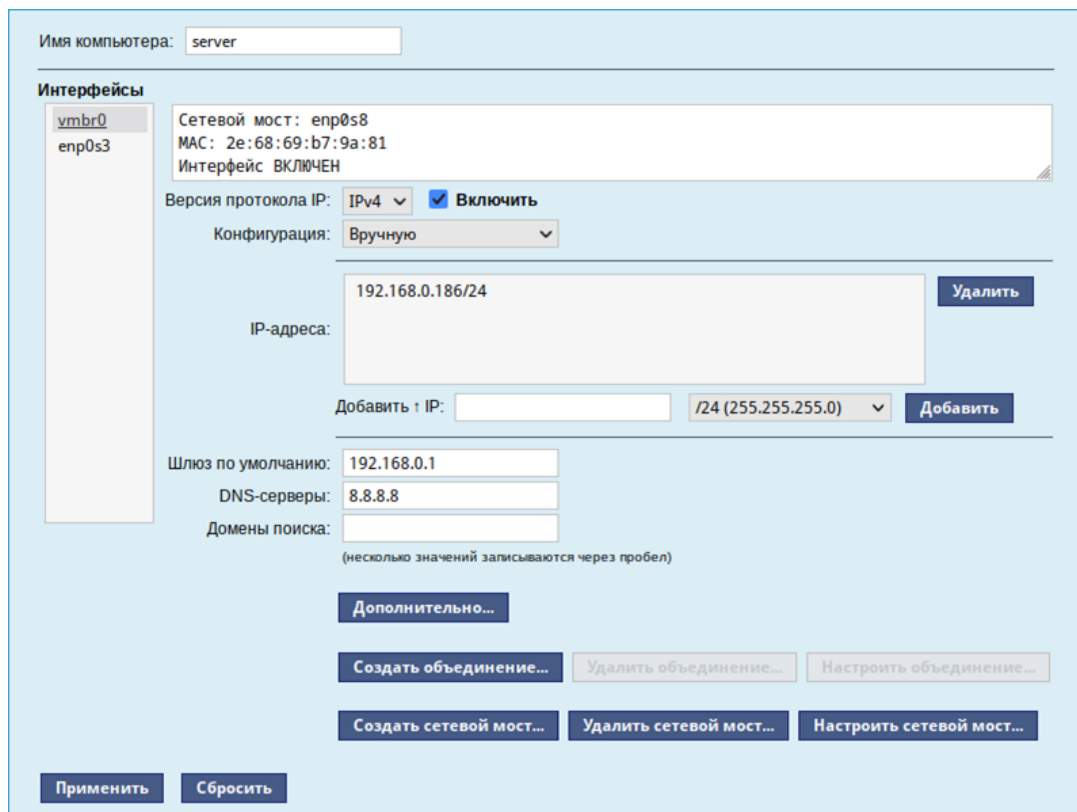


Рис. 125 – Настройка параметров сетевого интерфейса vmbr0

8) нажать на кнопку «Применить».

Для удаления интерфейса моста необходимо выбрать его в списке «Интерфейсы» и нажать кнопку «Удалить сетевой мост...».

8.2.4. Настройка общего подключения к сети Интернет

Пользователи корпоративных сетей обычно подключаются к сети Интернет через один общий канал. Для организации совместного доступа к сети Интернет стандартными средствами поддерживаются две технологии, которые могут использоваться как по отдельности, так и совместно:

- использование прокси-сервера;
- использование NAT.

Оба способа предполагают, что соединение с сетью Интернет компьютера, через который предполагается настроить общий выход, предварительно сконфигурировано. Сделать это можно в разделе ЦУС «Сеть» (см. п. 8.2.1).

8.2.4.1. Прокси-сервер

Отличительной особенностью использования прокси-сервера является то, что, помимо предоставления доступа к веб-сайтам, прокси-сервер кэширует загруженные страницы, а при повторном обращении к ним – отдает их из своего кэша. Это может существенно снизить потребление трафика.

У прокси-сервера есть два основных режима работы:

- прозрачный;
- обычный.

Для работы с прокси-сервером в прозрачном режиме не потребуется специальная настройка рабочих станций. Они лишь должны использовать сервер в качестве шлюза по умолчанию. Этого можно добиться, сделав соответствующие настройки на DHCP-сервере.

Для использования прокси-сервера в обычном режиме потребуется на каждом клиенте в настройках веб-браузера указать данные прокси-сервера (IP-адрес и порт).

Преимуществом обычного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть.

В различных веб-браузерах местоположение формы настройки на прокси-сервер различное. Например, в веб-браузере Firefox она доступна через меню «Правка» → «Настройки» → «Основные» → «Настройки сети» кнопка «Настроить...». Здесь следует выбрать «Ручная настройка прокси» и указать IP-адрес и порт прокси-сервера.

По умолчанию прокси-сервер не предоставляет доступ в Интернет никому кроме себя самого. Список сетей, обслуживаемых прокси-сервером можно изменить, нажав на кнопку «Разрешенные сети...» в модуле ЦУС «Прокси-сервер» (пакет alterator-squid) из раздела «Серверы» (рис. 126).

Основные параметры

Основные параметры управления прокси-сервером

☐ Включить сервис прокси-сервера

Выберите режим проксирования: **Прозрачный** ▾

Выберите способ аутентификации: **Без аутентификации** ▾

Порт прокси-сервера: **3128**

(номер порта)

Разрешённые сети... **Разрешённые протоколы...**

Применить

Доступ к доменам

Для каждой из выбранной группы может быть задана политика разрешения или запрета на доступ к указанным в поле внизу доменам.

Все пользователи

Авторизованные пользователи

Группа: **All users**

Политика доступа группы: **Разрешить доступ** ▾

Список суффиксов доменов:

(Список доменных суффиксов разделённых пробелами; каждый суффикс начинается с точки)

Сохранить

Рис. 126 – Модуль «Прокси-сервер»

Для того чтобы включить аутентификацию пользователей и контролировать их доступ во внешнюю сеть, необходимо выбрать обычный режим проксирования и способ аутентификации, отличный от «Без аутентификации» (рис. 127).

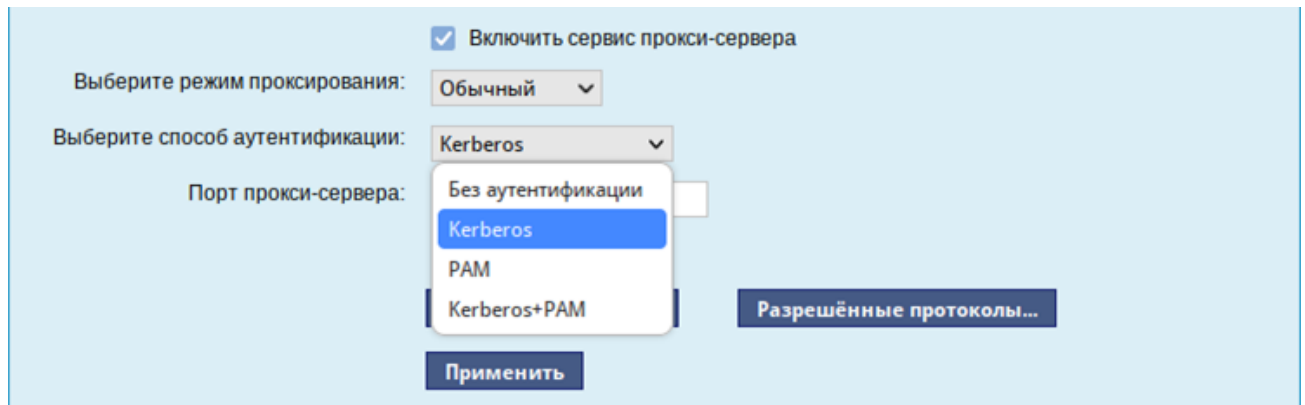


Рис. 127 – Модуль Настройка аутентификации пользователей

Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передает их во внешнюю сеть. Поступление запроса ожидается на определенном порту, который по умолчанию имеет стандартный номер 3128. Если по каким-то причинам не желательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе «Разрешенные сети» (рис. 128).

Вторым условием передачи запроса является принадлежность целевого порта к разрешенному диапазону. Посмотреть и отредактировать список разрешенных целевых портов можно в разделе «Разрешенные протоколы» (рис. 129).

Разрешённые сети

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

192.168.0.0/24 (Network1)

Сеть IP: 192.168.0.0/24
(IP-адрес/биты подсети)

Комментарий: Network1

Применить Сбросить

Удалить

Создать

Назад

Рис. 128 – Настройка списка внутренних сетей

Разрешённые протоколы

Запросы из указанных сетей будут обработаны. Запросы из других сетей будут проигнорированы.

HTTPS (C)
GSS-HTTP
GOPHER
WAIS
RSYNC
FTP
SWAT
HTTP
CUPS
SNEWS (C)
Multilingual HTTP
Filemaker

С порта: 443 По порт: 443
(номер порта) (номер порта)

Способ соединения: Сквозной
☐ Включить прозрачное перенаправление

Комментарий: HTTPS (C)

Применить Сбросить

Удалить

Создать

Назад

Рис. 129 – Настройка списка разрешенных целевых портов

Прокси-сервер позволяет вести статистику посещений страниц в Интернете. Она доступна в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) в разделе «Статистика» (см. п. 8.5.2). Основное предназначение статистики – просмотр отчета об объеме полученных из Интернета данных в привязке к пользователям (если включена аутентификация) или к IP-адресам клиентов.

Примечание. Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (раздел Статистика) (см. п. 8.5.2). Для этого отметьте «Включить сбор данных прокси-сервера» и нажмите кнопку «Применить».

Примечание. Для учета пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное – запрет неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

8.2.4.2. NAT

NAT (Network Address Translation, преобразование сетевых адресов) – это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Таким образом, компьютеры локальной сети, имеющие IP-адреса, зарезервированные для использования исключительно в локальных сетях, могут использовать общий канал доступа к сети Интернет (общий внешний IP-адрес). При этом на компьютере-шлюзе, непосредственно подключенном к сети Интернет, выполняется преобразование адресов.

Настройка NAT осуществляется в модуле ЦУС «Внешние сети» (пакет alterator-net-iptables) из раздела «Брандмауэр». Для минимальной настройки достаточно выбрать режим работы «Шлюз (NAT)», отметить правильный внешний сетевой интерфейс (рис. 130) и нажать на кнопку «Применить».

Рис. 130 – Настройка NAT

8.2.5. Автоматическое присвоение IP-адресов (DHCP-сервер)

DHCP (Dynamic Host Configuration Protocol) – протокол, позволяющий клиенту самостоятельно получить IP-адрес из зарезервированного диапазона адресов, а также дополнительную информацию о локальной сети (DNS-сервер сети, домен поиска, шлюз по умолчанию). Это облегчает администрирование клиентских машин, избавляя администратора домена от необходимости вручную настраивать сетевые интерфейсы на компьютерах локальной сети.

Чтобы настраивать DHCP-сервер, на машине должен быть хотя бы один статически сконфигурированный Ethernet-интерфейс.

Настройка DHCP-сервера осуществляется в модуле ЦУС «DHCP-сервер» (пакет alterator-dhcp) из раздела «Серверы».

Для включения DHCP-сервера необходимо установить флаг «Включить службу DHCP» (рис. 131), указать начальный и конечный IP-адрес, а также шлюз по умолчанию (обычно это IP-адрес сервера на сетевом интерфейсе, обслуживающем локальную сеть).

Общие настройки

Версия IP: IPv4 ▾

☒ Включить службу DHCP

Интерфейс: enp0s3 (192.168.0.1 - 192.168.0.254) ▾
(максимально допустимый диапазон адресов)

Начальный IP адрес: 192.168.0.50

Конечный IP адрес: 192.168.0.60

Срок действия адреса: 1 час ▾

Информация, предоставляемая клиентам

DNS-сервер: 192.168.0.251

Домен поиска: test.alt

Шлюз по умолчанию: 192.168.0.1

Применить Сбросить

Рис. 131 – Настройка DHCP-сервера

Теперь при включении любой клиентской машины с настройкой «получение IP и DNS автоматически» будет присваиваться шлюз 192.168.0.1, DNS 192.168.0.251 и адреса начиная с 192.168.0.50 по порядку включения до 192.168.0.60.

Иногда бывает полезно выдавать клиенту один и тот же IP-адрес независимо от момента обращения. В этом случае он определяется по аппаратному адресу (MAC-адресу) сетевой карты клиента. Для добавления своих значений в таблицу соответствия статических адресов следует ввести IP-адрес и соответствующий ему MAC-адрес и нажать кнопку «Добавить» (рис. 132).

Статические адреса

☐	IP-адрес	MAC-адрес	Имя компьютера
☐	192.168.0.55	08:00:27:4c:d4:84	teacher

Удалить выделенные

Новый статический адрес:

IP-адрес: 192.168.0.59

MAC-адрес: 3c:21:9c:ae:28:b0

Имя компьютера: test

Добавить

Рис. 132 – Привязка IP-адреса к MAC-адресу

Выданные IP-адреса можно увидеть в списке «Текущие динамически выданные адреса». Здесь также имеется возможность зафиксировать выданные адреса, за данными компьютерами. Для этого необходимо отметить хост, за которым нужно закрепить IP-адрес, и нажать кнопку «Зафиксировать адрес для выбранных компьютеров» (рис. 133).

Текущие динамически выделенные адреса				
☐	Имя компьютера	MAC-адрес	IP-адрес	Годен до
☐	teacher	9c:2d:cd:60:4e:03	192.168.0.51	Чт 14 сен 2023 21:08:20 EET

Зафиксировать адрес для выбранных компьютеров

Рис. 133 – Список динамически выданных адресов

8.3. Соединение удаленных офисов (OpenVPN-сервер)

ОС Альт СП предоставляет возможность безопасного соединения удаленных офисов используя технологию VPN (англ. Virtual Private Network – виртуальная частная сеть), которая позволяет организовать безопасные зашифрованные соединения через публичные сети (например, Интернет) между удаленными офисами или локальной сетью и удаленными пользователями. Таким образом, можно связать различные офисы организации, что делает работу с документами, расположенными в сети удаленного офиса, более удобной.

Помимо соединения целых офисов, также существует возможность организовать доступ в офисную сеть для работы в ней извне. Это означает, например, что сотрудник может работать в своем привычном окружении, даже находясь в командировке или просто из дома.

8.3.1. Настройка OpenVPN-сервера

Для организации VPN соединения на стороне сервера предусмотрен модуль ЦУС «OpenVPN-сервер» (пакет alterator-openvpn-server) из раздела «Серверы».

Используя модуль «OpenVPN-сервер», можно:

- включить/отключить OpenVPN-сервер;
- настроить параметры сервера: тип, сети сервера, использование сжатия и т. д.;
- управлять сертификатами сервера;
- настроить сети клиентов.

Особое внимание при планировании и настройке подключений следует обратить на используемые сети. Они не должны пересекаться.

Для создания соединения нужно установить флаг «Включить службу OpenVPN» (рис. 134), выбрать тип подключения: маршрутизируемое (используется TUN) или через мост (используется TAP), и проверить открываемую по соединению сеть (обычно это локальная сеть в виде IP-адреса и маски подсети).

Включить службу OpenVPN

Тип: Маршрутизируемое (TUN)

Сети сервера: 192.168.0.0/255.255.255.0 Удалить

Новая сеть: Маска сети: /24 (255.255.255.0) Добавить

VPN сеть: 10.8.0.0 Маска сети: /24 (255.255.255.0)

Алгоритм шифрования: default

Алгоритм шифрования TLS: default

Алгоритм хэширования: default

☐ Отключить согласование алгоритмов шифрования (NCP)

Порт: 1194

☐ Сжатие LZO

☐ Использовать соединение TCP

Сертификат и ключ SSL...

Положить сертификат УЦ: Обзор... Файл не выбран. Положить

Сети клиентов...

Применить Сбросить

Рис. 134 – Модуль «OpenVPN-сервер»

Для настройки сертификата и ключа SSL нужно нажать на кнопку «Сертификат и ключ SSL...». Откроется окно модуля «Управление ключами SSL» (пакет alterator-sslkey) (рис. 135).

Здесь нужно заполнить поле «Общее имя (CN)» и поле «Страна (C)» (прописными буквами), отметить пункт «(Пере)создать ключ и запрос на подпись» и нажать на кнопку «Подтвердить». После чего станет активной кнопка «Забрать запрос на подпись».

Если нажать на кнопку «Забрать запрос на подпись» (рис. 136), запрос на подпись (файл `openvpn-server.csr`) будет загружен в каталог загрузок.

Настройки SSL

Общее имя (CN):
(имя компьютера для сервера или что-либо другое для клиента)

Страна (C):
(двухбуквенный код страны)

Местоположение (L):
(название города или области, написанное латинскими буквами)

Организация (O):
(название организации, написанное латинскими буквами)

Подразделение (OU):
(название подразделения, написанное латинскими буквами)

E-mail адрес:
(ваш адрес электронной почты)

☒ (Пере)создать ключ и запрос на подпись **Подтвердить**

Рис. 135 – Модуль «Управление ключами SSL»

Подпись

Забрать запрос на подпись

Положить сертификат, подписанный УЦ: Файл не выбран.

Рис. 136 – Кнопка «Забрать запрос на подпись»

В модуле «Управление ключами SSL» появится новый ключ «openvpn-server (Нет сертификата)» (рис. 137).

Подписать сертификат на сервере можно в модуле «Удостоверяющий Центр» (пакет `alterator-ca`) → «Управление сертификатами» (рис. 138):

- заполнить поля «Страна» и «Организация»;

- нажать на кнопку «Создать»;
- открыть вкладку «Управление сертификатами»;
- нажать на кнопку «Обзор...»;
- указать путь до полученного файла `openvpn-server.csr`;
- нажать на кнопку «Загрузить запрос».

Примечание. Для доступа к модулям «Управление ключами SSL» и «Удостоверяющий Центр» необходимо переключиться в режим эксперта.



Рис. 137 – SSL ключи

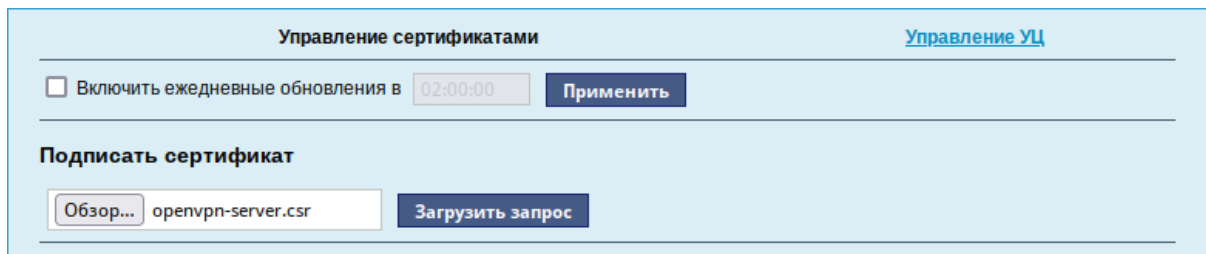


Рис. 138 – Кнопка «Подписать сертификат»

В результате на экране появится две группы цифр и кнопка «Подписать». Нужно нажать на кнопку «Подписать» (рис. 139), подписанный сертификат (файл `output.pem`) будет загружен в каталог загрузок.



Рис. 139 – Подписание сертификата

Можно также подписать сертификат в консоли, с помощью openssl. Для этого необходимо выполнить следующие действия:

- 1) изменить значение параметра policy в файле /var/lib/ssl/openssl.cnf для возможности подписывать любые сертификаты:

```
policy = policy_anything
```

- 2) создать каталоги:

```
# mkdir -p /root/CA/demoCA
# cd /root/CA
# mkdir -p ./demoCA/newcerts
```

Создать файл базы с действующими и отозванными сертификатами:

```
# touch ./demoCA/index.txt
```

Создать файл индекса для базы ключей и сертификатов:

```
# echo '01' > ./demoCA/serial
```

Создать файл индекса для базы отозванных сертификатов:

```
# echo '01' > ./demoCA/crlnumber
```

- 3) создать «самоподписанный» сертификат ca-root.pem и закрытый ключ ca-root.key, которыми будут заверяться/подписываться ключи и сертификаты клиентов:

```
# openssl req -new -x509 -keyout ca-root.key -out ca-root.pem
```

Ввести пароль для закрытого ключа и ответить на запросы о владельце ключа.

Пароль должен быть не короче 4 символов;

4) подписать запрос на сертификат своим «самоподписанным» `ca-root.pem` сертификатом и ключом `ca-root.key` с помощью следующей команды:

```
# openssl ca -cert ca-root.pem -keyfile ca-root.key -days 3650 \
-in /home/user/openvpn-server.csr -out /home/user/output.pem
```

где:

- `/home/user/openvpn-server.csr` – запрос на сертификат, файл, полученный в модуле «Управление ключами SSL» (пакет `alterator-sslkey`) (см. рис. 136);
- `/home/user/output.pem` – файл, в который будет записан подписанный сертификат.

Подписанный сертификат (файл `output.pem`) следует положить к его ключу. Для этого в разделе «Управление ключами SSL» нужно выделить ключ «`openvpn-server (Нет сертификата)`» и нажать кнопку «Изменить». В появившемся окне, в пункте «Положить сертификат, подписанный УЦ» нужно нажать на кнопку «Обзор», указать путь до файла `output.pem` и нажать на кнопку «Положить» (рис. 140).

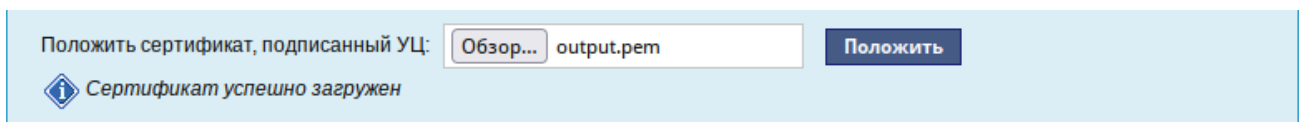


Рис. 140 – Сертификат, подписанный УЦ

В модуле «Управление ключами SSL» видно, что ключ «`openvpn-server (истекает_и_дата)`» изменился. Ключ создан и подписан.

В модуле «OpenVPN-сервер» необходимо положить сертификат УЦ. Для этого в графе «Положить сертификат УЦ» следует нажать на кнопку «Обзор...», указать путь к файлу сертификата УЦ (`ca-root.pem`) и нажать на кнопку «Положить».

Появится сообщение: «Сертификат УЦ успешно загружен» (рис. 141).

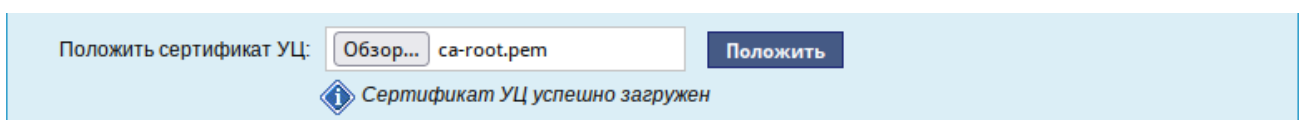


Рис. 141 – Выбор сертификата УЦ в модуле «OpenVPN-сервер»

Примечание. Если использовался модуль «Удостоверяющий Центр», для получения сертификата УЦ необходимо перейти в модуле «Удостоверяющий Центр» на вкладку «Управление УЦ» и забрать сертификат, нажав на ссылку «Сертификат: ca-root.pem» (рис. 142).



Рис. 142 – Сертификат УЦ

Для включения OpenVPN нужно отметить пункт «Включить службу OpenVPN» и нажать на кнопку «Применить».

8.3.2. Настройка клиентов

Со стороны клиента соединение настраивается в графическом интерфейсе (GUI) ЦУС модуле «OpenVPN-соединения» (пакет alterator-net-openvpn) из раздела «Сеть». Доступ к настроенной приватной сети могут получить пользователи, подписавшие свои ключи и получившие сертификат в удостоверяющем центре на том же сервере.

Для создания нового соединения нужно отметить пункт «Сетевой туннель (TUN)» или «Виртуальное Ethernet устройство (TAP)» и нажать на кнопку «Создать соединение» (рис. 143).

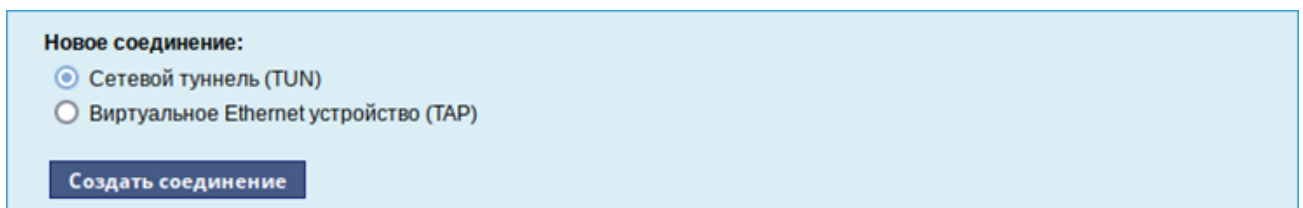


Рис. 143 – Создание нового OpenVPN- соединения

Необходимо обратить внимание, что на стороне клиента должен быть выбран тот же тип виртуального устройства, что и на стороне сервера. Для большинства случаев подходит маршрутизируемое подключение.

В результате станут доступны настройки соединения. На клиенте в модуле «OpenVPN-соединение» нужно указать:

- состояние – «запустить»;

- сервер – IP-адрес сервера или домен;
- порт – 1194;
- ключ – выбрать подписанный на сервере ключ. Ключ (например, openvpn) можно создать в модуле «Управление ключами SSL» и подписать его в модуле «Удостоверяющий Центр» (пакет alterator-ca) на сервере.

Для применения настроек нажать на кнопку «Применить» (рис. 144).

Состояние с «Выключено» должно поменяться на «Включено».

Выполнить команду для проверки появилось ли соединение с сервером:

```
ip addr
```

должно появиться новое соединение tun0. При обычных настройках это может выглядеть так:

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.6 peer 10.8.0.5/32 scope global tun0
        valid_lft forever preferred_lft forever
```

tun0

Состояние: **Выключено** запустить

Сервер: 192.168.0.191

Порт: 1194

Ключ: openvpn

Управление ключами...

☐ Запускать при загрузке

☐ Маршрут по умолчанию через VPN

☐ Сжатие LZO

☐ Использовать соединение TCP

Алгоритм шифрования: default

Алгоритм шифрования TLS: default

Алгоритм хеширования: default

☒ Отключить согласование алгоритмов шифрования (NCP)

Применить Сбросить Удалить соединение

Положить сертификат УЦ: Обзор... ca-root.pem Положить

Рис. 144 – Модуль «OpenVPN- соединения»

8.4. Доступ к службам из сети Интернет

8.4.1. Внешние сети

ОС предоставляет возможность организовать доступ к своим службам извне. Например, можно предоставить доступ к корпоративному веб-сайту из сети Интернет. Для обеспечения такой возможности нужно разрешить входящие соединения на внешних интерфейсах. По умолчанию такие соединения блокируются.

Для разрешения внешних и внутренних входящих соединений предусмотрен раздел ЦУС «Брандмауэр».

В списке «Разрешить входящие соединения на внешних интерфейсах» модуля «Внешние сети» (пакет alterator-net-iptables) перечислены наиболее часто используемые службы, отметив которые, можно сделать их доступными для соединений на внешних сетевых интерфейсах (рис. 145). Если нужно предоставить доступ к службе, отсутствующей в списке, то нужно задать используемые этой службой порты в соответствующих полях.

Внешние сети

Версия IP: ☒ Включить брандмауэр

Выберите режим работы:

Выберите внешние интерфейсы: ☐ enp0s3 (Intel Corporation 82540EM Gigabit Ethernet Controller) 192.168.0.91/24

Разрешить входящие соединения на внешних интерфейсах:

Службы:

- ☒ Центр управления системой (www)
- ☐ Система печати CUPS
- ☐ DHCP
- ☐ DNS
- ☐ Передача файлов (FTP)
- ☐ Почтовый сервер (IMAP)
- ☐ LDAP
- ☒ OpenVPN
- ☐ Почтовый сервер (POP3)
- ☐ Прокси-сервер
- ☐ Файловый сервер (Samba)

Рис. 145 – Модуль «Внешние сети»

Можно выбрать один из двух режимов работы:

- роутер – перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов;
- шлюз (NAT) – в этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если на компьютере настроен, по крайней мере, один внешний и один внутренний интерфейс.

Примечания:

1. В любом режиме включено только перенаправление пакетов с внутренних интерфейсов. Перенаправление пакетов с внешних интерфейсов всегда выключено.
2. Все внутренние интерфейсы открыты для любых входящих соединений.

8.4.2. Список блокируемых хостов

Модуль ЦУС «Список блокируемых хостов» (пакет alterator-net-iptables) предназначен для блокирования любого трафика с указанными узлами. Данный модуль позволяет блокировать любой сетевой трафик с указанными в списке узлов (входящий, исходящий и пересылаемый).

Блокирование трафика с указанных в списке узлов начинается после установки флага «Использовать черный список» (рис. 146).

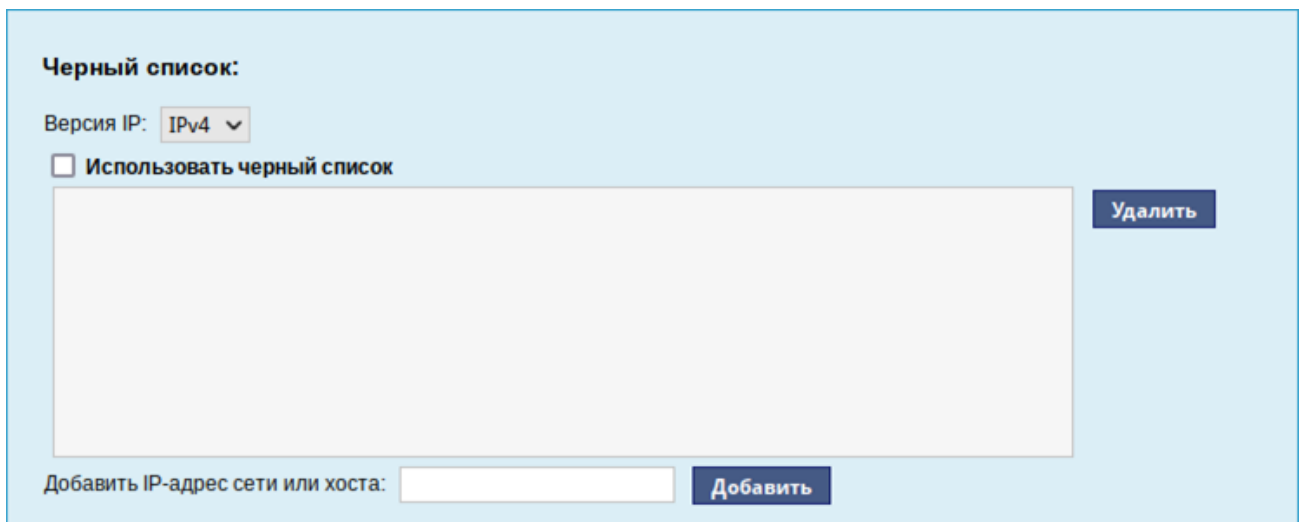


Рис. 146 – Модуль «Список блокируемых хостов»

Для добавления блокируемого узла нужно ввести IP-адрес в поле «Добавить IP-адрес сети или хоста» и нажать на кнопку «Добавить».

Для удаления узла нужно выбрать его из списка и нажать на кнопку «Удалить».

8.5. Статистика

8.5.1. Сетевой трафик

Все входящие и исходящие с сервера сетевые пакеты могут подсчитываться, и выводиться по запросу для анализа.

Модуль ЦУС «Сетевой трафик» (пакет alterator-ulogd) из раздела «Статистика» предназначен для просмотра статистики входящих и исходящих с сервера сетевых пакетов. Данный модуль позволяет оценить итоговый объем полученных и переданных данных за все время работы сервера, за определенный период времени и по каждой службе отдельно.

Для включения сбора данных нужно установить флаг «Включить сбор данных», и нажать на кнопку «Применить» (рис. 147).

☐ Включить сбор данных

Применить

Период с:

2023-09-01

по

2023-09-30

Интерфейс:

enp0s3 - 192.168.0.185

Показать

Служба	Входящий трафик(Кб)	Исходящий трафик(Кб)
Центр управления системой (www)	0.0	0.0
Система печати CUPS	0.0	0.0
DHCP	0.0	0.0
DNS	0.0	0.0
Передача файлов (FTP)	0.0	0.0
Почтовый сервер (IMAP)	0.0	0.0
LDAP	0.0	0.0
OpenVPN	0.0	0.0
Почтовый сервер (POP3)	0.0	0.0
Прокси-сервер	0.0	0.0
Файловый сервер (Samba)	0.0	0.0
Почтовый сервер (SMTP)	0.0	0.0
Управление сетью (SNMP)	0.0	0.0
Удалённый доступ (SSH)	0.0	0.0

Рис. 147 – Просмотр статистики входящих и исходящих пакетов

Для просмотра статистики указывается период (в виде начальной и конечной дат). Дата указывается в формате YYYY-MM-DD (год-месяц-день) или выбирается из календаря справа от поля ввода даты. Из списка доступных сетевых интерфейсов нужно выбрать интересующий и нажать на кнопку «Показать» (рис. 147).

Трафик на указанном интерфейсе за заданный период показывается в виде:

- служба (название протокола);
- входящий трафик в Кбайтах;
- исходящий трафик в Кбайтах.

8.5.2. Прокси-сервер

Пересылка каждого запроса во внешнюю сеть фиксируется прокси-сервером в специальном журнале. На основании этих данных автоматически формируются отчеты о статистике использования ресурсов сети, в том числе потраченного времени и количества переданных данных (трафика).

Статистика не собирается по умолчанию. Включить ее сбор следует в модуле ЦУС «Прокси-сервер» (пакет alterator-squidmill) из раздела «Статистика». Для включения сбора статистики прокси-сервера нужно установить флаг «Включить сбор данных прокси-сервера» (рис. 148).

В том случае, если на прокси-сервере производилась аутентификация пользователей, отчеты будут содержать данные об обращениях каждого пользователя. Иначе отчеты будут формироваться только на основании адресов локальной сети.

Рис. 148 – Настройка сбора статистики прокси-сервера

Для показа отчета нужно задать условия фильтра и нажать на кнопку «Обновить».

Данные в таблице отсортированы по объему трафика в порядке убывания.

Для учета пользователей в статистике нужно добавить хотя бы одно правило. Самое очевидное правило – запрет неаутентифицированных пользователей. Только после этого в статистике начнут показываться пользователи.

8.6. Обслуживание системы

Для безотказной работы системы очень важно следить за корректной работой. Регулярный мониторинг состояния системы, своевременное резервное копирование, обновление установленного ПО, являются важной частью комплекса работ по обслуживанию.

8.6.1. Мониторинг состояния системы

Для обеспечения бесперебойной работы ОС крайне важно производить постоянный мониторинг ее состояния. Все события, происходящие с ОС, записываются в журналы, анализ которых помогает избежать сбоев в работе системы и предоставляет возможность разобраться в причинах некорректной работы.

Для просмотра журналов предназначен модуль ЦУС «Системные журналы» (пакет alterator-logs) из раздела «Система». Интерфейс позволяет просмотреть различные типы журналов с возможностью перехода к более старым или более новым записям.

Различные журналы могут быть выбраны из списка «Журналы» (рис. 149).

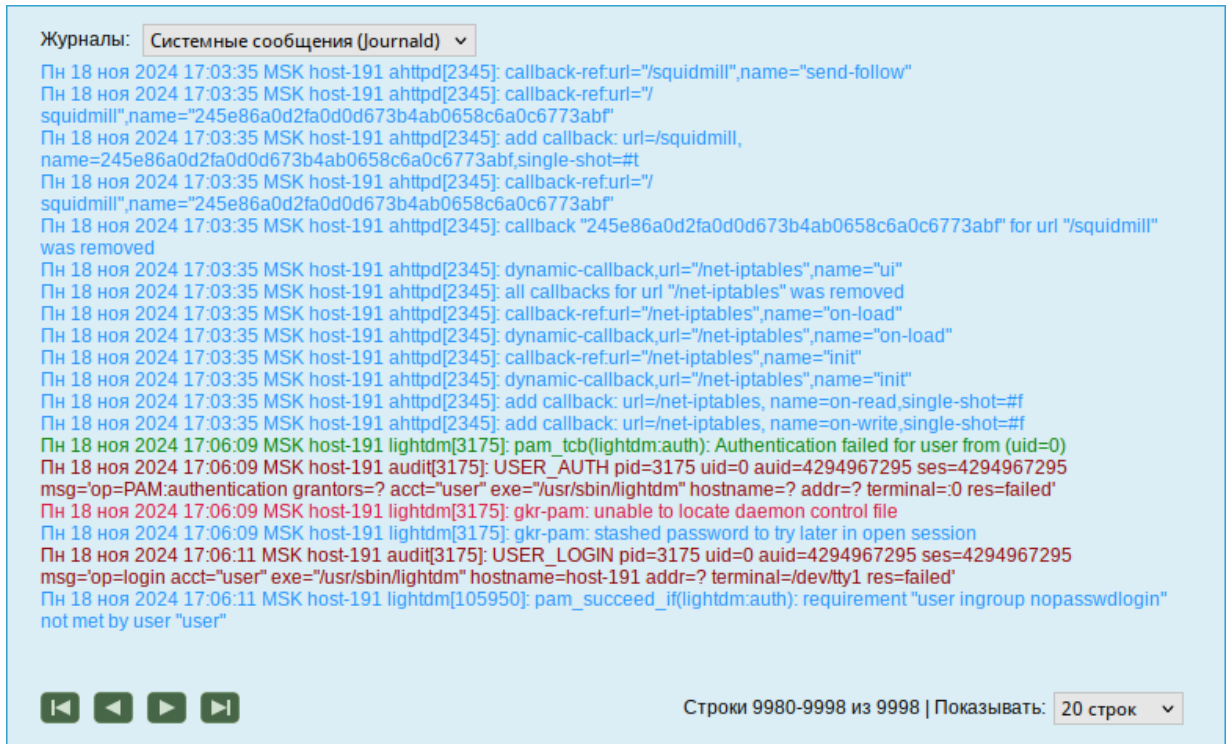


Рис. 149 – Модуль «Системные журналы»

Доступны следующие виды журналов:

- брандмауэр – отображаются события безопасности, связанные с работой межсетевого экрана ОС;
- системные сообщения (Journald) – отображаются события процессов ядра и пользовательской области. У каждого сообщения в этом журнале есть приоритет, который используется для пометки важности сообщений. Сообщения в зависимости от уровня приоритета подсвечиваются цветом.

Каждый журнал может содержать довольно большое количество сообщений. Уменьшить, либо увеличить количество выводимых строк можно, выбрав нужное значение в списке «Показывать».

8.6.2. Системные службы

Для изменения состояния служб можно использовать модуль ЦУС «Системные службы» (пакет alterator-services) из раздела «Система». Интерфейс позволяет изменять текущее состояние службы и, если нужно, применить опцию запуска службы при загрузке системы (рис. 150).

После выбора названия службы из списка отображается описание данной службы, а также текущее состояние: Работает/Остановлена/Неизвестно.

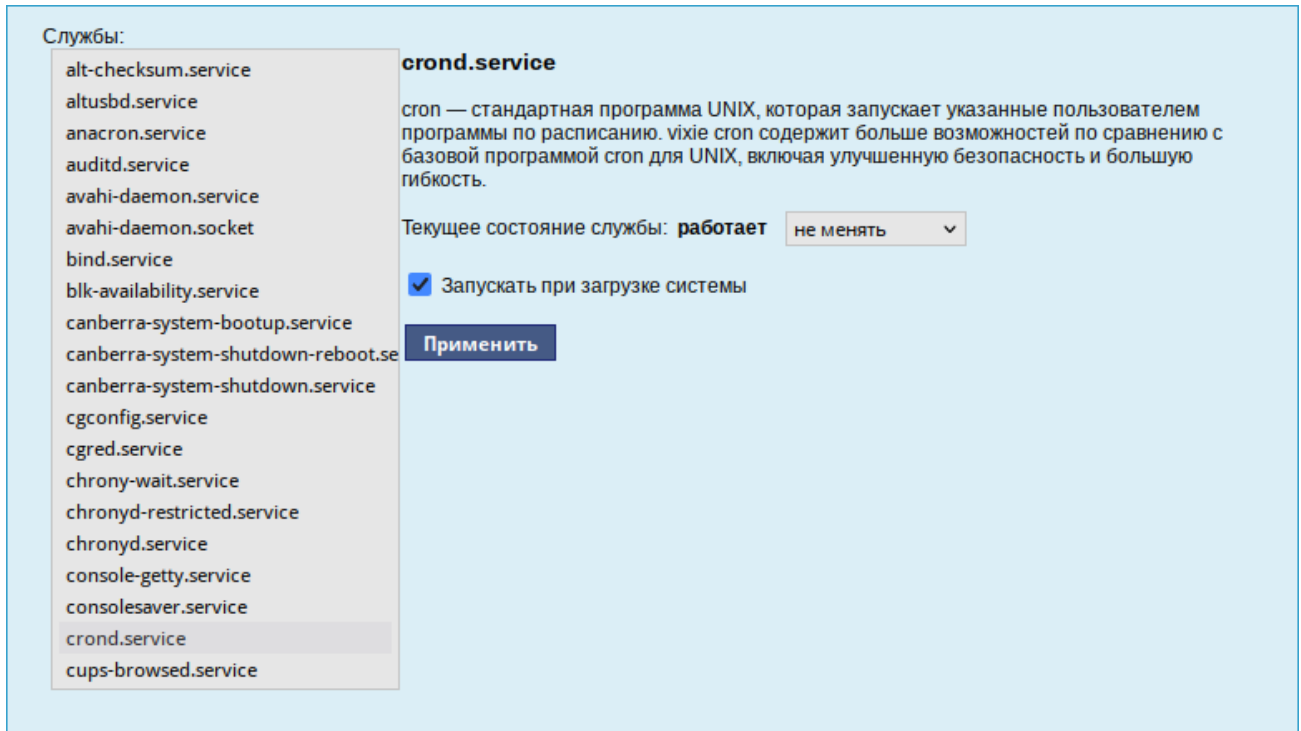
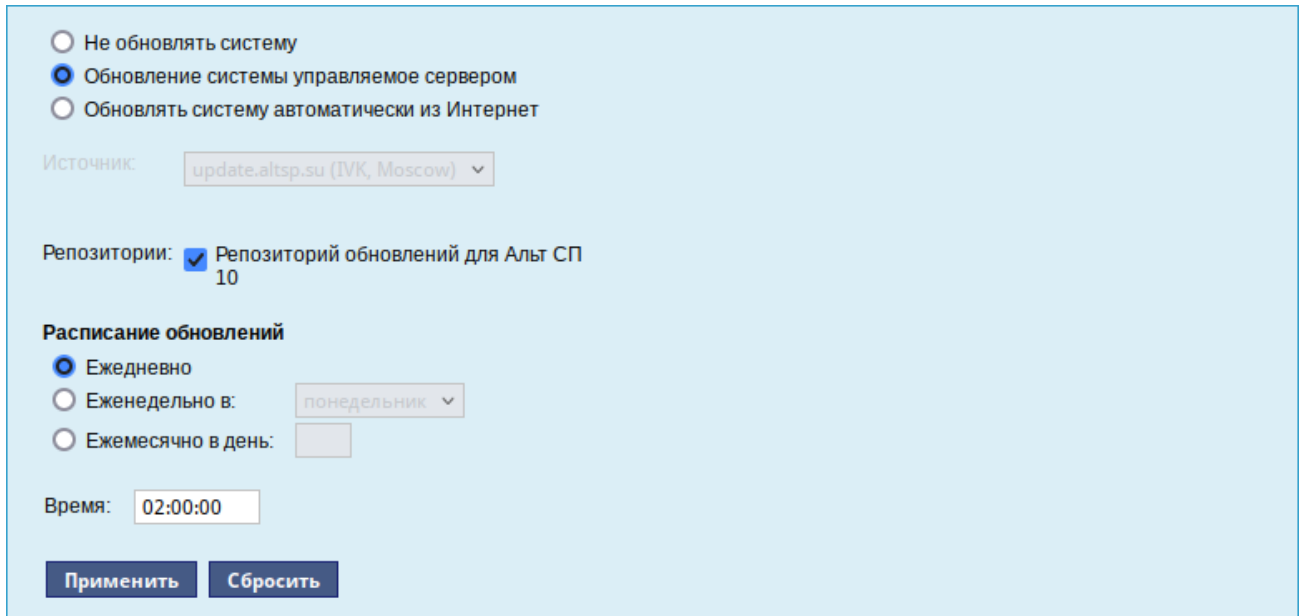


Рис. 150 – Модуль «Системные службы»

8.6.3. Обновление системы

После установки системы крайне важно следить за обновлениями ПО. Обновления для ОС Альт СП могут содержать как исправления, связанные с безопасностью, так и новый функционал или просто улучшение и ускорение алгоритмов. В любом случае настоятельно рекомендуется регулярно обновлять систему для повышения надежности работы системы.

Для автоматизации процесса установки обновлений предусмотрен модуль ЦУС «Обновление системы» (пакет alterator-updates) из раздела «Система». Здесь можно включить автоматическое обновление через Интернет с одного из предлагаемых серверов или задать собственные настройки (рис. 151).



The screenshot shows a configuration window for system updates. At the top, there are three radio buttons: 'Не обновлять систему' (unselected), 'Обновление системы управляемое сервером' (selected), and 'Обновлять систему автоматически из Интернет' (unselected). Below these is a dropdown menu for 'Источник' (Source) with the value 'update.altsp.su (IVK, Moscow)'. Under 'Репозитории' (Repositories), the checkbox 'Репозиторий обновлений для Альт СП 10' is checked. The 'Расписание обновлений' (Update schedule) section has three radio buttons: 'Ежедневно' (selected), 'Еженедельно в:' (unselected, with a dropdown showing 'понедельник'), and 'Ежемесячно в день:' (unselected, with an empty input field). A 'Время:' (Time) field is set to '02:00:00'. At the bottom are 'Применить' (Apply) and 'Сбросить' (Reset) buttons.

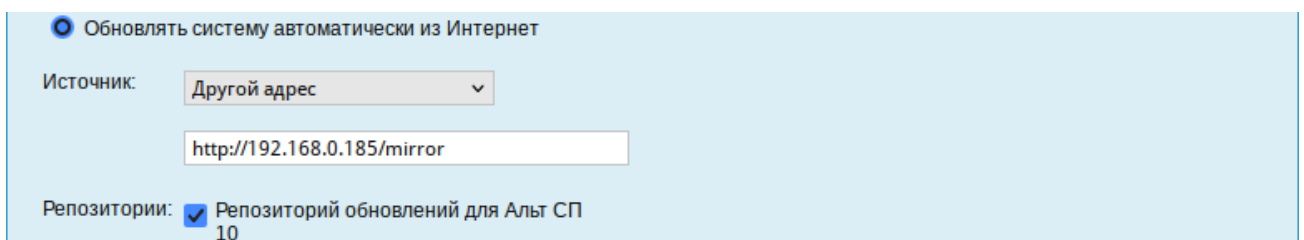
Рис. 151 – Модуль «Обновление системы»

Источник обновлений указывается явно (при выбранном режиме «Обновлять систему автоматически из Интернет») или вычисляется автоматически (при выбранном режиме «Обновление системы, управляемое сервером» и наличии в локальной сети настроенного сервера обновлений (см. в п. 15.14)).

Примечание. Рабочие станции «видят» локальный сервер обновлений, при выборе режима «Обновление системы управляемое сервером» (рис. 151), если они находятся в домене (при этом сервер обновлений должен быть настроен на «Опубликовать как репозиторий для автоматических обновлений»).

Процесс обновления системы будет запускаться автоматически согласно заданному расписанию.

Примечание. Чтобы указать в качестве сервера обновлений локально настроенный источник, необходимо выбрать режим «Обновлять систему автоматически из Интернет», выбрать в списке «Другой адрес» и указать адрес локального сервера обновлений (рис. 152), например, `http://<ip-сервера>/mirror`.



This screenshot shows the same configuration window as Figure 151, but with the 'Обновлять систему автоматически из Интернет' (Update system automatically from Internet) radio button selected. The 'Источник' (Source) dropdown is now set to 'Другой адрес' (Other address). Below it, a text input field contains the URL 'http://192.168.0.185/mirror'. The 'Репозитории' (Repositories) section remains the same, with the checkbox for 'Репозиторий обновлений для Альт СП 10' checked.

Рис. 152 – Указание источника обновлений

8.6.4. Обновление систем, не имеющих выхода в Интернет

Для систем, не имеющих прямого выхода в Интернет, рекомендуется установка отдельного сервера обновлений, находящегося вне защищенного контура и организация ограниченного доступа к этому серверу.

Модуль ЦУС «Сервер обновлений» (пакет alterator-mirror) из раздела «Серверы» предназначен для зеркалирования репозиторий и публикации их для обновлений рабочих станций и серверов.

Сервер обновлений – технология, позволяющая настроить автоматическое обновление ПО, установленного на клиентских машинах (рабочих местах), работающих под управлением ОС Альт СП Рабочая станция.

На странице настройки сервера обновлений ЦУС (рис. 153) можно выбрать, как часто выполнять загрузку пакетов, можно выставить время, когда начинать зеркалирование (рис. 154).

Репозиторий	Источник	Архитектуры	Локальное зеркало	Опубликовано
Репозиторий обновлений для Альт СП 10	update.altsp.su	x86_64 x86_64-i586	(31 Гб)	☐

Свободное место: 114 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

☐ Отключить зеркалирование
☐ Зеркалировать ежедневно
☒ Зеркалировать еженедельно в: понедельник
☐ Зеркалировать ежемесячно в день: 1

Время: 02:00

Рис. 153 – Пример меню «Сервер обновлений»

Свободное место: 114 Гб

Предупреждение: зеркалирование потребует наличия большого количества места на диске.

☐ Отключить зеркалирование

☒ Зеркалировать ежедневно

☐ Зеркалировать еженедельно в: понедельник ▾

☐ Зеркалировать ежемесячно в день: 1 ▾

Время: 02:00

Применить Сбросить

Рис. 154 – Настройка расписания

Здесь также можно выбрать репозитории, локальные срезы которых необходимы. При нажатии на название репозитория, появляются настройки этого репозитория (рис. 155). Необходимо выбрать источник (сайт, откуда будет скачиваться репозиторий), архитектуру процессора (если их несколько, то стоит выбрать соответствующие).

Примечание. При выборе любой архитектуры также будет добавлен источник с poarch.

Примечание. Источник `update.altsp.su` не отдает пакеты по `rsync`, если требуется использовать протокол `rsync`, нужно указать другой источник.

Репозиторий: Репозиторий обновлений для Альт СП 10

Источник: update.altsp.su (IVK, Moscow) ▾

Архитектуры:

- ☐ aarch64
- ☐ i586
- ☒ x86_64
- ☒ x86_64-i586

☐ Локальное зеркало репозитория

☐ Опубликовать как репозиторий для автоматических обновлений

Исключить каталоги и файлы (каждый шаблон в отдельной строке)

SRPMS

RPMS.debuginfo

-debuginfo-

Применить Сбросить Очистить локальное зеркало

Рис. 155 – Пример настройки репозитория

Сервер обновлений предоставляет возможность автоматически настроить обновление клиентских машин в нужном режиме:

- локальное зеркало репозитория – в этом режиме на сервере создается копия удаленного репозитория. Загрузка ПО клиентскими машинами может производиться с локального сервера по протоколам HTTP, HTTPS, FTP, rsync (для каждого протокола нужно настроить соответствующие службы, ниже приведен пример настройки HTTP- и FTP-сервера). Наличие на локальной машине зеркала репозитория при большом количестве машин в сети позволяет существенно сэкономить трафик;

⚠ Зеркалирование потребует наличия большого количества места на диске.

Уменьшить размер скачиваемых файлов и занимаемое репозиторием место на диске можно, указав имена каталогов и файлов, которые будут исключены из синхронизации. Например, не скачивать пакеты с исходным кодом и пакеты с отладочной информацией:

SRPMS

-debuginfo-

Шаблоны указываются по одному в отдельной строке. Символ «*» используется для подстановки любого количества символов.

- публикация репозитория – в этом случае публикуется или URL внешнего сервера, содержащего репозиторий или, если включено локальное зеркало репозитория, адрес этого сервера обновлений. Такая публикация позволяет клиентским машинам автоматически настроить свои менеджеры пакетов на использование внешнего или локального репозитория. Со стороны клиентских машин, в этом случае, необходимо настроить модуль «Обновление системы», отметив в нем «Обновление системы управляемое сервером».

Настройка локального репозитория заканчивается нажатием на кнопку «Применить».

Примечание. По умолчанию локальное зеркало репозитория находится в /srv/public/mirror. Для того чтобы зеркалирование происходило в другую папку, необходимо эту папку примонтировать в папку /srv/public/mirror. Для этого в файл /etc/fstab следует вписать строку:

```
/media/disk/localrepo /srv/public/mirror none rw,bind,auto 0 0
```

где /media/disk/localrepo – папка-хранилище локального репозитория.

Примечание. Если в каталогах

/srv/public/mirror/<репозиторий>/branch/<архитектура>/base/. нет файлов pkglist.* значит зеркалирование не закончено (т. е. не все файлы загружены на сервер обновлений).

8.6.4.1. Настройка веб-сервера

Установить веб-сервер nginx:

```
# apt-get install nginx
```

Создать файл конфигурации веб-сервера в /etc/nginx/sites-available.d/repo.conf:

```
server {
    listen 80;
    server_name localhost .local <ваш ip>;

    access_log /var/log/nginx/repo-access.log;
    error_log /var/log/nginx/repo-error.log;

    location /mirror {
        root /srv/public;
        autoindex on;
    }
}
```

Сделать ссылку в /etc/nginx/sites-enabled.d/:

```
# ln -s /etc/nginx/sites-available.d/repo.conf /etc/nginx/sites-enabled.d/repo.conf
```

Запустить nginx и добавить его в автозагрузку:

```
# systemctl enable --now nginx
```

На клиентских машинах необходимо настроить репозитории. Сделать это можно в программе управления пакетами Synaptic («Параметры» → «Репозитории») или в командной строке:

```
# apt-repo rm all
# apt-repo add http://<ip-сервера>/mirror/c10f2/branch
```

Проверить правильность настройки репозитория, например:

```
# apt-repo
rpm http://192.168.0.185/mirror c10f2/branch/x86_64 classic
rpm http://192.168.0.185/mirror c10f2/branch/noarch classic
```


8.6.4.2. Настройка FTP-сервера

Пример настройки FTP-сервера для ОС Альт СП Рабочая станция релиз 10 64 бит (x86_64)/AArch64 (ARMv8).

Установить, настроить и запустить сервер FTP:

- установить пакеты vsftpd и lftp:

```
# apt-get install vsftpd lftp
```

Настроить параметры использования vsftpd в файле /etc/xinetd.d/vsftpd:

```
# default: off
# description: The vsftpd FTP server.
service ftp
{
    disable = no # включает службу
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    nice = 10
    rlimit_as = 200M
    server = /usr/sbin/vsftpd
    only_from = 0.0.0.0 # предоставить доступ для всех IP
}
```

Перезапустить xinetd:

```
# systemctl restart xinetd
```

Изменить настройку прав доступа в файле /etc/vsftpd/conf:

```
local_enable=YES
```

Создать каталог /var/ftp/mirror:

```
# mkdir -p /var/ftp/mirror
```

Примонтировать каталог /srv/public/mirror в /var/ftp/mirror с опцией --bind:

```
# mount --bind /srv/public/mirror /var/ftp/mirror
```

Примечание. Для автоматического монтирования каталога /srv/public/mirror при загрузке системы необходимо добавить следующую строку в файл /etc/fstab:

```
/srv/public/mirror /var/ftp/mirror none defaults,bind 0 0
```

На клиентских машинах необходимо настроить репозитории:

```
# apt-repo rm all
```

```
# apt-repo add ftp://<ip-сервера>/mirror/c10f2/branch
```

```
# apt-repo
rpm ftp://192.168.0.185/mirror c10f2/branch/x86_64 classic
rpm ftp://192.168.0.185/mirror c10f2/branch/noarch classic
```

8.6.5. Локальные учетные записи

Модуль «Локальные учетные записи» (пакет alterator-users) из раздела «Пользователи» предназначен для администрирования системных пользователей.

Для создания новой учетной записи нужно ввести имя новой учетной записи и нажать на кнопку «Создать», после чего имя отобразится в списке слева (рис. 156).

Для дополнительных настроек нужно выделить добавленное имя, либо, если нужно изменить существующую учетную запись, выбрать ее из списка.

⚠ При создании пользователя через ЦУС нужно снимать отметку с пунктов «Входит в группу администраторов» (рис. 156) и «Автоматический вход в систему».

The screenshot shows a web interface for managing local users. At the top left, there is a text input field labeled "Новая учётная запись:" followed by a "Создать" button. To the right of this are two buttons: "Выбрать аватар" and "Удалить аватар".

Below the input field is a list box containing the names "user" and "test".

In the center, there are several configuration fields:

- "Комментарий:" with an empty text input.
- "Домашний каталог:" with a text input containing "/home/user".
- "Интерпретатор команд:" with a dropdown menu showing "/bin/bash".
- A checked checkbox labeled "Входит в группу администраторов".
- A section titled "Назначенные системные роли:" containing an unchecked checkbox "Создать автоматически".
- "Пароль:" with two text input fields for password entry, with prompts "(введите фразу)" and "(повторите фразу)".

At the bottom center are two buttons: "Применить" and "Удалить пользователя".

On the right side, there is a section titled "Группы, в которые входит пользователь:" followed by a list box containing the following group names: audio, camera, cdrom, cdwriter, floppy, proc, radio, scanner, user, users, uucp, vboxusers, wheel, and xgrp.

Рис. 156 – Управление локальными пользователями в веб-интерфейсе ЦУС

8.6.6. Администратор системы

В модуле «Администратор системы» (пакет alterator-root) из раздела «Пользователи» можно изменить пароль суперпользователя (root), заданный при начальной настройке системы (рис. 157).

В данном модуле (только в веб-интерфейсе) можно добавить публичную часть ключа RSA или DSA для доступа к серверу по протоколу SSH.



Пароль системного администратора:

☐ Создать автоматически

(введите фразу)

(повторите фразу)

Сменить пароль

Разрешённые ssh ключи:

SHA256:yq6obTGscjxzmqMA2g6mjl/pi65d7yfAdHWldP7augY **Удалить ключ**

Новый ключ: **Обзор...** **Файл не выбран.** **Добавить**

Рис. 157 – Модуль «Администратор системы»

8.6.7. Дата и время

В модуле «Дата и время» (пакет alterator-datetime) из раздела «Система» можно изменить дату и время на сервере, сменить часовой пояс, а также настроить автоматическую синхронизацию часов на самом сервере по протоколу NTP и предоставление точного времени по этому протоколу для рабочих станций локальной сети (рис. 158).

Системное время зависит от следующих факторов:

- часы в BIOS – часы, встроенные в компьютер; они работают, даже если он выключен;
- системное время – часы в ядре ОС. Во время работы системы все процессы пользуются именно этими часами;
- часовые пояса – регионы Земли, в каждом из которых принято единое местное время.

При запуске системы происходит активация системных часов и их синхронизация с аппаратными, кроме того, в определенных случаях учитывается значение часового пояса. При завершении работы системы происходит обратный процесс.

☒ Получать точное время с NTP-сервера: pool.ntp.org
☐ Работать как NTP-сервер

Текущая дата: **Ноябрь 2024**

Пн	Вт	Ср	Чт	Пт	Сб	Вс
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Текущее время: 17:58:37

2024-11-18

☒ Хранить время в BIOS по Гринвичу
Часовой пояс: Европа/Москва [Изменить...](#)

Выбрать источник сигналов времени: tsc

[Применить](#) [Сбросить](#)

Рис. 158 – Модуль «Дата и время»

Если настроена синхронизация времени с NTP-сервером, то сервер сможет сам работать как сервер точного времени. Для этого достаточно отметить соответствующий пункт «Работать как NTP-сервер» и нажать на кнопку «Применить» (см. рис. 158).

Примечание. Выбор источника сигналов времени (источника тактовой частоты) доступен в режиме эксперта.

8.6.8. Настройка прокси-сервера

Модуль «Прокси-сервер» (пакет alterator-sysconfig) в разделе «Сеть» позволяет настроить параметры прокси-сервера, используемого для выхода в Интернет (рис. 159).

Данный модуль позволяет настроить:

- IP-адрес и порт используемого прокси-сервера;

- логин и пароль для доступа, если прокси-сервер требует аутентификацию.

Прокси-сервер: Порт:

Учётная запись:

Пароль:

Внимание! Учётная запись и пароль работают только для curl и wget. Если используете apt-get или любой графический веб-браузер, оставьте эти поля пустыми.

Не использовать прокси для:

Рис. 159 – Веб-интерфейс модуля Прокси-сервер

После нажатия кнопки «Применить» все параметры запишутся в файл `/etc/sysconfig/network` в следующем виде:

```
HTTP_PROXY=http://username:password@address:port
HTTPS_PROXY=http://username:password@address:port
FTP_PROXY=http://username:password@address:port
NO_PROXY=""
```

Указанный прокси-сервер будет использоваться ПО для доступа в сеть Интернет.

Примечание. Для применения настроек прокси-сервера необходимо перезагрузить систему.

8.6.9. Ограничение использования диска

Модуль «Использование диска» (пакет `alterator-quota`) в разделе «Пользователи» позволяет ограничить использование дискового пространства пользователями, заведенными в системе в модуле «Пользователи».

Модуль позволяет задать ограничения (квоты) для пользователя при использовании определенного раздела диска. Ограничить можно как суммарное количество Кбайт, занятых файлами пользователя, так и количество этих файлов (рис. 160).

Для управления квотами файловая система должна быть подключена с параметрами `usrquota`, `grpquota`. Для этого следует выбрать нужный раздел в списке «Файловая система» и установить отметку в поле «Включено» (рис. 160).

Для того чтобы задать ограничения для пользователя, необходимо выбрать пользователя в списке «Пользователь», установить ограничения и нажать на кнопку «Применить».

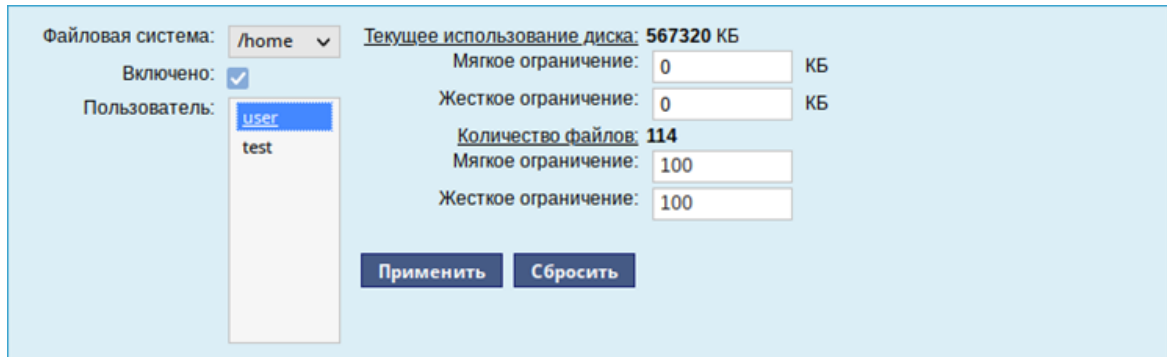


Рис. 160 – Модуль «Использование диска»

При задании ограничений различают жесткие и мягкие ограничения:

- мягкое ограничение: нижняя граница ограничения, которая может быть временно превышена. Временное ограничение – одна неделя;
- жесткое ограничение: использование диска, которое не может быть превышено ни при каких условиях.

Значение 0 при задании ограничений означает отсутствие ограничений.

8.6.10. Выключение и перезагрузка компьютера

Иногда, в целях обслуживания или по организационным причинам необходимо корректно выключить или перезагрузить компьютер. Для этого можно воспользоваться модулем ЦУС «Выключение компьютера» в разделе «Система».

Модуль «Выключение компьютера» позволяет:

- выключить компьютер;
- перезагрузить компьютер;
- приостановить работу компьютера;
- погрузить компьютер в сон.

Возможна настройка ежедневного применения данных действий в заданное время.

Так как выключение и перезагрузка – критичные для функционирования компьютера операции, то по умолчанию настройка выставлена в значение

«Продолжить работу». Для выключения, перезагрузки или перехода в энергосберегающие режимы нужно отметить соответствующий пункт и нажать «Применить».

Для ежедневного автоматического выключения компьютера, перезагрузки, а также перехода в энергосберегающие режимы необходимо отметить соответствующий пункт и задать желаемое время (рис. 161). Например, для выключения компьютера следует отметить пункт «Выключать компьютер каждый день в», задать время выключения в поле ввода справа от этого флага и нажать кнопку «Применить».

The screenshot shows a settings window titled «Выключение компьютера» (Computer Shutdown). It contains several radio buttons for immediate actions: «Продолжить работу» (selected), «Выключить компьютер сейчас», «Перезагрузить компьютер сейчас», «Приостановить компьютер сейчас», and «Погрузить компьютер в сон сейчас». Below these are four checkboxes for scheduled actions, each with a time input field: «Выключать компьютер каждый день в: 23:00:00», «Перезагружать компьютер каждый день в: 11:00:00» (checked), «Приостанавливать компьютер каждый день в: 23:00:00», and «Погружать компьютер в сон каждый день в: 23:00:00». At the bottom, there is a checked checkbox «При изменении состояния системы отправлять электронное письмо по адресу: ivanov@test.alt» and two buttons: «Применить» and «Сбросить».

Рис. 161 – Модуль «Выключение компьютера»

Примечание. Для возможности настройки оповещений на e-mail, должен быть установлен пакет `state-change-notify-postfix`:

```
# apt-get install state-change-notify-postfix
```

Для настройки оповещений необходимо отметить пункт «При изменении состояния системы отправлять электронное письмо по адресу», ввести e-mail адрес и нажать кнопку «Применить».

По указанному адресу, при изменении состоянии системы будут приходить электронные письма. Например, при включении компьютера, содержание письма будет следующее:

```
Thu Sep 14 11:46:59 EET 2023: The host-15.test.alt is about to start.
```

При выключении:

Thu Sep 14 12:27:02 EET 2023: The host-15.test.alt is about to shutdown.

Кнопка «Сбросить» возвращает сделанный выбор к безопасному значению по умолчанию: «Продолжить работу», перечитывает расписания и выставляет отметки для ежедневного автоматического действия в соответствие с прочитанным.

8.6.11. FTP-сервер

Модуль «FTP-сервер» (пакет alterator-vsftpd) из раздела «Серверы» (рис. 162) предназначен для настройки FTP-сервера (vsftpd).

Чаще всего протокол FTP (File Transfer Protocol) используется для организации файлового сервера с анонимным доступом. Возможность анонимного доступа управляется параметром «Разрешить вход анонимному пользователю». Менее распространенный вариант – сервер с возможностью загружать на него файлы, в том числе и анонимным пользователям. Возможность загрузки включается параметром «Разрешить запись». Еще один вариант – сервер, позволяющий локальным пользователям скачивать и загружать файлы из своих домашних каталогов. Этот вариант используется редко, что связано с небезопасностью протокола FTP. Возможность работы с локальными пользователями управляется параметром «Разрешить вход локальным пользователям». Чтобы пользователи могли загружать файлы, требуется включить параметр «Разрешить запись».

Разрешение на загрузку файлов можно настраивать индивидуально, для этого нужно отметить параметр «Разрешить настройку локальных пользователей».

Общие параметры

- ☒ Включить службу FTP
- ☐ Разрешить запись
- ☒ Разрешить вход анонимному пользователю
- ☐ Разрешить вход локальных пользователей
- ☐ Разрешить настройки для локальных пользователей

Параметры записи для анонимного пользователя

- ☐ Разрешить создание каталогов
- ☐ Разрешить загрузку файлов
- ☐ Стандартный каталог для приёма файлов (/var/ftp/incoming)
- ☐ Разрешить переименование/удаление файлов

Применить **Сбросить**

Параметры локальных пользователей

☐	Пользователь	Доступ на запись
☐	Пользователь	Доступ на запись

Для выделенных: **ОК**

Добавить пользователя: **ОК**

Рис. 162 – Настройка модуля «FTP-сервер»

8.6.12. Удостоверяющий центр

Модуль «Удостоверяющий центр» (пакет alterator-ca) из раздела «Система» позволяет управлять SSL-сертификатами, используемыми для обеспечения безопасных соединений между сетевыми узлами.

Для обеспечения безопасности соединения для клиента (в качестве клиентского ПО может выступать, например, веб-браузер) основным является вопрос о принятии сертификата. При принятии сертификата возможно несколько вариантов.

8.6.12.1. Сертификат сервера подписан одним из известных клиенту удостоверяющих центров (УЦ)

В этом случае сертификат принимается и устанавливается безопасное SSL-соединение. Обычно клиентское ПО (например, веб-браузер) содержит список наиболее известных УЦ и предоставляет возможность управления (добавление/удаление) сертификатами таких УЦ.

8.6.12.2. Сертификат сервера подписан УЦ неизвестным клиенту

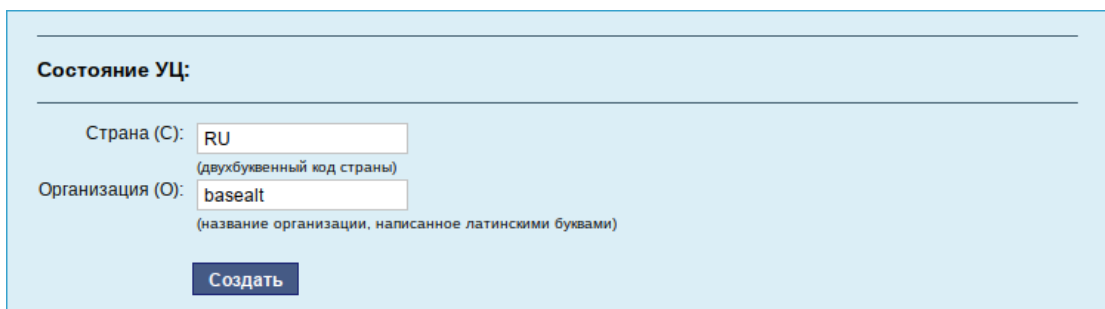
В этом случае следует самостоятельно решить вопрос о принятии такого сертификата:

- можно временно (на время одной сессии) принять сертификат сервера;
- можно принять сертификат сервера на постоянной основе;
- если вы доверяете УЦ, подписавшему сертификат, можно добавить сертификат самого УЦ к списку известных сертификатов, и таким образом, в дальнейшем все сертификаты, подписанные этим УЦ, будут приниматься автоматически.

8.6.12.3. Сертификат сервера является самоподписанным

Это случай, когда сертификат сервера не подтвержден вообще никакой третьей стороной. Такие сертификаты используются в локальных сетях, где вы самостоятельно можете проверить аутентичность сервера. В случае самоподписанных сертификатов вы должны самостоятельно убедиться в том, что сервер является тем, за кого себя выдает. Сделать это можно, сверив отпечатки полученного сертификата и реально находящегося на сервере.

При первом обращении к модулю «Удостоверяющий центр» необходимо создать УЦ, указав страну и организацию (рис. 163).



Состояние УЦ:

Страна (C): RU
(двухбуквенный код страны)

Организация (O): basealt
(название организации, написанное латинскими буквами)

Создать

Рис. 163 – Модуль «Удостоверяющий центр». Создание УЦ

На вкладке «Управление УЦ» (рис. 164) можно:

- просмотреть информацию о сертификате УЦ;
- выгрузить для дальнейшего использования сертификат УЦ (файл `ca-root.pem`). Этот файл можно будет добавить к списку УЦ,

используемому клиентским ПО, после чего все сертификаты, подписанные данным УЦ будут приниматься автоматически;

- выгрузить, для дальнейшего использования, запрос на подпись сертификата УЦ (файл `ca-root.csr`). Этот запрос можно подписать сторонним УЦ;
- регенерировать сертификат УЦ с другими параметрами (можно изменить параметры «Страна (C)» и «Организация (O)»).

Управление сертификатами

Управление УЦ

Состояние УЦ: ОК

Сертификат выдан
Общее имя (CN): basealt Root Certification Authority
Подразделение (OU): basealt Certification Authority
Организация (O): basealt
Страна (C): RU
Центр выдачи
Общее имя (CN): basealt Root Certification Authority
Подразделение (OU): basealt Certification Authority
Организация (O): basealt
Страна (C): RU
Разное
Дата выдачи: Nov 18 13:25:22 2024 GMT
Истекает: Nov 16 13:25:22 2034 GMT
SHA1-сумма D6:AD:C8:67:E2:66:0A:9F:A4:59:F0:5D:BF:7C:56:02:AA:E5:DE:DE
MD5-сумма C0:A9:C2:7F:49:75:25:DA:8B:B4:F7:D6:6E:60:92:F5
Сертификат: [ca-root.pem](#)
Запрос на подпись: [ca-root.csr](#)

☐ Регенерировать УЦ

Страна (C):
(двухбуквенный код страны)
Организация (O):
(название организации, написанное латинскими буквами)

Рис. 164 – Модуль «Удостоверяющий центр». Вкладка «Управление УЦ»

На вкладке «Управление сертификатами» (рис. 165) можно:

- настроить ежедневное обновление подписей сертификатов, используемых локальными службами и службами подчиненных серверов;
- подписать произвольный сертификат (запрос на подпись) корневым сертификатом УЦ, настроенным на вкладке «Управление УЦ»;
- просмотреть состояния и подпись локальных сертификатов и сертификатов подчиненных серверов (рис. 166).

[Управление УЦ](#)

Управление сертификатами

☐ Включить ежедневные обновления в

Подписать сертификат

Файл не выбран

Управляемые hosts

☐	Хост	⬇
☐	Локальные сертификаты	

Для выделенных:

Добавить хост:

Рис. 165 – Модуль «Удостоверяющий центр». Вкладка «Управление сертификатами»

[Вернуться к списку](#)

сертификаты

☐	Имя ⬇	Состояние ⬇	Дата выдачи ⬇	Годен до ⬇	Сертификат выдан ⬇
☐	ahhttpd	self-signed certificate	Nov 13 14:03:06 2024 GMT	Nov 13 14:03:06 2025 GMT	/CN=host-191/O=ahhttpd
☐	openvpn-server	OK	Nov 18 13:28:16 2024 GMT	Nov 18 13:28:16 2025 GMT	/C=RU/CN=openvpn-server

Для выделенных:

Рис. 166 – Модуль «Удостоверяющий центр». Локальные сертификаты

Чтобы подписать сертификат, необходимо на вкладке «Управление сертификатами» нажать кнопку «Выберите файл», выбрать файл с запросом на подпись и нажать кнопку «Загрузить запрос». В результате на экране отобразится запрос на подпись. Далее следует нажать кнопку «Подписать». Подписанный сертификат (файл output.pem) будет загружен в каталог загрузок.

8.7. Сервер электронной почты (SMTP, POP3/IMAP)

8.7.1. Сервер электронной почты

ОС Альт СП Сервер может служить как почтовым сервером, обслуживающим определенный домен, так и посредником (шлюзом) для пересылки почты. Почтовый сервер отвечает как за отправку писем (SMTP-сервер, см. п. 8.8.3) исходящих от почтовых клиентов рабочих станций, так и за предоставление им входящей почты (сервер POP3/IMAP см. п. 8.7.3).

Для настройки параметров работы сервера предусмотрен модуль ЦУС «Почтовый сервер» (пакет alterator-postfix-dovecot) из раздела «Серверы» (рис. 167).

Рис. 167 – Настройка параметров работы сервера

8.7.2. Сервер SMTP

Сервер SMTP отвечает за отправку сообщений и может работать в двух режимах:

- 1) посредник – в этом режиме исходящая почта пересылается для дальнейшей отправки на указанный сервер;
- 2) сервер – в этом режиме сервер доставляет почту самостоятельно.

8.7.3. Сервер POP3/IMAP

Сервер POP3/IMAP используется для доступа пользователей к электронной почте на сервере.

Для доступа к службам POP3 и IMAP пользователь должен включить в своем почтовом клиенте аутентификацию и указать свое имя и пароль.

Выбор конкретного используемого протокола для получения почты зависит от предпочтений пользователя:

- 1) POP – при проверке почты клиентом она передается на его машину и сохраняется там. Возможность просмотра принятой/отправленной почты при этом существует, даже если клиент не имеет соединения с сервером;
- 2) IMAP – все сообщения хранятся на сервере. Почтовый клиент может просматривать их только при наличии соединения с сервером.

Помимо включения/отключения служб, модуль ЦУС «Почтовый сервер» позволяет произвести дополнительные настройки: фильтрацию спама, настройку параметров аутентификации и т. д.

8.8. Сервер электронной почты postfix

Postfix представляет собой агент передачи электронной почты и позволяет организовать обмен почтой внутри локальной сети, а также с внешней сетью.

Для расширения возможностей postfix используется ряд дополнений, выделенных в отдельные пакеты, полный список которых можно получить с помощью следующей команды:

```
$ apt-cache search ^postfix-
```

Настройка сервера электронной почты postfix осуществляется с помощью конфигурационных файлов, хранящихся в каталоге `/etc/postfix`. Основные параметры определяются в файле конфигурации `main.cf`. В файле `main.cf` указываются только параметры, выставленные администратором, и некоторые из значений по умолчанию, которые администратору с большой вероятностью нужно будет изменить. Значения по умолчанию для всех остальных параметров перечислены в файле `main.cf.default` (этот файл не следует редактировать, он служит только для справок).

Если конфигурация была изменена при запущенной службе postfix, новые настройки нужно активизировать командой:

```
# service postfix reload
```

Postfix сохраняет все сообщения в журнале `mail.log`, расположенном в каталоге `/var/log/`. Сообщения об ошибках и предупреждения сохраняются отдельно в журналы `mail.err` и `mail.warn` соответственно.

Запуск postfix осуществляется с помощью следующей команды:

```
# postfix start
```

8.8.1. Утилиты командной строки

Postfix поставляется с набором утилит командной строки, которые помогают решать административные задачи. Они выполняют разнообразные функции (обращение к картам, просмотр файлов очередей, постановка сообщений в очередь и извлечение из очереди, изменение конфигурации).

Команда `postfix` останавливает, запускает и перезагружает конфигурацию с помощью параметров `stop`, `start` и `reload`.

Команда `postalias` создает индексированную карту псевдонимов из файла псевдонимов и работает аналогично команде `postmap`, при этом уделяя особое внимание нотации в файле псевдонимов (ключ и значение разделяются двоеточием).

Команда `postcat` выводит содержимое сообщения, находящегося в почтовой очереди. Для того чтобы прочитать сообщение, находящееся в очереди, нужно знать

идентификатор очереди. Для получения списка идентификаторов очередей следует выполнить следующую команду:

```
# mailq
```

После получения идентификатора очереди нужно указать его в качестве параметра команды `postcat` для просмотра содержимого файла следующим образом:

```
# postcat -q <идентификатор очереди>
```

Основная задача команды `postmap` заключается в построении индексированных карт на основе обычных текстовых файлов.

Для того чтобы создать карту `/etc/postfix/virtual.db` на основе `/etc/postfix/virtual`, нужно выполнить следующую команду:

```
# postmap hash:/etc/postfix/virtual
```

Также команда `postmap` обеспечивает возможность тестирования карт любого вида, поддерживаемых конфигурацией `postfix`.

Команда `postdrop` считывает почту из стандартного ввода и записывает результат в каталог `maildrop` (программа работает в связке с утилитой `sendmail`).

Команда `postkick` отправляет запрос демону `postfix` по локальному транспортному каналу, делая межпроцессное взаимодействие `postfix` доступным для сценариев оболочки и других программ.

Команда `postlock` предоставляет монопольный доступ к файлам `mbox`, в которые выполняет запись `postfix`, а затем исполняет команду, удерживая блокировку.

Команда `postlog` позволяет внешним программам, таким как сценарии командного интерпретатора, писать сообщения в журнал электронной почты (представляет собой `postfix`-совместимый интерфейс регистрации).

Команда `postqueue` представляет собой пользовательский интерфейс для очередей `postfix`, предоставляющий возможности, обычно доступные в рамках выполнения команды `sendmail`.

Команда `postqueue` с параметром `-f` просит диспетчер очередей доставить всю стоящую в очереди почту вне зависимости от места назначения:

```
# postqueue -f
```

Команда `postqueue` с параметром `-p` выводит содержимое очереди:

```
# postqueue -p
```

Команда `postqueue` с параметром `-s domain` пытается доставить всю стоящую в очереди почту для домена `domain`:

```
# postqueue -s example.com
```

Команда `postsuper` обслуживает задания внутри очередей postfix (в отличие от `postqueue`, эта команда доступна только пользователю с идентификатором `root`, и она может быть выполнена, когда сервер не запущен).

8.8.2. Первичная настройка

В первую очередь после установки postfix нужно настроить параметры, отвечающие за домен и имя сервера. Чтобы установить значение параметра `myhostname`, нужно отредактировать конфигурационный файл `main.cf`. (для параметра `myhostname` нужно ввести полностью определенное доменное имя хоста):

```
myhostname = mail.example.com
```

Postfix может автоматически получить значение `mydomain` после того, как параметр `myhostname` настроен, для этого postfix отбрасывает первую часть значения `myhostname` до первой точки включительно:

```
mydomain = example.com
```

Далее нужно указать домен, с которого отправляется локальная почта. Postfix будет добавлять значение из `mydomain` к любому адресу, если он задан не полностью. Для этого нужно в конфигурационном файле `main.cf` для параметра `myorigin` установить следующее значение:

```
myorigin = $mydomain
```

Примечание. Сообщение от процесса `cron` пользователю `root` получит адрес `root@$mydomain`, которое будет преобразовано в `root@example.com`.

Далее нужно указать домены, для которых данный сервер является конечной точкой доставки электронной почты. Для того чтобы postfix принимал любую почту, адресованную в домен `example.com` нужно в файл конфигурации внести следующие изменения:

```
mydestination = $mydomain
```

Домены, для которых сервер получает почту, отличные от значения `mydomain` и не сконфигурированные как виртуальные домены postfix, нужно перечислить с помощью параметра `mydestination`, либо в дополнительном файле, на который ссылается этот параметр.

Адресаты указываются через запятую следующим образом:

```
mydestination =  
$mydomain,  
$myhostname
```

Аналогичным образом параметр `mynetworks` описывает блоки IP-адресов, которые считаются внутренними и с которых разрешен прием исходящих сообщений.

После внесения изменений в конфигурацию postfix для применения новых настроек нужно перезапустить службу postfix:

```
# service postfix reload
```

8.8.3. Работа в режиме SMTP-сервера

После установки служба postfix функционирует в режиме `local`, в котором сервер электронной почты postfix не принимает соединения из внешней сети, ограничиваясь приемом локальных соединений посредством сокетов семейства UNIX (UNIX-domain socket).

Для настройки возможности приема сообщений по протоколу SMTP или ESMTP, как из внешней сети, так из внутренней, нужно переключить службу postfix в режим работы `server` с помощью следующей команды:

```
control postfix server
```

Рабочие станции в локальной сети или машины в сети провайдера, отделенной от внешней сети, должны перенаправлять исходящую почту на почтовый сервер, обслуживающий данную сеть.

Для того чтобы postfix отправлял почту из локальной сети на SMTP-сервер провайдера, нужно для параметра relayhost установить следующее значение:

```
relayhost = [smtp.provider.net]
```

8.8.4. SMTP-аутентификация

SMTP-аутентификация обеспечивает идентификацию клиентов независимо от их IP-адресов и позволяет серверу пересылать сообщения от почтовых клиентов, чьи IP-адреса не входят в список доверенных. Postfix реализует SMTP-аутентификацию при помощи протокола SASL (Simple Authentication and Security Layer) и использует библиотеки Cyrus-SASL.

Для защиты соединений используется протокол SSL/TLS (для включения поддержки нужно установить пакет postfix-tls).

Для проверки поддержки SMTP-аутентификации postfix нужно от имени от имени администратора (root) выполнить следующую команду:

```
ldd `postconf -h daemon_directory`/smtpd
```

Если в выводе команды присутствует строка libsassl.so.2, значит, пакет postfix был собран с поддержкой SASL.

8.8.4.1. Настройки SMTP-аутентификации на сервере

Настройка SMTP-аутентификации на сервере осуществляется в несколько этапов:

- 1) включение SMTP-аутентификации на серверной части;
- 2) настройка механизмов SASL, которые будут предоставляться клиентам;
- 3) настройка поддержки SMTP-аутентификации для нестандартных почтовых клиентов;
- 4) настройка области (realm), которую postfix будет передавать библиотеке SASL;
- 5) определение разрешения на пересылку в postfix.

Чтобы включить SMTP-аутентификацию, нужно в конфигурационный файл main.cf добавить следующую запись:

```
smtpd_sasl_auth_enable = yes
```

8.8.4.1.1. Настройка механизмов SASL

Управление предоставляемыми механизмами осуществляется с помощью параметра `smtpd_sasl_security_options`, в котором через запятые следует указать список из одного или более значений:

- 1) `noanonymous` – значение параметра, позволяющее включить проверку сервером верительных данных клиента (список значений параметра `smtpd_sasl_security_options` всегда должен включать в себя значение `noanonymous`);
- 2) `noplaintext` – значение параметра, позволяющее исключить использование всех механизмов открытого текста, таких как PLAIN и LOGIN (значение, рекомендуемое для использования, так как отправляемые открытым текстом верительные данные могут быть легко перехвачены в сети);
- 3) `noactive` – значение параметра, исключающее использование механизмов SASL, которые восприимчивы к активным атакам);
- 4) `nodictionary` – значение параметра, исключающее все механизмы, не устойчивые к атакам по словарю (атаки, осуществляемые методом полного перебора паролей);
- 5) `mutual_auth` – значение параметра, позволяющее включить поддержку только механизмов, обеспечивающих взаимную аутентификацию (сервер аутентифицирует себя для клиента).

8.8.4.1.2. Настройка SMTP-аутентификации для нестандартных почтовых клиентов

Для настройки альтернативной нотации для устаревших клиентов, не распознающих SMTP-аутентификацию по стандарту RFC 2222, но распознающих более раннюю нотацию, использованную в черновом варианте этого стандарта (где между командой AUTH и названиями механизмов стоял не пробел, а знак равенства), нужно в конфигурационном файле `main.cf` установить параметр `broken_sasl_auth_clients`:

```
broken_sasl_auth_clients = yes
```

8.8.4.1.3. Настройка области SASL

Для аутентификации клиента сервер postfix отправляет службе паролей Cyrus SASL область аутентификации (realm) вместе с верительными данными клиента. Такая необходимость определяется версией Cyrus SASL и выбором службы. Для указания области аутентификации в файле `main.cf` используется параметр `smtpd_sasl_local_domain`. По умолчанию этот параметр пуст и должен оставаться пустым, если только не используется вспомогательный плагин, которому действительно требуется область аутентификации.

8.8.4.1.4. Настройка разрешений на пересылку

Для разрешения пересылки для клиентов, прошедших аутентификацию SASL, нужно добавить параметр `permit_sasl_authenticated` в список ограничений `smtpd_recipient_restrictions` своей конфигурации следующим образом:

```
smtpd_recipient_restrictions =  
[...]  
permit_sasl_authenticated,  
permit_mynetworks,  
reject_unauth_destination  
[...]
```

Нужно поместить ключевое слово `permit_sasl_authenticated` достаточно близко к началу списка ограничений, чтобы аутентифицированный клиент не был случайно отвергнут из-за несоответствия какому-то другому правилу (например, `reject_unauth_destination`).

8.8.4.2. Настройка SMTP-аутентификации на стороне клиента

Для настройки SMTP-аутентификации для клиента нужно выполнить следующее:

- 1) запросить у удаленного сервера список поддерживаемых механизмов аутентификации;
- 2) включить SMTP-аутентификацию на клиентской части;
- 3) предоставить файл для хранения верительных данных;
- 4) настроить postfix на работу с файлом верительных данных;
- 5) отключить ненадежные механизмы аутентификации.

Клиентская ПЭВМ должна поддерживать механизмы аутентификации, поддерживаемые сервером. Для получения списка механизмов аутентификации нужно подключиться к почтовому серверу и отправить приветствие EHLO с помощью следующих команд:

```
$ telnet mail.remoteexample.com 25
EHLO mail.example.com
```

По умолчанию SMTP-аутентификация на стороне клиента выключена. Для того чтобы включить SMTP-аутентификацию нужно в конфигурационный файл `main.cf` добавить следующую запись:

```
smtp_sasl_auth_enable = yes
```

После включения аутентификации на клиентской ПЭВМ нужно сообщить серверу postfix, где следует искать данные, которые нужны для аутентификации, и какой из механизмов (из предлагаемых удаленным сервером) postfix может использовать.

8.8.4.2.1. Хранение верительных данных

Нужно подготовить данные, которые клиент postfix будет использовать для того, чтобы аутентифицировать себя на сервере, для этого следует создать от имени root файл карты `/etc/postfix/sasl_passwd` (если он еще не существует) с помощью следующей команды:

```
# touch /etc/postfix/sasl_passwd
```

Далее нужно отредактировать этот файл, поместив полностью определенное доменное имя почтового сервера, который требует аутентификации, с левой стороны, а разделенную двоеточием пару «имя пользователя – пароль» – с правой. Для имен пользователей `mail.example.com` и `relay.another.example.com`, а также соответствующих паролей файл `sasl_passwd` будет выглядеть следующим образом:

```
mail.example.com test:testpass
relay.another.example.com username:password
```

После редактирования файла `sasl_passwd` нужно изменить права на него так, чтобы читать его мог только пользователь root (в файле хранится конфиденциальная

информация, которая не должна быть доступна локальным пользователям), для этого нужно использовать команды `chown` и `chmod`:

```
# chown root:root /etc/postfix/sasl_passwd && chmod 600  
/etc/postfix/sasl_passwd
```

Затем нужно преобразовать файл карты в индексированную карту для быстрого доступа postfix (нужно выполнять при каждом изменении файла `sasl_passwd`) с помощью следующей команды:

```
# postmap hash:/etc/postfix/sasl_passwd
```

8.8.4.2.2. Настройка postfix для использования верительных данных

Нужно сообщить клиенту postfix, где хранится созданная карта верительных данных аутентификации, для этого нужно в параметре `smtp_sasl_password_maps` в файле `main.cf` указать полный путь к файлу `sasl_passwd`, указывая при этом (с помощью спецификатора `hash:`), что значения карты хранятся в хеш-файле, например:

```
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
```

8.8.4.2.3. Отключение некоторых механизмов аутентификации

Для отключения использования ненадежных механизмов следует указать в параметре `smtp_sasl_security_options` список (через запятую) типов механизмов, которые клиент не может использовать. По умолчанию параметр `smtp_sasl_security_options` установлен в значение «noanonymous», но по возможности (если сервер поддерживает механизм с шифрованием, такой как DIGEST-MD5 или CRAM-MD5) следует также отключить использование механизмов открытого текста. Для этого нужно добавить в файл `main.cf` следующую строку:

```
smtp_sasl_security_options = noanonymous, noplaintext
```

8.8.5. Триггеры ограничений

Ограничения позволяют почтовому серверу принять или отвергнуть сообщения на основе данных SMTP-соединения между клиентом и сервером. Информация, полученная из этого диалога, позволяет postfix наложить или отменить ограничения на клиента (отправителя и получателя).

Postfix поддерживает следующие триггеры:

- 1) `smtpd_client_restrictions` – триггер применяется к IP-адресу или имени хоста клиента либо к ним обоим (по умолчанию postfix разрешает подключение любому клиенту);
- 2) `smtpd_helo_restrictions` – триггер применяется к аргументу `HELO/EHLO` клиента и к IP-адресу и (или) имени хоста клиента (по умолчанию допускается любой аргумент `HELO/EHLO`);
- 3) `smtpd_sender_restrictions` – набор триггеров, который относится к частям конверта (Postfix применяет его к отправителю конверта, аргументу `HELO/EHLO` и клиенту, по умолчанию любому отправителю конверта разрешено отправлять сообщения);
- 4) `smtpd_recipient_restrictions` – триггер применяется к получателям конверта, отправителю конверта, аргументу `HELO/EHLO` и к IP-адресу и (или) имени хоста клиента (по умолчанию postfix допускает любых получателей для клиентов, которые определены в параметре конфигурации `mynet_works`, для остальных же разрешены получатели в доменах из `relay_domains` и `mydomains`);
- 5) `smtpd_data_restrictions` – триггер выявляет клиенты, которые отправляют содержимое письма прежде, чем postfix ответит на команду `DATA` (Postfix выполняет это посредством трассировки `DATA`, когда клиент отправляет команду на сервер, по умолчанию ограничения нет);
- 6) `smtpd_etrn_restrictions` – специальный триггер может ограничить клиенты, которые могут запрашивать у postfix очистку очереди сообщений (по умолчанию всем клиентам разрешено выдавать команду `ETRN`).

В postfix существуют несколько видов ограничений, которые можно разбить на четыре группы:

- 1) общие ограничения;
- 2) переключаемые ограничения;
- 3) настраиваемые ограничения;
- 4) дополнительные параметры контроля спама.

Общие ограничения выполняют следующие команды:

- 1) `permit` – разрешает запрос;
- 2) `defer` – откладывает запрос;
- 3) `reject` – отвергает запрос;
- 4) `warn_if_reject` – содействует последующим ограничениям (если ограничение после `warn_if_reject` решает отвергнуть запрос, то postfix записывает в журнал сообщение `reject_warning`);
- 5) `reject_unauth_pipelining` – отвергает запрос, когда клиент отправляет команды SMTP раньше времени, еще не зная о том, действительно ли postfix поддерживает конвейерную обработку команд ESMTP (таким образом, достигается противодействие программам массовой рассылки, которые некорректно используют конвейерную обработку команд ESMTP для ускорения доставки).

Переключаемые ограничения работают как переключатели, при активации которых они проверяют выполнение некоторого условия. К переключаемым ограничениям относятся следующие:

- 1) `smtpd_helo_required` – ограничение, требующее от клиентов отправки команды HELO (или EHLO) в начале сеанса SMTP (наличия команды HELO/EHLO требуют RFC 821 и RFC 2821);
- 2) `strict_rfc821_envelopes` – ограничение, регулирующее степень терпимости postfix к ошибкам в адресах, указанных в команде MAIL FROM (отправитель конверта) или RCPT TO;
- 3) `disable_vrfy_command` – SMTP-команда VRFY позволяет клиентам проверять существование получателя (ограничение позволяет отменить команды VRFY);
- 4) `allow_percent_hack` – ограничение, регулирующее преобразование из формы «user%domain» в «user@domain»;
- 5) `swap_bangpath` – ограничение, контролирующее преобразование из формы «site!user» в «user@site» (нужно, если ПЭВМ подключена к сети UUCP).

Настраиваемые ограничения представляют собой карты, которые работают как фильтры. В каждой записи карты ключ является фильтром, а значение – тем действием, которое нужно выполнить при совпадении:

- 1) `HELO (EHLO)` имя хоста – ограничения, относящиеся к именам хостов, которые клиенты могут отправлять с командой `HELO` или `EHLO`;
- 2) имя хоста/адрес клиента – ограничения, определяющие клиенты, которые могут устанавливать SMTP-соединения с почтовым сервером;
- 3) адрес отправителя – ограничения, определяющие адреса отправителей (конвертов), которые postfix разрешает для использования в командах `MAIL FROM`;
- 4) адрес получателя – ограничения, определяющие адреса получателей (конвертов), которые postfix разрешает для использования в командах `RCPT TO`;
- 5) `ETRN!команды` – ограничение, накладываемое на клиенты, которые могут выдавать команды `ETRN`;
- 6) проверка заголовка – ограничение, регулирующее заголовки сообщений;
- 7) проверка тела – ограничения, накладываемые на текст, который может появляться в строках тела сообщения;
- 8) черные списки DNSBL – черные списки, ограничивающие соединения от IP-адресов (клиентов), которые включены в черные списки DNSBL;
- 9) черные списки RHSBL – черные списки, запрещающие те домены отправителей (конверта), которые присутствуют в черных списках RHSBL.

Дополнительные параметры контроля спама поддерживают другие ограничения или возможности, не входящие в функциональность postfix по умолчанию:

- 1) `default_rbl_reply` – создает шаблон ответа по умолчанию, который будет использоваться при блокировании запроса SMTP-клиента ограничением `reject_rbl_client` или `reject_rhsbl_sender`;
- 2) `permit_mx_backup_networks` – ограничивает использование функции контроля за пересылкой `permit_mx_backup` теми адресатами, у которых основные хосты MX входят в указанный список сетей;

- 3) `rbl_reply_maps` – определяет таблицы поиска и шаблоны ответов DNSBL, индексированные по имени домена DNSBL;
- 4) `relay_domains` – указывает postfix на необходимость приема почты для этих доменов несмотря на то, что данный сервер не является местом их конечного назначения;
- 5) `smtpd_sender_login_maps` – определяет пользователя, которому разрешено использовать определенный адрес MAIL FROM.

В postfix по умолчанию встроен набор ограничений. Для того чтобы посмотреть список ограничений нужно выполнить следующую команду:

```
# postconf -d smtpd_recipient_restrictions
```

Для включения режима фильтрации почты в postfix в зависимости от наличия в них нежелательной информации (спам) нужно выполнить следующую команду:

```
control postfix filter
```

8.8.6. Алиасы и преобразование адресов

В postfix для передачи сообщений электронной почты используются алиасы, которые позволяют создавать псевдонимы для длинных или плохо запоминаемых адресов электронной почты. Настройка алиасов в postfix осуществляется с помощью таблиц `aliases`.

При установке postfix в таблице создается алиас на имя пользователя `root`: вся корреспонденция, предназначенная администратору и поступающая на другие системные адреса, будет отправляться на имя реального пользователя, который осуществляет функции администратора.

Рабочий образ таблицы строится с помощью следующей команды:

```
newaliases
```

а также при актуализации всех изменений посредством следующей команды:

```
service postfix reload
```

При отправке сообщения postfix формирует адрес отправителя автоматически из имени учетной записи пользователя и значения собственного домена (или значения «myorigin»). Преобразование адресов отправителей в глобальные адреса задаются в таблице типа canonical:

```
sender_canonical_maps = cdb:/etc/postfix/sender_canonical
```

Аналогичная таблица recipient_canonical и соответствующий параметр recipient_canonical_maps могут быть использованы для преобразования адресов назначения.

8.8.7. Настройка ограничений размера почтового ящика и отправляемого сообщения

По умолчанию размер файла почтового ящика при локальной доставке ограничен 51 200 000 байтами. Это ограничение можно изменить с помощью параметра mailbox_size_limit.

Например, снять ограничение можно установив этот параметр в 0:

```
mailbox_size_limit = 0
```

Также можно установить требуемый размер, указав в значении параметра величину:

```
mailbox_size_limit = <размер почтового ящика в байтах>
```

Для настройки размера отправляемого сообщения используется параметр message_size_limit:

```
message_size_limit = <размер сообщения в байтах>
```

Для настройки виртуальных аккаунтов используется параметр virtual_mailbox_limit:

```
virtual_mailbox_limit= <размер почтового ящика виртуального аккаунта в байтах>
```

8.9. Настройка удаленного подключения

Для получения удаленного доступа к другим ПЭВМ и предоставления такого доступа в ОС Альт СП используется протокол SSH (Secure Shell).

SSH реализует соединение с удаленным компьютером, защищающее от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;

- манипулирование данными на пути от клиента к серверу;
- подмена клиента, либо сервера, путем манипулирования IP-адресами, DNS, либо маршрутизацией.

SSH обладает следующими возможностями:

- сжатие передаваемых данных;
- туннелирование каналов внутри установленного соединения – в том числе соединений с X-сервером;
- широкая распространенность: существуют реализации SSH для самых различных аппаратных платформ и ОС.

OpenSSH – реализация SSH, входящая в состав дистрибутива. Эта реализация включает в себя следующие программы и утилиты:

- клиентские программы `ssh`, `scp` и `sftp` (используются для запуска программ на удаленных серверах и копирования файлов по сети);
- серверные программы `sshd`, `sftp-server` (используются для предоставления доступа по протоколу SSH);
- вспомогательные программы `scp`, `rescp`, `ssh-keygen`, `ssh-add`, `ssh-agent`, `ssh-copy-id`, `ssh-keyscan`.

8.9.1. OpenSSH, сервер протокола SSH (sshd)

OpenSSH Daemon (`sshd`) – программа-сервер, обслуживающая запросы программы-клиента `ssh`. Вместе эти программы заменяют `rlogin` и `rsh` и обеспечивают защищенную и кодированную связь между двумя непроверенными компьютерами через незащищенную сеть.

`sshd` – это служба, принимающая запросы на соединения от клиентов. Для каждого нового соединения создается (с помощью вызова «fork») новый экземпляр службы. Ответвленный экземпляр обрабатывает обмен ключами, кодирование, аутентификацию, выполнение команд и обмен данными.

Параметры определяются при помощи ключей командной строки или файла конфигурации (по умолчанию – `sshd_config`). Ключи командной строки имеют больший приоритет, чем значения, указанные в файле конфигурации. При

получении сигнала отбоя SIGHUP перечитывает свой файл конфигурации путем запуска собственной копии с тем же самым именем, с которым был запущен, например, /usr/sbin/sshd.

Синтаксис команды:

```
sshd [-4Ddeiqt] [-b длина_ключа_1] [-f файл_конфигурации] [-g
время_задержки_регистрации] [-h файл_ключа_хоста] [-k
частота_генерации_ключа] [-o директива] [-p порт] [-u длина]
```

Доступны ключи, приведенные в таблице 10.

Т а б л и ц а 10 – Ключи команды sshd

Ключ	Описание
-4	Использовать только адреса IPv4
-6	Использовать только адреса IPv6
-b длина_ключа_1	Определяет число битов в ключе сервера протокола версии 1 (по умолчанию 1024)
-D	Не переходить в фоновый режим и не становиться службой. Это упрощает слежение за экземпляром sshd
-d	Режим отладки. Сервер посылает расширенную отладочную информацию в файл журнала событий системы и не переходит в фоновый режим работы. Сервер не создает дочерних процессов и обрабатывает только одно соединение. Параметр предназначен только для отладки работы сервера. Несколько параметров -d указанных один за другим, повышают уровень отладки. Максимум – это 3
-e	Направлять вывод в консоль (stderr) вместо механизма журналирования событий системы
-f файл_конфигурации	Определяет имя файла конфигурации (по умолчанию – /etc/openssh/sshd_config). Не работает, если нет файла конфигурации
-g время_задержки_регистрации	Определяет период, в течение которого клиент должен себя идентифицировать (по умолчанию – 120 секунд). Если клиент не смог идентифицировать себя в течение этого времени, экземпляр сервера прекращает свою работу. Значение равное нулю отменяет ограничение на время ожидания
-h файл_ключа_хоста	Определяет файл, из которого будет считан ключ хоста. Этот параметр должен быть указан, если запущен не от имени пользователя с идентификатором root (так как обычно стандартные файлы хоста доступны для чтения только пользователю с идентификатором root). Стандартное расположение файла – /etc/openssh/ssh_host_key для протокола версии 1, и /etc/openssh/ssh_host_dsa_key, /etc/openssh/ssh_host_ecdsa_key и

Окончание таблицы 10

Ключ	Описание
	/etc/openssh/ssh_host_rsa_key для протокола версии 2. Можно иметь несколько ключей хоста для разных версий протокола и алгоритмов генерации ключей
-i	Позволяет уведомить программу о том, что она запускается службой inetd. Обычно sshd не запускается из inetd, так как требуется генерировать ключ сервера до ответа клиенту, а это может отнять десятки секунд. Клиент будет вынужден ожидать слишком долго, если ключ будет повторно генерироваться каждый раз. Однако, при малых размерах ключа (например, 512), использование из inetd может быть оправдано
-k частота_генерации_ключа	Определяет, как часто будет регенерироваться ключ сервера протокола версии 1 (по умолчанию 3600 секунд – один раз в час). Значение ноль означает, что ключ никогда не будет регенерирован
-o директива	Позволяет указывать директивы в формате файла конфигурации, например, такие, для которых нет соответствующего ключа командной строки. Директивы файла конфигурации описаны в sshd_config
-p порт	Порт, на котором сервер будет ожидать соединения (по умолчанию – 22). Возможно указание нескольких ключей с разными портами. Если данный ключ указан, параметр Port файла конфигурации игнорируется, однако порты, указанные в ListenAddress имеют больший приоритет, чем указанные в командной строке
-q	Не заносить в системный журнал регистрации событий никакой информации. В обычном режиме в нем фиксируется подключение, аутентификация и разрыв каждого соединения.
-t	Режим тестирования. Выполняется только проверка соответствия файла конфигурации и готовность ключей. Полезно для проверки состояния службы после обновления, при котором были изменены файлы конфигурации
-u длина	Размер поля в структуре utmp хранящей имя удаленного хоста. Если разрешенное имя хоста превышает указанное значение, то взамен будет использован десятичное представление IP-адреса через точку. Это позволяет уникально идентифицировать машины со слишком длинными именами. Указание -u0 включает использование в файле utmp IP-адресов во всех случаях. При этом будет производить DNS-запросы только если это явно требуется конфигурацией (from="pattern-list") или механизмом аутентификации (либо RhostsRSAAuthentication либо HostbasedAuthentication). Использование DNS также обязательно в случае задания параметрам AllowUsers и DenyUsers значения в формате USER@HOST

8.9.1.1. Аутентификация

Служба OpenSSH SSH поддерживает версии протокола SSH 1 и 2. При этом использование протокола версии 1 крайне не рекомендуется. Запретить использование одного протокола версии 1 можно, указав в параметре `Protocol` файла `/etc/openssh/sshd_config`:

```
Protocol 2
```

Протокол 2 поддерживает ключи DSA, ECDSA и RSA; протокол 1 поддерживает только ключи RSA. Независимо от протокола, каждый подключающийся хост имеет собственный, обычно 2048-битный идентифицирующий его ключ.

Для протокола версии 1 подтверждение субъекта сервера обеспечивается 768-битным ключом, который генерируется при запуске сервера. Ключ генерируется заново каждый час, при условии его использования, и не хранится на диске. При получении запроса на подключение со стороны клиента служба посылает в ответ свой открытый ключ и свои ключи. Клиент сравнивает ключ хоста RSA со своими данными, чтобы убедиться в том, что это тот же сервер. Затем клиент генерирует 256-битное произвольное число, шифрует его при помощи обеих ключей (своего и сервера) и отправляет результат серверу. Это число становится ключом сеанса, и с его помощью выполняется кодирование всех последующих данных, по согласованному методу – Blowfish или 3DES (клиент выбирает метод из предложенных сервером). В настоящее время по умолчанию используется 3DES.

Для протокола версии 2 подтверждение субъекта сервера обеспечивается по схеме Диффи-Хеллмана, в результате которой также получается общий ключ сеанса. Дальнейший обмен данными шифруется симметричным кодом, 128-битным AES, Blowfish, 3DES, CAST128, Arcfour, 192-битным AES или 256-битным AES, который выбирает клиент из предложенных сервером. Кроме того, целостность передаваемых данных обеспечивается кодом подтверждения подлинности сообщения (hmac-md5, hmac-sha1, umac-64, hmac-ripemd160, hmac-sha2-256 или hmac-sha2-512).

Независимо от типа аутентификации служба проверяет доступность соответствующей учетной записи в системе. Так, она может быть заблокирована посредством добавления ее в параметр `DenyUsers` или ее группы в `DenyGroups`. Для запрета только аутентификации по паролю укажите в файле `passwd` `'NP'` или `'*NP*'`.

Наконец, клиент запрашивает оболочку или выполнение команды, после чего стороны входят в режим сеанса. В этом режиме, каждая из сторон в любой момент может пересылать данные и эти данные будут переданы оболочке или команде на стороне сервера и на пользовательский терминал соответственно.

8.9.1.2. Вход в систему

- если регистрация в системе произведена на терминале (tty) и не указана никакая команда, то отображается время последнего входа в систему и содержимое файла `/etc/motd` (если только это не отключено в файле конфигурации или `~/.hushlogin`);
- если регистрация в системе произведена на терминале, записывается время регистрации;

- проверяется `/etc/nologin` если он присутствует, выводится его содержимое и завершается работа (исключение – `root`);
- осуществляется переход к выполнению с правами обычного пользователя;
- устанавливаются значения основных переменных среды;
- интерпретируется файл `~/.ssh/environment`, если таковой имеется, и пользователям разрешено изменять среду;
- происходит переход в домашний каталог пользователя;
- если имеется файл `~/.ssh/rc`, то производится его выполнение, а если нет и имеется `/etc/openssh/sshrс`, то выполняется он, в противном случае выполняется `xauth`. Файлам `rc` на стандартный ввод передается протокол аутентификации X11 и `cookie`;
- запускается оболочка пользователя или выполняется указанная команда.

8.9.1.3. SSHRC

Если файл `~/.ssh/rc` существует, он будет выполняться после файлов определения переменных среды, но перед запуском оболочки пользователя или команды. Если используется подмена X11, то на его стандартный ввод будет передана пара «proto cookie», также ему будет доступна переменная среды `DISPLAY`. Сценарий должен вызывать `xauth` самостоятельно для добавления `cookie` X11.

Основная цель этого файла состоит в выполнении процедур инициализации, прежде, чем станет доступным основной каталог пользователя. AFS – пример такой среды.

Этот файл будет, содержать блок аналогичный следующему:

```
if read proto cookie && [ -n "$DISPLAY" ]; then
if [ `echo $DISPLAY | cut -c1-10` = 'localhost:' ]; then
# X11UseLocalhost=yes
echo add unix:`echo $DISPLAY |
cut -c11-` $proto $cookie
else
# X11UseLocalhost=no
echo add $DISPLAY $proto $cookie
fi | xauth -q -
fi
```

Если этот файл отсутствует, то выполняется `/etc/openssh/sshrс`, а если отсутствует и он, то для добавления cookie используется `хauth`.

8.9.1.4. Формат файла `authorized_keys`

Параметр `AuthorizedKeysFile` файла конфигурации определяет путь к файлу с открытыми ключами. Значение по умолчанию – `~/.ssh/authorized_keys` и `~/.ssh/authorized_keys2`. Каждая строка файла содержит один ключ (пустые строки или строки, начинающиеся с символа «#» считаются комментариями и игнорируются). Открытые ключи протокола 1 (RSA) состоят из следующих полей, разделенных пробелами: параметры, битность, порядок, модуль, комментарий. Открытые ключи протокола версии 2 состоят из полей: параметр, тип ключа, ключ в виде `base64`, комментарий. Поля параметров необязательны; их отсутствие определяется наличием в начале строки цифры (поле параметра никогда не начинается с цифры). Поля битности, порядка, модуля и комментарий определяют ключ RSA; поле комментария не используется (но может быть удобно пользователю для отметки ключа). Для протокола версии 2 типом ключа является `ecdsa-sha2-nistp256`, `ecdsa-sha2-nistp384`, `ecdsa-sha2-nistp521`, `ssh-dss` или `ssh-rsa`.

Строки в этих файлах, обычно имеют длину в несколько сотен байт (из-за размера открытого ключа RSA) и могут достигать длины в 8 килобайт (таким образом, максимальный размер ключа DSA – 8 килобит, а RSA – 16 килобит). Очевидно, не стоит вводить их вручную. Вместо этого следует скопировать файл `identity.pub`, `id_dsa.pub` или `id_rsa.pub` и отредактировать их.

Минимальная длина модуля RSA независимо от протокола составляет 768 бит.

Параметры (если таковые имеются) состоят из разделенных запятой определений. Для указания пробелов следует воспользоваться двойными кавычками. Поддерживаются следующие определения параметров (регистра названий параметров не учитывается):

- `command="команда"` – выполнять команду при каждом использовании данного ключа для аутентификации. Команда, передаваемая пользователем, будет игнорироваться. Команда выполняется на псевдо-терминале, если последний запрашивается клиентом; в противном случае она выполняется

без терминала. Если требуется «чистый» 8-битный канал, запрашивать псевдо-терминал или указывать по-pty нельзя. В команду может быть включена кавычка, предваренная обратной косой чертой. Данный параметр полезен для ограничения использования определенных RSA-ключей. Примером может служить ключ, по которому можно выполнять удаленные операции резервного копирования и ничего более. Учтите, что клиент по-прежнему может запросить перенаправление TCP и (или) X11, если только это не запрещено явно. Команда, запрашиваемая клиентом, заносится в переменную `SSH_ORIGINAL_COMMAND`. Заметьте, что данный параметр относится к выполнению оболочки, команды или подсистемы;

- `environment="ПЕРЕМЕННАЯ=значение"` – добавить переменную в среду (или переопределить ее значение) при регистрации в системе с использованием данного ключа. Допускается указание нескольких таких директив. По умолчанию изменение переменных среды таким образом отключено. За его включение отвечает параметр `PermitUserEnvironment`. Этот параметр отключается автоматически при включении `UseLogin`;
- `From="список-шаблонов"` – если параметр определен, то в дополнение к прохождению аутентификации по открытому ключу каноническое имя удаленного хоста должно соответствовать одному из шаблонов в списке (шаблоны указываются через запятую). Цель этого параметра – увеличение степени защиты: если частный ключ хоста каким-либо образом удастся похитить, то он позволит злоумышленнику войти в систему из любой точки мира. Этот дополнительный параметр делает использование ворованных ключей более затруднительным (кроме перехвата ключа, требуется взлом серверов имен и (или) маршрутизаторов). Смотрите секцию ШАБЛОНЫ в `ssh_config`;
- `no-agent-forwarding` – запретить перенаправление агента аутентификации при аутентификации данным ключом;
- `no-port-forwarding` – запретить перенаправление TCP/IP при аутентификации данным ключом. Любой запрос на перенаправление порта

приведет к получению клиентом сообщения об ошибке. Это может быть использовано, например, вместе с параметром `command`;

- `no-pty` — запретить назначение терминала (запросы на назначение псевдо-терминала не будут удовлетворены);
- `no-X11-forwarding` — запретить перенаправление X11 при аутентификации данным ключом. Любой запрос на перенаправление порта возвратит клиенту сообщение об ошибке;
- `permitopen="хост:порт"` — для функции перенаправления данных с локального клиентского порта на порт удаленной системы (выполняемого при указании `ssh -L`) ограничить набор возможных целей для перенаправления указанной машиной и портом. Для указания адресов IPv6 можно использовать альтернативный синтаксис: `хост/порт`. Допускается указание нескольких целей через запятую. Значение параметра не интерпретируется как шаблон (т. е. является литеральным);
- `tunnel="n"` — принудительно использовать устройство `tun` на сервере. Без этого параметра при запросе клиентом туннеля используется ближайшее доступное для этого устройство.

Пример файла `authorized_keys`:

```
# допустимы комментарии только на всю строку
ssh-rsa AAAAB3Nza...LiPk== user@example.test
from="*.sales.example.test,!pc.sales.example.test" ssh-rsa
AAAAB2...19Q== test@example.test
command="dump /home",no-pty,no-port-forwarding ssh-dss
AAAAC3...51R== example.test
permitopen="192.0.2.1:80",permitopen="192.0.2.2:25" ssh-dss
AAAAB5...21S==
tunnel="0",command="sh /etc/netstart tun0" ssh-rsa AAAA...==
user@example.test
```

8.9.1.5. Формат файла `ssh_known_hosts`

В файлах `/etc/openssh/ssh_known_hosts` и `~/.ssh/known_hosts` хранятся открытые ключи всех машин, с которыми когда-либо устанавливалась связь. Глобальный файл должен быть подготовлен администратором (это необязательно), пользовательский файл поддерживается автоматически: каждый раз, когда поступает запрос на соединение от неизвестной машины, ее ключ автоматически заносится в пользовательский файл.

Каждая строка в этом файле содержит следующие поля: имена хостов, битность, порядок, модуль, комментарий. Поля разделены пробелами.

Имена хостов – это разделенный запятыми список шаблонов (символы подстановки – '*' и '?'); каждый шаблон сопоставляется с каноническим именем машины (при аутентификации клиента) или с именем, которое указано пользователем (при аутентификации сервера). Этот шаблон может также быть предварен знаком '!' для обозначения отрицания: если имя машины соответствует отрицаемому шаблону, оно будет отвергнуто (этой строкой) даже если оно соответствует другому шаблону в этой же строке. Также можно, заключив имя хоста или IP-адрес в квадратные скобки – '[' и ']', – через ':' указать нестандартный порт.

Вместо имен хостов можно записывать их хеши. Это позволит скрыть их от злоумышленника в случае попадания файла в его руки. Для различия хешей от имен хостов первые предваряются символом '|'. На одной строке может быть не больше одного хеша, операция отрицания в этом случае не доступна.

Разрядность, порядок и модуль копируются из ключа хоста RSA, например, `/etc/openssh/ssh_host_key.pub`. Необязательное поле комментария занимает всю оставшуюся часть строки и игнорируется.

Комментариями также считаются пустые и строки, начинающиеся с «#».

Идентификация машины принимается, если любая совпавшая строка содержит правильный ключ. Таким образом, можно (хотя это не рекомендуется) иметь несколько строк или различных ключей для одного и того же хоста. Это неизбежно случается при помещении в файл кратких форм имен хостов из различных доменов. В файлах может содержаться противоречивая информация. Идентификация принимается, если адекватная информация имеется в любом из них.

Заметьте, что строки в этих файлах, обычно имеют длину в несколько сотен символов и, очевидно, не стоит вводить имена хостов вручную. Вместо этого их можно сгенерировать при помощи сценария оболочки или взять из файла `/etc/ssh/ssh_host_key.pub`, добавив вначале имя хоста.

Пример файла `ssh_known_hosts`:

```
# допустимы явные комментарии только на всю строку
closenet,...,192.0.2.53 1024 37 159...93 closenet.example.test
```

```

cvs.example.test,192.0.2.10 ssh-rsa AAAA1234.....=
# хеш имени хоста
|1|JfKTdBh7rNbXkVAQCRp40QoPfmI=|USECr3SWf1JUPsms5AqfD5QfxkM= ssh-
rsa
AAAA1234.....=

```

8.9.1.6. Файлы

`~/.hushlogin` — позволяет отключить вывод времени последнего входа в систему и содержимого файла `/etc/motd`, если в файле конфигурации включены соответственно `PrintLastLog` и `PrintMotd`. Файл не влияет на вывод содержимого `Banner`.

`~/.rhosts` — используется для аутентификации по хосту. На некоторых машинах, если каталог пользователя находится на разделе NFS, для того чтобы он был доступен пользователю `root`, он должен быть доступен для чтения всем. Файл должен принадлежать пользователю и не должен быть доступен для записи другим. Рекомендуемый набор прав доступа в общем случае — чтение/запись для пользователя и недоступность для других.

`~/.shosts` — аналогичен файлу `.rhosts`, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью `rlogin/rsh`.

`~/.ssh/authorized_keys` — содержит список открытых ключей (DSA/ECDSA/RSA), которые могут быть использованы для регистрации данного пользователя. Формат файла описан выше. Этот файл не очень важен для злоумышленника, но мы рекомендуем сделать его доступным только пользователю (чтение/запись).

Если этот файл, каталог `~/.ssh` или домашний каталог пользователя доступны для записи другим пользователям, этот файл может быть изменен или заменен любым пользователем системы, имеющим сколько угодно мало прав. В этом случае `sshd` не будет использовать этот файл, если только параметр `StrictModes` не имеет значение «но». Установить рекомендуемый набор прав доступа можно командой `chmodgo-w ~/ ~/.ssh ~/.ssh/authorized_keys`.

`~/.ssh/environment` – этот файл (при его наличии) считывается в среду при регистрации в системе. Он может содержать только пустые строки, строки комментария (начинающиеся с «#»), и определения значений переменных в виде: переменная=значение. Правом на запись этого файла должен обладать только пользователь; он не должен быть доступен остальным. Задание переменных среды отключено по умолчанию, за что отвечает параметр `PermitUserEnvironment`.

`~/.ssh/known_hosts` – список адресов, к которым когда-либо подключался пользователь, и которые отсутствуют в общесистемном файле, и соответствующих им открытых ключей. Формат файла описан выше. Файл должен быть доступен для записи только владельцу и администратору. Он может также быть доступен для чтения всем остальным, но это не обязательно.

`~/.ssh/rc` – сценарий инициализации, запускаемый перед запуском оболочки пользователя или команды. Этот файл должен быть доступен для записи только пользователю и не должен быть вообще доступен другим.

`/etc/hosts.allow` и `/etc/hosts.deny` – данные о разрешении и запрете соединений с хостами для надстроек TCP.

`/etc/hosts.equiv` – используется для аутентификации на основе хоста. Должен быть доступен для записи только `root`.

`/etc/openssh/moduli` – модули для схемы Диффи-Хеллмана.

`/etc/motd` – содержимое файла отображается программой `login` после того, как осуществлен успешный вход в систему, перед запуском команды интерпретатора.

`/etc/nologin` – если существует, подключение будет разрешено только пользователю с идентификатором `root`. Любому, кто пытается войти в систему, будет показано содержимое этого файла, и запросы на регистрацию в качестве не пользователя с идентификатором `root` будут отвергнуты. Этот файл должен быть доступен для чтения всем.

`/etc/shosts.equiv` – аналогичен `hosts.equiv`, но позволяет проводить аутентификацию на основе хоста, не разрешая вход в систему с помощью `rlogin/rsh`.

`/etc/openssh/ssh_known_hosts` – общесистемный список известных хостов и их ключей. Этот файл должен составляться администратором. В него следует включать открытые ключи всех компьютеров организации. Формат файла описан выше. Файл должен быть доступен всем для чтения и владельцу/администратору для записи.

`/etc/openssh/ssh_host_key`, `/etc/openssh/ssh_host_dsa_key`, `/etc/openssh/ssh_host_ecdsa_key`, `/etc/openssh/ssh_host_rsa_key` – содержат частные ключи хостов. Файлы должны принадлежать `root`, и быть доступными только для него. Не запустится если эти файлы доступны для чтения кому-либо кроме пользователя с идентификатором `root`.

`/etc/openssh/ssh_host_key.pub`, `/etc/openssh/ssh_host_dsa_key.pub`, `/etc/openssh/ssh_host_ecdsa_key.pub`, `/etc/openssh/ssh_host_rsa_key.pub` – содержат открытые ключи хостов. Должны быть доступны всем для чтения и только пользователю с идентификатором `root` для записи. Содержимое файлов должно соответствовать содержимому соответствующих файлов с частными ключами. Эти файлы не используются программой и предназначены для копирования пользователем в файлы `known_hosts`. Эти файлы создаются командой `ssh-keygen`.

`/etc/openssh/sshd_config` – конфигурация службы `sshd`.

`/etc/openssh/sshrd` – аналогичен `~/.ssh/rc`, позволяет задавать инициализационный сценарий глобально для всех пользователей. Должен быть доступен всем для чтения и только `root` для записи.

`/var/empty` – каталог `chroot` используемый при отделении полномочий на предаутентификационном этапе. В папке не должно быть никаких файлов, она должна принадлежать только `root` и не должна быть доступна другим для записи.

`/var/run/sshd.pid` – идентификатор процесса, ожидающего запросов на подключение (если одновременно работает несколько экземпляров служб для нескольких портов, в него записывается идентификатор экземпляра, запущенного

последним). Содержимое этого файла может не быть защищено и может быть доступно всем.

8.9.1.7. Использование openssh и openssh-gostcrypto

По умолчанию, в ОС используется openssh-gostcrypto – сборка с использованием библиотек криптоалгоритмов, описанных в ГОСТ 34.11–2018 «Информационная технология. Криптографическая защита информации. Функция хэширования». При необходимости использовать openssh вместо openssh-gostcrypto, предварительно следует удалить все пакеты openssh-* в которых встречается gostcrypto, а затем установить аналогичные пакеты openssh-*.

Для этого выполнить команду (от пользователя root):

```
apt-get install `rpm -qa |grep openssh |grep gostcrypto |sed 's/-gostcrypto-.*//'\`
```

8.9.2. SSHD_CONFIG

8.9.2.1. Описание файла конфигурации

Служба sshd считывает данные о конфигурации из файла /etc/openssh/sshd_config (или из файла, указанного в командной строке при помощи параметра -f). Файл содержит пары «параметр-значение», по одной на строку. Пустые строки и строки, начинающиеся с «#» интерпретируются как комментарии. В случае, если аргументы содержат пробелы, они должны быть заключены в двойные кавычки (").

Файл /etc/openssh/sshd_config должен быть доступен для записи только пользователю root, и рекомендуется делать его доступным для чтения всем.

В таблице 11 приведены описания возможных параметров (регистр имен аргументов учитывается, регистр имен параметров – нет).

Т а б л и ц а 11 – Описание параметров

Параметр	Описание
AcceptEnv	Список переменных среды, которые, будучи заданы клиентом, будут копироваться в environ сеанса. Соответствующая настройка на стороне клиента выполняется параметром SendEnv и описана в ssh_config. Переменные указываются по имени, допускаются символы подстановки «*» и «?» Несколько переменных среды можно указывать через пробелы или в нескольких параметрах AcceptEnv. Данный параметр введен для предотвращения обхода ограничений среды пользователя посредством изменения значений переменных среды. По умолчанию не принимаются никакие переменные среды
AddressFamily	Семейство адресов, которое должна использовать служба sshd. Допустимые значения: «any» «inet» (только IPv4) и «inet6» (только IPv6). Значение по умолчанию – «any»
AllowGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе разрешается только тем пользователям, чья главная или вспомогательная группы соответствуют какому-либо из шаблонов. Допустимы только имена групп. По умолчанию разрешена регистрация в системе для членов всех групп. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
AllowTcpForwarding	Определяет, будет ли разрешено перенаправление TCP. Значение по умолчанию – «yes». Отключение пересылки TCP не увеличит уровень защищенности системы, пока пользователям не запрещен доступ к командной оболочке, так как они всегда могут установить свои собственные перенаправления
AllowUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом, разрешая доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
AuthorizedKeysFile	Файл с открытыми ключами, которые могут быть использованы для аутентификации пользователей. Допустимо указание шаблонов, они преобразуются при настройке соединения: %% заменяется на символ '%', %h заменяется на домашний каталог идентифицируемого пользователя, %u – на имя пользователя. После преобразования AuthorizedKeysFile интерпретируется либо как абсолютный путь, либо как путь относительно домашнего каталога пользователя. Значение по умолчанию: /etc/openssh/authorized_keys/%u /etc/openssh/authorized_keys2/%u .ssh/authorized_keys .ssh/authorized_keys2.

Продолжение таблицы 11

Параметр	Описание
Banner	Содержимое указанного файла будет отправлено удаленному пользователю прежде, чем будет разрешена аутентификация. Этот параметр доступен только с протоколом версии 2. По умолчанию не выводится никакой информации
ChallengeResponseAuthentication	Определяет, разрешается ли беспарольная аутентификация «вызов-ответ». Поддерживаются все схемы аутентификации <code>login.conf</code> . Значение по умолчанию – «no»
Ciphers	Допустимые для протокола версии 2 шифры. Несколько кодов указываются через запятую. Поддерживаются следующие шифры: «3des-cbc», «aes128-cbc», «aes192-cbc», «aes256-cbc», «aes128-ctr», «aes192-ctr», «aes256-ctr», «arcfour128», «arcfour256», «arcfour», «blowfish-cbc» и «cast128-cbc». Значение по умолчанию: - aes256-ctr, aes192-ctr, aes128-ctr, arcfour256, arcfour128; - blowfish-cbc, aes256-cbc, aes192-cbc, aes128-cbc, 3des-cbc, cast128-cbc, arcfour
ClientAliveCountMax	Количество запросов, проверяющих доступность клиента, которые могут оставаться без ответа. Если предел достигнут, <code>sshd</code> отключит клиента и завершит сеанс. Запросы <code>client alive</code> отличаются от <code>TCPKeepAlive</code> . Данные запросы отправляются через защищенный канал и поэтому не могут быть подменены. Параметр <code>TCPKeepAlive</code> допускает возможность подмены данных. Механизм <code>client alive</code> полезен, если поведение клиента или сервера зависит от активности соединения. Значение по умолчанию – 3. Если <code>ClientAliveInterval</code> равно 15, а для <code>ClientAliveCountMax</code> оставлено значение по умолчанию, не отвечающие клиенты SSH будут отключаться приблизительно через 45 секунд. Данный параметр относится только к протоколу версии 2
ClientAliveInterval	Время бездействия со стороны клиента в секундах, после которого <code>sshd</code> отправляет через защищенный канал запрос отклика клиенту. Значение по умолчанию – 0, что означает, что клиенту не будут направляться такие запросы. Этот параметр применим только с протоколом версии 2
Compression	Разрешить сжатие сразу, после аутентификации или вообще запретить его. Допустимые значения – «yes», «delayed» и «no». Значение по умолчанию – «delayed»
DenyGroups	Список шаблонов имен групп через пробел. Если параметр определен, регистрация в системе пользователям, чья главная или вспомогательная группа соответствуют содержащимся в списке шаблонам, не разрешается. Допустимы только имена групп. По умолчанию регистрация в системе разрешена для всех групп. Разрешающие/запрещающие (<code>allow/deny</code>) директивы обрабатываются в следующем порядке: <code>DenyUsers AllowUsers DenyGroups AllowGroups</code>

Продолжение таблицы 11

Параметр	Описание
DenyUsers	Список имен пользователей через пробел. Если параметр определен, регистрация в системе пользователей, чьи имена соответствуют одному из шаблонов, будет запрещена. Допустимы только имена пользователей; числовой идентификатор пользователя не распознается. По умолчанию разрешена регистрация в системе для всех пользователей. Если шаблон указывается в форме ПОЛЬЗОВАТЕЛЬ@ХОСТ, его две части проверяются отдельно, таким образом, запрещается доступ только пользователям с указанными именами, подключающимся с указанных хостов. Разрешающие/запрещающие (allow/deny) директивы обрабатываются в следующем порядке: DenyUsers AllowUsers DenyGroups AllowGroups
ForceCommand	Выполнять указанную команду после регистрации пользователя в системе, игнорируя команду, запрашиваемую им. Команда запускается оболочкой пользователя с ключом -c. Это относится к выполнению оболочки, команды или подсистемы, обычно применяется внутри блока Match. Команда, запрошенная пользователем, помещается в переменную среды SSH ORIGINAL COMMAND
GatewayPorts	Определяет, разрешено ли удаленным машинам подключение к портам, выделенным для туннелирования трафика клиентов. По умолчанию sshd делает доступными порты, используемые для туннелирования иницируемого сервером, только для кольцевого (loopback) адреса, то есть удаленные машины подключаться к перенаправляемым портам не могут. С помощью данного параметра можно исправить такое положение дел. Значение «no» разрешает туннелирование только в рамках данной системы, «yes» разрешает туннелирование для хостов, соответствующих шаблону, а «clientspecified» позволяет клиенту самостоятельно выбирать адрес для туннелирования. Значение по умолчанию – «no»
GSSAPIAuthentication	Допускать аутентификацию по GSSAPI. Значение по умолчанию – «no» Данный параметр относится только к протоколу версии 2
GSSAPICleanupCredentials	Очищать ли кэш аутентификационных данных клиента при завершении сеанса. Значение по умолчанию – «yes» Данный параметр относится только к протоколу версии 2
HostbasedAuthentication	Допускать аутентификацию по хостам, т. е. аутентификацию по rhosts или /etc/hosts.equiv в сочетании с открытым ключом клиента. Этот параметр схож с RhostsRSAAuthentication и применим только к протоколу версии 2. Значение по умолчанию – «no»
HostbasedUsesNameFromPacketOnly	Отключить выполнение запросов имени хоста при обработке файлов ~/.shosts, ~/.rhosts и /etc/hosts.equiv в рамках аутентификации по хосту (HostbasedAuthentication). При значении «yes» для сравнения будет использоваться имя, указанное клиентом, а не имя, которое может быть получено стандартными средствами соединения TCP. По умолчанию – «no»

Продолжение таблицы 11

Параметр	Описание
HostKey	Файл с частными ключами хоста. Значение по умолчанию – /etc/ssh/ssh_host_key для протокола 1, и /etc/ssh/ssh_host_dsa_key, /etc/ssh/ssh_host_ecdsa_key и /etc/ssh/ssh_host_rsa_key для протокола 2. sshd не будет принимать файлы частных ключей доступные для чтения всей группе или вообще всем пользователям. Можно указывать несколько файлов с ключами хоста. Ключи «rsa1» используются для протокола версии 1, ключи «dsa», «ecdsa» и «rsa» – для версии 2 протокола SSH
IgnoreRhosts	Не учитывать содержимое файлов .rhosts и .shosts при аутентификации RhostsRSAAuthentication и HostbasedAuthentication. При этом будут учитываться только /etc/hosts.equiv и /etc/openssh/shosts.equiv. Значение по умолчанию – «yes»
IgnoreUserKnownHosts	Не учитывать содержимое файла ~/.ssh/known_hosts при RhostsRSAAuthentication или HostbasedAuthentication. Значение по умолчанию – «no»
KerberosAuthentication	Определяет, дозволена ли аутентификация Kerberos. Проверять ли пароль, указанный пользователем для аутентификации PasswordAuthentication в Kerberos KDC. Это может быть либо в форме тикетов Kerberos или, если PasswordAuthentication установлена в «yes», пароль, предоставленный пользователем, будет утвержден через Kerberos KDC. Для использования этого параметра серверу нужна Kerberos servtab, которая разрешит проверку субъекта KDC. Значение по умолчанию – «no»
KerberosGetAFSToken	Если AFS активна и у пользователя имеется Kerberos 5 TGT, получать талон AFS перед обращением к домашнему каталогу пользователя. Значение по умолчанию – «no».
KerberosOrLocalPasswd	В случае непринятия аутентификации посредством Kerberos, проверять пароль другими механизмами, такими как /etc/passwd. Значение по умолчанию – «yes»
KerberosTicketCleanup	Очищать ли кэш талонов пользователя при завершении сеанса. Значение по умолчанию – «yes»
KeyRegenerationInterval	В протоколе версии 1 эфемерный ключ сервера будет автоматически регенерироваться по истечении этого количества секунд. Цель регенерации состоит в том, чтобы предохранить кодированные установленные сеансы от более поздних вторжений на машину и захвата ключей. Ключ нигде не сохраняется. Если установлено значение 0, то ключ не будет регенерироваться. Значение по умолчанию – 3600 (секунд)
ListenAddress	Локальные адреса, по которым sshd должен ожидать соединения. Могут быть использованы следующие форматы записей: ListenAddress хост адрес-IPv4 адрес-IPv6 ListenAddress хост адрес-IPv4:порт ListenAddress [хост адрес-IPv6]:порт

Продолжение таблицы 11

Параметр	Описание
	Если порт не указан, sshd будет ожидать соединения на указанном адресе и на всех указанных ранее (но не после) в параметре Port портах. По умолчанию ожидается соединение на всех локальных адресах. Допустимо указание нескольких параметров
LoginGraceTime	Сервер отключается по истечении этого времени, если пользователю не удалась регистрация в системе. Если стоит значение 0, то время ожидания не ограничено. Значение по умолчанию – 120 секунд
LogLevel	Задаёт степень подробности сообщений для протоколов sshd. Допустимыми являются значения: QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, и DEBUG3. Значение по умолчанию – INFO. Значения DEBUG и DEBUG1 эквивалентны. Использование значения DEBUG* нарушает конфиденциальность пользователей и потому не рекомендуется
MACs	Допустимые алгоритмы MAC (Message Authentication Code – код установления подлинности сообщения). Они используются в протоколе версии 2 для гарантирования целостности данных. Несколько алгоритмов следует указывать через запятую. Значение по умолчанию: hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-sha1-96,hmac-md5-96,hmac-sha2-256,hmac-sha256-96,hmac-sha2-512,hmac-sha2-512-96
Match	Начинает условный блок. Если все критерии на строке Match удовлетворены, указанные в блоке директивы будут иметь больший приоритет, чем указанные в глобальном разделе файла конфигурации. Концом блока считается либо следующая директива Match, либо конец файла. В качестве аргументов Match принимаются пары критерий-шаблон. Допустимые критерии: User Group Host и Address. В самом блоке Match допустимо указание следующих параметров: AllowAgentForwarding, AllowTcpForwarding, AuthorizedKeysFile, AuthorizedPrincipalsFile, Banner, ChrootDirectory, ForceCommand, GatewayPorts, GSSAPIAuthentication, HostbasedAuthentication, HostbasedUsesNameFromPacketOnly, KbdInteractiveAuthentication, KerberosAuthentication, Match, MaxAuthTries, MaxSessions, PasswordAuthentication, PermitEmptyPasswords, PermitOpen, PermitRoot-Login, PermitTunnel, PubkeyAuthentication, RhostsRSAAuthentication, RSAAuthentication, X11DisplayOffset, X11Forwarding и X11UseLocalHost
MaxAuthTries	Ограничение на число попыток идентифицировать себя в течение одного соединения. При достижении количества неудачных попыток аутентификации записи о последующих неудачах будут вноситься в протокол. Значение по умолчанию – 6
MaxSessions	Ограничение на число одновременно открытых сессий в каждом сетевом соединении. Значение по умолчанию – 10

Продолжение таблицы 11

Параметр	Описание
MaxStartups	Ограничение на число одновременных соединений, в которых не был пройден этап аутентификации. Все последующие соединения не будут приниматься, пока на уже существующем соединении не будет произведена аутентификация или не истечет время, указанное в параметре LoginGraceTime. Значение по умолчанию – «10:30:100». Как альтернатива может быть задействован ранний случайный отказ в подключении путем указания трех разделенных через двоеточие значений «старт:норма:предел» (например, «10:30:60»). Соединение будет сбрасываться с вероятностью «норма/100» (30%) если имеется «старт» (10) (10) соединений с не пройденным этапом аутентификации. Вероятность возрастает линейно и постоянно, попытки будут отвергаться при достижении числа «предел» (60)
PasswordAuthentication	Допускать аутентификацию по паролю. Значение по умолчанию – «yes»
PermitEmptyPasswords	Допускать использование пустых паролей при аутентификации по паролю. Значение по умолчанию – «no»
PermitOpen	Ограничить возможные конечные точки для туннелирования TCP. Допустимые формы указания точек: PermitOpen хост:порт PermitOpen адрес-IPv4:порт PermitOpen [адрес-IPv6]:порт Возможно указание нескольких конечных точек через пробел. Значение «any» снимает ограничение и является значением по умолчанию
PermitRootLogin	Допускать вход в систему через ssh в качестве пользователя с идентификатором root. Допустимые значения: «yes», «without-password», «forced-commands-only», «no». Значение по умолчанию – «without-password». Если этот параметр установлен в значение «without-password» войти в систему в качестве пользователя с идентификатором root, указав для аутентификации пароль, будет невозможно. Если этот параметр установлен в значение «forced-commands-only» будет разрешена регистрация пользователя с идентификатором root в системе по открытому ключу, но только если определен параметр command команда (может быть полезно для удаленного создания резервных копий, даже если регистрация пользователя с идентификатором root в системе не разрешена). Все другие методы аутентификации для пользователя с идентификатором root будут отключены. При значении «no» вход в систему в качестве root будет полностью запрещен
PermitTunnel	Допускать использование перенаправления для устройств tun. Допустимые значения: «yes» «point-to-point» (уровень 3), «ethernet» (уровень 2), «no». Значение «yes» эквивалентно «point-to-point» и «ethernet» одновременно. Значение по умолчанию – «no»

Продолжение таблицы 11

Параметр	Описание
PermitUserEnvironment	Учитывать ли файл ~/.ssh/environment и параметры environment= в файле ~/.ssh/authorized_keys. Значение по умолчанию – «no». Посредством изменения переменных среды пользователи могут обойти ограничения своих полномочий. Например, с помощью механизма LD_PRELOAD
PidFile	Файл в который следует записывать идентификатор процесса службы SSH. Значение по умолчанию – /var/run/sshd.pid
Port	Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22. Допустимо указание параметра несколько раз. См. также ListenAddress
PrintLastLog	Выводить ли время и дату предыдущего входа в систему при интерактивной регистрации пользователя в ней. Значение по умолчанию – «yes»
PrintMotd	Выводить ли содержимое файла /etc/motd при интерактивной регистрации пользователя в системе (в некоторых системах это выполняется оболочкой, сценарием /etc/profile или аналогичным). Значение по умолчанию – «yes»
Protocol	Версии протокола, которые следует принимать. Допустимые значения – «1» и «2» Несколько значений указываются через запятую. Значение по умолчанию – «2». Порядок указания протоколов не имеет значения, т.к. протокол выбирается клиентом из списка доступных
PubkeyAuthentication	Допускать аутентификацию по открытому ключу. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 2
RhostsRSAAuthentication	Допускать аутентификацию по rhosts или /etc/hosts.equiv совместно с аутентификацией по хосту RSA. Значение по умолчанию – «no» Данный параметр относится только к протоколу версии 1
RSAAuthentication	Допускать аутентификацию только по ключу RSA. Значение по умолчанию – «yes». Данный параметр относится только к протоколу версии 1
ServerKeyBits	Длина ключа сервера для эфемерного протокола 1. Минимальное значение – 512 (по умолчанию – 1024)
StrictModes	Проверять наборы прав доступа и принадлежность конфигурационных файлов и домашнего каталога пользователя перед разрешением регистрации в системе. Это рекомендуется выполнять потому, что новички иногда оставляют свои каталоги или файлы доступными для записи всем. Значение по умолчанию – «yes»
Subsystem	Позволяет настроить внешнюю подсистему (например, службу FTP). В качестве параметров должны выступать имя подсистемы и команда, которая будет выполняться при запросе подсистемы. Команда sftp-server реализует подсистему передачи файлов sftp. По умолчанию подсистемы не определены. Данный параметр относится только к протоколу версии 2

Продолжение таблицы 11

Параметр	Описание
SyslogFacility	Код источника сообщений для протокола syslog. Допустимые значения: DAEMON, USER, AUTHPRIV, LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7. Значение по умолчанию – AUTHPRIV
TCPKeepAlive	Указывает, будет ли система посылать другой стороне контрольные сообщения для удержания соединения активным. Если они посылаются, то разрыв соединения или аварийный отказ одной из машин будут должным образом замечены. При этом временная потеря маршрута также повлечет за собой разрыв соединения. С другой стороны, если контрольные сообщения не посылаются, сеанс на сервере может зависнуть, оставив после себя «пользователей-привидений» и отнимая ресурсы сервера. Значение по умолчанию – «yes». Это позволяет избежать бесконечно долгих сеансов. Для отключения отправки сообщений TCP keepalive установите значение «no»
UseDNS	Выполнять ли запросы DNS для получения имени удаленного хоста для того чтобы убедиться в том, что обратное преобразование выдает тот же самый IP-адрес. Значение по умолчанию – «no»
UseLogin	Использовать login для интерактивных сеансов регистрации в системе. Значение по умолчанию – «no». login никогда не используется для удаленного выполнения команд. Если этот параметр включен, функция x11Forwarding будет отключена, потому что login не может обрабатывать cookie xauth В случае использования разделения полномочий (UsePrivilegeSeparation) данный параметр будет отключен после прохождения аутентификации
UsePAM	Включить интерфейс модулей аутентификации Pluggable Authentication Module. При значении «yes» аутентификация PAM будет доступна через ChallengeResponseAuthentication и PasswordAuthentication в дополнение к учетной записи PAM и обработке модулей сеансов для всех типов аутентификации. Поскольку беспарольная аутентификация PAM «вызов-ответ» служит заменой аутентификации по паролю, нужно отключить либо PasswordAuthentication, либо ChallengeResponseAuthentication. При включенном UsePAM службу sshd можно будет выполнять только с правами root. Значение по умолчанию – «yes»
UsePrivilegeSeparation	Разделять полномочия посредством создания дочернего процесса с меньшими правами для обработки входящего трафика. После прохождения аутентификации для работы с клиентом будет создан специальный процесс, соответствующий его правам. Если значение параметра равно «sandbox», то на непривилегированный процесс до прохождения аутентификации будут наложены дополнительные ограничения. Значение по умолчанию – «sandbox»

Окончание таблицы 11

Параметр	Описание
X11DisplayOffset	Номер первого дисплея доступного для туннелирования трафика X11 sshd (по умолчанию – 10). Позволяет избежать вмешательства sshd в работу настоящих серверов X11
X11Forwarding	Допускать туннелирование X11. Допустимые значения – «yes» и «no». Значение по умолчанию – «yes». Если дисплей-посредник ожидает соединений от любых адресов (или по шаблону) sshd включение туннелирования X11 подвергает сервер и логические дисплеи клиентов дополнительной опасности. Поэтому такое поведение не является поведением по умолчанию. Проверка и подмена аутентификационных данных при атаке выполняются на стороне клиента. При туннелировании X11 графический сервер клиента может подвергаться атаке при запросе клиентом SSH туннелирования. Для большей защиты пользователей администратор может запретить туннелирование, установив значение «no». Туннелирование X11 отключается автоматически при включении UseLogin
X11UseLocalhost	К какому адресу следует привязывать сервер туннелирования X11: к кольцевому (loopback) или адресу, указанному по шаблону. По умолчанию сервер туннелирования привязывается к кольцевому адресу, а в качестве хоста в переменную среды DISPLAY заносится «localhost». Это не позволяет удаленным хостам подключаться к дисплею-посреднику. Однако, в случае старых клиентов X11, такая конфигурация может не сработать. Установите тогда X11UseLocalhost в «no». Допустимые значения – «yes» и «no». Значение по умолчанию – «yes»
XAuthLocation	Путь к команде xauth. Значение по умолчанию – /usr/bin/xauth

8.9.2.2. Указание времени

Ключи командной строки sshd и параметры файлы конфигурации могут требовать указания времени. Оно должно указываться в виде последовательности:

время [единицы]

где время – положительное целое, единицы могут принимать следующие значения:

- ничего – секунды;
- s | S – секунды;
- m | M – минуты;
- h | H – часы;
- d | D – дни;
- w | W – недели.

Итоговое время получается в результате сложения всех выражений.

Примеры:

- 600 – 600 секунд (10 минут);
- 10m – 10 минут;
- 1h30m – 1 час 30 минут (90 минут).

8.9.2.3. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на первом контроллере домена DC1):

```
# ssh-keygen -t ed25519
```

На вопрос о файле для сохранения ключа нажать клавишу «Enter» (по умолчанию).

На вопрос о пароле к ключу также нажать клавишу «Enter» (не указывать пароль).

Скопировать публичную часть SSH-ключа на второй контроллер домена (DC2) для пользователя user:

```
# ssh-copy-id -i ~/.ssh/id_ed25519.pub user@dc2.test.alt
```

Проверка, что ключ был скопирован на DC2:

```
# ssh user@dc2.test.alt
```

```
[user@dc2 ~]$ su -
```

```
Password:
```

```
[root@dc2 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
```

```
[root@dc2 ~]# exit
```

```
ВЫХОД
```

```
[user@dc2 ~]$ exit
```

```
ВЫХОД
```

```
Connection to dc2 closed.
```

Теперь есть возможность удаленно выполнять команды на DC2 с привилегиями администратора.

8.9.3. USB/IP

USB/IP выполняет задачу подключения USB-устройства к удаленному компьютеру через локальную сеть (проброс USB-устройств по локальной сети).

В качестве пробрасываемых устройств могут быть:

- USB-накопители (fdisk, mkfs, mount/umount, операции с файлами);
- USB-клавиатуры и USB-мыши;
- USB веб-камеры и динамики;
- USB-принтеры, USB-сканеры, USB-конвертеры последовательных интерфейсов и адаптеры USB-Ethernet.

На сервере USB/IP можно выводить перечень устройств, устанавливать и убирать их привязки. На клиенте USB/IP можно выводить перечень устройств, экспортированных серверами USB/IP, присоединять и отсоединять их.

Примечание. К серверу подключаются USB-устройства, которые экспортируются на хост-клиент. Хост-клиент виртуально импортирует USB-устройства.

8.9.3.1. Настройка сервера

Установить пакеты usbip, usbip-server:

```
# apt-get install usbip usbip-server
```

Подгрузить модули драйверов USB:

```
# modprobe usbip-core  
# modprobe usbip-host
```

Запустить сервис usbipd и добавить его в автозапуск:

```
# systemctl enable --now usbipd
```

8.9.3.2. Настройка клиента

Установить пакет usbip:

```
# apt-get install usbip
```

Подгрузить модули драйверов USB:

```
# modprobe usbip-core  
# modprobe vhci-hcd
```

8.9.3.3. Управление устройствами

8.9.3.3.1. Сервер

Вывести информацию о подключенных локальных устройствах:

```
# usbip list -l
- busid 1-1.1 (0402:9665)
  ALi Corp. : Gateway Webcam (0402:9665)

- busid 1-1.4 (13fe:4300)
  Kingston Technology Company Inc. : unknown product (13fe:4300)

- busid 2-1.2 (090c:1000)
  Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.) : Flash Drive (090c:1000)
```

Сделать устройство, например, с ID 2-1.2 доступным:

```
# usbip bind --busid 2-1.2
usbip: info: bind device on busid 2-1.2: complete
```

Теперь к устройству можно получить доступ с клиента.

Закрыть доступ к устройству:

```
# usbip unbind --busid 2-1.2
usbip: info: unbind device on busid 2-1.2: complete
```

8.9.3.3.2. Клиент

Получить список доступных устройств на указанном IP-адресе можно, выполнив команду:

```
# usbip list --remote <IP-адрес>
```

Например:

```
# usbip list --remote 192.168.0.118
Exportable USB devices
=====
- 192.168.0.118
  2-1.2: Silicon Motion, Inc. - Taiwan (formerly Feiya Technology Corp.) : Flash Drive (090c:1000)
        : /sys/devices/pci0000:00/0000:00:1d.0/usb2/2-1/2-1.2
        : (Defined at Interface level) (00/00/00)
```

Команда подключения к доступному USB-устройству:

```
# usbip attach --remote <IP-адрес> --busid <ID-устройства>
```

Например:

```
# usbip attach --remote 192.168.0.118 --busid 2-1.2
```

Получить список подключенных устройств:

```
# usbip port
Imported USB devices
=====
Port 00: <Port in Use> at High Speed(480Mbps)
        Silicon Motion, Inc. - Taiwan (formerly Feiya Technology
Corp.) : Flash Drive (090c:1000)
        3-1 -> usbip://192.168.0.118:3240/2-1.2
        -> remote bus/dev 002/003
```

Команда отключения устройства:

```
# usbip detach --port <Port_number>
```

Например:

```
# usbip detach --port 00
usbip: info: Port 0 is now detached!
```

8.9.3.4. Графическая утилита

Для проброса устройств, а также для присоединения/отсоединения USB-устройств с сервера можно воспользоваться графическим интерфейсом (пакет usbip-gui).

Установка:

```
# apt-get install usbip-gui
```

Примечание. Должны быть также установлены соответствующие пакеты для сервера и клиента.

Примечание. Для того чтобы использовать все возможности утилиты, ее необходимо запускать с правами суперпользователя:

```
# usbip-gui
```

После запуска программы будут отображены текущие подключенные устройства (рис. 168).

В поле «Remote USB Devices» отображается список устройств, доступных на удаленном сервере, в поле «Local USB Devices» – список локально-подключенных устройств, а в поле «Attached Devices» – список устройств, подключенных с удаленного сервера.

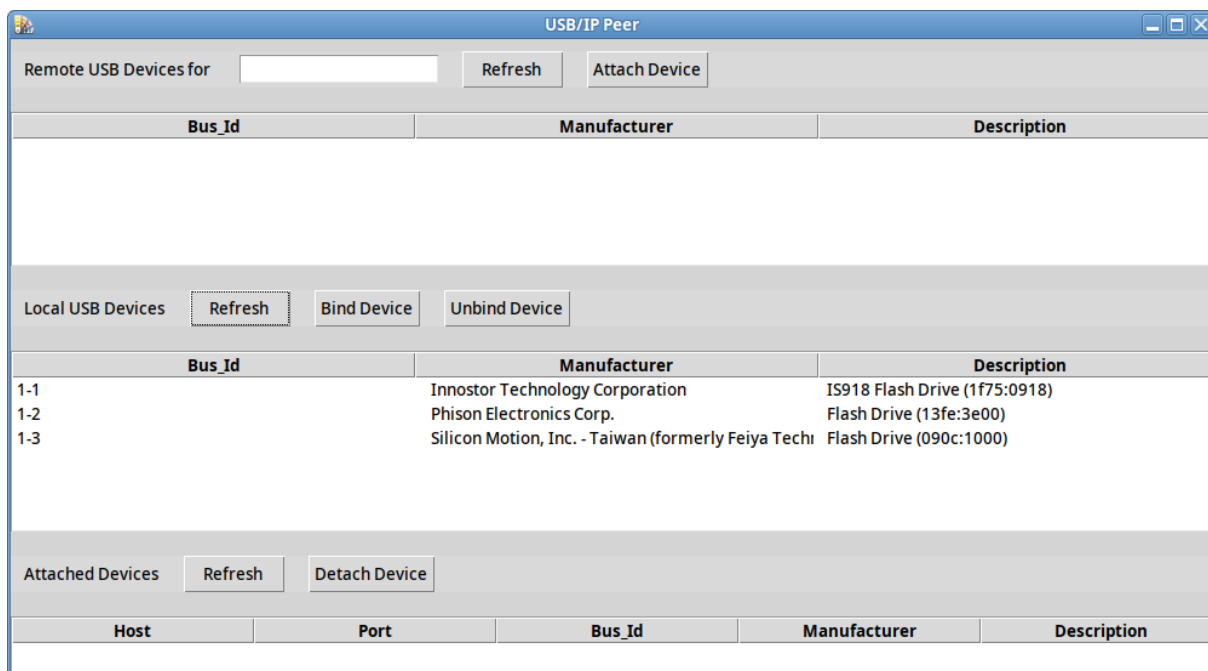


Рис. 168 – Usbip-gui. Подключенные USB-устройства

Кнопки «Refresh», расположенные над каждым полем, позволяют обновить соответствующий список USB-устройств.

Для подключения/отключения USB-устройства с удаленного сервера необходимо:

- 1) ввести IP-сервера в поле «Remote USB Devices for» и нажать на кнопку «Refresh»;
- 2) если на удаленном сервере есть доступные устройства, они появятся в списке «Remote USB Devices»;
- 3) выбрать нужное устройство и нажать на кнопку «Attach Device» (рис. 169);
- 4) устройство появится в списке «Attached Devices» (рис. 170).

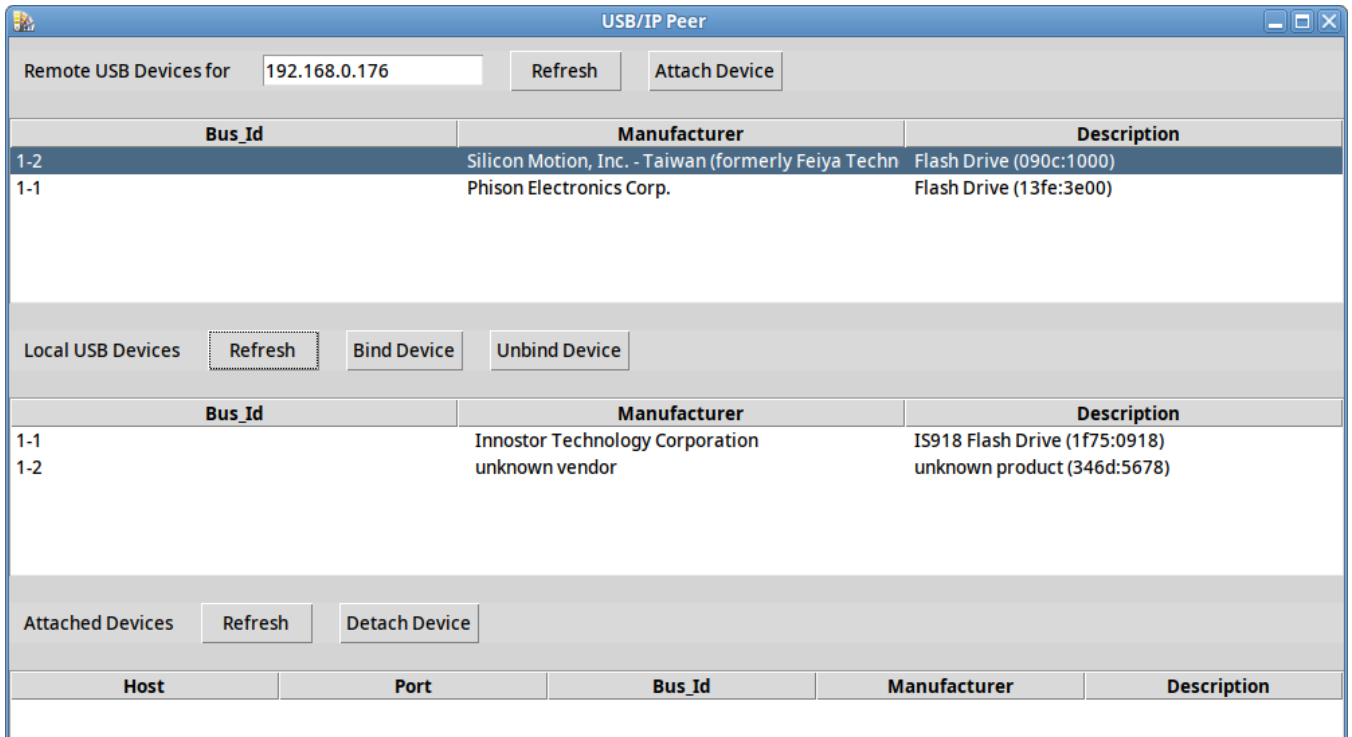


Рис. 169 – Usbip-gui. Подключение к доступному USB-устройству

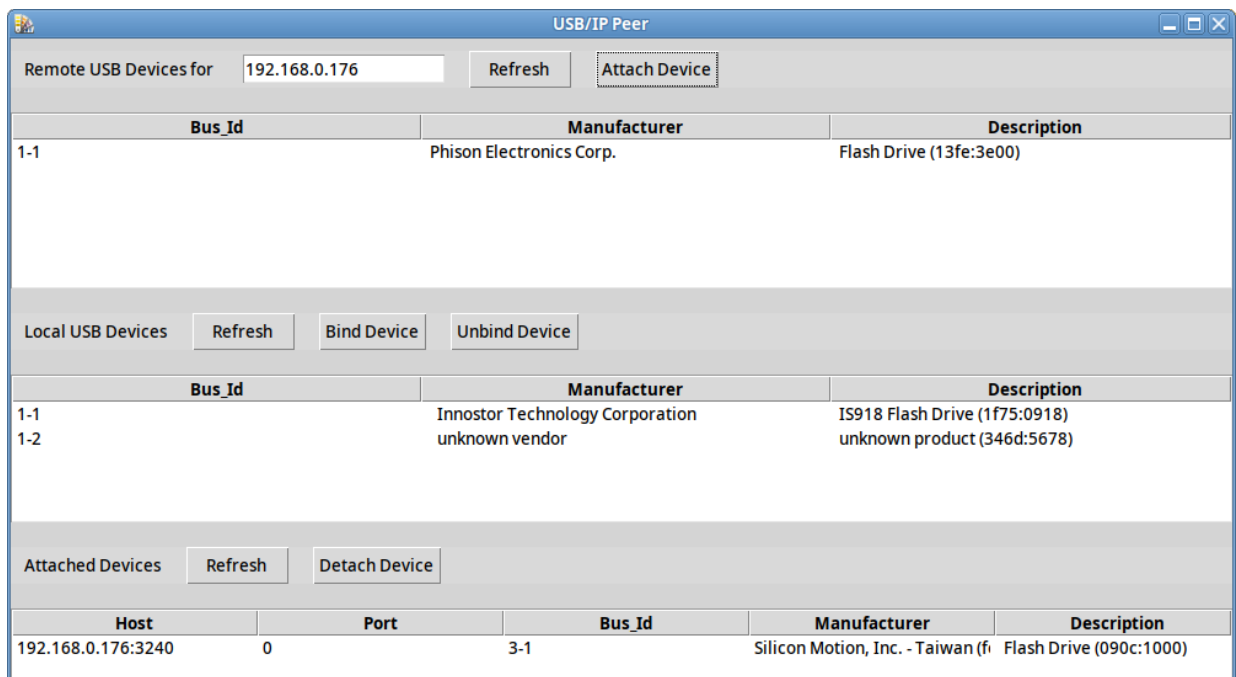


Рис. 170 – Usbip-gui. Список подключенных устройств

Для отключения устройства, достаточно выбрать его в списке «Attached Devices» и нажать на кнопку «Detach Device».

Для того чтобы открыть доступ к локальному USB-устройству, необходимо:

- 1) в поле «Local USB Devices» выбрать нужное устройство (рис. 171);
- 2) нажать кнопку «Bind Device».

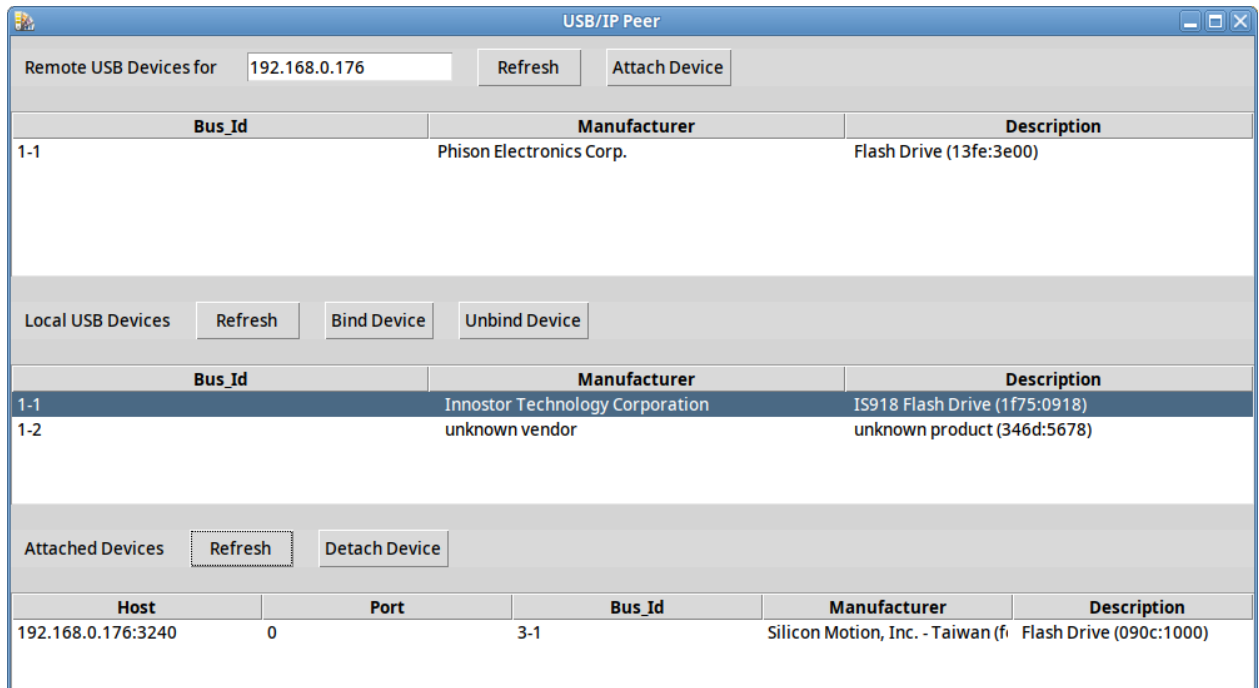


Рис. 171 – Usbip-gui. Локальное USB-устройство

Примечание. Чтобы закрыть доступ к локальному USB-устройству, следует выделить устройство и нажать на кнопку «Unbind Device».

8.10. Прокси-сервер (Squid)

Для обеспечения контролируемого доступа ПЭВМ локальной сети к сети Интернет в составе ОС Альт СП используется кэширующий прокси-сервер Squid.

Примечание. Пакет squid не установлен по умолчанию, для установки выполнить следующую команду:

```
# apt-get install squid
```

Для обеспечения возможности использования ПЭВМ, на которую установлен Squid, в качестве прокси-сервера нужно настроить таблицы управления доступом (Access Control Lists, далее – ACL), которые хранятся в конфигурационном файле squid.conf в директории /etc/squid/.

Для того чтобы сервер Squid принимал соединения из всей внутренней сети, нужно в раздел # TAG: acl включить следующую запись:

```
acl our_networks src <адреса внутренней сети>
http_access allow our_networks
```

При настройке таблиц управления доступом следует учитывать, что при обработке запроса на доступ к серверу Squid все строки http_access файла squid.conf просматриваются последовательно сверху вниз до первой строки, соответствующей параметрам запроса.

8.10.1. Настройка прозрачного доступа через прокси-сервер

Для настройки прозрачного доступа пользователей локальной сети к сети Интернет через прокси-сервер нужно выполнить настройку фильтра адресов, для этого нужно выполнить команду iptables, перенаправляющую HTTP-запросы к внешним серверам на порт Squid:

```
# iptables -t nat -A PREROUTING ! -d <прокси-сервер> \
-i <внутренний_интерфейс> -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128
```

Также можно выполнить альтернативную команду:

```
# iptables -t nat -A PREROUTING -p tcp -d 0/0 --dport www \
-i <внутренний_сетевой_интерфейс> -j DNAT \
--to <локальный_адрес_на_котором_слушает_прокси>:3128
```

Настройка squid.conf при этом использует обратное проксирование. Далее нужно добавить в конфигурационный файл squid.conf следующую строку:

```
http_port 80 intercept
```

Примечание. Параметр intercept заменяет параметр transparent, который также использовался в предыдущих версиях squid.conf.

8.10.2. Фильтрация доступа

В Squid существует гибкая схема фильтрации внешних ссылок, с помощью которой предоставляется возможность ограничить (запретить) доступ к определенным сетевым ресурсам. Содержимое фильтруется с помощью таблиц управления доступом ACL и настроек http_access deny, примеры которых приведены в конфигурационном файле squid.conf. При задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения,

определяя в одной строке фильтр для целого класса адресов или доменных имен.

Запрет доступа к домену `baddomain.com`, например, можно оформить следующим образом:

```
acl Bad dstdomain baddomain.com
http_access deny Bad
```

8.10.3. Авторизация доступа

Squid позволяет настраивать таблицы доступа ACL индивидуально для пользователей и (или) категорий пользователей. Если для определения того, какой именно пользователь подключается к серверу, недостаточно IP-адреса его компьютера, следует использовать схемы авторизации, принятые в Squid. Авторизация конфигурируется с помощью тега `TAG: auth_param`. Схемы (программы) авторизации, поддерживаемые Squid, хранятся в каталоге `/usr/lib/squid`.

Для настройки аутентификации в LDAP можно использовать следующую конфигурацию:

```
auth_param basic program /usr/lib/squid/squid_ldap_auth -b
ou=People,dc=office,dc=lan -f (uid=%s) -h ldap.office.lan
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
```

8.10.4. Кэширование данных

Squid обеспечивает возможность кэширования данных, полученных по запросам из сети Интернет (при повторных запросах данные извлекаются из сохраненной копии).

Настройка правил кэширования данных осуществляется с помощью таблиц доступа ACL, а также с помощью настройки конфигурационного файла `squid.conf`. Для отключения функции кэширования данных нужно использовать параметр `always_direct`, для включения принудительного кэширования – `never_direct`.

Например, чтобы запретить кэширование данных, получаемых по протоколу FTP, нужно в конфигурационный файл `squid.conf` добавить следующие строки:

```
acl FTP proto FTP
always_direct allow FTP
```

Squid поддерживает возможность обмена данными с кэшем авторизованного сервера (`parent peer` (родительский прокси-сервер) / `sibling peer` (братский прокси-сервер)), например, если запрашиваемый ресурс в локальном кэше Squid не найден.

8.10.5. Настройка режима работы в качестве обратного прокси-сервера

Squid поддерживает режим работы в качестве обратного прокси-сервера. Работа в таком режиме обеспечивает ретрансляцию запросов из внешней сети на один или несколько серверов, логически расположенных во внутренней сети, и позволяет скрыть реальное расположение и структуру серверов, а также уменьшить нагрузку на них.

Для настройки сервера Squid для работы в качестве единственного обратного прокси-сервера, принимающего HTTP-запросы из внешней сети, нужно в конфигурационный файл `squid.conf` добавить следующие строки:

```
http_port 80 accel defaultsite=internal.www.com
cache_peer <имя сервера> parent 80 <порт ICP> no-query
originserver
```

Примечания:

1. В примере в качестве порта, принимающего запросы из внешней сети по протоколу HTTP, используется порт 80.
2. Так как сервер Squid играет роль единственного обратного прокси-сервера, нужно выключить ICP, указав в качестве порта ICP значение 0.
3. `parent` (родительский прокси-сервер) – тип прокси-сервера в соответствии с иерархией серверов.

Для обратного проксирования нескольких внутренних серверов нужно, чтобы внешние запросы к ресурсам сети Интернет с разными доменными именами попадали на вход Squid, который бы ставил в соответствие каждому имени действительный адрес сервера во внутренней сети и в соответствии с этим перенаправлял запрос. Делается это с помощью механизма виртуальных хостов.

Для организации прокси для двух серверов (`www1.foo.bar` и `www2.foo.bar`), адреса которых в DNS указывают на машину со Squid-сервером нужно в конфигурационный файл `squid.conf` добавить следующую запись:

```
http_port 80 accel defaultsite=www1.foo.bar vhost
hosts_file /etc/hosts
```

Настройка `defaultsite` используется сервером для заполнения HTTP-заголовков. Для преобразования доменных имен в адреса серверов во внутренней сети следует использовать файл `/etc/hosts`:

```
10.0.0.1 www1.foo.bar
10.0.0.2 www2.foo.bar
```

8.10.6. Сбор статистики и ограничение полосы доступа

В состав Squid входит утилита кэш-менеджер, предназначенная для отображения статистики и загрузки сервера. Кэш-менеджер представляет собой cgi-приложение и должен выполняться под управлением сконфигурированного HTTP-сервера. Все настройки кэш-менеджера выполняются с помощью конфигурирования файла `squid.conf` (строки, которые относятся к кэш-менеджеру, обычно включают `cachemgr`).

Squid также обеспечивает возможность ограничения полосы пропускания для пользователей (для этого используются параметры `delay_pools` и `delay_class`).

8.10.7. Кеширование DNS-запросов

Squid содержит встроенный минисервер запросов DNS. Он выступает как посредник между Squid и внешними DNS-серверами. При запуске Squid производит начальное тестирование доступности DNS (можно отключить, используя опцию `-D`). Время кеширования удачного DNS-запроса по умолчанию составляет шесть часов.

9. ОГРАНИЧЕНИЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

9.1. Ограничение полномочий пользователей по использованию консолей

9.1.1. Настройка ограничения в ЦУС

Модуль ЦУС «Блокировка терминала» позволяет ограничить определенным пользователям возможность использования определенных ТТУ. Модуль является интерфейсом для файла конфигурации `/etc/security/access.conf`.

Примечание. Должен быть установлен пакет `alterator-secsetup`:
`# apt-get install alterator-secsetup`

Для включения модуля необходимо установить отметку в поле «возможность блокировки включена» (рис. 172).

Для каждого отдельного пользователя системы можно заблокировать любые необходимые ТТУ, для этого в окне «Список ТТУ» необходимо отметить консоли, которые должны быть заблокированы для данного пользователя, перенести их в окно «Заблокированные ТТУ» и нажать на кнопку «Применить» (рис. 172).

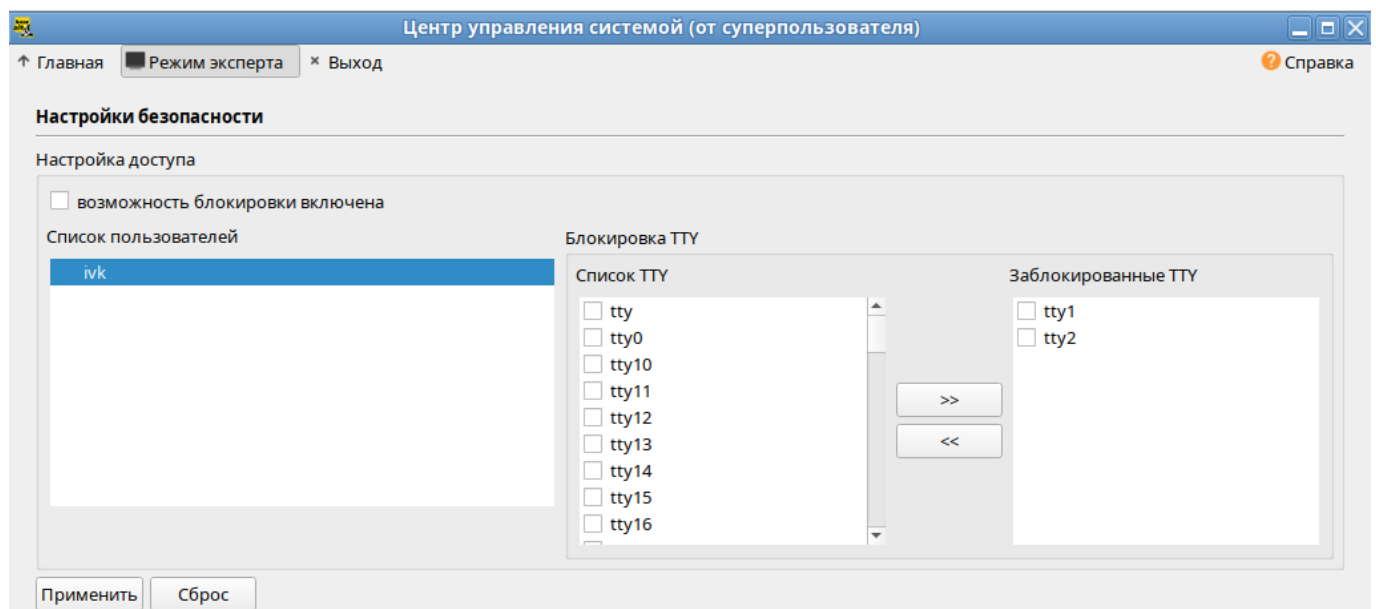


Рис. 172 – Ограничение полномочий пользователей по использованию консолей

9.1.2. Настройка ограничения в консоли

Чтобы ограничить консольный доступ для пользователей/групп с помощью модуля `pam_access.so` необходимо внести изменения в файл `/etc/security/access.conf`.

Примечание. Формат файла `/etc/security/access.conf`:

`permission:users:origins`

где:

- `permission` – знак «+» (плюс) – предоставление доступа, или знак «-» (минус) – отказ в доступе;
- `users` – список пользователей или групп пользователей или ключевое слово `ALL`;
- `origins` – список ТТУ (для локального доступа), имен хостов, доменных имен, IP-адресов, ключевое слово `ALL` или `LOCAL`.

Чтобы ограничить доступ для всех пользователей, кроме пользователя `root`, следует внести следующие изменения:

```
# vim /etc/security/access.conf
-:ALL EXCEPT root: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для конкретного пользователя:

```
# vim /etc/security/access.conf
-:user: tty2 tty3 tty4 tty5 tty6
```

Доступ может быть ограничен для группы, содержащей несколько пользователей:

```
# vim /etc/security/access.conf
-:group: tty2 LOCAL
```

Далее необходимо сконфигурировать стек РАМ для использования модуля `pam_access.so` для ограничения доступа на основе ограничений, определенных в файле `/etc/security/access.conf`. Для этого дописать в файл `/etc/pam.d/system-auth-local-only` строку `account required pam_access.so` после строки `account required pam_tcb.so`:

<code>auth</code>	<code>required</code>	<code>pam_tcb.so shadow fork nullok</code>
<code>account</code>	<code>required</code>	<code>pam_tcb.so shadow fork</code>
<code>account</code>	<code>required</code>	<code>pam_access.so</code>
<code>password</code>	<code>required</code>	<code>pam_passwdqc.so config=/etc/passwdqc.conf</code>
<code>password</code>	<code>required</code>	<code>pam_tcb.so use_authtok shadow fork nullok write_to=tcb</code>
<code>session</code>	<code>required</code>	<code>pam_tcb.so</code>

9.2. Ограничение неуспешных попыток входа в информационную систему

Для ограничения неуспешных попыток входа используется модуль `pam_faillock`, который считает количество попыток доступа/неудачные попытки аутентификации, может запретить доступ/блокировать учетную запись в случае, если слишком много попыток ввода пароля завершилось неудачно или превышено количество попыток входа.

Можно заблокировать учетную запись: либо на определенный срок, либо пока ее не разблокирует администратор.

Добавление следующей строки в файл `/etc/pam.d/login` заблокирует все учетные записи, кроме `root`, на два часа, после четырех неудачных попыток входа в систему:

```
auth required pam_faillock.so authfail deny=4 unlock_time=7200
```

Добавление этой строки в файл `/etc/pam.d/sshd` заблокирует все учетные записи, кроме `root`, на два часа, после четырех неудачных попыток входа в систему по `ssh`.

В случае, если необходимо, чтобы модуль `pam_faillock` контролировал и учетную запись суперпользователя `root`, в настройки нужно добавить параметр `even_deny_root`. Добавление следующей строки в файл `/etc/pam.d/login` заблокирует все учетные записи, включая учетную запись суперпользователя `root`, после четырех неудачных попыток входа в систему:

```
auth required pam_faillock.so authfail deny=4 even_deny_root unlock_time=7200
```

Модуль `pam_faillock` может отображать количество неудачных попыток входа пользователей, сбрасывать индивидуальные счетчики, или очищать все счетчики.

Примечание. Установка искусственно завышенных счетчиков может использоваться для блокировки пользователей без изменения их паролей.

Запуск утилиты `faillock` без опций позволяет просмотреть количество неуспешных попыток входа в систему всех пользователей.

Количество неудачных попыток входа конкретного пользователя test, в зависимости от используемого модуля, можно увидеть с помощью утилиты:

```
# faillock --user test
```

Примечание. Для получения дополнительной информации смотрите страницы `man pam_faillock` и `faillock`.

Разблокировать учетную запись пользователя без таймаута:

```
# faillock --user test --reset
```

РАМ фиксирует все неудачные попытки входа в систему в syslog, если необходимо записывать все попытки входа в систему (успешные и неуспешные), то в файл `/etc/pam.d/login` нужно добавить строку:

```
account required pam_warn.so
```

9.3. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы

В файле `/etc/security/limits.conf` определяются ограничения ресурсов системы для пользователя или группы пользователей. Формат файла:

```
<domain> <type> <item> <value>
```

Первое поле (`domain`) может содержать:

- имя пользователя;
- имя группы. Перед именем группы нужно указать символ «@»;
- символ «*». Данное ограничение будет ограничением по умолчанию;
- символ «%» – используется только с ограничением `maxlogins`. Группа, указанная после %, ограничивает число параллельных сеансов всех пользователей, которые являются членами группы. Если символ «%» используется отдельно, он идентичен использованию «*» с ограничением `maxsyslogins`;
- диапазон `uid`, заданный как `<min_uid>:<max_uid>`;
- диапазон `gid`, заданный как `@<min_gid>:<max_gid>`;
- `gid`, заданный как `%:<gid>` – используется только с ограничением `maxlogins`.

Второе поле – это 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. Символ «-» используется для одновременной установки как мягкого, так и жесткого ограничения.

Элементом ограничения (item) может быть:

- core – ограничение размера файла core (Кбайт);
- data – максимальный размер данных (Кбайт);
- fsize – максимальный размер файла (Кбайт);
- memlock – максимальное заблокированное адресное пространство (Кбайт);
- nofile – максимальное число открытых файлов;
- stack – максимальный размер стека (Кбайт);
- cpu – максимальное время процессора (минуты);
- nproc – максимальное число процессов;
- as – ограничение адресного пространства;
- maxlogins – максимальное число одновременных регистраций в системе;
- maxsyslogins – максимальное количество учетных записей;
- priority – приоритет запуска пользовательских процессов;
- locks – максимальное число файлов блокировки;
- sigpending – максимальное количество сигналов, которые можно передать процессу;
- msgqueue – максимальный размер памяти для очереди POSIX сообщений (байт);
- nice – максимальный приоритет, который можно выставить: [-20, 19];
- rtprio – максимальный приоритет времени выполнения.

Чтобы установить максимальное число процессов для пользователя user, в файл `limits.conf` нужно добавить записи:

```
user soft nproc 50
user hard nproc 60
```

Первая строка определяет мягкое ограничение (равное 50), а вторая – жесткое.

Следующие строки обеспечат одновременную работу не более 15 пользователей из каждой группы пользователей (group1 и group2):

```
%group1 - maxlogins 15
%group2 - maxlogins 15
```

В первом и втором случае из каждой группы пользователей одновременно работать смогут не более 15. При шестнадцатой регистрации пользователь из группы увидит сообщение:

```
There were too many logins for 'user'.
```

Следующая запись ограничит число параллельных сеансов доступа для каждой учетной записи пользователей:

```
* - maxlogins 5
```

9.4. Блокировка макросов в приложениях

Для того чтобы включить блокировку макросов в приложениях, необходимо в ЦУС перейти в раздел «Система» → «Настройки безопасности» (пакет alterator-secsetup).

В открывшемся окне следует отметить пункт «Блокировать макросы приложений» и нажать на кнопку «Применить» (рис. 173).

Макросы будут заблокированы.

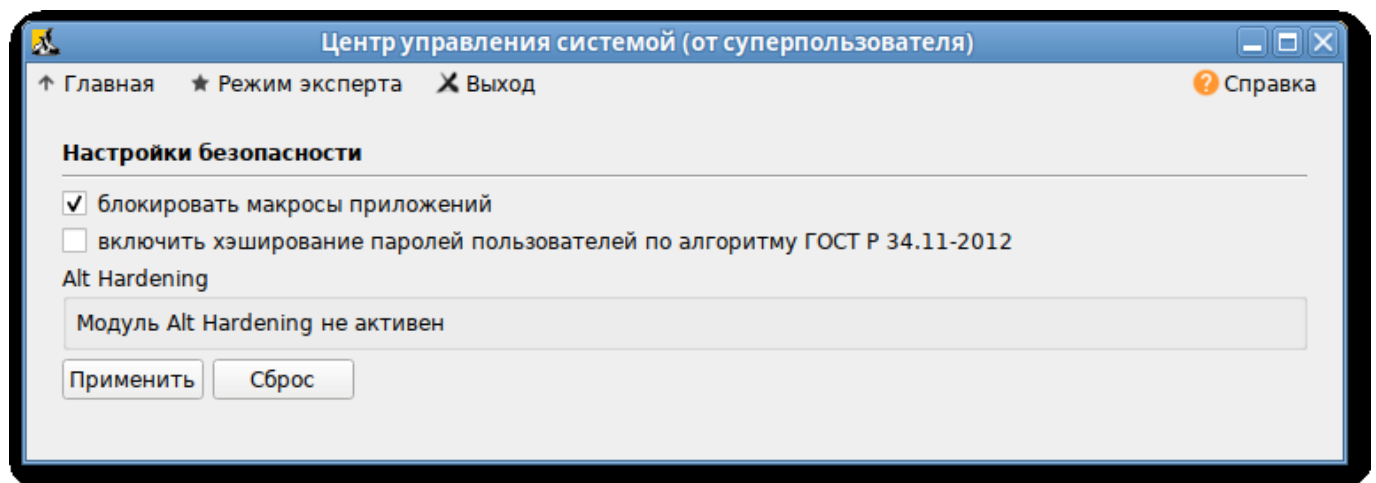


Рис. 173 – Блокировка макросов в приложениях

9.5. Настройка предупреждения пользователя при его входе в систему

Примечание. Для корректной работы функции предупреждения в системе должен быть установлен пакет zenity.

Для реализации функции предупреждения необходимо создать файл `user_login_message` в каталоге `/etc/X11/xinit` со следующим содержимым:

```
#!/bin/sh -e
[ $(id -u) -gt 0 ] || exit 0
[ -n $(which zenity) ] || exit 0
```

```
message="Предупреждение! В системе реализованы меры защиты информации, необходимо
соблюдать установленные оператором правила обработки информации. Для продолжения
работы нажмите 'Продолжить', если не хотите продолжения запуска пользовательской
сессии нажмите 'Выйти'"
exec zenity --warning --text "$message" --ok-label="Продолжить" --extra-button
"Выйти"
```

Для отображения пользователю другого сообщения – поправьте значение переменной "message".

Выполнить команду изменения прав на исполнение файла:

```
chmod +x /etc/X11/xinit/user_login_message
```

В файл конфигурации /etc/X11/Xsession сразу после строки

```
/etc/X11/xinit/xrootwarn || exit
```

добавить строку /etc/X11/xinit/user_login_message || exit

Выполнить перезагрузку ОС.

Теперь после ввода логина и пароля в окне загрузки, перед полным стартом сессии пользователь будет получать предупреждение с указанным в /etc/X11/xinit/user_login_message сообщением (рис. 174).

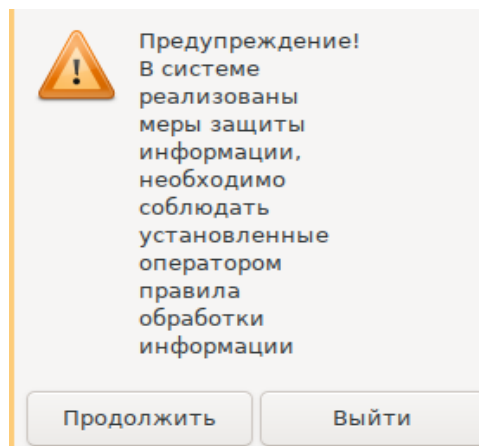


Рис. 174

9.6. Определение параметров уничтожения данных

Для пользователей нужно запретить использование команды `rm`. Для этого нужно выполнить команду:

```
# chmod o-x /bin/rm
```

Команда `srm` предназначена для удаления данных без возможности их восстановления. `srm` выполняет безопасную перезапись/переименование/удаление целевого файла(ов). Использование команды `srm` аналогично использованию `rm`.

Команда `shred` переписывает несколько раз файл, скрывая его содержимое, для того, чтобы сделать более трудоемким процесс восстановления данных даже в случае использования специального оборудования для восстановления:

```
shred [ОПЦИЯ] ФАЙЛ [...]
```

Стандартные опции для запуска команды:

- 1) `-f`, `--force` – изменить права для разрешения записи, если нужно;
- 2) `-n`, `--iterations=N` – переписать `N` раз вместо указанных (25) по умолчанию;
- 3) `-s`, `--size=N` – очистить `N` байт (возможны суффиксы вида К, М, G);
- 4) `-u`, `--remove` – обрезать и удалить файл после перезаписи;
- 5) `-v`, `--verbose` – показывать индикатор прогресса;
- 6) `-x`, `--exact` – не округлять размеры файлов до следующего целого блока;
- 7) `-z`, `--zero` – перезаписать в конце с нулями, чтобы скрыть перемешивание.

Если файл задан как `-`, перемешивать стандартный вывод.

Удаляет ФАЙЛЫ если указан `--remove (-u)`. По умолчанию файлы не удаляются, так как часто обрабатываются файлы-устройства вроде `/dev/hda`, а такие файлы нельзя удалять.

Команда `sfill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов (`inode`) указанного каталога. Процесс удаления данных выглядит следующим образом:

- 1) 1 проход с `0xff` (все данные затираются значением `0xff`);
- 2) 5 случайных проходов с `/dev/urandom` используя RNG;
- 3) 27 проходов со значениями Питера Гутмана;
- 4) обрезает файл.

Стандартные опции для запуска команды:

- 1) `-d` – игнорировать специальные файлы `"."` и `".."`;
- 2) `-f` – быстрый (и небезопасный режим);
- 3) `-l` – выполнить только два прохода, с `0xff` и случайное заполнение;

- 4) `-l -l` – выполнить только случайное заполнение (один проход);
- 5) `-r` – выполнить в рекурсивном режиме, удалить все подкаталоги;
- 6) `-v` – подробный режим;
- 7) `-z` – последний проход заполняет нулями, а не случайными данными.

Пользователю запрещено определять параметры уничтожения данных. Эти параметры определяет администратор.

Для определения параметров уничтожения данных в системе созданы скрипты с предопределенными настройками уничтожения данных, для их переопределения администратор должен внести правки в файл `/etc/sysconfig/s_rm`.

П р и м е ч а н и е . Должен быть установлен пакет `altsp-test-scripts`.

Пользователи для удаления данных должны использовать команды `s_rm` и `s_fill`.

9.7. Модуль AltNa

AltNa – это модуль безопасности Linux, может использоваться для настройки блокировки возможности удаления открытого файла.

Модуль в настоящее время имеет три варианта защиты пользовательского пространства:

- игнорировать биты SUID в двоичных файлах (возможны исключения);
- запретить запуск выбранных интерпретаторов в интерактивном режиме;
- отключить возможность удаления открытых файлов в выбранных каталогах.

Для включения модуля AltNa в файле `/boot/boot.conf` в значение переменной `CMDLINE` необходимо добавить опцию `altha=1`. Перезагрузить систему.

П р и м е ч а н и е . Для возможности управления настройками модуля AltNa в ЦУС, должен быть установлен пакет `alterator-secsetup`:

```
# apt-get install alterator-secsetup
```

9.7.1. Запрет бита исполнения (SUID)

При включенном подмодуле `altha.nosuid` биты SUID во всех двоичных файлах, кроме явно перечисленных, игнорируются в масштабе всей системы.

Для включения запрета бита исполнения следует установить значение переменной `kernel.altha.nosuid.enabled` равным 1:

```
# sysctl -w kernel.altha.nosuid.enabled=1
```

И добавить, если это необходимо, исключения (список включенных двоичных файлов SUID, разделенных двоеточиями), например:

```
# sysctl -w kernel.altha.nosuid.exceptions="/bin/su:/usr/libexec/hashe-priv/hashe-priv"
```

Проверка состояния режима запрета бита исполнения выполняется командой:

```
# sysctl -n kernel.altha.nosuid.enabled  
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

Для включения запрета бита исполнения в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности», в открывшемся окне отметить пункт «Отключить влияние suid бита на привилегии порождаемого процесса», внести изменения в список исключений и нажать кнопку «Применить» (рис. 175).

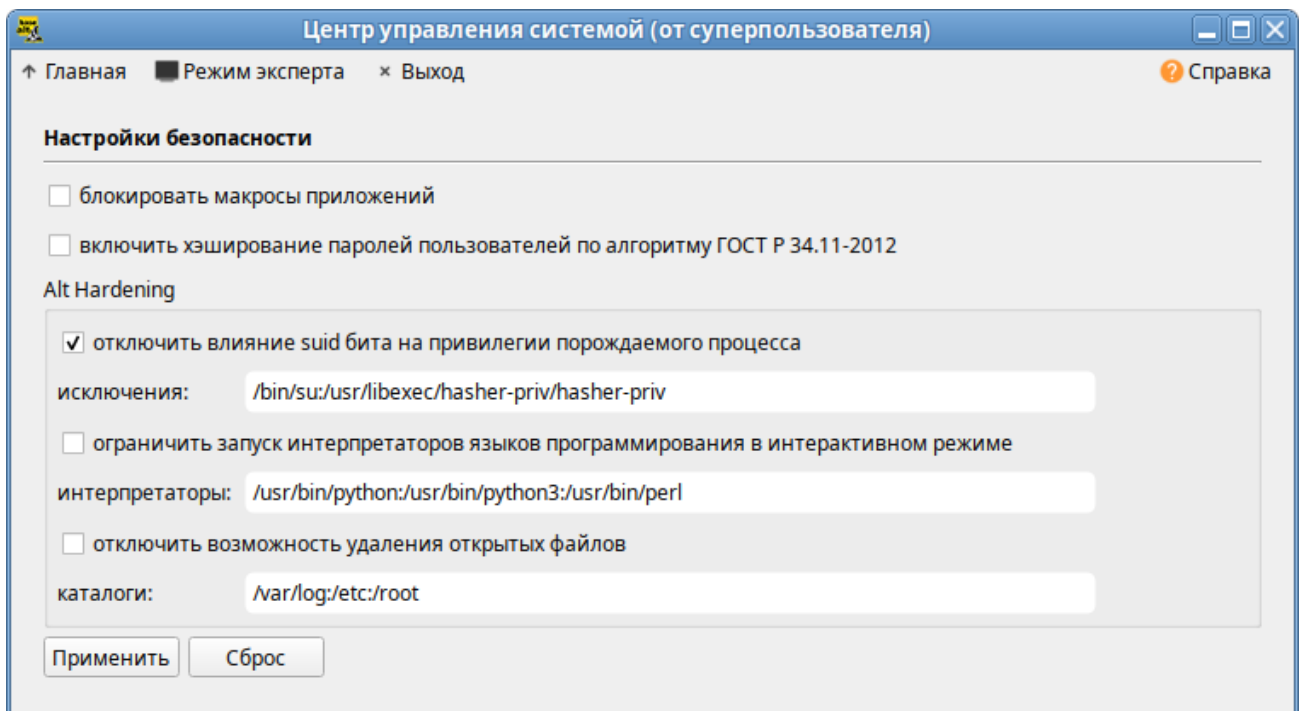


Рис. 175 – Отключение влияния бита SUID на привилегии порождаемого процесса

9.7.2. Блокировка интерпретаторов (запрет запуска скриптов)

При включении блокировки интерпретаторов блокируется несанкционированное использование интерпретатора для выполнения кода напрямую из командной строки.

Для включения режима блокировки интерпретаторов следует установить значение переменной `kernel.altha.rstrscript.enabled` равным 1:

```
# sysctl -w kernel.altha.rstrscript.enabled=1
```

Переменная `kernel.altha.rstrscript.interpreters` должна содержать разделенный двоеточиями список ограниченных интерпретаторов. Для изменения значения переменной `kernel.altha.rstrscript.interpreters` выполнить команду:

```
# sysctl -w kernel.altha.rstrscript.interpreters=
"/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh"
```

Примечание. В этой конфигурации все скрипты, начинающиеся с `#!/usr/bin/env python`, будут заблокированы.

Проверка состояния режима блокировки интерпретаторов выполняется командой:

```
# sysctl -n kernel.altha.rstrscript.enabled
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

Для получения списка заблокированных интерпретаторов выполнить команду:

```
# sysctl -n kernel.altha.rstrscript.interpreters
/usr/bin/python:/usr/bin/python3:/usr/bin/perl:/usr/bin/tclsh
```

Для включения режима блокировки интерпретаторов в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности» (рис. 175). В открывшемся окне следует отметить пункт «Ограничить запуск интерпретаторов языков программирования в интерактивном режиме» и нажать кнопку «Применить». Поле «Интерпретаторы» должно содержать разделенный запятыми список ограниченных интерпретаторов.

9.7.3. Отключение возможности удаления открытых файлов

Для отключения возможности удаления открытых файлов следует установить значение переменной `kernel.altha.oload.enabled` равным 1:

```
# sysctl -w kernel.altha.oload.enabled=1
```

Переменная `kernel.altha.oload.dirs` должна содержать разделенный двоеточиями список каталогов, например: `/var/lib/something:/tmp/something`. Для изменения значения переменной `kernel.altha.oload.dirs` следует выполнить команду:

```
# sysctl -w kernel.altha.oload.dirs="/var/lib/something:/tmp/something"
```

Проверка состояния режима выполняется командой:

```
# sysctl -n kernel.altha.oload.enabled  
1
```

Результат выполнения команды:

- 1 – режим включен;
- 0 – режим выключен.

При необходимости устанавливать эти переменные автоматически при каждой загрузке ОС, нужно добавить их в файл `/etc/sysctl.conf`. После редактирования `sysctl.conf` применить изменения, без перезагрузки ОС, можно выполнив команду:

```
# sysctl -p
```

Для отключения возможности удаления открытых файлов в ЦУС необходимо перейти в раздел «Система» → «Настройки безопасности» (рис. 175). В открывшемся окне следует отметить пункт «Отключить возможность удаления открытых файлов» и нажать кнопку «Применить».

10. FREEIPA

FreeIPA – это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag, состоит из веб-интерфейса и интерфейса командной строки.

FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux, FreeIPA-сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль за аккаунтами пользователей сохраняя сведения о пользователе, группах, узлах и других объектах, которые требуются для обеспечения сетевой безопасности.

10.1. Ввод рабочей станции в домен FreeIPA – установка клиента и подключение к серверу

Инструкция по вводу рабочей станции под управлением ОС Альт СП Рабочая станция в домен FreeIPA.

10.1.1. Установка FreeIPA клиента

Установить пакеты:

```
# apt-get install freeipa-client task-auth-freeipa libsss_sudo  
krb5-kinit bind-utils libbind zip
```

Примечание. Очистить конфигурацию freeipa-client невозможно. В случае если это нужно (например, для удаления, переустановки freeipa-client) следует переустановить систему.

10.1.2. Настройка сети. FreeIPA

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. При получении IP-адреса по DHCP данные о сервере DNS также должны быть получены от сервера DHCP. Ниже приведен пример настройки сетевого интерфейса со статическим IP-адресом.

В сетевых настройках нужно указать использовать сервер FreeIPA для разрешения имен. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли:

- 1) в ЦУС в разделе «Сеть» → «Ethernet-интерфейсы» задать имя компьютера, указать в поле DNS-серверы IP-адрес FreeIPA-сервера и в поле «Домены поиска» – домен для поиска (рис. 176);

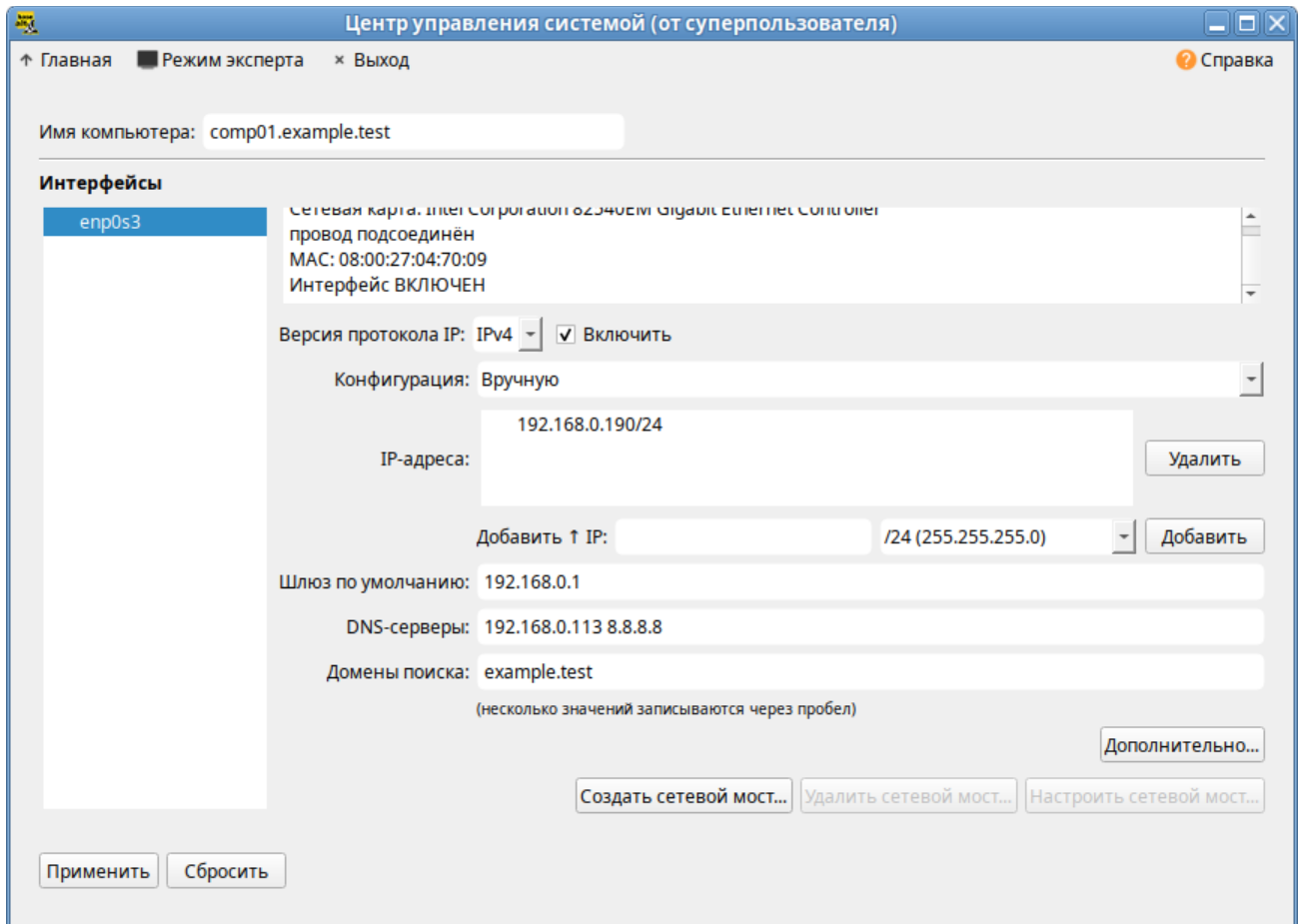


Рис. 176 – Настройка на использование DNS-сервера домена

- 2) в консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname comp01.example.test
```

- добавить DNS-сервер, для этого нужно создать файл /etc/net/ifaces/eth0/resolv.conf со следующим содержимым:

```
nameserver 192.168.0.113
```

где 192.168.0.113 – IP-адрес FreeIPA-сервера;

- указать службе resolvconf использовать DNS FreeIPA и домен для поиска. Для этого в файле `/etc/resolvconf.conf` добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* eth0'  
search_domains=example.test
```

где:

- а) `eth0` – интерфейс на котором доступен FreeIPA-сервер;
- б) `example.test` – домен;

- обновить DNS-адреса:

```
# resolvconf -u
```

Примечание. После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы нужно перезагрузить систему.

В результате выполненных действий в файле `/etc/resolv.conf` должны появиться строки:

```
search example.test  
nameserver 192.168.0.113
```

10.1.3. Подключение к серверу в ЦУС

Для ввода рабочей станции в домен FreeIPA, нужно в ЦУС перейти в раздел «Пользователи» → «Аутентификация» (пакет `alterator-auth`).

В открывшемся окне следует выбрать пункт «Домен FreeIPA», заполнить поля «Домен» и «Имя компьютера», затем нажать на кнопку «Применить» (рис. 177).

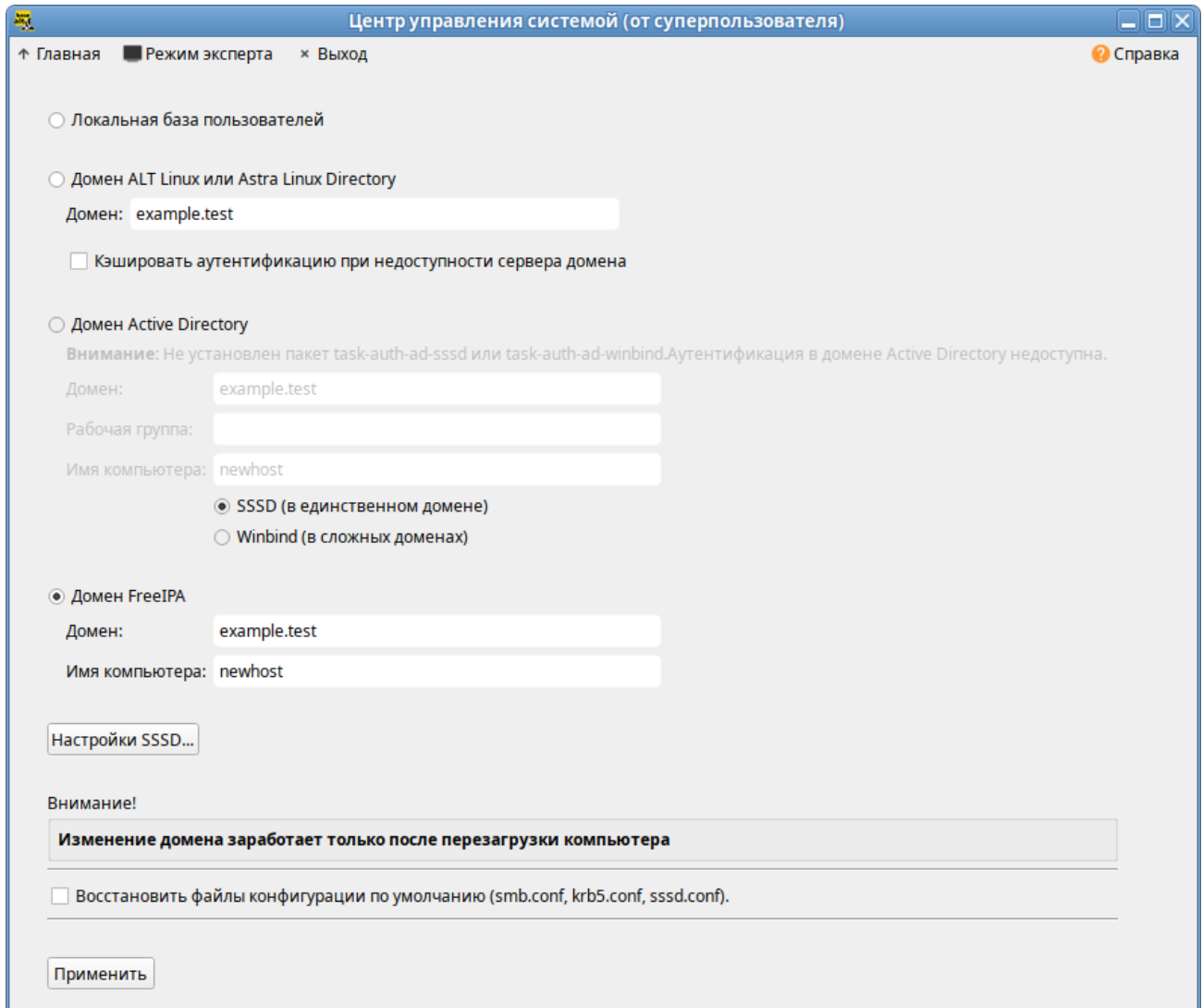


Рис. 177 – Ввод в домен в «Центре управления системой»

В открывшемся окне нужно ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать на кнопку «ОК» (рис. 178).

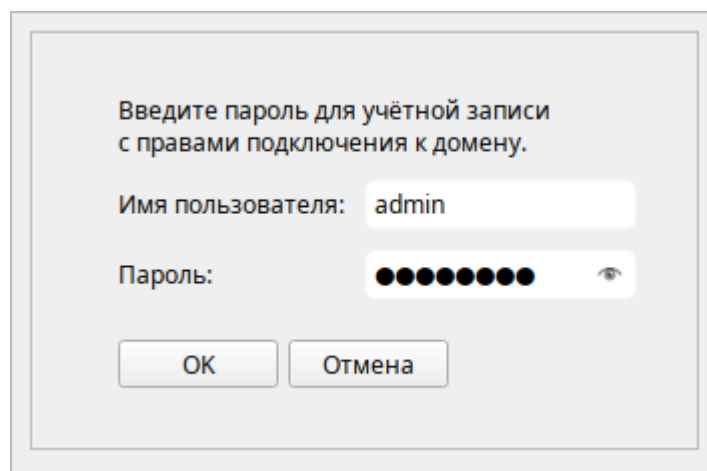


Рис. 178 – Параметры учетной записи с правами подключения к домену

В случае успешного подключения, будет выведено соответствующее сообщение (рис. 179).

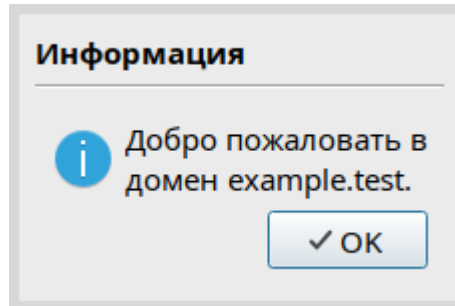


Рис. 179 – Успешное подключение к домену

Перезагрузить рабочую станцию.

10.1.4. Подключение к серверу в консоли

Запустить скрипт настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

или интерактивно:

```
# ipa-client-install
```

Если все настроено, верно, скрипт должен выдать такое сообщение:

```
'''Discovery was successful!'''
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test
Continue to configure the system with these values? [no]:
```

Нужно ответить `yes`, ввести имя пользователя, имеющего право вводить машины в домен, и его пароль.

ВНИМАНИЕ!

Если при входе в домен возникает такая ошибка:

```
Hostname (comp01.example.test) does not have A/AAAA record.
Failed to update DNS records.
```

Нужно проверить IP-адрес доменного DNS-сервера в файле `/etc/resolv.conf`.

В случае возникновения ошибки, нужно перед повторной установкой запустить процедуру удаления:

```
# ipa-client-install -U --uninstall
```

Для работы sudo-политик для доменных пользователей на клиентской машине нужно разрешить доступ к sudo:

```
# control sudo public
```

10.1.5. Вход пользователя

В окне входа в систему (рис. 180) необходимо ввести логин учетной записи пользователя FreeIPA и нажать кнопку «Войти», в открывшемся окне ввести пароль, соответствующий этой учетной записи и нажать кнопку «Войти».

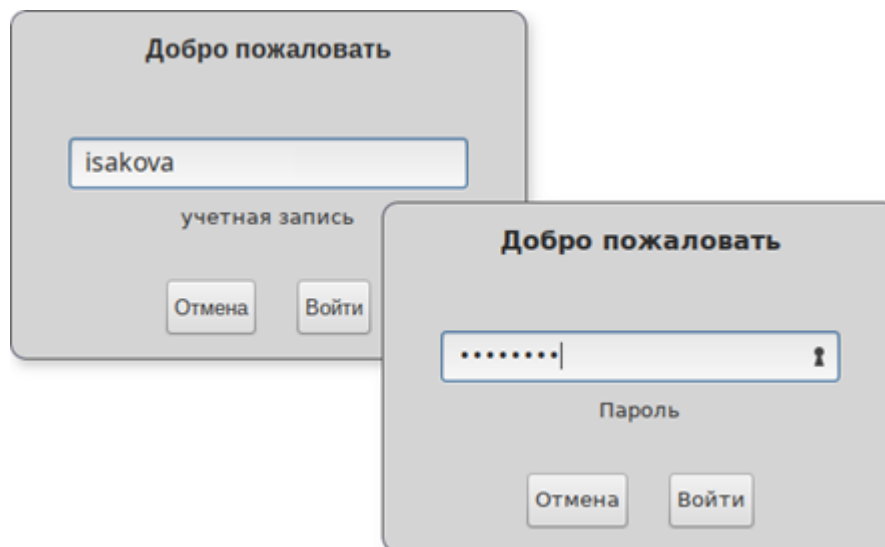


Рис. 180 – Вход пользователя

При первом входе пользователя будет запрошен текущий (установленный администратором) пароль и затем у пользователя запрашивается новый пароль (рис. 181) и его подтверждение.

Срок действия пароля истёк. Необходимо сейчас изменить ваш пароль.

Текущий пароль

Отмена Войти

Срок действия пароля истёк. Необходимо сейчас изменить ваш пароль.

Новый пароль

Отмена Войти

Рис. 181 – Запрос текущего пароля и нового пароля



Если машина до этого была в других доменах или есть проблемы со входом пользователей рекомендуется очистить кэш sssd:

```
# systemctl stop sssd
# rm -f /var/lib/sss/db/*
# rm -f /var/lib/sss/mc/*
# systemctl start sssd
```

10.1.6. Удаление клиента FreeIPA

При удалении, клиент удаляется из домена FreeIPA вместе с конфигурацией системных служб FreeIPA.

Для удаления клиента FreeIPA необходимо:

- на клиенте ввести команду:

```
# ipa-client-install --uninstall
...
Client uninstall complete.
The original nsswitch.conf configuration has been restored.
You may need to restart services or reboot the machine.
Do you want to reboot the machine? [no]: yes
The ipa-client-install command was successful
```

- на клиенте удалить, если они есть, старые принципалы Kerberos (кроме /etc/krb5.keytab):

```
# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.TEST
```

- на сервере FreeIPA удалить все записи DNS для клиентского узла:

```
# ipa dnsrecord-del
Имя записи: comp01
Имя зоны: example.test
Возможность удаления определенной записи не предусмотрена.
Удалить все? Yes/No (default No): yes
-----
Удалена запись "comp01"
-----
```

- на сервере FreeIPA удалить запись узла с сервера LDAP FreeIPA (при этом будут удалены все службы и отозваны все сертификаты, выданные для этого узла):

```
# ipa host-del comp01.example.test
-----
Удален узел "comp01.example.test"
-----
```

11. НАСТРОЙКА СЛУЖБ DNS (BIND)

11.1. Общие сведения

Службы DNS (Bind) в ОС Альт СП отвечают за преобразование доменного имени в IP-адрес и за обратную операцию.

Если локальная сеть не подключена к сети Интернет, вполне возможно, что внутренний DNS-сервер в ней не нужен. За преобразование доменного имени в IP-адрес и обратно в различные механизмы, лишь один из которых базируется на службе доменных имен. В самом простом случае имена всех компьютеров вместе с их адресами можно записать в файл `/etc/hosts`. Порядок просмотра различных пространств имен указывается в файле `/etc/nsswitch.conf`. Строка `hosts: files dns` этого файла предписывает приложениям, пользующимся стандартной функцией `gethostbyname()` сначала обратиться в `/etc/hosts`, а затем отправить запрос к DNS-серверу.

Если задачу преобразования имен в адреса взял на себя провайдер, собственный DNS-сервер также не требуется. В этом случае на всех компьютерах в качестве сервера имен указывается сервер провайдера (поле «nameserver» в файле `/etc/resolv.conf`), к которому и идут все запросы. Даже если внутренняя сеть организована согласно RFC1918 (т. н. интранет) и адреса компьютеров в ней недоступны из внешней сети, DNS-запросы во внешнюю сеть будут выполняться. Между собой компьютерам предлагается общаться с помощью `/etc/hosts` или IP-адресов.

Некоторые службы и системные утилиты, работающие с доменными именами, запускаются в ОС Альт СП с использованием `chroot` (в каталоге `/var/resolv`), поэтому после изменения упомянутых файлов рекомендуется выполнить команду:

```
update_chrooted conf
```

Собственную службу доменных имен рекомендуется настраивать для решения задач, описанных ниже.

11.2. Уменьшение времени ответа на DNS-запрос абонентов внутренней сети

Если канал подключения к сети Интернет обладает большим временем задержки, то работа с данными, включающими в себя много доменных имен (например, с `www`-страницами) может замедлиться. Общий объем трафика при этом не вырастет, поскольку система доменных имен – распределенная база данных, поддерживающая механизм кеширования запросов. Первое обращение к кеширующему DNS-серверу приводит к выполнению рекурсивного запроса: опрашивается сервер более высокого уровня, который, если не знает ответа, передаст запрос дальше. Результат запроса сохраняется в кэше, таким образом все последующие обращения именно к этой записи дальше кеширующего сервера не уйдут. Время жизни (Time To Live, TTL) записи в кэше определяется хозяином запрошенного доменного имени. По истечении TTL запись из кэша удаляется.

11.3. Именованние компьютеров в интранет-сети

Решение этой задачи может потребоваться, если среди компьютеров внутренней сети есть свои серверы (например, корпоративный `www`-сервер), к которым другие компьютеры обращаются по доменному имени.

Поскольку адреса такой сети не пойдут дальше межсетевого экрана, допускается использовать имя какого угодно – в том числе несуществующего – домена и сделать соответствующие записи `/etc/hosts`. Поддержание в актуальном состоянии файла `/etc/hosts` на всех компьютерах – нелегкая задача, и лучше все-таки воспользоваться DNS-сервером.

11.4. Примеры использования DNS-сервера Bind

Решение обеих поставленных задач предоставляется настройкой DNS-сервера Bind.

В ОС Альт СП сервер Bind запускается с использованием `chroot`. В `/etc` от Bind остается символьная ссылка на главный файл настроек `named.conf`. Корневым каталогом является `/var/lib/bind`, где у Bind есть собственный каталог `/etc` содержащий набор включаемых друг в друга конфигурационных файлов, каталоги `/var` и `/dev`.

Примечание. Все пути к файлам и каталогам в настройках Bind начинаются именно из этого каталога, и /zone соответствует /var/lib/bind/zone.

Чтобы запустить named в кеширующем режиме, достаточно раскомментировать и заполнить раздел настройки forwarders (вышестоящие серверы) в файле /var/lib/bind/etc/options.conf.

В связи с возможными ограничениями на право обращаться к серверу с обычными и рекурсивными запросами (настройки allow-query и allow-recursion), допускается раскомментировать установки по умолчанию. Эти настройки открывают доступ только абонентам локальных сетей, к которым компьютер подключен непосредственно:

```
# grep allow- /var/lib/bind/etc/options.conf
// allow-query { localnets; };
// allow-recursion { localnets; };
```

Использование Bind для полноценного именования компьютеров в локальной сети требует создания двух зон (прямой и обратной), содержащих в виде записей определенного формата информацию о доменных именах компьютеров и об их роли в этих доменах.

Каждая зона должна включать запись типа SOA (StateOfAuthority, сведения об ответственности). В этой записи определяются основные временные и административные параметры домена, в том числе электронный адрес лица, ответственного за домен (администратора) и серийный номер зоны.

Серийный номер – число в диапазоне от 0 до 4294967295 (232); каждое изменение, вносимое в зону, должно сопровождаться увеличением этого номера. Обнаружив увеличение серийного номера, кеширующие и вторичные серверы признают все закешированные записи из этой зоны устаревшими. Удобно использовать формат «годмесяцчисловерсия», где все числа, кроме года, двузначные, а версия может обнуляться раз в день, соответствовать времени (например, по формуле $100 * (\text{часы} * 60 + \text{минуты}) / (60 * 24)$) или иметь сквозную нумерацию (в этом случае появляется сложность с переходом от версии 99 к версии 100, то есть 0).

Даже если серийный номер генерируется автоматически, рекомендуется пользоваться этим форматом, наглядно отражающим время создания зоны.

Пример зоны, не содержащей ничего, кроме записи SOA и обязательной записи типа NS (NameServer), находится в файле `/var/lib/bind/zone/empty`.

Кроме записи типа SOA, в каждой зоне должна быть хотя бы одна запись типа NS, указывающая адрес DNS-сервера, авторитативного в этом домене (как минимум – адрес сервера, на котором запущен `named`).

Несколько зон включаются в настройку Bind автоматически (файл `/var/lib/bind/etc/rfc1912.conf`). Они нужны для обслуживания сети, привязанной к сетевой заглушке (127.0.0.1/8). Имя домена, который обслуживается зоной, задается в файле настроек, а в самом файле зоны можно использовать относительную адресацию (без «.» в конце имени), благодаря чему операция переименования домена выполняется редактированием одной строки.

В ОС Альт СП рекомендуется добавлять описания зон в конфигурационный файл `/var/lib/bind/etc/local.conf`.

Прямая зона нужна для преобразования доменного имени в IP-адрес – операции, нужной многим программам постоянно. Большинство записей в прямой зоне – типа A (Address) – предназначены именно для этого. Другие часто встречающиеся типы записей – это CNAME (CanonicalName, настоящее имя), позволяющий привязать несколько дополнительных имен к одному, и MX (MailExchange, обмен почтой), указывающий, куда пересылать почтовые сообщения, в поле адресат которых встречается определенное доменное имя.

Пример прямой зоны для домена `internal.domain.net` (незначащие поля соответствующих файлов заменены на «. . .»):

```
# cat /var/lib/bind/etc/local.conf

. . .
zone "internal.domain.net" {
type master;
file "internal.domain.net";
};

. . .
# cat /var/lib/bind/zone/internal.domain.net
$TTL 1D
@ IN SOA server root.server (
    2013082202 ; serial
```

```
12H ; refresh
1H ; retry
1W ; expire
1H ; ncache
)
    IN NS server
    MX 10 server
server A 10.10.10.1
www CNAME server
mail CNAME server
jack A 10.10.10.100
jill A 10.10.10.101
```

В этом примере используются правила по умолчанию: если в записи некоторое поле опущено, оно наследуется от предыдущей. Так, вместо А допускается написать INA, а вместо MX – @ IN MX, где @ означает имя домена, указанное в конфигурационном файле.

Как видно из примера, всю работу в сети делает компьютер с адресом 10.10.10.1, он же `server.internal.domain.net`, он же `www.internal.domain.net` и `mail.internal.domain.net`. Несмотря на наличие среди CNAME этого сервера имени «mail», MX-запись указывает на действительный адрес – так рекомендовано RFC (Request for Comments, документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, широко применяемые во всемирной сети).

Для того чтобы преобразовывать IP-адреса в доменные имена, у каждой сети должна быть обратная зона. Если такой зоны нет, и в файле `/etc/hosts` тоже ничего не написано, операция не выполнится. Такое преобразование нужно гораздо реже и в основном по соображениям административным: для того, чтобы выяснить принадлежность компьютера (с которого, допустим, пытаются атаковать сервер) по его IP-адресу. Некоторые почтовые серверы проверяют, содержится ли IP-адрес машины, передающей сообщение, в обратной зоне и похоже ли полученное доменное имя на то, что указано в сообщении, и при несовпадении отказываются принимать письмо.

Обратная зона состоит почти целиком из записей типа PTR (Pointer, указатель). Чтобы не умножать сущностей, решено было не вводить новый способ работы сервера имен и представить обратное преобразование IP-адреса как прямое преобразование доменного имени специального вида.

Например, чтобы выяснить доменное имя компьютера с адресом «1.2.3.4», нужно запросить информацию о доменном имени 4.3.2.1.in-addr.arpa. Таким образом, каждой подсети класса C (или выше) соответствует определенный домен, в котором можно найти ответ.

Обратная зона для домена, приведенного выше:

```
# cat /var/lib/bind/etc/local.conf

. . .
zone "12.11.10.in-addr.arpa" {
type master;
file "12.11.10.in-addr.arpa";
};
. . .
# cat /var/lib/bind/zone/12.11.10.in-addr.arpa
$TTL 1D
@ IN SOA server.internal.domain.net. root.server.internal.domain.net (
    2013082201 ; serial
    12H ; refresh
    1H ; retry
    1W ; expire
    1H ; ncache
)
    IN NS server.internal.domain.net.
0 PTR internal.domain.net.
1 PTR server.internal.domain.net.
100 PTR jack.internal.domain.net.
101 PTR jill.internal.domain.net.
```

Относительные адреса, использованные в левой части записей PTR, раскрываются в полные следующего вида: адрес.12.11.10.in-addr.arpa, а в правой части используются полные, которые могут указывать на имена в разных доменах.

Проверить синтаксическую правильность конфигурационного файла и файла зоны можно с помощью утилит named-checkconf и named-checkzone, входящих в пакет bind. Они же используются при запуске службы командой service bind start.

Стоит иметь в виду, что, в отличие от прямых зон, обратные описывают административную принадлежность компьютеров, но сами принадлежат хозяину сети (как правило, провайдеру).

Существует особого рода затруднение, связанное с работой DNS-сервера уже не во внутренней сети, а в сети Интернет. Связано это с тем, что подсети класса C (сети /24, в которых сетевая маска занимает 24 бита, а адрес компьютера – 8) выдаются только организациям, способным такую подсеть освоить (в сети класса C 254 абонентских IP-адреса, один адрес сети и один широковещательный адрес). Чаще всего выдаются совсем маленькие подсети – от /30 (на два абонентских адреса) до /27 (на 30 адресов) – или другие диапазоны, сетевая маска которых не выровнена по границе байта. Таких подсетей в обратной зоне получится несколько, а возможности просто разделить ее, отдав часть адресов в администрирование хостам, нет. Провайдер в таких случаях пользуется RFC2317, предписывающем в обратной зоне заводить не записи вида PTR, а ссылки CNAME на адреса в «классифицированных» обратных зонах специального вида. Обратное преобразование становится двухступенчатым, зато администрирование каждой классифицированной зоны можно отдать хосту.

DNS-сервер, отвечающий на запросы из глобальной сети, должен быть зарегистрирован в родительском домене. Правила требуют, чтобы при регистрации домена было указано не менее двух DNS-серверов, которые будут его обслуживать.

Из всех зарегистрированных серверов (записей типа NS в родительской зоне) только одна соответствует первичному (master) серверу, а остальные – вторичным (slave). Для внешнего пользователя вторичный сервер не отличается от первичного, отличия состоят только в способе администрирования: все изменения вносятся в зоны первичного сервера, а вторичный только кеширует эти зоны, целиком получая их по специальному межсерверному протоколу. Полученная зона складывается в файл, редактировать который бессмысленно: первичный сервер при изменении зоны рассылает всем своим вторичным указание скачать ее заново. Право на скачивание зоны можно ограничить настройкой allow-transfer (как правило, в ней перечисляются адреса вторичных серверов).

Пример задания вторичного сервера в файле настроек:

```
// We are a slave server for eng.example.com
zone "eng.example.com" {
type slave;
file "slave/eng.example.com";
// IP address of eng.example.com master server
masters { 192.168.4.12; };
};
```

Вторичный сервер рекомендуется размещать в сети, отличной от той, в которой помещается первичный, – так повышается надежность обработки запроса (если один сервер недоступен, возможно, ответит второй) и возрастает скорость распространения записей по кэшам промежуточных серверов.

Проверку работоспособности, доступности и вообще самочувствия DNS-сервера рекомендуется выполнять утилитой `dig` из пакета `bind-utils`, которая выдает максимум информации о том, что происходило с запросом (для информации об обратном преобразовании нужно добавить ключ `-x`):

```
dig basealt.ru
; <<>> DiG 9.10.4-P5 <<>> basealt.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32751
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;basealt.ru. IN A
;; ANSWER SECTION:
basealt.ru. 86400 IN A 194.107.17.41
;; Query time: 1177 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Mar 01 10:07:17 MSK 2025
;; MSG SIZE rcvd: 55
```

Можно также использовать утилиту `host` из того же пакета, например:

```
host basealt.ru
basealt.ru has address 194.107.17.41
```

Для выяснения административной принадлежности тех или иных доменов и сетей можно воспользоваться утилитой `whois` из одноименного пакета, которая обращается к специальной сетевой базе данных (не имеющей отношения к DNS).

12. СИСТЕМА МОНИТОРИНГА ZABBIX

Zabbix – система мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования.

Для управления системой мониторинга и чтения данных используется веб-интерфейс.

12.1. Установка сервера PostgreSQL

Перед установкой Zabbix должен быть установлен и запущен сервер PostgreSQL, с созданным пользователем zabbix и созданной базой zabbix.

Установить PostgreSQL, Zabbix-сервер и дополнительную утилиту fping:

```
# apt-get install postgresql16-server zabbix-server-pgsql
```

Подготовить к запуску и настроить службы PostgreSQL, для этого нужно выполнить следующие действия:

- создать системные базы данных (пароль пользователя PostgreSQL необходимо запомнить):

```
# /etc/init.d/postgresql initdb
```

Введите новый пароль суперпользователя:

Повторите его:

Это пункт нужно пропустить, если системные базы уже инициировались.

- включить по умолчанию и запустить службу:

```
# systemctl enable --now postgresql
```

- создать пользователя zabbix и базу данных zabbix (при запросе «Пароль» следует ввести пароль пользователя postgresql, созданный при создании системных баз данных):

```
# su - postgres -s /bin/sh -c 'createuser --no-superuser --no-createdb --no-createrole --encrypted --pwprompt zabbix'
```

Введите пароль для новой роли:

Повторите его:

Пароль:

```
# su - postgres -s /bin/sh -c 'createdb -O zabbix zabbix'
```

Пароль:

```
# systemctl restart postgresql
```

- добавить в базу данные для веб-интерфейса (последовательность команд важна):

```
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/schema.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/images.sql zabbix'
# su - postgres -s /bin/sh -c 'psql -U zabbix -f
/usr/share/doc/zabbix-common-database-pgsql-*/data.sql zabbix'
```

12.2. Установка Apache2

Установить пакеты:

```
# apt-get install apache2 apache2-mod_php8.3
```

Добавить в автозапуск и запустить apache2:

```
# systemctl enable --now httpd2
```

12.3. Установка PHP

Установить пакеты:

```
# apt-get install php8.3 php8.3-mbstring php8.3-sockets php8.3-gd
php8.3-xmlreader php8.3-pgsql php8.3-ldap php8.3-openssl
```

В файле `/etc/php/8.3/apache2-mod_php/php.ini` изменить некоторые опции `php`:

```
memory_limit = 256M
post_max_size = 32M
max_execution_time = 600
max_input_time = 600
date.timezone = Europe/Moscow
always_populate_raw_post_data = -1
```

Примечание. Актуальная версия PHP может быть другой.

Перезапустить apache2:

```
# systemctl restart httpd2
```

12.4. Настройка и запуск Zabbix-сервера

Внести изменения в конфигурационный файл

`/etc/zabbix/zabbix_server.conf`:

```
DBHost=localhost
DBName=zabbix
DBUser=zabbix
DBPassword=Пароль от базы
```

Добавить Zabbix-сервер в автозапуск и запустить его:

```
# systemctl enable --now zabbix_pgsql
```

12.5. Установка веб-интерфейса Zabbix

Установить метапакеты:

```
# apt-get install zabbix-phpfrontend-apache2-mod_php8.3 zabbix-  
phpfrontend-engine
```

Включить аддоны в apache2:

```
# ln -s /etc/httpd2/conf/addon.d/A.zabbix.conf /etc/httpd2/conf/extra-  
enabled/
```

Перезапустить apache2:

```
# systemctl restart httpd2
```

Изменить права доступа к конфигурационному каталогу веб-интерфейса, чтобы веб-установщик мог записать конфигурационный файл:

```
# chown apache2:apache2 /var/www/webapps/zabbix/ui/conf
```

В веб-браузере перейти на страницу установки Zabbix-сервера:

```
http://<IP-сервера>/zabbix
```

При первом заходе на страницу запустится мастер, который шаг за шагом проверит возможности веб-сервера, интерпретатора PHP и сконфигурирует подключение к базе данных.

Для начала установки нужно выбрать язык установки и нажать на кнопку «Далее» (рис. 182), что осуществит переход на страницу проверки предварительных условий (рис. 183).

Нужно доустановить то, что требуется и перейти на следующую страницу.

На следующей странице (рис. 184) следует ввести параметры подключения к базе данных (параметры подключения нужно указывать такие же, как у Zabbix-сервера). По умолчанию в качестве «Схемы базы данных» («Database schema») нужно указать «public».

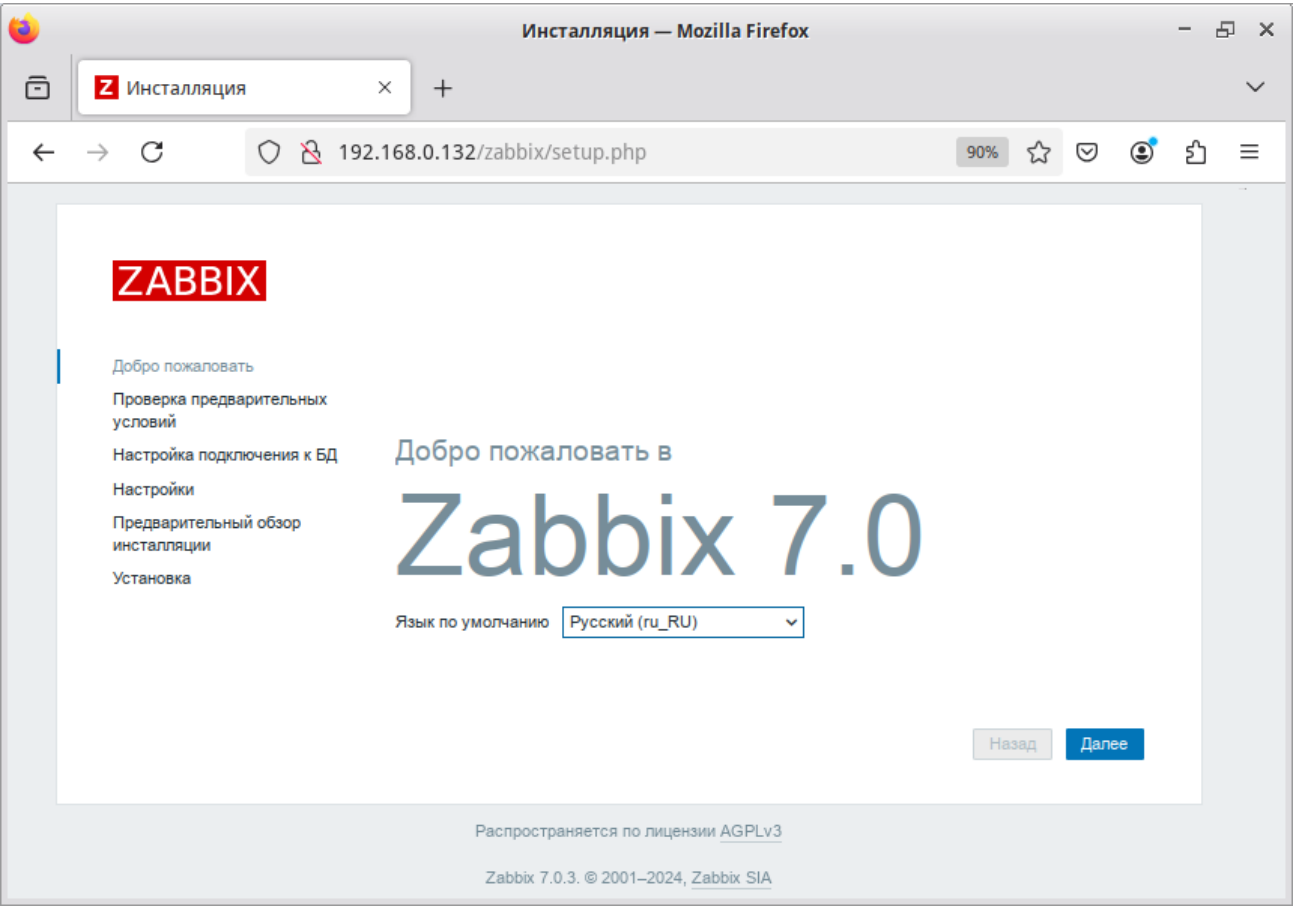


Рис. 182 – Страница установки Zabbix сервера

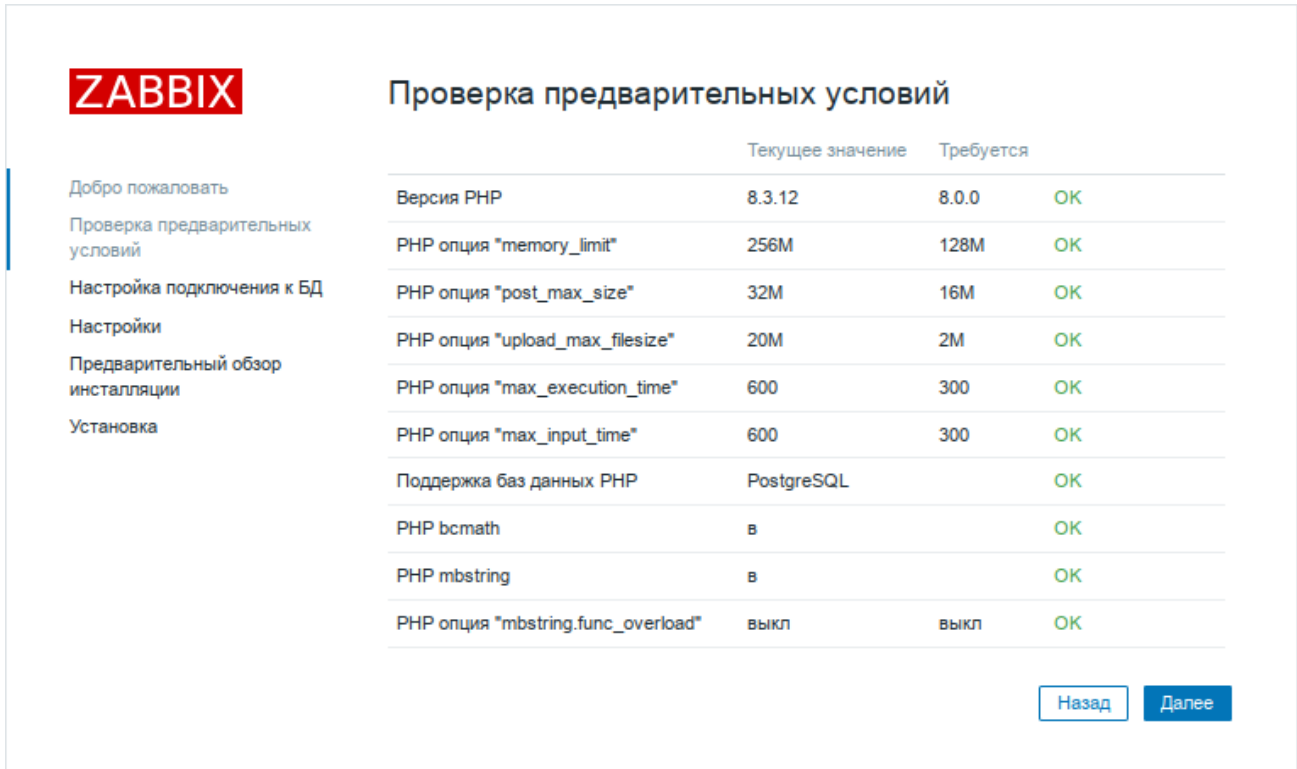


Рис. 183 – Страница проверки предварительных условий

The screenshot shows the 'Настройка подключения к БД' (Database Connection Configuration) screen in the Zabbix installer. On the left is a sidebar with navigation links: 'Добро пожаловать', 'Проверка предварительных условий', 'Настройка подключения к БД' (highlighted), 'Настройки', 'Предварительный обзор установки', and 'Установка'. The main area has a title 'Настройка подключения к БД' and a subtitle: 'Пожалуйста, создайте базу данных вручную и укажите параметры конфигурации для соединения с этой базой. Нажмите кнопку "Далее" при завершении.' Below this are several configuration fields: 'Тип базы данных' (PostgreSQL), 'Хост базы данных' (localhost), 'Порт базы данных' (0, with a note '0 - использовать порт по умолчанию'), 'Имя базы данных' (zabbix), 'Схема базы данных' (public), 'Хранение учётных данных в' (Simple text, with options for HashiCorp Vault and CyberArk), 'Пользователь' (zabbix), 'Пароль' (masked with dots), and a checkbox for 'TLS шифрование базы данных'. At the bottom right are 'Назад' and 'Далее' buttons.

Рис. 184 – Параметры подключения к базе данных

Примечание. Если выбрана опция «TLS шифрование базы данных», то в форме появятся дополнительные поля для настройки TLS-соединения с базой данных.

На следующих страницах необходимо выбрать настройки веб-интерфейса и задать имя сервера (рис. 185), и завершить установку.

The screenshot shows the 'Настройки' (Settings) screen in the Zabbix installer. The sidebar on the left is the same as in the previous screenshot, with 'Настройки' (highlighted) and 'Установка' at the bottom. The main area has a title 'Настройки' and three configuration fields: 'Имя сервера Zabbix' (zabbix_server), 'Часовой пояс по умолчанию' (Системный: (UTC+03:00) Europe/Moscow), and 'Тема по умолчанию' (Голубая). At the bottom right are 'Назад' and 'Далее' buttons.

Рис. 185 – Настройки сервера Zabbix

После окончания установки на экране будет отображаться форма входа в веб-интерфейс управления системой мониторинга (рис. 186). Параметры доступа по умолчанию:

Логин: Admin

Пароль: zabbix

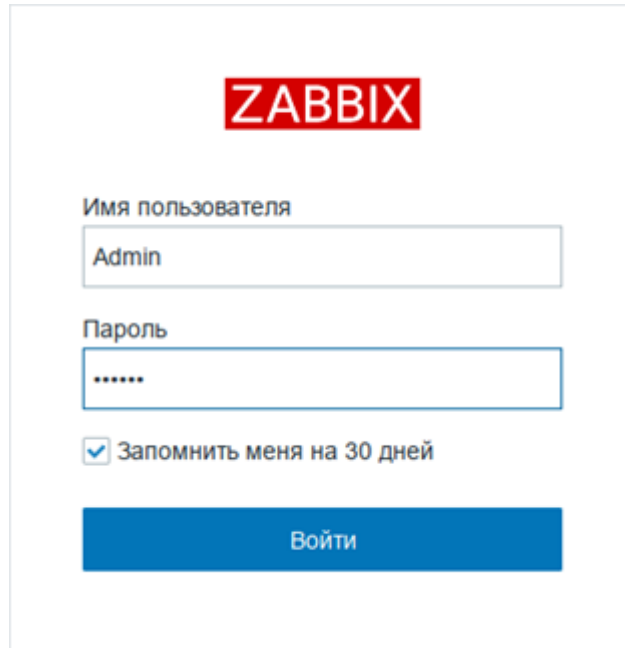


Рис. 186 – Форма входа в веб-интерфейс управления системой мониторинга

Войдя в систему, нужно сменить пароль администратора, завести других пользователей и затем можно переходить к настройкам Zabbix.

Примечание. В профиле пользователя можно настроить некоторые функции веб-интерфейса Zabbix, такие как язык интерфейса, цветовая тема, количество отображаемых строк в списках и т. п. Сделанные в профиле изменения будут применены только к пользователю, в профиле которого были сделаны эти изменения.

Чтобы собирать информацию с узлов, Zabbix-сервер использует информацию, получаемую от агентов. Чтобы добавить новый узел, следует установить на узел, который нужно мониторить, Zabbix-агент (п. 12.6) и добавить новый хост на Zabbix-сервере (п. 12.7, п. 12.8).

12.6. Установка Zabbix-агента (клиента)

Для установки Zabbix-агента нужно выполнить команду:

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

Если Zabbix-агент устанавливается не на сам сервер мониторинга, то в файле конфигурации агента `/etc/zabbix/zabbix_agentd.conf` нужно задать параметры сервера:

```
Server=<IP-сервера>
ServerActive=<IP-сервера>
Hostname=HostK.example.test
```

где `HostK.example.test` – имя узла мониторинга, которое будет указано на Zabbix-сервере.

Примечание. Если параметр `Hostname` будет пустой или закомментирован, то узел добавится под системным именем.

Добавить Zabbix-агент в автозапуск и запустить его:

```
# systemctl enable --now zabbix_agentd.service
```

12.7. Добавление нового хоста на Zabbix-сервере

Каждый хост нужно зарегистрировать на Zabbix-сервере, сделать это можно, используя веб-интерфейс.

Информация о настроенных узлах сети в Zabbix доступна в разделе меню «Сбор данных» → «Узлы сети». Для добавления нового узла сети следует нажать кнопку «Создать узел сети» (рис. 187).

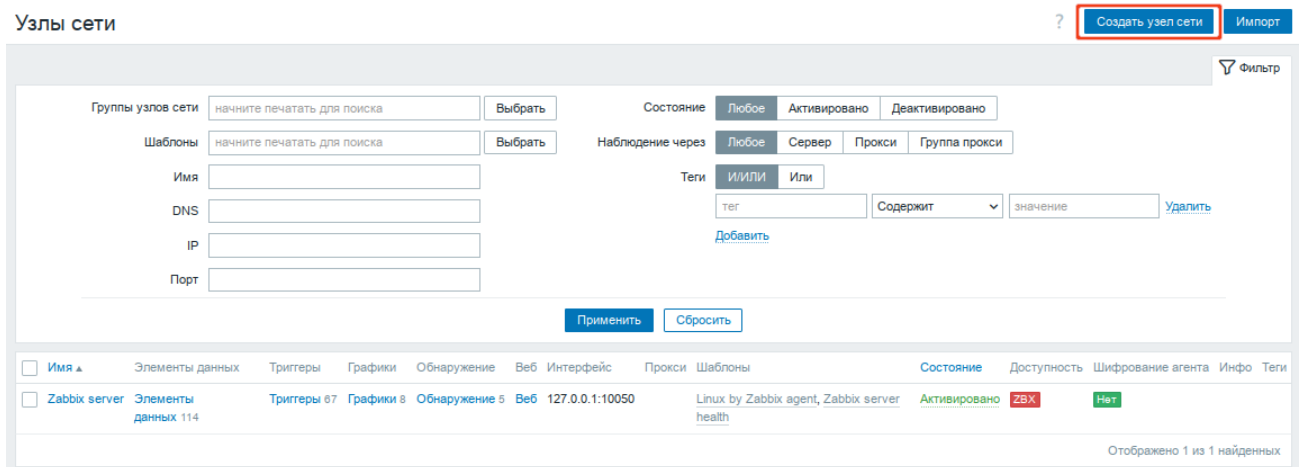


Рис. 187

В открывшемся окне нужно заполнить поля «Имя узла сети» и «IP адрес» согласно данным добавляемого хоста. Затем следует выбрать шаблон «Linux by Zabbix agent», добавить хост в определенную группу (выбрав одну из них из списка, либо создав новую группу) и нажать кнопку «Добавить» (рис. 188).

Примечание. В поле «Имя узла сети» ставится значение, которое указано в настройках агента (/etc/zabbix/zabbix_agentd.conf) в поле Hostname.

Примечание. Все права доступа назначаются на группы узлов сети, а не индивидуально узлам сети. Поэтому узел сети должен принадлежать хотя бы одной группе.

Новый узел сети

Узел сети IPMI Теги Макросы Инвентаризация Шифрование Преобразование значений

* Имя узла сети HostK.example.test

Видимое имя HostK

Шаблоны Linux by Zabbix agent × Выбрать
начните печатать для поиска

* Группы узлов сети Discovered hosts × Выбрать
начните печатать для поиска

Интерфейсы	Тип	IP адрес	DNS имя	Подключаться через	Порт	По умолчанию
Агент		192.168.0.113		IP DNS	10050	☒ Удалить

Добавить

Описание

Наблюдение через Сервер Прокси Группа прокси

Активировано ☒

Добавить Отмена

Рис. 188 – Создание нового узла сети

Получение первых данных может занять до 60 секунд. Для того чтобы просмотреть собранные данные нужно перейти в раздел «Мониторинг» → «Последние данные», выбрать в фильтре нужный узел сети и нажать кнопку «Применить» (рис. 189).

Последние данные

Группы узлов сети:

Узлы сети:

Имя:

Теги: Или Содержит

Отображать теги: 1 3

Приоритет отображения тегов:

Состояние:

Подробная информация: ☐

Подфильтр влияет только на отфильтрованные данные

УЗЛЫ СЕТИ

HostK 77

ТЕГИ

component 77 disk 16 filesystem 7 fstype 7 interface 9

ЗНАЧЕНИЯ ТЕГОВ

component: application 1 cpu 17 environment 1 memory 7 network 9 os 3 raw 4 security 1 storage 26 system 12

disk: ram 8 sda 8

filesystem: / 7

fstype: ext4 7

interface: enp0s3 9

СОСТОЯНИЕ

Не поддерживается 11 Нормальный 66

ДАННЫЕ

☐	Узел сети	Имя	Последняя проверка	Последнее значение	Изменение	Теги	Инфо
☐	HostK	Available memory	24с	784.89 MB		component: memory	График
☐	HostK	Available memory in %	23с	40.2246 %		component: memory	График
☐	HostK	Checksum of /etc/passwd	25с	822fb73a4ea82d...		component: security	История
☐	HostK	Context switches per second	8с	226.912		component: cpu	График

Рис. 189 – Собранные данные

12.8. Авторегистрация узлов

В Zabbix существует механизм, который позволяет Zabbix-серверу начинать мониторинг нового оборудования автоматически, если на этом оборудовании имеется установленный Zabbix-агент. Такой подход позволяет добавлять новые узлы сети на мониторинг без какой-либо настройки Zabbix-сервера вручную по каждому отдельному узлу сети.

Для настройки авторегистрации необходимо перейти в раздел «Оповещения» → «Действия» → «Действия авторегистрации» и нажать на кнопку «Создать действие» (рис. 190).

На открывшейся странице на вкладке «Действия» заполнить поле «Имя». В поле «Условия» следует задать правила, по которым будут идентифицироваться регистрируемые хосты (рис. 191).

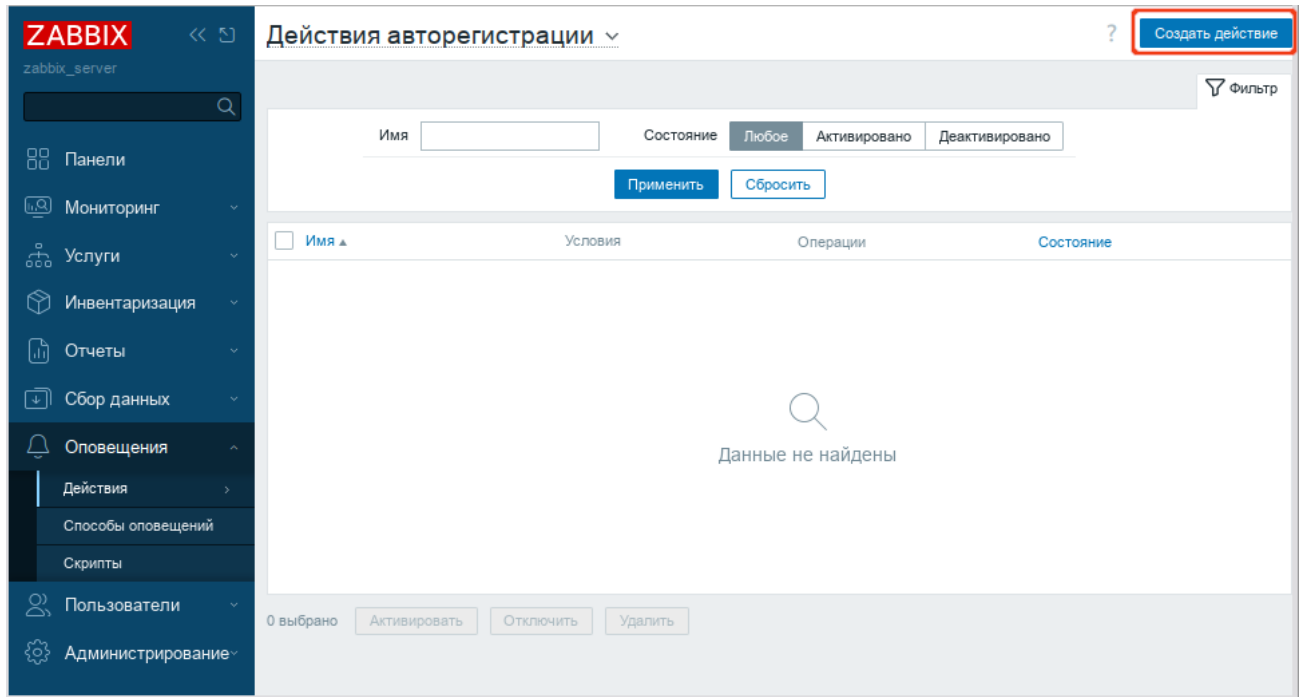


Рис. 190 – Авторегистрация узлов

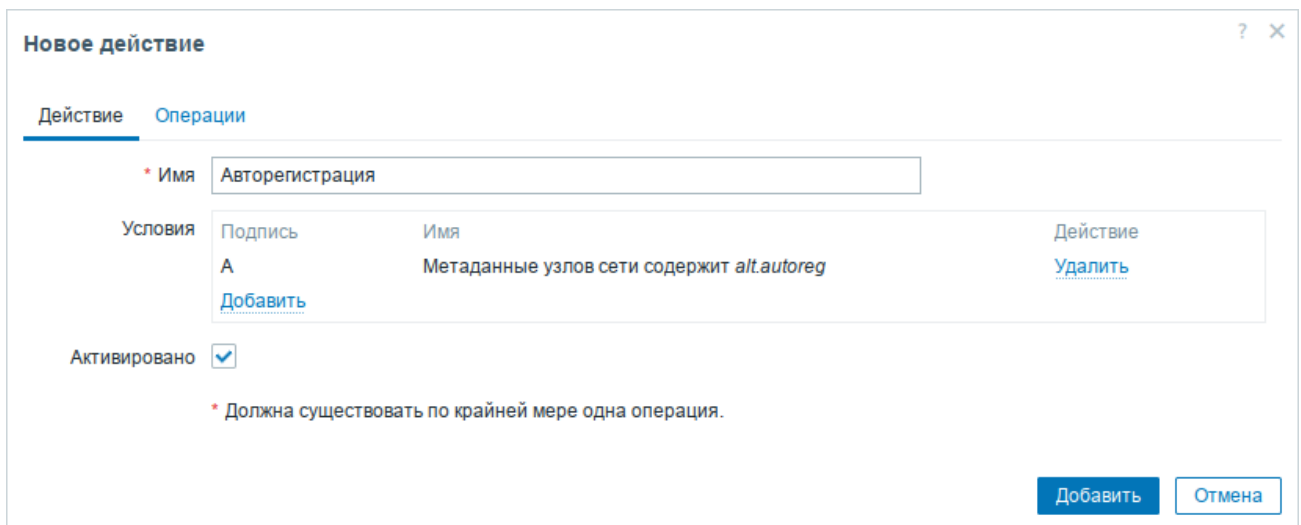


Рис. 191 – Условия идентификации узла

На вкладке «Операции» в поле «Операции» следует добавить правила, которые нужно применить при регистрации хоста. Например, для добавления узла, добавления его к группе «Discovered hosts» с присоединением к шаблону «Linux generic by Zabbix agent» (рис. 192).

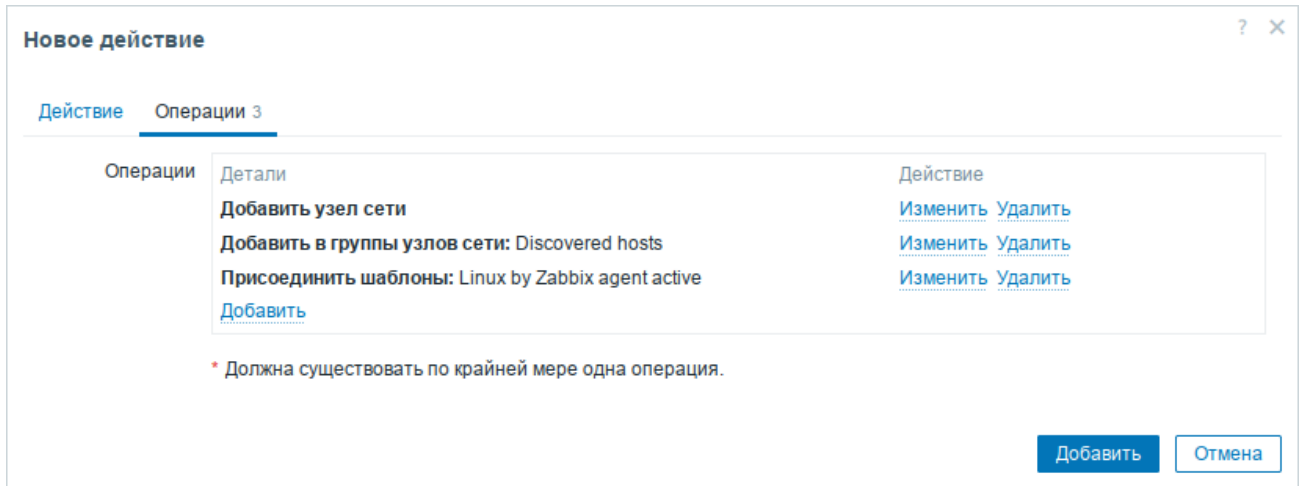


Рис. 192 – Правила, применяемые при регистрации узла

В конфигурационном файле агента `/etc/zabbix/zabbix_agentd.conf` следует указать следующие значения:

- в параметре `Hostname` – уникальное имя;
- в параметре `ServerActive` – IP-адрес сервера;
- в параметре `HostMetadata` – значение, которое было указано в настройках сервера (`HostMetadata=alt.autoreg`).

Перезапустить агент:

```
# systemctl restart zabbix_agentd.service
```

13. POSTGRESQL

СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. При этом единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов. Кроме таблиц, существуют другие объекты БД (виды, процедуры), которые предоставляют доступ к данным, хранящимся в таблицах.

Для работы СУБД на НЖМД выделяется область для хранения БД, называемая «кластером БД». Кластер БД является набором БД, управляемых одним экземпляром сервера СУБД. Настройка работы отдельного экземпляра сервера СУБД так же определяется в рамках кластера соответствующими конфигурационными файлами.

13.1. Состав

СУБД PostgreSQL состоит из нескольких компонентов:

- postgresql – сервисная служба, реализующая непосредственно сервер БД;
- libpq – клиентская библиотека, предоставляющая доступ к серверу СУБД;
- набор серверных утилит для управления работой сервера и создания кластеров БД;
- набор клиентских утилит для создания и управления БД.

13.2. Настройка

Настройка сервера СУБД осуществляется установкой параметров в конфигурационном файле `postgresql.conf`. В дополнение к файлу `postgresql.conf` в PostgreSQL используется еще два конфигурационных файла, которые контролируют аутентификацию клиента.

По умолчанию все эти три файла находятся в каталоге данных кластера БД или в соответствующем кластеру конфигурационном каталоге, например, `/etc/postgresql/x.x/main`.

За расположение указанных файлов отвечают конфигурационные параметры, описанные ниже:

- `data_directory` – определяет каталог для хранения данных;
- `config_file` – определяет основной конфигурационный файл сервера (`postgresql.conf`), значение этого параметра может быть задано только в командной строке `postgres`;
- `hba_file` – определяет конфигурационный файл для аутентификации по узлам (`pg_hba.conf`);
- `ident_file` – определяет конфигурационный файл для аутентификации по методу `ident` (`pg_ident.conf`);
- `external_pid_file` – определяет имя дополнительного файла с идентификатором процесса, который сервер создает для использования программами администрирования сервера.

13.3. Использование postgresql

13.3.1. Конфигурирование сервера

Установить пакет `postgresql-deploy-cert` (если при установке ОС Альт СП релиз 10 Сервер не была отмечена группа пакетов «Сервер Postgresql»):

```
# apt-get install postgresql-deploy-cert
```

Разворачивание системы управления базами данных (СУБД) `postgresql` выполняется командой:

```
# deploy postgresql-cert
```

ввести и записать пароль для `postgres`.

Расскомментировать строку `default_realm` в `/etc/krb5.conf` и изменить значение на `POSTGRESQL`:

```
default_realm = POSTGRESQL
```

Выполнить создание базы данных (БД) ключей для `realm POSTGRESQL`. Во время выполнения команды будет запрошен пароль от `master key`, необходимо указать пароль, который был указан при разворачивании `postgresql` через команду `deploy`:

```
# kdb5_util create -s -r POSTGRESQL
```

13.3.2. Конфигурирование ролей

13.3.2.1. Конфигурирование администратора СУБД

Отредактировать файл `/etc/hosts` и привести его к виду:

```
localhost 127.0.0.1
```

Выполнить создание принцепала `pgadmin` и `postgres`:

```
# kadmin.local ank pgadmin/admin
# kadmin.local ank postgres/admin
```

Выполнить перезапуск сервиса `postgresql` и запуск сервиса `krb5kdc.service`:

```
# systemctl restart postgresql
# systemctl start krb5kdc.service
```

Выполнить создание пользователя СУБД `pgadmin`:

```
# createuser -U postgres --superuser pgadmin
```

ввести пароль, который был задан при создании базы при помощи `deploy` (см. п. 13.3.1).

Выполнить перезапуск сервиса `postgresql`:

```
# systemctl restart postgresql
```

Создать парольную политику для `kerberos`:

```
# kadmin.local add_policy -minlength 8 -minclasses 4 -maxfailure 4 \
-failurecountinterval 180 -lockoutduration 3600 lockout_policy
```

Где:

- `--minlength` – минимальная длина пароля. В примере – 8 символов;
- `--minclasses` – минимальное количество классов символов, разрешенных в пароле. В примере пароль должен содержать символы не менее четырех различных классов (например, строчные буквы, заглавные буквы, цифры, специальные символы);
- `--maxfailure` – максимальное количество неудачных попыток ввода пароля перед блокировкой учетной записи. В данном случае – 4;
- `--failurecountinterval` – интервал времени в секундах, в течение которого учитываются неудачные попытки ввода пароля. Если неудачная попытка аутентификации происходит после того, как с момента предыдущей неудачи прошло `failuretime`, количество неудачных попыток аутентификации

сбрасывается до 1. Интервал подсчета неудач, равный 0, означает «всегда». В данном случае – 180 секунд (3 минуты);

- `--lockoutduration 3600` – длительность блокировки учетной записи в секундах. Длительность 0 означает, что учетная запись будет заблокирована навсегда. В данном случае – 3600 секунд (1 час).

Добавить сервисы в автозапуск:

```
# systemctl enable postgresql --now
# systemctl enable krb5kdc --now
# systemctl enable kadmindb1 --now
```

Создать пользователей `pgadmin`, `admindb1`, `userdb1` и задать им пароли:

```
# useradd pgadmin
# useradd admindb1
# useradd userdb1
# passwd pgadmin
# passwd admindb1
# passwd userdb1
```

13.3.3. Создание администратора БД и БД

От имени учетной записи `pgadmin` (администратор СУБД) выполнить создание принципа `admindb1`:

```
$ kadmin ank +requires_preauth -policy lockout_policy admindb1/admin
```

ввести пароль принципа `pgadmin` и новый пароль для `admindb1`. Пароль для `admindb1` должен удовлетворять парольной политике для `kerberos`.

Создать пользователя `admindb1` в СУБД:

```
$ createuser admindb1 --createrole
```

при запросе пароля следует ввести пароль принципа `pgadmin`.

Выполнить создание БД:

```
$ createdb -O admindb1 db1
```

при запросе пароля следует ввести пароль принципа `pgadmin`.

13.3.4. Работа роли администратора БД

Выполнить авторизацию в ОС от имени учетной записи `admindb1`.

Создать принципал для пользователя userdb1:

```
$ kadmin ank +requires_preauth -policy lockout_policy userdb1/user
```

при запросе пароля следует ввести пароль принципала admindb1 и новый пароль userdb1. Пароль для userdb1 должен удовлетворять парольной политике для kerberos.

```
$ createuser userdb1
```

при запросе пароля следует ввести пароль принципала admindb1.

Подключиться к БД и назначить пользователю userdb1 права на БД (при запросе пароля следует ввести пароль принципала admindb1):

```
$ psql db1
db1=> grant all on database db1 to userdb1;
db1=> grant all on schema public to userdb1;
db1=> \q
```

13.4. Настройка кластера postgresql

В качестве кластера выступают три ноды (узла) с установленной группой пакетов «Сервер Postgresql». В качестве сервера аутентификации Kerberos в примере далее выступает arm3(node3).

Следующие действия следует выполнить на всех трех нодах:

1) прописать соответствие имени хостов их IP-адресам в файл /etc/hosts:

```
192.168.10.1   arm1.POSTGRESQL arm1
192.168.10.2   arm2.POSTGRESQL arm2
192.168.10.3   arm3.POSTGRESQL arm3
```

2) создать каталог:

```
# mkdir /srv/pgsql
```

3) развернуть postgresql:

```
# deploy postgresql-cert
```

4) создать символические ссылки и изменить права для PGDATA:

```
# mv /var/lib/pgsql/data /srv/pgsql
# ln -s /srv/pgsql/data /var/lib/pgsql/data
# chown postgres:postgres -R /var/log/postgres
# chown postgres:postgres -R /srv/pgsql
```

- 5) переключить `sudo` в режим работы `public`, изменить оболочку для пользователя `postgres` и сгенерировать ключи SSH:

```
# control sudo public
# usermod -s /bin/bash postgres
# su - postgres -c 'ssh-keygen -t ed25519'
```

- 6) записать открытый ключ с каждой ноды в файл `/var/lib/pgsql/.ssh/authorized_keys`.

Файл должен иметь следующий вид, на каждой из нод:

```
# cat /var/lib/pgsql/.ssh/authorized_keys
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJQaH2TiiTJUkPRqhXgUMkjnLBsWrkxw2Vzyu2ThW7Bw postgres@arm1.POSTGRESQL
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIJih4kd9QL8Iam6pkDuJgvaXu88gnNJ9PSO7Ds30XLFn postgres@arm2.POSTGRESQL
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIAtPE8584kT5JHVrs4F86NRDARTfMlF4ohvtP3bASEd3 postgres@arm3.POSTGRESQL
```

- 7) выполнить SSH-подключение с каждой на каждую ноду для появления записей в `known_hosts`. Для этого выполнить команды:

```
# su - postgres
$ ssh postgres@arm1
$ ssh postgres@arm2
$ ssh postgres@arm3
```

На ноде `arm1` в файле `/var/lib/pgsql/data/pg_hba.conf` добавить правила для сетевого подключения:

```
host      all             all      192.168.10.0/24    pam pamservice=postgres
host      replication    all      192.168.10.0/24    pam pamservice=postgres
```

На ноде `arm1` в файле `/var/lib/pgsql/data/postgresql.conf` изменить параметр `listen_addresses` на:

```
listen_addresses = '*'
```

Выполнить перезапуск службы:

```
# systemctl restart postgresql
```

Далее в руководстве нода будет `arm1` определена как `primary` СУБД, ноды `arm2` и `arm3` – `standby`.

На всех нодах раскомментировать строчку `default_realm` в `/etc/krb5.conf` и изменить значение на `POSTGRESQL`:

```
default_realm = POSTGRESQL
```

На всех нодах в файле `/etc/krb5.conf.d/postgresql_krb5.conf` параметры `kdc` и `admin_server` заменить на `arm3`.

Пример файла:

```
# cat /etc/krb5.conf.d/postgresql_krb5.conf

[libdefaults]
default_realm=POSTGRESQL
[realms]
POSTGRESQL = {
    kdc = arm3
    admin_server = arm3:749
}
```

На ноде `arm3` в файле `/var/lib/kerberos/krb5kdc/kdc.conf` заменить `EXAMPLE.COM` на `POSTGRESQL`.

На ноде `arm3`, выступающей в роли сервера аутентификации Kerberos, выполнить настройки из п. 13.3 и выполнить создание принципа для роли СУБД `repmgr`, которая будет выполнять репликацию нод:

```
# kadmin.local ank +requires_preauth -policy lockout_policy
repmgr/admin
```

На всех нодах создать файл с правами 600 и владельцем `postgres:postgres` `/var/lib/pgsql/.pgpass`:

```
# su - postgres -c 'touch /var/lib/pgsql/.pgpass'
# chmod 600 /var/lib/pgsql/.pgpass
```

Со следующим содержимым файла:

```
*:5432:repmgrdb:repmgr:ПАРОЛЬ_ЧТО_НАЗНАЧЕН_В_Kerberos
*:5432:replication:repmgr:ПАРОЛЬ_ЧТО_НАЗНАЧЕН_В_Kerberos
```

На ноде `arm1 (primary)` выполнить создание пользователей СУБД (при запросе пароля следует ввести пароль принципа `repmgr`):

```
# createuser -U postgres --superuser pgadmin
# createuser -U pgadmin --superuser repmgr
# createdb -U repmgr repmgrdb
```

На каждой ноде выполнить настройку конфигурационного файла `/etc/repmgr/repmgr.conf`, в конфигурационном файле на разных нодах отличаются только четыре поля, поля указаны <<< символами.

⚠ Обратите внимание на расположение bin-файлов postgres.

Нода с более высоким значением в поле `priority=` становится `primary` в случае отказа первой `primary` ноды (`arm1`):

```
# ID узла (сервера). В рамках кластера указывать уникальный
node_id=1
# hostname
node_name='arm1.POSTGRESQL'
# строка подключения к БД
conninfo='host=arm1.POSTGRESQL user=repmgr dbname=repmgrdb connect_timeout=2'
# каталог с данными postgres.
data_directory='/var/lib/pgsql/data/'
# режим репликации
replication_type=physical

# log file.
log_file='/var/log/repmgr/repmgr.log'
# записывать статус каждые 5 минут (300 секунд)
log_status_interval=300

# расположение bin-файлов postgres
# pg_bindir='/usr/bin/'

use_primary_conninfo_password=false
ssh_options='-q -o ConnectTimeout=10'

# режим failover
failover=automatic
# очередность выборов мастера в случае отказа
priority=100
reconnect_attempts=3
reconnect_interval=5
promote_command='/usr/bin/repmgr -f /etc/repmgr/repmgr.conf standby promote --log-to-file'
follow_command='/usr/bin/repmgr standby follow -f /etc/repmgr/repmgr.conf --log-to-file --upstream-node-id=%n'

# команды запуска, остановки и перезапуска сервиса. Должны соответствовать записям в
sudoers
service_start_command = 'sudo -n /sbin/service postgresql start'
service_stop_command = 'sudo -n /sbin/service postgresql stop'
service_restart_command = 'sudo -n /sbin/service postgresql restart'
service_reload_command = 'sudo -n /sbin/service postgresql reload'
```

Назначить arm1 primary node в кластере, для этого выполнить команду на arm1:

```
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf primary register'
```

Убедиться, что arm1 является primary node:

```
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf cluster show'
```

ID	Name	Role	Status	Upstream	Location	Priority
1	arm1	primary	* running		default	100

Добавить ноды arm2 и arm3 в кластер как standby ноды:

```
# systemctl stop postgresql
# rm -rf /var/lib/pgsql/data/*
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf -h arm1 -U
repmgr -d repmgrdb standby clone'
```

Вся иерархия файлов СУБД будет скопирована на ведомую ноду утилитой pg_basebackup.

Выполнить запуск сервиса postgresql:

```
# systemctl start postgresql
```

Выполнить на каждой standby ноде регистрацию нод в кластере:

```
# su - postgres -c 'repmgr -f /etc/repmgr/repmgr.conf standby
register'
# systemctl enable repmgr.service --now
```

14. ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ ОС

14.1. Управление системными сервисами, основные команды

14.1.1. Сервисы

Сервисы – это программы, которые запускаются и останавливаются через инициализированные скрипты, расположенные в каталоге `/etc/init.d`. Многие из этих сервисов запускаются на этапе старта ОС Альт СП.

Каталог `/sbin/service` обеспечивает интерфейс (взаимодействие) пользователя с инициализированными скриптами. В свою очередь, скрипты обеспечивают интерфейс для управления сервисами, предоставляя пользователю опции для запуска, остановки, перезапуска, запроса состояния сервиса и выполнения других воздействий на сервис.

Инициализированный скрипт сервиса `openssh` имеет следующие опции:

```
/etc/init.d/sshd
Usage: sshd
{start|stop|reload|restart|condstop|condrestart|condreload|check|
status}
```

Текущее состояние всех системных служб в ОС Альт СП можно просмотреть с помощью команды `systemctl`:

```
systemctl
...
sshd.service
loaded active running   OpenSSH server daemon
systemd-binfmt.service
loaded active exited   Set Up Additional Binary F
systemd-fsck-root.service
loaded active exited   File System Check on Roo
...
```

Информация о запусценности и включенности сервисов может быть получена или изменена с помощью команды `systemctl`. Например, для службы удаленного доступа `ssh` установки по умолчанию выглядят следующим образом:

```
/sbin/systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/lib/systemd/system/sshd.service; enabled;
   vendor preset: ena
```

```
Active: active (running) since Mon 2025-04-10 09:48:34 MSK; 4h
0min ago
```

```
Process: 921 ExecStartPre=/usr/sbin/sshd -t (code=exited,
status=0/SUCCESS)
```

```
Process: 904 ExecStartPre=/usr/bin/ssh-keygen -A (code=exited,
status=0/SUCCESS)
```

```
Main PID: 942 (sshd)
```

```
CGroup: /system.slice/sshd.service
```

```
└─942 /usr/sbin/sshd -D
```

Сервис `sshd` запускается автоматически. Для того чтобы отключить его автоматический запуск сервиса, можно воспользоваться следующей опцией команды `systemctl`:

```
/sbin/systemctl disable sshd
```

Запуск, остановка, перезапуск и перезагрузка настроек служб выполняются соответственно командами:

```
/sbin/systemctl start <служба>
```

```
/sbin/systemctl stop <служба>
```

```
/sbin/systemctl restart <служба>
```

```
/sbin/systemctl reload <служба>
```

14.1.2. Команды

Далее приведены основные команды, использующиеся в ОС Альт СП:

- `ar` – создание и работа с библиотечными архивами;
- `at` – формирование или удаление отложенного задания (см. п. 14.8.2);
- `awk` – язык обработки строковых шаблонов;
- `batch` – планирование команд в очереди загрузки (см. п. 14.8.3);
- `bc` – строковый калькулятор;
- `chfn` – управление информацией учетной записи (имя, описание);
- `chsh` – управление выбором командного интерпретатора (по умолчанию – для учетной записи);
- `cut` – разбивка файла на секции, задаваемые контекстными разделителями;
- `df` – вывод отчета об использовании дискового пространства;
- `dmesg` – вывод содержимого системного буфера сообщений;
- `du` – вычисление количества использованного пространства элементов ФС;

- `echo` – вывод содержимого аргументов на стандартный вывод;
- `egrep` – поиск в файлах содержимого согласно регулярным выражениям;
- `fgrep` – поиск в файлах содержимого согласно фиксированным шаблонам;
- `file` – определение типа файла;
- `find` – поиск файла по различным признакам в иерархии каталогов (см. п. 14.5.1);
- `gettext` – получение строки интернационализации из каталогов перевода;
- `grep` – вывод строки, содержащей шаблон поиска (см. п. 14.4.4);
- `groupadd` – создание новой учетной записи группы;
- `groupdel` – удаление учетной записи группы;
- `groupmod` – изменение учетной записи группы;
- `groups` – вывод списка групп;
- `gunzip` – распаковка файла;
- `gzip` – упаковка файла;
- `hostname` – вывод и задание имени хоста;
- `install` – копирование файла с установкой атрибутов;
- `ipcrm` – удаление ресурса IPC;
- `ipcs` – вывод характеристик ресурса IPC;
- `kill` – прекращение выполнения процесса (см. п. 14.2.6);
- `killall` – удаление процессов по имени (см. п. 14.2.6);
- `lpr` – система печати;
- `ls` – вывод содержимого каталога (см. п. 14.3.1);
- `lsb_release` – вывод информации о дистрибутиве;
- `m4` – запуск макропроцессора;
- `md5sum` – генерация и проверка MD5-сообщения;
- `mknod` – создание файла специального типа (см. п. 14.4.6);
- `mktemp` – генерация уникального имени файла;
- `more` – постраничный вывод содержимого файла;
- `mount` – монтирование ФС (см. п. 14.3.12);

- `msgfmt` – создание объектного файла сообщений из файла сообщений;
- `newgrp` – смена идентификатора группы;
- `nice` – изменение приоритета процесса перед его запуском (см. п. 14.2.4);
- `nohup` – работа процесса после выхода из системы (см. п. 14.2.3);
- `od` – вывод содержимого файла в восьмеричном и других видах;
- `passwd` – смена пароля учетной записи (см. п. 17.3);
- `patch` – применение файла описания изменений к оригинальному файлу;
- `pidof` – вывод идентификатора процесса по его имени;
- `ps` – вывод информации о процессах (см. п. 14.2.2);
- `renice` – изменение уровня приоритета процесса (см. п. 14.2.5);
- `rm` – удаление файлов или каталогов;
- `sed` – строковый редактор;
- `sendmail` – транспорт системы электронных сообщений;
- `sh` – командный интерпретатор;
- `shutdown` – команда останова системы;
- `srm` – безопасная перезапись/переименование/удаление целевого файла;
- `su` – изменение идентификатора запускаемого процесса (см. п. 17.2.4);
- `sync` – сброс системных буферов на носители;
- `tar` – файловый архиватор (см. п. 14.6.1);
- `umount` – размонтирование ФС;
- `useradd` – создание новой учетной записи или обновление существующей (см. п. 17.3);
- `userdel` – удаление учетной записи и соответствующих файлов окружения (см. п. 17.3);
- `usermod` – модификация информации об учетной записи (см. п. 17.3);
- `w` – список пользователей, кто в настоящий момент работает в системе и с какими файлами;
- `who` – вывод списка пользователей системы (см. п. 14.2.1).

Узнать об опциях команд можно с помощью команды `man`.

14.2. Администрирование многопользовательской и многозадачной среды

14.2.1. Команда `who`

Для получения списка пользователей, работающих в ОС, используется команда `who`, которая позволяет вывести в консоль идентификаторы активных пользователей, терминалы и время входа в систему.

Для получения списка пользователей, зарегистрировавшихся в системе, нужно выполнить команду `who`. Задавая различные опции, с помощью команды `who` можно получить информацию о времени начала и конца сеансов работы пользователей, перезагрузок, корректировках системных часов, а также о других процессах, порожденных процессом `init`.

Синтаксис команды `who`:

```
who [-u] [-T] [-l] [-H] [-q] [-p] [-d] [-b] [-r] [-t] [-a] [-s]
[имя файла]
```

Опции команды `who` приведены в таблице 12.

Т а б л и ц а 12 – Опции команды `who`

Опция	Описание
<code>-u</code>	Позволяет вывести информацию о пользователях, которые в настоящее время являются активными (работают в ОС).
<code>-H</code>	Опция, аналогичная опции <code>-u</code> (дополнительно в консоль выводится название столбцов).
<code>-s</code>	Позволяет вывести в консоль имена активных пользователей и терминальных линий, а также время и дату начала сессии пользователей.
<code>-t</code>	Позволяет вывести информацию о последней корректировке системных часов администратором.
<code>-r</code>	Позволяет вывести текущий уровень выполнения процесса <code>init</code> , кроме этого, будут выведены идентификатор процесса, системный код завершения и пользовательский код завершения процесса.
<code>-a</code>	Позволяет обработать файл <code>/etc/utmp</code> или файл, указанный в команде, считая, что все опции (кроме <code>THqs</code>) включены.
<code>-b</code>	Позволяет вывести время и дату последней загрузки системы.
<code>-d</code>	Позволяет вывести информацию обо всех процессах, которые прекратили существование и не были заново порождены процессом <code>init</code> .

Окончание таблицы 12

Опция	Описание
-p	Позволяет вывести список всех других процессов, активных в настоящий момент, которые были порождены процессом init.
-q	Позволяет вывести имена и количество пользователей, работающих в настоящий момент в системе.
-l	Позволяет вывести список линий, на которых система ожидает входа в нее какого-либо пользователя.
-T	Аналогична опции -s с той разницей, что дополнительно в позиции STATE выводится информация о состоянии терминальной линии.

Сообщения, выводимые после выполнения команды `who`, имеют следующий формат:

```
NAME [STATE] LINE TIME [IDLE] [PID] [COMMENT] [EXIT]
```

Информация `NAME`, `LINE` и `TIME` выводится при использовании всех опций, кроме `-q`, `STATE` — только при использовании опции `-T`, `IDLE` и `PID` — только при использовании опции `-u` и `-l`, `COMMENT` и `EXIT` — только при использовании опции `-a`.

В сообщениях, выводимых после выполнения команды `who`, фигурируют следующие параметры:

- `NAME` — имя пользователя;
- `STATE` — состояние терминальной линии (состояние — возможность передавать сообщения на терминал от кого-либо другого терминала: состояние «+» — свидетельствует о том, что терминалу может передавать сообщения любой другой терминал, состояние «-» — терминалу сообщения передаваться не могут; пользователь `root` может передавать сообщения во все линии, которым отвечает состояние «+» или «-»; при обнаружении неисправной линии выводится «?»);
- `LINE` — имя терминальной линии;
- `TIME` — время и дата начала сеанса работы пользователя в системе;
- `IDLE` — время, прошедшее со времени последней активной работы пользователя;
- `PID` — идентификатор процесса входной оболочки пользователя;

- COMMENT — комментарий, характеризующий данную линию (если таковые имеются в файле `/etc/inittab` — этот файл может содержать, например, сведения о местоположении терминала, телефонном номере комнаты или о типе физического терминала).

Чтобы получить сведения о сеансе, учетной записи и PID запущенного процесса нужно выполнить следующую команду:

```
who -uH
```

На экран монитора будет выведено сообщение следующего вида:

```
ИМЯ          ЛИНИЯ      ВРЕМЯ          IDLE      PID      КОММЕНТАРИЙ
user-name line-name mm-dd hh:mm .          10340 (:0)
```

где:

- user-name — имя пользователя;
- line-name — имя терминальной линии;
- yy-mm-dd hh:mm — дата (в формате гг — мм — дд, гг — год, мм — месяц, дд — день) и время (в формате чч:мм, чч — час, мм — минута) начала сеанса работы пользователя;
- 10340 — PID-идентификатор процесса;
- (:0) — отсутствующий комментарий.

Точка (.) в параметре IDLE свидетельствует о том, что данный терминал находился в активном состоянии не более минуты тому назад.

14.2.2. Команда ps

Для получения информации о состоянии запущенных процессов используется команда `ps`. Она выдает следующую информацию о процессах: какие из них выполнены, какие вызвали проблемы в системе, как долго выполняется тот или иной процесс, какие он затребовал системные ресурсы, идентификатор процесса (который будет нужен, например, для прекращения работы процесса с помощью команды `kill`).

Команда `ps`, запущенная без опций командной строки, выдает список процессов, которые порождены учетной записью администратора.

Наиболее распространенное применение `ps` – отслеживание работы фоновых и других процессов в системе. Поскольку в большинстве случаев фоновые процессы никак не взаимодействуют ни с экраном, ни с клавиатурой, команда `ps` остается основным средством наблюдения за ними.

Синтаксис команды `ps`:

```
ps [-e] [-d] [-a] [-f] [-l] [-n файл_с_системой] [-t список_терминалов]
[-p список_идентификаторов_процессов]
[-u список_идентификаторов_пользователей]
[-g список_идентификаторов_лидеров_групп]
```

Опции команды `ps` приведены в таблице 13.

Т а б л и ц а 13 – Опции команды `ps`

Опция	Описание
<code>-e</code>	Позволяет вывести информацию обо всех процессах
<code>-d</code>	Позволяет вывести информацию обо всех процессах, кроме лидеров групп
<code>-a</code>	Позволяет вывести информацию обо всех наиболее часто запрашиваемых процессах, то есть обо всех процессах, кроме лидеров групп и процессов, не ассоциированных с терминалом
<code>-f</code>	Позволяет сгенерировать полный листинг
<code>-l</code>	Генерировать листинг в длинном формате
<code>-n файл_с_системой</code>	Считать, что ОС загружена из файла_с_системой, а не из файла <code>/unix</code>
<code>-t список_терминалов</code>	Позволяет вывести информацию только о процессах, ассоциированных с терминалами из заданного списка_терминалов (терминал – это либо имя файла-устройства, например, <code>tty</code> , номер или <code>console</code> , либо просто номер, если имя файла начинается с <code>tty</code>)
<code>-p</code>	Список_идентификаторов_процессов – позволяет вывести информацию только об указанных процессах
<code>-u</code>	Список_идентификаторов_пользователей – позволяет вывести информацию только о процессах с заданными идентификаторами или входными именами пользователей (идентификатор пользователя выводится в числовом виде, а при наличии опции <code>-f</code> – в символьном)
<code>-g</code>	Список_идентификаторов_лидеров_групп – позволяет вывести информацию только о процессах, для которых указаны идентификаторы лидеров групп (лидер группы – это процесс, номер которого идентичен его идентификатору группы)

`ps` выводит четыре основных поля информации для каждого процесса:

- PID – идентификатор процесса;
- TTY – терминал, с которого был запущен процесс;
- TIME – время работы процесса;

- COMMAND – имя выполненной команды.

При указании опции `-f` команда `ps` пытается определить имя команды и аргументы, с которыми был создан процесс, исследуя пользовательский блок процесса. В случае если это не удастся, имя процесса выводится так же, как и при отсутствии опции `-f`, только заключается в квадратные скобки.

В таблице 14 приводятся заголовки колонок листинга, и поясняется смысл их содержимого. Буквы «l» или «f» в скобках означают, что эта колонка появляется соответственно при длинном или полном формате листинга, отсутствие букв означает, что данная колонка выводится всегда. При этом опции `-l` и `-f` влияют только на формат выдачи, но не на список процессов, информация о которых будет предоставлена.

Т а б л и ц а 14 – Описание заголовков колонок листинга

Заголовок	Значение	Описание
F (l)	Флаги (шестнадцатеричные), логическая сумма которых характеризует процессы следующим образом:	
	00	Процесс терминирован, элемент таблицы процессов свободен.
	01	Системный процесс: всегда в основной памяти.
	02	Процесс трассируется родительским процессом.
	04	Родительский трассировочный сигнал остановил процесс, родительский процесс находится в состоянии ожидания
	08	Процесс не может быть разбужен сигналом
	10	Процесс в основной памяти
	20	Процесс в основной памяти, блокирован до завершения события
	40	Идет сигнал к удаленной системе
	80	Процесс в очереди на ввод/вывод
S (l)	Статус процесса:	
	O	Процесс обрабатывается процессором
	S	Процесс ожидает завершения события
	R	Процесс стоит в очереди на выполнение
	I	Процесс создается
	Z	Процесс завершен, но родительский процесс не ждет этого
	T	Процесс остановлен сигналом, так как родительский процесс трассирует его

Окончание таблицы 14

Заголовок	Значение	Описание
	X	Процесс ожидает получения большего объема основной памяти
UID (f,l)		Идентификатор владельца процесса, при указании опции - f выдается входное имя пользователя
PID		Идентификатор процесса (нужен для терминирования процесса)
PPID(f,l)		Идентификатор родительского процесса
C (f,l)		Доля выделенного планировщиком времени центрального процессора
STIME (f)		Время запуска процесса (часы:минуты:секунды). Если процесс запущен более чем 24 часа назад, выводится месяц и день запуска
PRI (l)		Приоритет процесса: большее число означает меньший приоритет
NI (l)		Поправка к приоритету
ADDR (l)		Адрес процесса в памяти
SZ (l)		Размер (в блоках по 512 байт) образа процесса в памяти
WCHAN (l)		Адрес события, которого ожидает процесс (у активного процесса эта колонка пуста)
TTY		Управляющий терминал (обычно – терминал, с которого был запущен процесс). В случае если такового нет, выводится символ «?»
TIME		Истраченное процессом время на выполнение центральным процессором
COMMAND		Имя программы: если указана опция - f, выводится полное имя команды и ее аргументы

14.2.3. Команда nohup

Команда nohup применяется для того, чтобы процесс продолжал выполняться даже после выхода из системы, поскольку выполнение стандартного дочернего процесса завершается сразу после прекращения работы родительского, и, если был запущен фоновый процесс, он также прекращает работу при выходе из системы.

При выполнении, команду nohup следует поместить в начало командной строки следующим образом:

```
nohup sort sales.dat &
```

В данном примере nohup заставляет ОС игнорировать выход из нее и продолжать выполнение до тех пор, пока процесс не закончится сам по себе. Будет запущен процесс, который продолжит свое выполнение, не требуя контроля администратора.

14.2.4. Команда `nice`

Команда `nice` позволяет запустить другую команду с предопределенным приоритетом выполнения, предоставляя администратору возможность определять приоритет при выполнении своих задач.

При обычном запуске все задачи имеют один и тот же приоритет, и ОС равномерно распределяет между ними процессорное время. С помощью команды `nice` можно понизить приоритет какой-либо задачи, предоставив другим задачам больше процессорного времени. Повысить приоритет той или иной задачи имеет право только пользователь с идентификатором `root`.

Команда `nice` обладает следующим синтаксисом:

```
nice -number command
```

Уровень приоритета определяется параметром `number`, при этом большее его значение означает меньший приоритет команды. Значение по умолчанию равно «10», и `number` представляет собой число, на которое он должен быть уменьшен.

Например, если запущен процесс сортировки:

```
sort sales.dat > sales.srt &
```

Далее, чтобы дать ему преимущество над следующим процессом, нужно запустить следующий процесс с уменьшенным приоритетом:

```
nice -5 lp mail_list &
```

Для того чтобы назначить процессу самый низкий приоритет из возможных, нужно выполнить следующую команду:

```
nice -10 lp mail_list &
```

Примечание. В случае команды `nice` тире означает знак опции.

Только пользователь с идентификатором `root` может повысить приоритет того или иного процесса, применяя для этого отрицательное значение аргумента. Максимально возможный приоритет – «20», присвоить его процессу пользователь с идентификатором `root` может с помощью команды:

```
nice --10 job &
```

Наличие символа «&» в примере достаточно условно, можно изменять приоритеты, как фоновых процессов, так и процессов переднего плана.

14.2.5. Команда `renice`

Команда `renice` позволяет изменить приоритет работающего процесса.

Формат этой команды подобен формату команды `nice`:

```
renice -n PID
```

Для изменения приоритета работающего процесса нужно знать его идентификатор, получить который можно с помощью команды `ps`, например, вызвав:

```
ps -e | grep name
```

В данной команде нужно заменить `name` именем интересующего процесса. Команда `grep` отфильтрует только те записи, в которых будет встречаться имя нужной команды. В случае, если нужно изменить приоритет всех процессов пользователя или группы пользователей, в команде `renice` используется идентификатор пользователя или группы.

Далее приводится пример использования команды `renice`, предположив, что имя пользователя – `pav`:

```
ps -ef | grep $LOGNAME
pav 11805 11804 0 Dec 22 ttysb 0:01 sort sales.dat > sales srt
pav 19955 19938 4 16:13:02 ttyo 0:00 grep pav
pav 19938 1 0 16:11:04 ttyo 0-00 bash
pav 19940 19938 42 16:13:02 ttyo 0:33 find . -name core -exec nn
{};
```

Теперь, чтобы понизить приоритет процесса `find` с идентификатором 19940, нужно ввести:

```
renice -5 19940
```

В случае команды `renice` работают те же правила, что и в случае команды `nice`, а именно:

- ее можно использовать только со своими процессами;
- пользователь с идентификатором `root` может применить ее к любому процессу;
- только пользователь с идентификатором `root` может повысить приоритет процесса.

14.2.6. Команда `kill` и `killall`

В отдельных ситуациях нужно прекратить выполнение процесса, не дожидаясь его нормального завершения. Это может произойти в следующих случаях:

- процесс использует слишком много времени процессора и ресурсов компьютера;
- процесс работает слишком долго, не давая ожидаемых результатов;
- процесс производит слишком большой вывод информации на экран или в файл;
- процесс привел к блокировке терминала или другой сессии;
- из-за ошибки пользователя или программы используются не те файлы или параметры командной строки;
- дальнейшее выполнение процесса бесполезно.

В случае если процесс работает не в фоновом режиме, нажатие клавиш `<Ctrl>+<C>` должно прервать его выполнение, но, если процесс фоновый, то прервать его выполнение можно только с помощью команды `kill`, которая посылает процессу сигнал, требующий от процесса завершения. Для этого используются две формы:

```
kill PID(s)
kill -signal PID(s)
```

Для завершения процесса с идентификатором 127 ввести:

```
kill 127
```

Для того чтобы завершить процессы 115, 225 и 325, ввести:

```
kill 115 225 325
```

С помощью опции `-signal` можно, например, заставить процесс перечитать конфигурационные файлы без прекращения работы.

Список доступных сигналов можно получить с помощью команды:

```
kill -l
```

При успешном завершении процесса никакое сообщение не выводится.

Сообщение появится при попытке завершения процесса без наличия соответствующих прав доступа или при попытке завершить несуществующий процесс.

Завершение родительского процесса иногда приводит к завершению дочерних, однако для полной уверенности в завершении всех процессов, связанных с данным, следует указывать их в команде `kill`.

В случае, если терминал оказался заблокированным, можно войти в систему с другого терминала:

```
ps -ef | grep $LOGNAME
```

и завершить работу оболочки на заблокированном терминале.

При выполнении команда `kill` посылает процессу соответствующий сигнал. Программы ОС могут посылать и принимать более 20 сигналов, каждый из которых имеет свой номер. Например, при выходе администратора ОС посылает всем его процессам сигнал 1, который заставляет все процессы (кроме запущенных с помощью `nohup`) прекратить работу.

Программы могут быть написаны и таким образом, что будут игнорировать посылаемые им сигналы, включая сигнал 15, который возникает при запуске команды `kill` без указания конкретного сигнала.

Однако сигнал 9 не может быть проигнорирован – процесс все равно будет завершен. Таким образом, если команда `kill PID` не смогла завершить процесс (он виден при использовании команды `ps`), нужно воспользоваться следующей командой:

```
kill -9 PID
```

Команда `kill -9` прекращает процесс, не давая возможности, например, корректно закрыть файлы, что может привести к потере данных. Использовать эту возможность следует только в случае крайней необходимости.

Для завершения всех фоновых процессов нужно ввести следующую команду:

```
kill 0
```

Команда `killall` завершает все процессы с данным именем, обладает следующим синтаксисом:

```
killall [имя процесса]
```

Пример использования `killall`:

```
killall httpd
```

Преимущественное право контроля над процессом принадлежит владельцу. Права владельца могут отменяться только пользователем с идентификатором `root`.

Ядро назначает каждому процессу четыре идентификатора: реальный и эффективный `UID`, реальный и эффективный `GID`. Реальные ID используются для учета использования системных ресурсов, а эффективные – для определения прав доступа. Как правило, реальные и эффективные ID совпадают. Владелец процесса может посылать в процесс сигналы, а также понижать приоритет процесса.

Процесс, приступающий к выполнению другого программного файла, осуществляет один из системных вызовов семейства `exec`. Когда такое случается, эффективные `UID` и `GID` процесса могут быть установлены равными `UID` и `GID` файла, содержащего образ новой программы, если у этого файла установлены биты смены идентификатора пользователя и идентификатора группы.

Системный вызов `exec` – это механизм, с помощью которого такие команды, как `passwd`, временно получают права пользователя с идентификатором `root` (команде `passwd` они нужны для того, чтобы изменить `/etc/passwd`).

14.3. Основные утилиты для операций с файлами и каталогами

14.3.1. Команда `ls`

Команда `ls` предназначена для вывода информации о файлах или каталогах. Команда `ls` для каждого имени каталога распечатывает список входящих в этот каталог файлов; для файлов – повторяется имя файла и выводится дополнительная информация в соответствии с указанными флагами.

По умолчанию имена файлов выводятся в алфавитном порядке. Если имена не заданы, выдается содержимое текущего каталога.

Синтаксис:

```
ls [параметры]... [файл]...
```

Параметры:

- 1) `-a, --all` — вывести список всех файлов (обычно не выводятся файлы, имена которых начинаются с точки);
- 2) `-A, --almost-all` — не показывать подразумеваемые «.» и «..»;
- 3) `--block-size=РАЗМЕР` — выдает размеры в блоках по РАЗМЕР байт. Например, `--block-size=M` для вывода объема в единицах равных 1048576 байтов;
- 4) `-B, --ignore-backups` — не показывать файлы, заканчивающиеся на «~», если они не заданы в командной строке;
- 5) `-c, --time=ctime, --time=status` — сортировать содержимое каталога в соответствии со временем изменения состояния файла. Если с помощью опции `-l` задан этот формат, то выдавать время изменения файла вместо времени его модификации. С опцией `-t` показать время последней модификации описания файла и сортировать по имени;
- 6) `-C, --format=vertical` — вывод в несколько колонок с сортировкой по вертикали;
- 7) `--color[=КОГДА]` — использовать цвета в выводе. КОГДА по умолчанию `always`. Также можно использовать `never` и `auto`;
- 8) `-d, --directory` — если аргумент является каталогом, то выводить только его имя, а не содержимое. Часто используется с флагом `-l` для получения сведений о состоянии каталога;
- 9) `-h, --human-readable` — в сочетании с `-l` показывает размеры в удобочитаемом формате (например, 1K 234M 2G);
- 10) `-i, --inode` — показывать индекс каждого файла;
- 11) `-I, --ignore=ШАБЛОН` — не показывать записи, соответствующие ШАБЛОНУ командного интерпретатора;
- 12) `-k, --kibibytes` — использовать блоки по 1024 байта;
- 13) `-l` — вывод в длинном формате;

- 14) `-m` – показать записи в список шириной в размер терминала, имена файлов разделяются запятыми;
- 15) `-r, --reverse` – изменить порядок сортировки на обратный;
- 16) `-R, --recursive` – рекурсивно обойти встретившиеся подкаталоги;
- 17) `-s, --size` – выдавать размер файлов в блоках;
- 18) `-S` – отсортировать по размеру файлов, большие сначала;
- 19) `--sort=СЛОВО` – сортировать по СЛОВУ, а не по имени: `none` (без сортировки) `-U, extension` (расширение) `-X, size` (размер) `-S, time` (время) `-t` или `version` (версия) `-v`;
- 20) `-t` – файлы сортируются по времени последнего изменения (сначала идут самые новые файлы);
- 21) `-U` – не сортировать, отображать записи в обычном порядке;
- 22) `-v` – сортировать по номерам (версии) в текстовом представлении;
- 23) `-x` – вывод в несколько колонок с сортировкой по строкам;
- 24) `-Z, --context` – вывести контекст для каждого файла;
- 25) `-l` – отображать по одному файлу в строке.

Режим доступа к файлу при указании флага `-l` выводится в виде 10 символов.

При этом первый символ означает:

- 1) `d` – файл является каталогом;
- 2) `b` – файл является специальным блочным файлом;
- 3) `c` – файл является специальным символьным файлом;
- 4) `p` – файл является именованным каналом;
- 5) `-` – обычный файл.

Остальные 9 символов делятся на три группы по три символа: права доступа владельца, других пользователей из его группы, всех прочих пользователей. Внутри каждой группы используются три символа, обозначающие права на чтение, запись и выполнение файла соответственно.

Для каталога под правом на выполнение подразумевается право на просмотр в поисках требуемого файла.

Пример:

```
ls -l /util/by
-rwxr-xr-x 1 root sys 50 Jun 22 10:42 /util/by
```

Права обозначаются следующим образом:

- 1) *r* – право на чтение;
- 2) *w* – право на запись;
- 3) *x* – право на выполнение (поиск в каталоге);
- 4) – – данное право доступа отсутствует;
- 5) *l* – учет блокировки доступа (бит переустановки идентификатора группы равен 1, бит права на выполнение членами группы равен 0). Располагается на месте права на выполнение для членов группы;
- 6) *s* – право переустанавливать идентификатор группы или идентификатор владельца и право выполнения файла для членов группы или владельца;
- 7) *S* – неопределенная комбинация бит: право переустанавливать идентификатор владельца есть, а право выполнения файла для владельца отсутствует;
- 8) *t* – установлен бит навязчивости у файла, который могут выполнять прочие пользователи. Располагается на месте права на выполнение для прочих пользователей;
- 9) *T* – бит навязчивости установлен, а права на выполнение у прочих пользователей нет. Располагается на месте права на выполнение для прочих пользователей.

Примеры:

- 1) если файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения, он имеет режим:

```
-rwxr--r-
```

- 2) файл доступен владельцу для чтения, записи и выполнения, а членам группы и прочим пользователям только для чтения и выполнения. Разрешена переустановка при выполнении идентификатора пользователя на идентификатор владельца файла:

```
-rwsr-xr-x
```


- 3) файл доступен для чтения и записи только владельцу и членам группы; может быть заблокирован при доступе:

```
-rw-rwl--
```

- 4) вывести имена всех файлов в текущем каталоге, включая и те, которые начинаются с точки и обычно не выдаются:

```
ls -a
```

- 5) вывести разнообразную информацию: список всех файлов, включая те, которые обычно не выводятся (a); номера описателей файлов будут выведены в левой колонке (i); размеры файлов (в блоках) выводятся во второй колонке (s); наконец, будут выданы числовые идентификаторы владельцев и групп (n):

```
ls -aisn
```

Возможные сообщения об ошибках, при использовании команды `ls`:

```
ls: невозможно открыть каталог <путь>: Отказано в доступе
```

```
ls: невозможно получить доступ к <путь>/<файл>: Нет такого файла  
или каталога
```

14.3.2. Команда `cp`

Команда `cp` предназначена для копирования файлов и каталогов.

Синтаксис:

```
cp [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ  
cp [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ  
cp [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Копирует ИСТОЧНИК в НАЗНАЧЕНИЕ или несколько ИСТОЧНИКОВ в КАТАЛОГ.

Основные опции:

- 1) `--backup [=CONTROL]` – сделать резервную копию каждого целевого файла;
- 2) `-b` – тоже что и `--backup`, но не принимает аргументы;
- 3) `-f`, `--force` – если невозможно открыть существующий файл, то удалить его и попробовать еще раз (данная опция игнорируется, если используется совместно с `-n`);
- 4) `-i`, `--interactive` – спросить перед перезаписью (отменяет ранее указанный ключ `-n`);

- 5) `-H` – следовать символическим ссылкам в источнике;
- 6) `-l`, `--link` – создавать жесткие ссылки вместо копирования;
- 7) `-n`, `--no-clobber` – не перезаписывать существующие файлы (отменяет стоящую перед ней опцию `-i`);
- 8) `-R`, `-r`, `--recursive` – копировать каталоги рекурсивно;
- 9) `-s`, `--symbolic-link` – создать символическую ссылку вместо копирования;
- 10) `-u`, `--update` – копировать, только если файл источник новее, чем файл назначения или если файл назначения отсутствует;
- 11) `-v`, `--verbose` – выводить имя каждого файла перед копированием.

По умолчанию суффикс для резервных копий «~». Его можно переопределить при помощи опции `--suffix` или переменной окружения `SIMPLE_BACKUP_SUFFIX`. Способ контроля версий может быть задан через опцию `--backup` или через переменную окружения `VERSION_CONTROL`. Допустимые значения:

- 1) `none`, `off` – никогда не делать резервные копии (даже если задана опция `--backup`);
- 2) `numbered`, `t` – создать нумерованные резервные копии;
- 3) `existing`, `nil` – если существуют нумерованные резервные копии, то создавать нумерованные резервные копии, если нет, то создавать простые;
- 4) `simple`, `never` – всегда создавать простые резервные копии.

Следующий пример использования команды `cp` демонстрирует копирование файла `srcfile1` в каталог `dest_dir`: `cp srcfile1 dest_dir`

14.3.3. Команда `rsync`

Команда `rsync` выполняет синхронизацию файлов и каталогов, использует протокол удаленного обновления для ускорения передачи файлов, которые существуют в месте назначения.

Синтаксис:

`rsync [ОПЦИИ] источник место_назначения`

Опции:

- 1) `-v` – подробный режим;
- 2) `-r` – копировать данные рекурсивно;
- 3) `-a` – режим архивирования, позволяет копировать данные рекурсивно, с сохранением прав доступа на файлы, символических ссылок и другой информации);
- 4) `-h` – вывод данных в удобном формате;
- 5) `-z` – сжатие данных.

Примеры:

- 1) скопировать или синхронизировать все файлы из одного каталога в другой:

```
rsync -avh /tmp/firstdir /tmp/seconddir
```

- 2) копирование локальных данных на удаленный хост:

```
rsync -avzh /tmp/firstdir user@10.110.2.1:/tmp/seconddir
```

Возможные сообщения об ошибках, при использовании команды `sfill`:

```
rsync: change_dir#1 <каталог> failed: Отказано в доступе
```

```
rsync: change_dir <каталог> failed: Нет такого файла или каталога
```

14.3.4. Команда `mv`

Команда `mv` – перемещение (переименование) файлов.

Синтаксис:

```
mv [ОПЦИЯ]... [-T] ИСТОЧНИК НАЗНАЧЕНИЕ
```

```
mv [ОПЦИЯ]... ИСТОЧНИК... КАТАЛОГ
```

```
mv [ОПЦИЯ]... -t КАТАЛОГ ИСТОЧНИК...
```

Переименовать ИСТОЧНИК в НАЗНАЧЕНИЕ или переместить ИСТОЧНИК (и) в КАТАЛОГ.

Основные опции:

- 1) `-i`, `--interactive` – просит подтверждения на замену существующего файла;
- 2) `-n`, `--no-clobber` – не переписывать существующий файл. Если указано несколько опций `-i`, `-f` и `-n`, то действовать будет только последняя;

3) `-u, --update` – перемещать только, если файл источник новее, чем файл назначения или если файл назначения отсутствует;

4) `-v, --verbose` – выдавать имя каждого файла перед его переносом.

Возможные сообщения об ошибках, при использовании команды `mv`:

`mv: невозможно переместить <файл> в <файл>: Операция не позволена`

`mv: не удалось выполнить stat для <файл>: Отказано в доступе`

`mv: не удалось выполнить stat для <файл>: Нет такого файла или каталога`

14.3.5. Команда `dd`

Команда `dd` предназначена для копирования файла (по умолчанию из стандартного ввода на стандартный вывод), используя заданные размеры блоков для ввода и вывода, и в тоже время, выполняя его преобразование.

Синтаксис:

`dd [параметр]`

Основные опции:

1) `if=ФАЙЛ` – читает данные из ФАЙЛа вместо стандартного ввода;

2) `of=ФАЙЛ` – пишет данные в ФАЙЛ вместо стандартного вывода;

3) `ibs=ЧИСЛО` – читает по ЧИСЛО байт за раз. По умолчанию 512;

4) `obs=ЧИСЛО` – пишет по ЧИСЛО байт за раз. По умолчанию 512;

5) `bs=ЧИСЛО` – читает и пишет по ЧИСЛО байт за раз. По умолчанию 512.

Примеры:

1) Заполнить устройство случайными данными:

```
dd if=/dev/urandom of=/dev/sda bs=4k
```

2) Скопировать раздел в другой раздел:

```
dd if=/dev/sda3 of=/dev/sdb3 bs=4096 conv=notrunc,noerror
```

Возможные сообщения об ошибках, при использовании команды `dd`:

`dd: не удалось открыть <файл>: Отказано в доступе`

14.3.6. Команда `s_rm`

Команда `s_rm` выполняет безопасное удаление целевого файла.

Синтаксис:

`s_rm ФАЙЛ...`

Возможные сообщения об ошибках, при использовании команды `s_rm`:

Ошибка: файл <файл>: Отказано в доступе

Ошибка: файл <файл>: Нет такого файла или каталога

Примечание. Для работы команды `s_rm` и `s_fill` должен быть установлен пакет `altsp-test-scripts`.

14.3.7. Команда `s_fill`

Команда `s_fill` выполняет безопасную перезапись свободного пространства на разделе, в котором находится указанная директория и всех свободных индексных дескрипторов указанного каталога.

Синтаксис:

`s_fill каталог...`

Возможные сообщения об ошибках, при использовании команды `s_fill`:

Ошибка: не достаточно прав для <каталог>: Отказано в доступе

14.3.8. Команда `cd`

Команда `cd` предназначена для смены каталога. Команда работает как с абсолютными, так и с относительными путями. Если каталог не указан, используется значение переменной окружения `HOME` (домашний каталог пользователя). Если каталог задан полным маршрутным именем, он становится текущим. По отношению к новому каталогу нужно иметь право на выполнение, которое в данном случае трактуется как разрешение на поиск.

Синтаксис:

`cd [-L|-P] [каталог]`

Опция `-L` заставляет следовать по символическим ссылкам.

Поскольку для выполнения каждой команды создается отдельный процесс, `cd` не может быть обычной командой; она распознается и выполняется командной оболочкой.

Если в качестве аргумента задано `-`, то это эквивалентно `$OLDPWD`.

Если переход был осуществлен по переменной окружения `CDPATH` или в качестве аргумента был задан `-` и смена каталога была успешной, то абсолютный путь нового рабочего каталога будет выведен на стандартный вывод.

14.3.9. Команда `pwd`

Команда `pwd` выводит абсолютный путь текущего (рабочего) каталога.

Синтаксис: `pwd [-LP]`

Опции:

- 1) `-P` – вывод не будет содержать символических ссылок;
- 2) `-L` – вывод может содержать символические ссылки.

14.3.10. Команда `mkdir`

Команда `mkdir` предназначена для создания каталогов.

Синтаксис:

`mkdir [опция]... каталог...`

Опции:

- 1) `-m`, `--mode=РЕЖИМ` – установить права доступа для создаваемых каталогов;
- 2) `-p`, `--parents` – перед созданием нового каталога предварительно создаются все несуществующие вышележащие каталоги. В случае существования каталога не будет выведена ошибка;
- 3) `-v`, `--verbose` – выводить сообщение для каждого созданного каталога;
- 4) `-Z`, `--context [=CTX]` – задать контекст для каждого создаваемого каталога.

Если `CTX` не задан, то контекст будет равным типу по умолчанию.

Чтобы создать поддерево каталогов `tmpdir/temp/dir`, надо выполнить команду:

```
mkdir -p tmpdir/temp/dir
```

Возможные сообщения об ошибках, при использовании команды `mkdir`:

```
mkdir: невозможно создать каталог <каталог>: Отказано в доступе
```

```
mkdir: невозможно создать каталог <каталог>: Нет такого файла или
```

каталога

14.3.11. Команда `rmdir`

Команда `rmdir` предназначена для удаления каталога, при условии, что он пуст.

Синтаксис:

`rmdir [опция]... каталог...`

Для команды `rmdir` доступна опция `-p` – при указании пути к каталогу (а не просто имени каталога), команда удалит каталог и его потомков:

```
rmdir -p a/b/c
```

Команда `rmdir` часто заменяется командой `rm -rf`, которая позволяет удалять каталоги, даже если они не пусты.

14.3.12. Команда `mount`

Команда `mount` используется для монтирования файловых систем.

Синтаксис:

```
mount [-lhV]
mount -a [опция]
mount [опция] [--source] <source> | [--target] <directory>
mount [опция] <source> <directory>
```

Опции:

- 1) `-t` – определение типа файловой системы раздела, предполагаемого для размещения;
- 2) `-o` – указание параметров монтирования.

Примеры:

- 1) просмотр примонтированных устройств:

```
mount -l
```

- 2) монтирование разделов жесткого диска:

```
mount -t ext3 /dev/sdb1 /home/user/test
```

Возможные сообщения об ошибках, при использовании команды `mount`:

```
mount: точка монтирования <каталог> не существует
```

14.4. Создание, просмотр и редактирование файлов

14.4.1. Команда `cat`

Команда `cat` позволяет просмотреть файл целиком, копируя файлы в стандартный поток вывода и объединяя их.

Синтаксис:

```
cat [ОПЦИЯ]... [ФАЙЛ]...
```

Опции:

- 1) `-A`, `--show-all` – тоже что и `-vET`;

- 2) `-e` – тоже что и `-vE`;
- 3) `-E`, `--show-ends` – отображать символ «\$» в конце каждой строки;
- 4) `-n`, `--number` – нумеровать выводимые строки;
- 5) `-s`, `--squeeze-blank` – скрывать повторяющиеся пустые строки в выводе;
- 6) `-t` – тоже что и `-vT`;
- 7) `-T`, `--show-tabs` – отображать символ табуляции как `^I`;
- 8) `-v`, `--show-nonprinting` – использовать `^-` и M-нотацию для всех непечатаемых символов кроме LFD (перевод строки и табуляция) и табуляции.

Если файл не задан или задан как «-», то читать из стандартного ввода.

Примеры:

- 1) вывести содержимое файла `f`, затем со стандартного ввода, затем – содержимое файла `g`:

```
cat f - g
```

- 2) скопировать стандартный ввод на стандартный вывод:

```
cat
```

Возможные сообщения об ошибках, при использовании команды `cat`:

```
cat: <файл>: Отказано в доступе
```

```
cat: <файл>: Нет такого файла или каталога
```

14.4.2. Команда `less`

Команда `less` позволяет просматривать текст постранично.

```
less [ опции ] файл
```

Опции:

- 1) `-c` – очистка экран перед тем, как отобразить следующую страницу;
- 2) `-m` – вывод информации о том, какая часть файла выведена на данный момент (в процентах);
- 3) `-N` – вывод номеров строк;
- 4) `-r` – вывод управляющих (непечатаемых) символов;
- 5) `-s` – объединение нескольких пустых строк в одну;
- 6) `-S` – урезание длинных строк до длины экрана вместо переноса.

Возможные сообщения об ошибках, при использовании команды `less`:

<файл>: Отказано в доступе

<файл>: Нет такого файла или каталога

14.4.3. Команда `echo`

Команда `echo` выводит текст на стандартное устройство вывода.

`echo [опции] [строка]`

Опции:

- 1) `-n` – не выводить в конце символ новой строки;
- 2) `-e` – включить интерпретацию управляющих символов;
- 3) `-E` – отключить интерпретацию управляющих символов;

Возможные сообщения об ошибках, при использовании команды `echo`:

<файл>: Отказано в доступе

<файл>: Нет такого файла или каталога

14.4.4. Команда `grep`

Команда `grep` предназначена для поиска текста, соответствующего регулярному выражению в файлах или потоке вывода.

Синтаксис:

`grep [ опции ] шаблон_поиска [файл]`

Опции:

- 1) `-r` – рекурсивный поиск во всех каталогах;
- 2) `-n` – вывод номеров строк, в которых найдено совпадение;
- 3) `-l` – вывод списка файлов, содержащих шаблон;
- 4) `-v` – поиск строк, не содержащих шаблон (инверсия);
- 5) `-i` – поиск с игнорированием регистра.

14.4.5. Команда `touch`

Создание и редактирование файлов выполняется командой `touch`, которая устанавливает время последнего изменения и доступа в текущее системное время у заданного файла. Если файл не существует – он создается.

Синтаксис:

`touch [опции]... файл`

Основные опции:

- 1) `-a` – изменить только время доступа к файлу;
- 2) `-c, --no-create` – не создавать файл;
- 3) `-d, --date=СТРОКА` – проанализировать строку и использовать вместо текущего времени;
- 4) `-m` – изменить время последней модификации файла;
- 5) `-r, --reference=ФАЙЛ` – использовать соответствующий временной штамп от ФАЙЛ в качестве нового значения для изменяемого временного штампа;
- 6) `-t время` – использовать заданное время в качестве нового значения для изменяемого временного штампа.

Следующий пример использования команды `touch` создает файл `myfile.txt`:

```
touch myfile.txt
```

Возможные сообщения об ошибках, при использовании команды `touch`:

```
touch: невозможно выполнить touch для <файл>: Отказано в доступе
```

```
touch: невозможно выполнить touch для <путь>/<файл>: Нет такого  
файла или каталога
```

14.4.6. Команда `mknod`

Утилита `mknod` создает специальные блочные или символьные файлы. Специальный файл записывается в файловой системе с помощью тройки параметров: один логический и два целых. Логический параметр говорит о том, является ли специальный файл символьным или блочным. Два целых параметра задают старший и младший номера устройства. Специальный файл практически не занимает места на диске и используется только для общения с операционной системой, а не для хранения данных.

Синтаксис:

```
mknod [опции] имя {bc} старший_номер младший_номер  
mknod [опции] имя p
```

Основные опции:

- 1) `-m, --mode=РЕЖИМ` – установить РЕЖИМ доступа;
- 2) `-z` – установить контекст безопасности равным типу по умолчанию.

Тип устройства может принимать следующие значения:

- 1) `b` – создать файл блочного устройства (буферизированный);
- 2) `c` – создать файл символьного устройства (небуферизированный);
- 3) `p` – создать именованный канал.

Возможные сообщения об ошибках, при использовании команды `mknod`:

`mknod: <файл>: Файл существует`

14.5. Поиск файлов

14.5.1. Команда `find`

Утилита `find` используется для поиска файлов.

Синтаксис:

```
find [-H] [-L] [-P] [-0уровень] [-D help | tree | search | stat |  
rates | opt | exec] [путь...] [выражение]  
find [путь] [опции] [критерии поиска] [действия над файлами]
```

В качестве пути для поиска можно использовать как абсолютные, так и относительные пути, а также список путей, разделенных пробелом. Путем по умолчанию является текущий подкаталог. Выражение по умолчанию `-print`.

Основные опции:

- 1) `-d, -depth` – поиск в подкаталогах перед поиском в самом каталоге;
- 2) `-L` – при поиске следовать по символическим ссылкам;
- 3) `-P` – никогда не следовать по символическим ссылкам;
- 4) `-maxdepth N` – при поиске проверять не более чем `N` вложенных уровней каталогов;
- 5) `-mindepth N` – не проверять вложенные каталоги уровня `N` и меньше;
- 6) `-mount` – не искать в каталогах других файловых систем.

У команды `find` может быть несколько критериев поиска (tests). Каждый критерий представляет собой определенное условие проверки, которое возвращает либо `true` либо `false`.

В процессе обработки очередного файла команда `find` по очереди проверяет каждый критерий, и, если очередной критерий возвращает `false`, тогда команда `find` переходит к следующему файлу.

Основные критерии поиска:

- 1) `-name шаблон` – имя файла (шаблон имени) без указания пути.
Рекомендуется всегда заключать шаблон в кавычки;
- 2) `-atime N` – последний доступ к файлу производился N дней назад.
`-atime +1` найдет файлы, доступ к которым осуществлялся как минимум два дня назад;
- 3) `-mtime N` – последнее изменение файла было N дней назад;
- 4) `-ctime N` – статус файла последний раз изменялся N дней назад;
- 5) `-newer другой_файл` – файл был модифицирован позднее, чем другой_файл;
- 6) `-size [±]N[cwbkMG]` – размер файла равен N блокам, если указано +N, тогда размер файла больше N, -N – меньше. Символ после N означает размер блока (b – 512 байт, c – байт, w – 2 байта, k – Кбайт, M – Мбайт, G – Гбайт);
- 7) `-type c` – файл имеет тип c, где c есть b (блочный специальный файл), c (символьный специальный файл), d (каталог), p (именованный канал), f (обычный файл), l (символьная ссылка) или s (сокеты);
- 8) `[-perm] [-]восьмеричное_число` – режим доступа к текущему файлу в точности равен восьмеричному_числу. Если перед восьмеричным_числом указан знак -, то для сравнения из режима файла берутся только биты, соответствующие битам восьмеричного_числа, равным единице;
- 9) `-links n` – на файл имеется n ссылок;
- 10) `-user имя_пользователя` – файл принадлежит пользователю с данным именем. Разрешены цифровые идентификаторы пользователя;
- 11) `-group имя_группы` – файл принадлежит группе с данным именем.
Разрешены цифровые идентификаторы группы.

Критерии можно объединять, используя операторы. Ниже приведены операторы в порядке убывания их приоритета:

- унарная операция отрицания, обозначается ! (! критерий);
- логическое И, обозначается пробелом (критерий1 критерий2);

- логическое ИЛИ, обозначается -o (критерий1-о критерий2).

Когда выполняется команда `find`, можно выполнять различные действия над найденными файлами.

Основные действия:

- 1) `-exec` команда `\;` – выполнить команду. Запись команды должна заканчиваться экранированной точкой с запятой. Строка «`{}`» заменяется текущим маршрутным именем файла;
- 2) `execdir` команда `\;` – то же самое что и `exec`, но команда вызывается из подкаталога, содержащего текущий файл;
- 3) `-ok` команда – эквивалентно `-exec` за исключением того, что перед выполнением команды запрашивается подтверждение (в виде сгенерированной командной строки со знаком вопроса в конце) и она выполняется только при ответе: `y`;
- 4) `-print` – вывод имени файла на экран.

Примеры:

- 1) найти в текущем каталоге обычные файлы (не каталоги), имя которых начинается с символа «`~`»:

```
find . -type f -name "~*" -print
```

- 2) найти в текущем каталоге файлы, измененные позже, чем файл `file.bak`:

```
find . -newer file.bak -type f -print
```

- 3) удалить все файлы с именами `a.out` или `*.o`, доступ к которым не производился в течение недели:

```
find / \( -name a.out -o -name '*.o' \) -atime +7 -exec rm {} \;
```

- 4) удалить из текущего каталога и его подкаталогов все файлы нулевого размера, запрашивая подтверждение:

```
find . -size 0c -ok rm {} \;
```

14.5.2. Команда `whereis`

Команда `whereis` сообщает путь к исполняемому файлу программы, ее исходным файлам (если есть) и соответствующим страницам справочного руководства.

Опции:

- 1) `-b` – вывод информации только об исполняемых файлах;
- 2) `-m` – вывод информации только о страницах справочного руководства;
- 3) `-s` – вывод информации только об исходных файлах.

14.6. Средства архивирования файлов

Команды `tar`, `cpio`, `gzip` представляют собой инструменты создания резервных копий и архивирования ФС.

При создании архива командами `tar` (п. 14.6.1) и `gzip` передается список файлов и каталогов, указываемых как параметры командной строки. Любой указанный каталог просматривается рекурсивно.

При создании архива с помощью команды `cpio` (п. 14.6.2) ей предоставляется список объектов (имена файлов и каталогов, символические имена любых устройств, гнезда доменов UNIX, именованные каналы).

14.6.1. Команда `tar`

Команда `tar` предназначена для преобразования файла или группы файлов в архив без сжатия (`tarfile`).

Синтаксис:

```
tar [Опции] [АРГ]
```

Опции:

- 1) `-c` – создает архив;
- 2) `-x` – восстанавливает файлы из архива на устройстве, заданном по умолчанию или определенном опцией `f`;
- 3) `-f name` – создает (или читает) архив с `name`, где `name` – имя файла или устройства, определенного в `/dev`, например, `/dev/rmt0`;
- 4) `-Z` – сжимает или распаковывает архив с помощью `compress`;
- 5) `-z` – сжимает или распаковывает архив с помощью `gzip`;
- 6) `-M` – создает многотомный архив;
- 7) `-t` – создает список сохраненных в архиве файлов и выводит его на консоль;

8) `-v` – выводит подробную информацию о процессе.

Упаковка файлов в архив чаще всего выполняется следующей командой:

```
tar -cf [имя создаваемого файла архива] [упаковываемые файлы  
и (или) директории]
```

Пример использования команды упаковки архива:

```
$ tar -cf moi_dokumenti.tar Docs project.tex
```

Распаковка содержимого архива в текущий каталог выполняется следующей командой:

```
tar -xf [имя файла архива]
```

Далее приводится пример использования команды распаковки архива:

```
$ tar -xf moi_dokumenti.tar
```

Для сжатия файлов используются специальные программы сжатия: `gzip`, `bzip2` и `7z`.

14.6.2. Команда `cpio`

Команда `cpio` предназначена для копирования файлов. Ее можно использовать с опцией `-o` для создания резервных архивов и с опцией `-i` – для восстановления файлов. Команда получает информацию от стандартного устройства ввода и посылает выводимую информацию на стандартное устройство вывода.

Команда `cpio` может архивировать любой набор файлов и специальные файлы, хранит информацию более эффективно, чем `tar`, пропускает сбойные сектора или блоки при восстановлении данных, и ее архивы могут быть восстановлены в ОС.

Недостатком команды `cpio` является то, что для обновления архива следует использовать язык программирования оболочки, чтобы создать соответствующий сценарий.

Синтаксис:

```
cpio [Опции] < список-имен [> архив]
```

Опции:

1) `-o` – создание архива в стандартное устройство вывода;

2) `-i` – восстановление файлов из архива, передаваемого на стандартное устройство ввода;

3) `-t` – создание списка содержимого стандартного устройства ввода.

Ниже приводятся примеры использования команды `cpio` для решения различных задач.

Копирование файлов из каталога `/home` в архив `home.cpio` выполняется следующим образом:

```
find /home/* | cpio -o > /tmp/home.cpio
```

Восстановление файлов из архива `home.cpio` с сохранением дерева каталогов и создание списка в файле `bkup.index` выполняется следующим образом:

```
cpio -id < /tmp/home.cpio > bkup.index
```

Использование команды `find` для поиска измененных за последние сутки файлов и сохранение их в архив `home.new.cpio` выполняется следующим образом:

```
find /home -mtime 1 -type f | cpio -o > /tmp/home.new.cpio
```

Восстановление файла `/home/dave/notes.txt` из архива `home.cpio` выполняется следующим образом:

```
cpio -id /home/dave/notes.txt < home.cpio
```

Для восстановления файла с помощью `cpio` следует указывать его полное имя.

Все эти команды могут выполняться автоматически путем их размещения в файле `crontab` пользователя с идентификатором `root`.

Пример записи, выполняющей резервное копирование каталога `/home` ежедневно в 01:30:

```
30 02 *** ls /home : cpio -o > /tmp/home.cpio
```

При необходимости выполнения резервного копирования более сложного уровня можно создать соответствующий сценарий оболочки. Запуск подобных сценариев также может быть осуществлен посредством `cron`.

Создание резервных копий означает определение политики создания резервных копий для снижения потерь и восстановления информации после возможной аварии системы.

14.7. Средства редактирования файлов

14.7.1. Текстовый редактор Vi

Текстовый редактор Vi – системный редактор, назначаемый ОС по умолчанию для работы с текстовыми файлами.

Текстовый редактор Vi имеет модальный интерфейс – одни и те же клавиши в разных режимах работы выполняют разные действия.

В редакторе Vi есть несколько режимов работы:

- 1) командный режим – перемещение по файлу, удаление текста и другие редактирующие функции. По умолчанию, работа начинается в командном режиме. Перейти в него из любого другого режима <ESC>, иногда два раза;
- 2) режим ввода – ввод текста (удаление и ввод текста происходит в двух разных режимах). Переход в режим ввода из командного режима осуществляется командой <i>;
- 3) режим строчного редактора ED – это специальный режим, в котором редактору даются сложные команды. При вводе этих команд они отображаются в последней строке экрана. Например, команда <wq> позволяет записать файл и покинуть редактор Vi, а команда <q!> – выйти из редактора Vi без сохранения изменений. В этом режиме обычно вводятся команды, название которых состоит из нескольких символов. Переход в него из командного режима осуществляется командой <:>.

Далее описаны операции, которые можно произвести с файлом в командном режиме.

14.7.1.1. Открыть (создать) файл

Управляющая команда открытия файла выглядит следующим образом:

```
vi <имя_файла>
```

Создание файла происходит при помощи той же команды, поскольку создание файла происходит в момент сохранения.

Для открытия или создания нового файла в командном режиме нужно набрать:

```
:e filename
```

Перед этим нужно сохранить предыдущий файл с помощью следующих команд:

- <:w> – сохраняет файл с существующим именем;
- <:sav filename> – или «Сохранить как».

14.7.1.2. Навигация по файлу

Навигация по файлу происходит с помощью управляющих клавиш на клавиатуре. Также допускается использовать клавиши быстрого перемещения:

- <^> или <0> – в начало текущей строки;
- <\$> – в конец текущей строки;
- <w> – на слово вправо;
- – на слово влево.

14.7.1.3. Редактирование файла

Для редактирования текста нужно перейти в режим ввода (нажать <i>).

Основные команды редактирования:

- <R>, <i> – переход в режим ввода, замена текста под курсором;
- <I> – переход в режим ввода с начала текущей строки;
- <o> – переход в режим ввода с новой строки под курсором;
- <O> – переход в режим ввода с новой строки над курсором;
- <a> – переход в режим ввода после курсора;
- <x> – стирание символа под курсором;
- <X> – стирание символа перед курсором;
- <dd> – стирание текущей строки;
- <d<число>d> – стирание выбранного числа строк, начиная с текущей;
- <y> – копирование текущей строки в неименованный буфер;
- <y<число>y> – копирование выбранного числа строк, начиная с текущей в неименованный буфер;
- <p> – вставка строки из неименованного буфера под курсор;
- <P> – вставка строки из неименованного буфера над курсором;
- <J> – слияние текущей строки со следующей;

- <u> – отмена последней команды;
- <.> – повтор последней команды.

Для перехода в режим строчного редактора ED нужно нажать <Shift>+<:>.

14.7.1.4. Запись в файл и выход из редактора

Запись в файл выполняется следующей командой:

<Esc>:w<Enter>

В случае, если файл заблокирован другим пользователем либо отсутствуют права на запись, нужно использовать следующую команду:

<Esc>:w!<Enter>

При попытке записи без «!» будет выдано соответствующее предупреждение.

Создать новый файл <имя_файла> и записать в него текущее содержимое:

<Esc>:w имя_файла <Enter>

В случае, если файл с таким именем уже существует, редактор выдаст предупреждение. После успешного создания файла и осуществления записи информации в него работа продолжится со старым файлом.

Для выхода из редактора нужно использовать следующую команду:

<Esc>:q<Enter>

В случае, если в файл были внесены изменения, нужно добавлять после команды «!».

Выйти из редактора не сохраняя изменения:

<Esc>:q!<Enter>

Сохранить изменения в файле и выйти:

<Esc>:wq<Enter> или <Esc>ZZ<Enter>.

14.7.1.5. Дополнительные возможности

Текстовый редактор Vi обладает рядом дополнительных возможностей, которые вызываются следующими командами:

- ^G – показать информацию о файле;
- G – перейти в конец файла;
- <number>G – перейти на конкретную строку <number>;
- :<number> – перейти на <number> строк вперед;

- `:set number` – отобразить слева нумерацию строк (`:set nonumber` – спрятать нумерацию);
- `:set wrap` – переносить длинные строки (`:set nowrap` – не переносить);
- `:colorscheme <name>` – задать цветовую тему (где `<name>` имя темы, `TAB` работает как автодополнение);
- `/мама` – поиск текста «мама» в файле;
- `n` – повторить поиск;
- `:h` или `:help` – список возможной помощи (`:viusage`, `:exusage`).

Привести концы строк в файле к виду `dos` или `unix` соответственно:

```
:set fileformat=dos
:set fileformat=unix
```

Задать размер табуляции в четыре пробела:

```
:set ts=4
```

14.7.2. Редактор Vim

Vim – свободный режимный текстовый редактор, созданный на основе Vi.

14.7.2.1. Основной режим работы

Основной режим работы Vim предназначен для просмотра файлов, ввода команд и перехода из него в другие режимы. В командный режим можно попасть по нажатию клавиши `<Esc>`.

При нажатии клавиши «`:`» становится доступна командная строка Vim, в которой вводятся следующие команды:

- команда выхода – `quit` либо `q`;
- команда сохранения – `write` либо `w`, параметром которой может быть имя файла;
- вызов справки – `help` либо `h`.

Для остальных клавиш (и их последовательностей) допускается задавать любые команды либо использовать значения по умолчанию.

Перечисленные ниже команды вводятся в основном режиме (если нет специального уточнения). Все они имеют команднострочные аналоги и могут быть легко переопределены.

14.7.2.2. Визуальный режим работы

Визуальный режим работы предназначен, в первую очередь, для выделения блоков текста. Переход в визуальный режим выполняется с помощью следующих сочетаний клавиш:

- <v> для посимвольного выбора;
- <Shift>+<v> для построчного выбора;
- <Ctrl>+<v> для блочного выбора.

В режиме посимвольного выделения (при переходе по клавише «v») допускается оперировать следующими сущностями:

- слово («w»);
- предложение («s»);
- параграф («p»);
- блок («b»).

Выделение при этом нужно начинать с позиции курсора («a»), или же с начала блока («i»). Например, выделение текущего блока (участка, ограниченного парными элементами) можно произвести следующим образом:

<Esc>vib

Копирование в буфер выделенного текста осуществляется по «u», вырезание по «d» а вставка, соответственно, «r».

14.7.2.3. Режим редактирования

Режим редактирования предназначен для ввода текста. Переключение на режим редактирования осуществляется нажатием клавиши <Insert>.

14.7.2.4. Переходы

Для перехода на строку с номером n используется команда G. Так для перехода к началу текста нужно набрать 1G, для сотой строки 100G, а для перехода в конец текста – \$G.

Для перехода на n символов в нужную сторону используются клавиши навигации на клавиатуре. То есть для перехода на 1000 символов вниз нужно набрать «1000» и нажать клавишу «↓».

Для перемещения по тексту допускается использовать следующие команды:

- «(», «)» – для перемещения по предложениям;
- «{», «}» – для параграфов;
- «[[«, «]]» – для функций;
- «%» – переход к парной скобке;
- «'» – к предыдущему положению;
- <Ctrl>+<O>, <Ctrl>+<I> – соответственно, назад и вперед по истории переходов.

14.7.2.5. Метки

Используются для отметки позиции (<буква>-метка, где меткой является любая буква) и быстрого к ней перехода (<'>-метка). Метки нижнего регистра действительны в пределах данного файла, метки верхнего регистра действуют во всех открытых файлах.

Список всех меток можно получить командой `marks`.

14.7.2.6. Регистры

Регистр отмечается видом <"буква>. К нему применимы все стандартные действия: копирование в него ("<метка>y), вырезание ("<метка>d), и вставка из него ("<метка>p), можете вместо p использовать [p,]p для вставки соответственно перед, или после курсора).

В режиме редактирования вставка из регистра осуществляется по <Ctrl>+R<метка>. Для добавления данных в регистр используйте заглавную метку.

Также допускается писать в регистр, воспользовавшись командой «q<метка>» и завершив запись по q. Таким образом сохраняется макрос, выполнить который можно по «@<метка>».

Регистры с метками «*» и «+» совпадают с X-Window clipboards, «%» – соответствует редактируемому файлу. Для просмотра содержимого всех регистров нужно воспользоваться командой `:registers`, либо `:reg метка1метка2...` для просмотра только выбранных регистров.

14.7.2.7. Фолды

Фолды предназначены для сокрытия строк, ненужных в данный момент.

По умолчанию фолды активированы в режиме ручной расстановки. Все команды для работы с фолдами начинаются с `z`:

- создание фолд выполняется командой `zf`;
- открытие фолд производится командой `zo` либо нажатием навигационной стрелки «→»;
- закрытие кода в существующий фолд – по `zc`.

Для автоматического подключения фолд по отношению к табуляции нужно добавить в файл настроек следующую строку:

```
set foldmethod=indent
```

14.7.2.8. Сессии

Сессии предназначены для сохранения текущего состояния и настройки редактора таким образом, что при следующем запуске работа продолжится с того же места.

Сессии создаются следующей командой:

```
:mksession /path/to/Session.vim
```

Чтение сессий выполняется командой:

```
:so /path/to/Session.vim
```

Для сохранения текущего контекста (текст, положение курсора в коде, текущая расстановка фолдов) нужно использовать команду `:mkview`, а для чтения – `:loadview`.

Автоматическое сохранение и чтение контекста при начале и окончании редактирования файла может быть реализовано следующим кодом (применяется для всех файлов, имеющих точку в имени):

```
au BufWinLeave *.* mkview  
au BufWinEnter *.* silent loadview
```

14.7.2.9. Поиск и замена

Поиск по тексту осуществляется следующими командами:

- `/` – поиск по регулярному выражению вперед;
- `?` – поиск по регулярному выражению в обратном направлении;
- `n` – продолжение поиска далее по тексту;
- `N` – повторение предыдущего запроса;

- # либо * – поиск слова под установленным курсором.

Для поиска с заменой рекомендуется использовать следующую команду:

```
%s/что/на что/gic
```

где % означает работу со всем текстом (а не с текущей строкой), g – глобальная замена (а не первое совпадение), i – игнорирование регистра, а c – подтверждение каждого действия.

14.7.2.10. Автодополнение, отмена, смена регистра, повтор

Автодополнение производится по содержимому данного файла, а также указанных в переменной dictionary по нажатию клавиш ``.

Для отмены предыдущих действий в режиме автодополнения используется u.

Для смены регистра выделенного участка (или буквы под курсором) используется ~. При этом команда U – принудительно устанавливает верхний регистр, а u – нижний.

Для повтора прошлой команды используется символ «.».

14.7.2.11. Конфигурация

Файл конфигурации используется для настройки различных аспектов поведения и внешнего вида Vim. Комментарии в этом файле начинаются с символа «"» (двойная кавычка) и продолжаются до конца строки. Основным конфигурационным файлом является ~/.vimrc.

Активация русского шрифта в GUI-режиме, плюс выбор темы для обоих режимов осуществляется, например, следующим кодом:

```
if has("gui_running")
  colorscheme ron
  set guifont=-cronyx-courier-medium-r-normal-**-120-***-m-*-koi8-r
endif
if !has("gui_running")
  colorscheme elflord
endif
```

В файл конфигурации можно добавить привычное поведение и привычные сочетания клавиш:

```
"Выход по F10
nmap <F10> :q<CR>
imap <F10> <ESC>:q<CR>
"Сохранение по F2
nmap <F2> :w<CR>
```



```
imap <F2> <ESC>:w<CR>i<Right>  
"Компиляция по F9  
nmap <F9> :make<CR>  
imap <F9> <ESC>:make<CR>
```

В Vim присутствует подробная документация по настройкам – `:options`.

14.8. Средства настройки отложенного исполнения команд

14.8.1. Служба `crond`

Для регулярного запуска команд в ОС Альт СП используется служба `crond`.

Служба `crond` запускается при загрузке системы и проверяет очередь заданий `at` и заданий пользователей в файлах `crontab`. При запуске, служба `crond` сначала проверяет каталог `/var/spool/cron` на наличие файлов `crontab`, файлы `crontab` имеют имена пользователей, соответствующие именам пользователей из `/etc/passwd`. Каждый пользователь может иметь только один файл `crontab`, записей в файле может быть несколько.

В случае, если задание не было обнаружено, `crond` переходит в режим ожидания на одну минуту и затем вновь приступает к поискам команды, которую следует запустить в этот момент. Большую часть времени служба `crond` проводит в режиме ожидания, и для ее работы используется минимум системных ресурсов.

Чтобы определить список задач для `cron`, используется команда `crontab`.

14.8.1.1. `Crontab`

Утилита `crontab` управляет доступом пользователя к службе `crond` путем копирования, создания, выдачи содержимого и удаления файлов `crontab`, таблиц заданий. При вызове без опций, `crontab` копирует указанный файл или стандартный входной поток (если файл не указан) в каталог, в котором хранятся пользовательские таблицы заданий `cron`. Каждый пользователь может иметь свои собственные файлы `crontab`, и, хотя эти файлы доступны в `/var/spool/cron`, они не предназначены для редактирования напрямую.

Синтаксис:

```
crontab [имя_файла]  
crontab [ -elr ] имя_пользователя
```

Опции:

- 1) `-e` – редактирует копию файла `crontab` текущего пользователя или создает пустой файл для редактирования, если соответствующего файла `crontab` не существует. Когда редактирование завершается, файл устанавливается в качестве пользовательского файла `crontab`. Переменная среды `EDITOR` задает редактор, вызываемый при указании опции `-e`. Все задания в файле `crontab` должны создаваться с помощью утилиты `crontab`;
- 2) `-l` – отображает текущий файл `crontab` на стандартный вывод;
- 3) `-r` – удаляет текущий файл `crontab`.

14.8.1.2. Контроль доступа к `crontab`

Доступ пользователя к `crontab` разрешен, если:

- имя пользователя указано в файле `/etc/cron.d/cron.allow`;
- файл `/etc/cron.d/cron.allow` не существует и имя пользователя не указано в файле `/etc/cron.d/cron.deny`.

Доступ пользователя к `crontab` не разрешен, если:

- файл `/etc/cron.d/cron.allow` существует и имя пользователя в нем не указано;
- файл `/etc/cron.d/cron.allow` не существует и имя пользователя указано в файле `/etc/cron.d/cron.deny`.

Правила разрешения и запрещения выполнения заданий применимы к пользователю `root`, только если существуют файлы `allow/deny`.

В файлах `allow/deny` надо задавать по одному имени пользователя в строке.

14.8.1.3. Формат записи файла `crontab`

Редактировать `crontab` пользователя можно используя команду:

```
crontab -e
```

Файл `crontab` состоит из строк, содержащие шесть полей. Поля разделяются пробелами или символами табуляции. Первые пять полей – целочисленные шаблоны, задающие:

- минуту (0 – 59);
- час (0 – 23);

- день месяца (1 – 31);
- месяц года (1 – 12);
- день недели (0 – 6, причем 0=воскресенье).

Каждый из этих шаблонов может представлять собой звездочку (которая обозначает все допустимые значения) или список элементов через запятые. Элемент – число или два числа через дефис (что обозначает закрытый интервал). Обратите внимание, что дни можно указывать в двух полях (день месяца и день недели). Оба поля учитываются, если заданы в виде списка элементов (запись: 30 4 1,15 * 5 приведет к выполнению команды в 4:30 пополуночи первого и пятнадцатого числа каждого месяца, плюс в каждую пятницу). При указании диапазона можно пропускать некоторые его значения, указав шаг в форме «/число». Например: «0-23/2» для поля час означает запуск команды через два часа. Шаг можно указывать также после звездочки: «каждые два часа» соответствует значению «*/2». Для задания полей месяц и день_недели можно использовать имена. Указывайте первые три буквы нужного дня или месяца на английском, регистр букв не имеет значения. Диапазоны или списки имен не разрешены.

Служба `crond` запускает команды, когда значения полей минута, час, месяц и хотя бы одно из полей число и день_недели, совпадают с текущим временем. Служба `crond` сверяет директивы с текущим временем раз в минуту.

Вместо первых пяти полей допустимо указание одного из восьми специальных триггеров:

- `@reboot` – выполнить команду один раз, при запуске `crond`;
- `@yearly` – выполнять команду каждое 1 января, «0 0 1 1 *»;
- `@annually` – эквивалентно `@yearly`;
- `@monthly` – выполнять команду в начале каждого месяца, «0 0 1 * *»;
- `@weekly` – выполнять команду каждое воскресенье, «0 0 * * 0»;
- `@daily` – выполнять команду в полночь, «0 0 * * *»;
- `@midnight` – эквивалентно `@daily`;
- `@hourly` – выполнять команду раз в час, «0 * * * *».

Шестое поле в строке файла `crontab` – строка, выполняемая командным интерпретатором в указанные моменты времени. Символ `%` (процент) в этом поле, если он не замаскирован «`\`» (обратной косой), преобразуется в символ новой строки.

Только первая строка (до символа `%` или до конца строки) поля команды выполняется командным интерпретатором. Другие строки передаются команде как стандартный входной поток. Пустые строки, ведущие пробелы и символы табуляции игнорируются. Строки, начинающиеся с символа («`#`») считаются комментариями и игнорируются. Комментарии не допускаются в тех же строках, где расположены команды `cron`, так как они будут распознаны как части команды. По этой же причине комментарии не разрешены в строках, задающих переменные среды.

Строка-директива представляет собой либо задание переменной среды, либо команду `cron`.

Демон `crond` предоставляет каждому командному интерпретатору стандартную среду, задавая переменные `HOME`, `LOGNAME`, `SHELL(=/bin/sh)`, `TZ` и `PATH`. Стандартное значение переменной `PATH` для пользовательских заданий `cron` – `/usr/bin`, а для заданий `cron` пользователя `root` – `/usr/sbin:/usr/bin`.

Если стандартный выходной поток и стандартный поток ошибок команд не перенаправлены, любые сгенерированные результаты или сообщения об ошибках будут отправлены пользователю по электронной почте.

14.8.1.4. Примеры

Далее приведены примеры использования таблиц `crontab` в ходе администрирования ОС Альт СП.

14.8.1.4.1. Пример 1

```
$ crontab -e
#minute (0-59),
#| hour (0-23),
#| | day of the month (1-31),

#| | | month of the year (1-12),
#| | | | day of the week (0-6 with 0=Sunday).
#| | | | | commands
# Каждые 5 минут записывать результат вывода
# команды date в файл date.txt в домашнем каталоге
*/5 * * * * date > ~/date.txt
```

```
# Выполнять задание в 18 часов 7 минут 13 числа
# каждого месяца и по пятницам
7 18 13 * 5 /home/www/myscript.pl
# Выполнять задание по воскресеньям в 10 час 30 минут
30 10 * * 0 /home/www/myscript.pl
crontab: installing new crontab
```

Вывод crontab: installing new crontab означает, что новый crontab успешно установлен.

14.8.1.4.2. Пример 2

```
# использовать для запуска команд /bin/sh
# не обращая внимание на то, что написано в /etc/passwd
SHELL=/bin/sh
# отправлять вывод выполнения команд по электронной
# почте пользователю 'paul'
# не обращая внимания на то, чей это crontab
MAILTO=paul
#
# запускать пять минут пополуночи, каждый день
5 0 * * * $HOME/bin/daily.job >> $HOME/tmp/out 2>&1
# запускать в 14:15 первого числа каждого месяца
15 14 1 * * $HOME/bin/monthly
# запускать в 22.00 каждый рабочий день
0 22 * * 1-5 mail -s "Уже 10 вечера"
23 0-23/2 * * * echo "запуск в 00:23, 2:23, 4:23 ..., каждый день"
5 4 * * sun echo "запуск в 4:05 каждое воскресенье"
```

14.8.1.5. Дополнительные возможности таблиц

Таблицы crontab обладают следующими дополнительными возможностями:

- при задании дня недели 0 и 7 соответствуют воскресенью;
- допускается указывать одновременно и списки, и диапазоны в одном и том же поле;
- допускается указывать диапазоны с пропусками — например, «1-9/2» соответствует «1,3,5,7,9»;
- допустимо указание месяцев или дней недели по имени;
- в crontab разрешено задавать переменные среды вручную;
- вывод команд отсылается почтой владельцу файла crontab, а также может отправляться кому-либо другому, либо отправка может быть отключена (функция не поддерживается в SysV);
- любая из команд с префиксом «@» может заменять первые пять полей файла.

14.8.2. Команда `at`

Для запуска одной или более команд в заранее определенное время используется команда `at`. В ней можно определить время и (или) дату запуска той или иной команды.

Команда `at` требует двух (или большего числа) параметров – как минимум, следует указать время запуска, и какая команда должна быть запущена. Параметры запуска с помощью команды `at` указываются в виде списка строк, следующих за ней. Ввод каждой строки завершается нажатием клавиши `<Enter>`. По окончании ввода всей команды нажать клавиши `<Ctrl>+<D>` для ее завершения.

Например, если нужно запустить команды в 1:23, следует ввести:

```
at 1:23
lpr /usr/sales/reports/.
echo "Files printed"
```

В указанном примере будут распечатаны все файлы каталога `/usr/sales/reports`, и пользователю будет выведено сообщение на экран монитора.

После ввода всей команды отобразится следующая запись:

```
job 756603300.a at Tues Jan 21 01:23:00 2007
```

Это означает, что указанные команды будут запущены, как и было задано, в 1:23. В сообщении также приведен идентификатор задания (756603300.a), который понадобится, если нужно отменить задание:

```
at -d 756603300.a
```

В случае, если список команд находится в файле, например, `getdone`, и нужно запустить все перечисленные в нем команды в 10:00, следует воспользоваться одной из двух форм команды `at`:

```
at 10:00 < getdone либо at 10:00 -f getdone
```

Обе приведенные команды эквивалентны. Разница заключается в том, что в первой команде используется механизм перенаправления потоков ввода-вывода, во второй команде – дисковый файл.

Кроме времени, в команде `at` может быть также определена дата:

```
at 17:00 Jan 24
lp /usr/sales/reports/
echo "Files printed"
```

Задания, определяемые администратором, помещаются в очередь, которую ОС периодически просматривает. Администратору необязательно находиться в системе для того, чтобы `at` отработала задания, команда будет работать в фоновом режиме.

Для того чтобы просмотреть очередь заданий, нужно ввести следующую команду:

```
at -l
```

В случае, если предыдущие примеры были запущены, то будет выведено:

```
job 756603300.a at Sat Dec 20 01:23:00 2007 job 756604200.a at Sat Jan 24  
17:00:00 2008
```

Администратор видит только свои задания по команде `at`.

Для удаления задания из очереди следует запустить `at` с опцией `-d` и номером удаляемого задания следующим образом:

```
at -d 756604200.a
```

Далее представлены варианты использования команды `at`.

Выполнить задание во время `hh:mm` в 24-часовом формате:

```
at hh:mm
```

Выполнить задание во время `hh:mm` в 24-часовом формате в соответствующий день:

```
at hh:mm месяц день год
```

Вывести список заданий в очереди (псевдоним команды — `atq`):

```
at -l
```

Выполнить задание через определенное время, которое задано параметром `count` в соответствующих единицах — неделях, днях, часах или минутах:

```
at now+count time-units
```

Удалить задание с идентификатором `job_ID` из очереди (псевдоним команды — `atrm`):

```
at -d job_ID
```

Администратор может применять все эти команды. Для других пользователей права доступа к команде `at` определяются файлами `/etc/at.allow` и `/etc/at.deny`. В случае, если существует файл `/etc/at.allow`, то применять команду `at` могут только перечисленные в нем пользователи. В случае, если же такого файла нет,

проверяется наличие файла `/etc/at.deny`, в котором отражено, кому запрещено пользоваться командой `at`. Также если ни одного из файлов, описывающих доступ к «alt», нет, то команда `at` доступна только пользователю с идентификатором `root`.

14.8.3. Команда `batch`

Команда `batch` позволяет ОС самой решить, когда наступает подходящий момент для запуска задачи – например, когда система находится в состоянии наименьшей загрузки, и процессы запускаются в фоновом режиме.

Формат команды `batch` представляет собой список заданий для выполнения, следующих в строках за ней, заканчивается список комбинацией клавиш `<Ctrl>+<D>`. Также допускается поместить список команд в файл и перенаправить его на стандартный ввод команды `batch`.

Например, для сортировки набора файлов, печати результатов и вывода сообщения нужно ввести следующие команды:

```
batch
sort /usr/sales/reports ; lp
echo "Files printed"
```

В ответ на это система выдаст:

```
job 7789001234.b at Fri Feb 21 11:43:09 1999
```

Примечание. Дата и время, приведенные в сообщении, соответствуют нажатию клавиш `<Ctrl>+<D>`.

14.9. Control

В дистрибутивах ОС Альт СП для управления доступом к важным службам используется подсистема `control`. `control` – механизм переключения между неким набором фиксированных состояний для задач, допускающих такой набор.

Команда `control` доступна только для суперпользователя (`root`).

Для того чтобы посмотреть, что означает та или иная политика `control` (разрешения выполнения конкретной команды, управляемой `control`), запустите команду с ключом `help`, например:

```
# control su help
public: Any user can execute /bin/su
```


wheel: Any user can execute /bin/su, but only "wheel" group members can switch to superuser

wheelonly: Only "wheel" group members can execute /bin/su

restricted: Only root can execute /bin/su

То есть для управления командой su есть такие политики:

- public – любой пользователь может выполнить команду /bin/su;
- wheel – любой пользователь может выполнить команду su, но только пользователи, входящие в группу wheel, могут получить через нее права root;
- wheelonly – только пользователи, входящие в группу wheel, могут выполнить команду su;
- restricted – только root может выполнять команду su.

Для получения текущего значения control, необходимо выполнить команду:

```
# control <команда>
```

Например:

```
# control fusermount
fuseonly
```

Для переключения состояния control, необходимо выполнить команду:

```
# control <команда> <состояние>
```

Например:

```
# control fusermount public
```

Для переключения состояния control вызывает соответствующий скрипт из /etc/control.d/facilities/.

Запустив control без параметров, можно увидеть полный список команд, управляемых командой (facilities) вместе с их текущим состоянием и набором допустимых состояний.

14.10. Защищенный интерпретатор команд SSH

Защищенный интерпретатор команд SSH – клиент-серверная система для организации защищенных туннелей для удаленного доступа к другим компьютерам.

SSH реализует соединение с удаленным компьютером, которое позволяет защититься от следующих угроз:

- прослушивание данных, передаваемых по этому соединению;

- манипулирование данными на пути от клиента к серверу;
- подмена клиента либо сервера путем манипулирования IP-адресами, DNS либо маршрутизацией.

Для создания защищенного туннеля используется программа ssh.

Инициировать соединение с сервером можно командой:

```
ssh <имя_клиента>@IP_addr
```

где IP_addr – IP-адрес компьютера с запущенной службой sshd.

При использовании идентификации по паролю на сервере должна существовать учетная запись с указанным именем клиента.

Параметры, относящиеся к способу аутентификации, а также все прочие настройки ssh (см. п. 8.9.1) указываются в конфигурационном файле /etc/ssh/ssh_config.

Конфигурационные файлы разбиты на разделы, установки которых относятся к отдельному компьютеру, группе компьютеров или ко всем компьютерам, при этом установки разных разделов могут конфликтовать друг с другом. Предпочтение в данном случае будет отдаваться тому параметру, который указан раньше.

14.11. Средство управления процессами xinetd

Средство управления процессами xinetd (далее – сервер xinetd) выполняет функции управления процессами, которые обеспечивают работу сервисов подключения к локальным и глобальным сетям.

Сервер xinetd представляет собой единственный процесс, который выполняет прослушивание всех портов на наличие запросов от других сервисов, перечисленных в файле конфигурации xinetd.conf (расположен в директории /etc): когда на порт поступает запрос, сервер xinetd запускает соответствующий сервер.

Сервисы, перечисленные в конфигурационном файле сервера xinetd, можно разделить на две группы.

Сервисы из первой группы («multi-threaded») на каждый новый запрос запускают новый серверный процесс.

Для таких сервисов сервер `xinetd` продолжает прослушивать сеть на соответствующем порту, ожидая новых запросов на порождение нового процесса.

В другую группу («single-threaded») включаются сервисы службы, которые в состоянии обрабатывать новые соединения. В ходе работы с ними сервер `xinetd` прекращает обработку новых запросов до тех пор, пока серверный процесс не завершит свою работу. Сервисы в этой группе также обычно относят к группе «datagram-based», работающих с дейтаграммными протоколами передачи данных формата UDP.

Сервер `xinetd` позволяет сохранять системные ресурсы за счет контроля запуска серверных процессов. Полностью соответствуя назначению запускать требуемые сервисы, сервер `xinetd` осуществляет также функции контроля доступа и регистрации событий. Кроме того, сервер `xinetd` не ограничен сервисами, перечисленными в файле `/etc/services`. Также допускается использовать сервер `xinetd` для запуска сервисов специального назначения.

Синтаксис:

```
xinetd [опции]
```

Опции:

- `-d` – активирует режим отладки. Указание этой опции приводит к большому количеству отладочных сообщений, которые делают возможным использование отладчика на `xinetd`;
- `-syslog syslog_facility` – разрешает протоколирование создаваемых `xinetd` сообщений через `syslog` с заданным `syslogfacility`. Поддерживаются следующие имена `facility`: `daemon`, `auth`, `user`, `local[0-7]` (назначение можно посмотреть в `syslog.conf`). Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;
- `-filelog файл_журнала` – сообщения, создаваемые `xinetd` будут помещаться в указанный файл. Сообщения всегда добавляются к уже существующему файлу. Если файл не существует, то он будет создан. Данная опция неэффективна в режиме отладки, так как все сообщения отправляются на терминал;

- `-f файл_настроек` – задает файл, который `xinetd` использует для настройки.
По умолчанию это `/etc/xinetd.conf`;
- `-pidfile pid_файл` – в этот файл записывается идентификатор процесса.
Данная опция неэффективна в режиме отладки;
- `-stayalive` – `xinetd` будет оставаться запущенным, даже если не задано никаких служб;
- `-loop rate` – устанавливает верхнюю величину цикла, по которой определяется, что служба работает с ошибками и по которой она отключается. Величина цикла задается в терминах количества серверов в секунду, которое может быть запущено в обработку (`fork`). Для этой опции, корректное значение определяется скоростью вашей машины. По умолчанию равно 10;
- `-reuse` – `xinetd` будет устанавливать опцию сокета `SO_REUSEADDR` перед привязкой сокета службы к какому-либо интернет-адресу. Это позволяет привязать адрес, даже если есть программа, которая уже использует его, например, в том случае, если некоторые серверы были запущены во время предыдущего запуска `xinetd` и еще не завершили свою работу. Данная опция не оказывает влияния на службу RPC;
- `-limit proc_limit` – устанавливает ограничение на количество одновременно запущенных процессов, которые может запустить `xinetd`. Ее назначение предотвращать переполнение таблицы процессов;
- `-logprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов на один идентификатор удаленного пользователя;
- `-shutdownprocs limit` – устанавливает ограничение на количество одновременно запущенных серверов для завершения работы службы;
- `-version` – вывести информацию о версии `xinetd`;
- `-cc interval` – `xinetd` будет выполнять периодические проверки своего внутреннего состояния каждые `interval` секунд.

Опции `syslog` и `filelog` являются взаимноисключающими. Если ни одна из них не задана, то по умолчанию используется `syslog` с `daemonfacility`. Не путайте сообщения `xinetd` с сообщениями, которые создаются службами. Последние протоколируются только если это задано в файле с настройками.

Сервер `xinetd` выполняет определенные действия при получении определенных сигналов. Действия, ассоциированные с соответствующими сигналами, могут быть переопределены путем редактирования `config.h` и последующей компиляции.

Сигналы:

- `SIGHUP` – заставляет выполнить жесткую перенастройку, означающую, что `xinetd` перечитает файл с настройками и завершит работу серверов для тех служб, которые больше не доступны. Управление доступом выполняется снова на уже запущенных серверах через проверку удаленных подключений, времени доступа и копий серверов. Если количество копий серверов уменьшается, то некоторые произвольно выбранные сервера будут убиты, чтобы соблюсти ограничение; это случится после завершения работы тех серверов, которые попадают под ограничение доступа с удаленных адресов или ограничение времени доступа. Также, если флаг `INTERCEPT` был сброшен и происходит его установка, то будет завершена работа любых запущенных серверов для служб с этим флагом. Цель такого поведения – убедиться, что после жесткой перенастройки не будет запущено серверов, которые могут принимать пакеты с тех адресов, которые не соответствуют критериями управления доступом;
- `SIGQUIT` – приводит к завершению работы;
- `SIGTERM` – завершает работу всех запущенных серверов перед завершением работы `xinetd`;
- `SIGUSR1` – приводит к снятию дампа внутреннего состояния (по умолчанию файл дампа это `/var/run/xinetd.dump`; чтобы изменить данное имя файла нужна правка `config.h` и перекомпиляция);

- SIGIOT – производит внутреннюю проверку того, что структуры данных, используемые программой не повреждены. Когда проверка завершится, xinetd сгенерирует сообщение о том, успешно прошла проверка или нет.

При реконфигурации файлы журналов закрываются и вновь открываются. Это позволяет удалять старые файлы журналов.

14.12. Работа со смарт-картами

Для настройки работы со смарт-картами нужно установить дополнительные пакеты:

- 1) синхронизировать файлы описаний пакетов с источником пакетов, выполнив команду:

```
# apt-get update
```

- 2) установить пакеты для поддержки программно-аппаратного комплекса электронно-цифровой подписи и хранения ключевой информации «RUTOKEN», выполнив команду:

```
# apt-get install opensc pcsc-lite pam_pkcs11 librtpkcs11ecp
pcsc-lite-ccid libp11 nss-utils lightdm-gtk-greeter
```

14.12.1. Двухфакторная аутентификация

На токене должны присутствовать ключевая пара и сертификат.

Для генерирования ключевой пары на токене и создания самоподписанного сертификата, используя openssl, нужно выполнить следующие действия (путь зависит от архитектуры, в примере для x86_64):

- 1) запустить сервис поддержки смарт-карт, выполнив команду:

```
# systemctl start pcscd
```

- 2) сгенерировать ключевую пару, выполнив команду:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen
--key-type rsa:2048 -l --id 45
```

- 3) сгенерировать сертификат в формате PEM:

```
# openssl
OpenSSL> engine dynamic -pre
SO_PATH:/usr/lib64/openssl/engines-*/libpkcs11.so -pre ID:pkcs11 -
pre LIST_ADD:1 -pre LOAD -pre
MODULE_PATH:/usr/lib64/librtpkcs11ecp.so
```

где engines-* - текущая версия модулей openssl;

4) конвертировать сертификат из формата PEM в формат CRT:

```
OpenSSL> x509 -in CA.pem -out cert.crt -outform DER
```

5) сохранить сертификат на аутентифицирующий носитель:

```
# pkcs11-tool --module /usr/lib64/librtppkcs11ecp.so -l -y cert  
-w cert.crt --id 45
```

Для настройки двухфакторной аутентификации нужно выполнить следующие действия:

1) отредактировать файл /etc/security/pam_pkcs11/pam_pkcs11.conf для установки аутентификации по «RUTOKEN» следующим образом:

- закомментировать строку # use_pkcs11_module = opensc;

и добавить строку use_pkcs11_module = rutoken;:

```
# use_pkcs11_module = opensc;  
use_pkcs11_module = rutoken;
```

- после строки use_pkcs11_module = rutoken; добавить модуль rutoken:

```
use_pkcs11_module = rutoken;  
pkcs11_module rutoken {  
  ca_dir = /etc/security/pam_pkcs11/cacerts;  
  crl_dir = /etc/security/pam_pkcs11/crls;  
  module = /usr/lib64/librtppkcs11ecp.so;  
  cert_policy = subject;  
  description = "Rutoken ECP";  
  slot_description = "none";  
}
```

2) включить сервисы поддержки смарт-карт, выполнив команды:

```
# systemctl enable pcscd  
# systemctl start pcscd
```

3) включить системную аутентификацию по смарт-картам в графическом интерфейсе, выполнив команду:

```
# control system-auth pkcs11
```

4) добавить информацию об удостоверяющем центре на машину (файл о сертификате создан в начальных условиях):

```
cp CA.pem /etc/security/pam_pkcs11/cacerts/  
certutil -A -n 'Root CA' -t 'CT,C,C' -a -d /etc/pki/nssdb/ -i  
./CA.pem
```

5) добавить информацию о сертификате в домашний каталог пользователя:

```
mkdir /home/user/.eid/  
cat CA.pem > /home/user/.eid/authorized_certificates
```

б) для возможности аутентификации по сертификату в консоли нужно в файл

`/etc/pam.d/login` вначале добавить строку:

```
auth [success=done authinfo_unavail=ignore ignore=ignore  
default=die] pam_pkcs11.so
```

14.13. Поддержка файловых систем

Файловая система представляет собой набор правил, определяющих то, как хранятся и извлекаются документы, хранящиеся на устройстве.

В ОС Альт СП поддерживаются следующие файловые системы:

- ext2 – нежурналируемая файловая система; относительно проста в восстановлении, но нуждается в относительно долгой проверке целостности после сбоя питания или ядра. Может использоваться для `/boot` или `readonly`-разделов;
- ext3 – журналируемая и достаточно надежная файловая система, имеет среднюю производительность;
- ext4 – журналируемая файловая система, логическое продолжение ext3, позволяет полностью отключить журналирование;
- btrfs – поддерживает снимки (копии файловой системы на определенный момент времени), сжатие и подтома;
- iso9660 – файловая система ISO 9660 для дисков с данными компакт-дисков.

Файловые системы FAT/FAT32/NTFS поддерживаются в установленной системе, но не для установки на них Linux.

Проверка поддержки файловых систем ext2, ext3, ext4, iso9660, fat16, fat32, ntfs:

1) создать раздел объемом менее 4 Гбайт на flash-накопителе (например, `/dev/vdc1`).

2) для создания ISO-файла установить пакет `genisoimage`:

```
# apt-get install genisoimage
```

3) создать каталог `/mnt/filesystem`, в который будет монтироваться раздел:

```
# mkdir /mnt/filesystem
```


4) отформатировать раздел в проверяемую файловую систему:

- для ext2:

```
# mkfs.ext2 /dev/vdc1
```

- для ext3:

```
# mkfs.ext3 /dev/vdc1
```

- для ext4:

```
# mkfs.ext4 /dev/vdc1
```

- для fat16:

```
# mkfs.fat -F 16 /dev/vdc1
```

- для fat32:

```
# mkfs.fat -F 32 /dev/vdc1
```

- для ntfs:

```
# mkfs.ntfs /dev/vdc1
```

- для iso9660 – создать iso-файл из каталога /etc:

```
# mkisofs -r -jcharset koi8-r -o /root/cd.iso /etc
```

5) для проверки поддержки файловых систем ext2, ext3, ext4, fat16, fat32, ntfs:

- примонтировать раздел с файловой системой в каталог /mnt/filesystem:

```
# mount /dev/vdc1 /mnt/filesystem
```

- проверить возможность записи файла на текущую файловую систему:

```
# echo test_content > /mnt/filesystem/test.fs
```

- проверить командой:

```
# ls -l /mnt/filesystem/test.fs
```

```
-rw-r--r--.  1  root  root   13   май   23   20:10  
/mnt/filesystem/test.fs
```

- проверить возможность чтения файла с текущей файловой системой:

```
# cat /mnt/filesystem/test.fs
```

6) для проверки поддержки файловой системы iso9660 смонтировать созданный ISO-файл в каталог /mnt/filesystem/ (файл образа диска будет примонтирован в режиме «только для чтения»):

```
# mount -o loop,ro /root/cd.iso /mnt/filesystem/
```

Примечание. Для просмотра файловых систем на физических дисках можно воспользоваться командой `df`:

```
$ df -Th | grep "^/dev"
```

или `lsblk`:

```
$ lsblk -f
```

Команда `fsck` позволяет узнать файловую систему раздела, который еще не примонтирован:

```
# fsck -N /dev/sdc1
```

```
fsck из util-linux 2.39.2
```

```
[/sbin/fsck.ext4 (1) -- /dev/sdc1] fsck.ext4 /dev/sdc1
```

14.14. Поддержка сетевых протоколов

14.14.1. SMB

Samba – пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных ОС по протоколу SMB/CIFS. Имеет клиентскую и серверную части.

14.14.1.1. Настройка Samba

Samba настраивается с помощью конфигурационного файла `/etc/samba/smb.conf`.

Примечание. После редактирования файла `smb.conf`, следует запускать команду `testparm` для проверки файла на синтаксические ошибки.

14.14.1.1.1. Добавление пользователя

Samba использует отдельную от системной базу данных пользователей. Для возможности доступа пользователя к папке (если запрещен гостевой доступ) необходимо внести его в базу данных Samba и установить пароль для доступа к общим ресурсам (он может совпадать с основным паролем пользователя). Следует учитывать, что в базу данных Samba можно добавлять только тех пользователей, которые уже есть в системе.

Добавить пользователя в базу данных Samba можно, выполнив команду:

```
# smbpasswd -a <имя_пользователя>
```

Можно создать отдельного пользователя, которому разрешить только доступ к Samba-ресурсам и запретить полноценный вход в систему:

```
# useradd user_samba -d /dev/null -s /sbin/nologin
```

```
# smbpasswd -a user_samba
```

14.14.1.1.2. Создание ресурсов общего доступа

Создать папку `sharefolder`, для общих ресурсов:

```
# mkdir /mnt/sharefolder
```

Назначить нового владельца:

```
# chown -R user_samba:users /mnt/sharefolder
```

```
# chmod -R ugo+rwX /mnt/sharefolder
```

Добавить в конфигурационный файл сервера Samba `/etc/samba/smb.conf`

строки:

```
[public]
    #путь к общей папке
    path=/mnt/sharefolder
    read only=No
    #открыть гостевой доступ
    guest ok=Yes
    comment = Public
```

Перезапустить службу:

```
# systemctl restart smb
```

```
# systemctl restart nmb
```

14.14.1.1.3. Создание ресурсов общего доступа от имени обычного пользователя

Пользователи могут добавлять, изменять и удалять собственные ресурсы общего доступа. Эта возможность называется `usershares` и предоставляется службой Samba.

Чтобы предоставить общий доступ к папке, нужно в контекстном меню папки выбрать пункт «Опции публикации», затем в открывшемся окне отметить пункт «Опубликовать эту папку», настроить параметры публикации (рис. 193) и нажать кнопку «Создать публикацию».

Примечание. Домашняя папка пользователя по умолчанию не отображается в списке доступных общих ресурсов в сетевом окружении. Обращение к домашней папке выполняется по имени пользователя. Например, для получения доступа к домашней папке пользователя `user` на компьютере с IP-адресом `192.168.0.190`, необходимо указать в адресной строке `smb://192.168.0.190/user`. Для возможности получения доступа к домашней папке по сети, необходимо добавить каждого локального пользователя в список пользователей Samba.

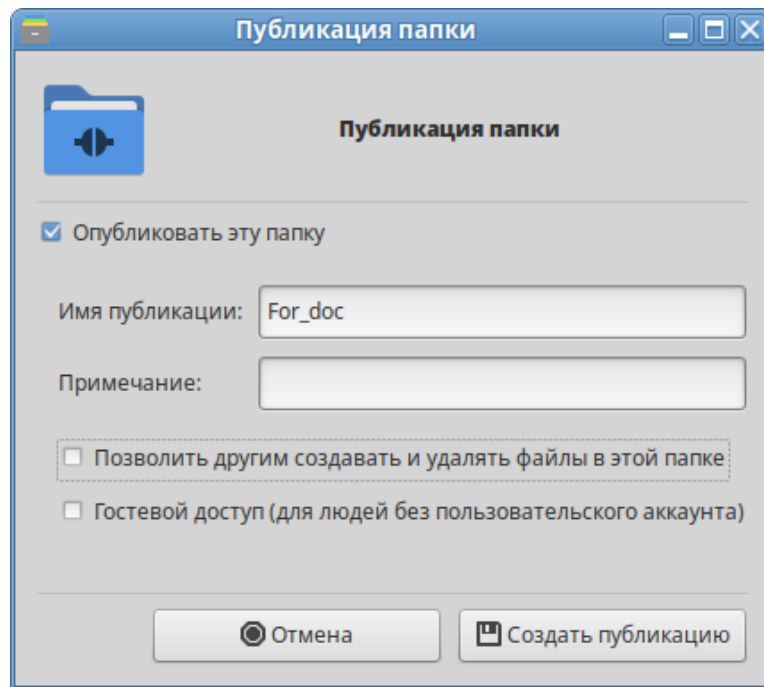


Рис. 193 – Разрешить общий доступ к папке

14.14.1.2. Настройка клиента

14.14.1.2.1. Подключение по протоколу SMB в графической среде

Для создания подключения по протоколу SMB в графической среде MATE можно, запустить файловый менеджер, указать в адресной строке протокол и адрес сервера (рис. 194). Нажать клавишу <Enter>. Будут показаны ресурсы с общим доступом (рис. 195). Для доступа к папке, необходимо указать имя пользователя, пароль и нажать кнопку «Подключиться» (рис. 196).

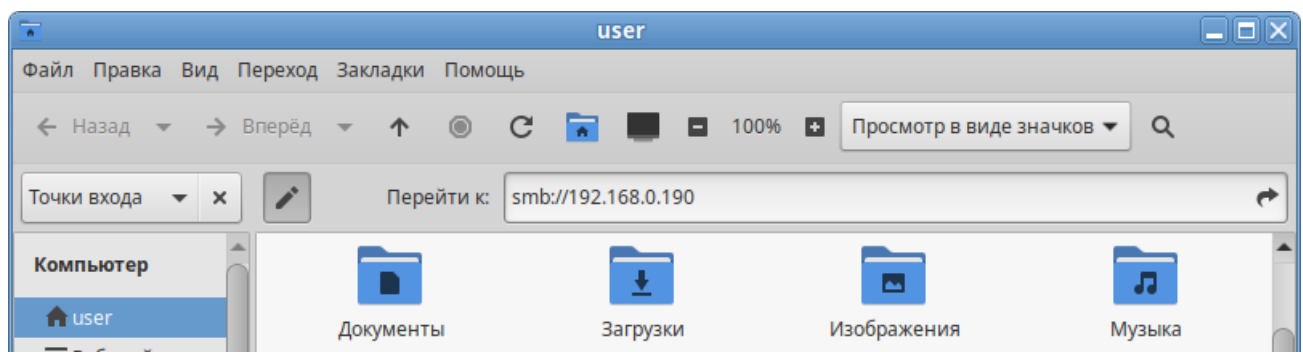


Рис. 194 – Обращение к общей папке по сети

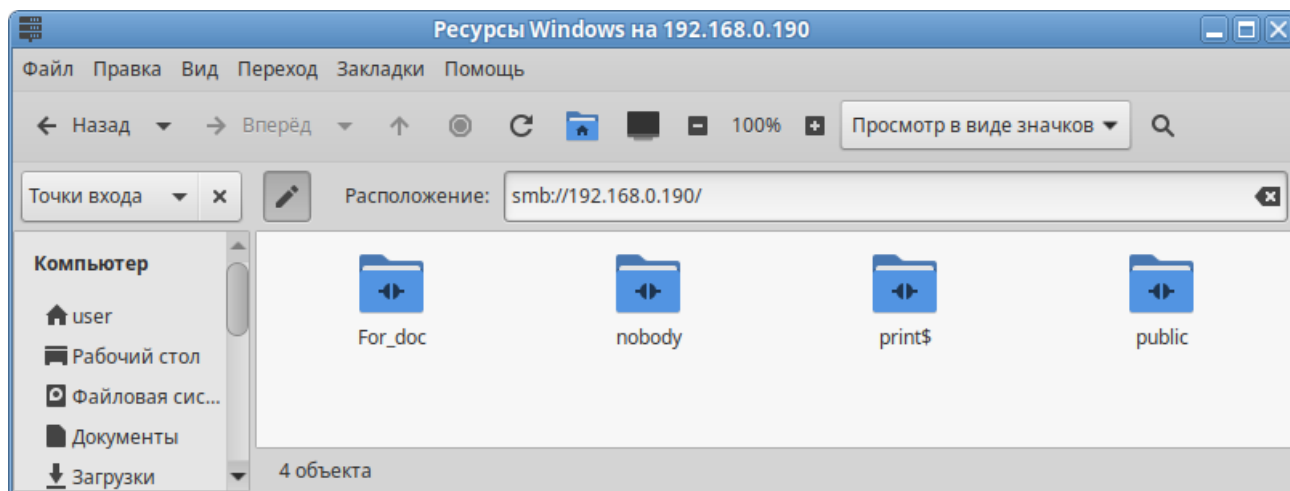


Рис. 195 – Создание подключения по протоколу SMB

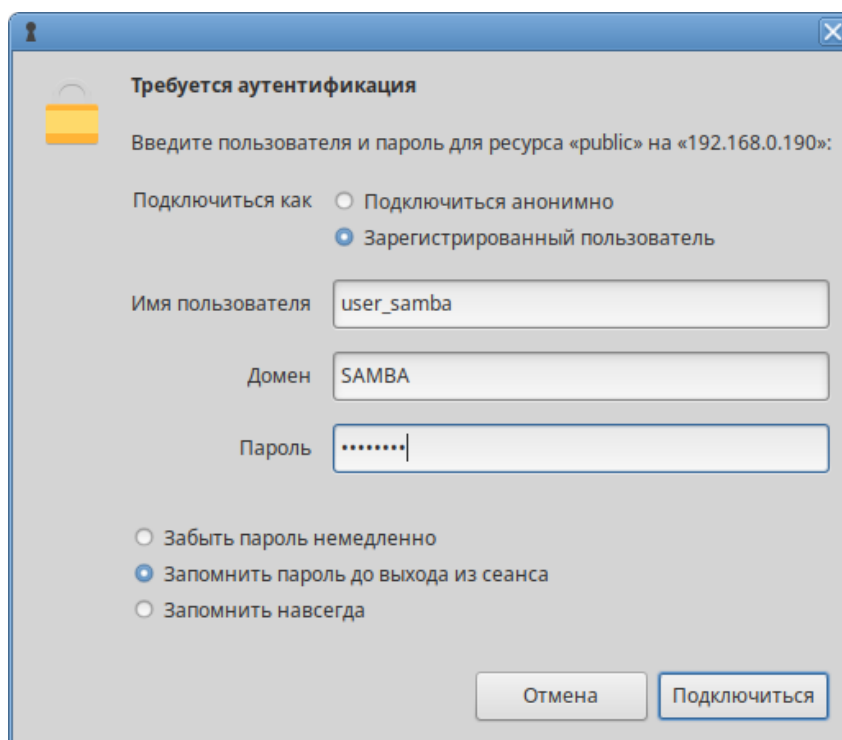


Рис. 196 – Параметры подключения к общей папке

14.14.1.2.2. Монтирование ресурса Samba через /etc/fstab

Просмотреть список общедоступных ресурсов на сервере:

```
$ smbclient -L 192.168.0.190 -U%
```

Просмотреть список ресурсов на сервере доступных пользователю user_samba:

```
$ smbclient -L 192.168.0.190 -Uuser_samba
```

```
Password for [SAMBA\user_samba]:
```

Sharename	Type	Comment

```

-----
print$      Disk      Printer Drivers
public      Disk      Public
IPC$        IPC       IPC Service (Samba 4.19.7-alt4)
For_doc     Disk
user_samba  Disk      Home Directories
SMB1 disabled -- no workgroup available

```

Создать файл `/etc/samba/smbacreds` с содержимым:

```

username=имя_пользователя
password=пароль

```

Для защиты информации, права на файл `/etc/samba/smbacreds`, надо установить так, чтобы файл был доступен на чтение и запись только пользователю-владельцу файла:

```
# chmod 600 /etc/samba/smbacreds
```

и принадлежать `root`:

```
# chown root: /etc/samba/smbacreds
```

Для монтирования ресурса Samba в `/etc/fstab` необходимо прописать, строку вида:

```

//СЕРВЕР/ИМЯ_РЕСУРСА      /mnt/точка_монтирования      cifs
credentials=/путь/к/полномочиям/smbacreds 0 0

```

Например:

```

//192.168.0.190/public  /mnt/server_public  cifs  users,_netdev,x-
systemd.automount,credentials=/etc/samba/smbacreds 0 0

```

14.14.2. NFS

14.14.2.1. Настройка сервера NFS

П р и м е ч а н и е . Должен быть установлен пакет `nfs-server`:

```
# apt-get install nfs-server
```

Запустить NFS-сервер и включить его по умолчанию:

```
# systemctl enable --now nfs
```

В файле `/etc/exports` следует указать экспортируемые каталоги (каталоги, которые будет разрешено монтировать с других машин):

```
/mysharedir ipaddr1(rw)
```

Например, чтобы разрешить монтировать каталог `/home` на сервере необходимо добавить в `/etc/exports` строку:

```
/home 192.168.0.0/24 (no_subtree_check,rw)
```

где:

- `192.168.0.0/24` – разрешение экспорта для подсети `192.168.0.X`;
- `rw` – разрешены чтение и запись.

Подробную информацию о формате файла можно посмотреть, выполнив команду:

```
$ man exports
```

После внесения изменений в файл `/etc/exports` необходимо выполнить команду:

```
# exportfs -r
```

Проверить список экспортируемых файловых систем можно, выполнив команду:

```
# exportfs
/home          192.168.0.0/24
/srv/public    <world>
```

14.14.2.2. Использование NFS

Подключение к NFS-серверу можно производить как вручную, так и настроив автоматическое подключение при загрузке.

Для ручного монтирования:

- создать точку монтирования:

```
# mkdir /mnt/nfs
```

- примонтировать файловую систему:

```
# mount -t nfs 192.168.0.193:/home /mnt/nfs
```

где:

- `192.168.0.193` – IP-адрес сервера NFS;
 - `/mnt/nfs` – локальный каталог, куда монтируется удаленный каталог.
- проверить наличие файлов в `/mnt/nfs`:

```
# ls -al /mnt/nfs
```

Должен отобразиться список файлов каталога `/home`, расположенного на сервере NFS.

Для автоматического монтирования к NFS-серверу при загрузке, необходимо добавить следующую строку в файл `/etc/fstab`:

```
192.168.0.193:/home /mnt/nfs nfs
intr,soft,nolock,_netdev,x-systemd.automount 0 0
```

Примечание. Прежде чем изменять `/etc/fstab`, необходимо смонтировать каталог вручную, для того чтобы убедиться, что все работает.

14.14.3. NTP

14.14.3.1. Настройка сервера NTP

В качестве NTP-сервера/клиента используется сервер времени `chrony`:

- `chronyd` – демон, работающий в фоновом режиме. Он получает информацию о разнице системных часов и часов внешнего сервера времени и корректирует локальное время. Демон реализует протокол NTP и может выступать в качестве клиента или сервера;
- `chronus` – утилита командной строки для контроля и мониторинга программы. Утилита используется для тонкой настройки различных параметров демона, например, позволяет добавлять или удалять серверы времени.

Выполнить настройку NTP-сервера можно следующими способами:

- 1) в ЦУС настроить модуль «Дата и время» на получение точного времени с NTP-сервера (см. п. 8.6.7);
- 2) указать серверы NTP в директиве `server` или `pool` в файле конфигурации NTP `/etc/chrony.conf`:

```
allow all #Разрешить NTP-клиенту доступ из локальной сети
pool pool.ntp.org iburst #параметр iburst используется для
ускорения начальной синхронизации
```

- 3) и перезапустить сервис командой:

```
# systemctl restart chronyd
```

Убедиться в нормальной работе NTP-сервера, выполнив команду:

```
# systemctl status chronyd.service
```


14.14.3.2. Настройка рабочей станции

Настроить в ЦУС модуль «Дата и время» на получение точного времени с NTP-сервера (в качестве NTP-сервера указать IP-адрес сервера NTP) и нажать на кнопку «Применить» (рис. 197).

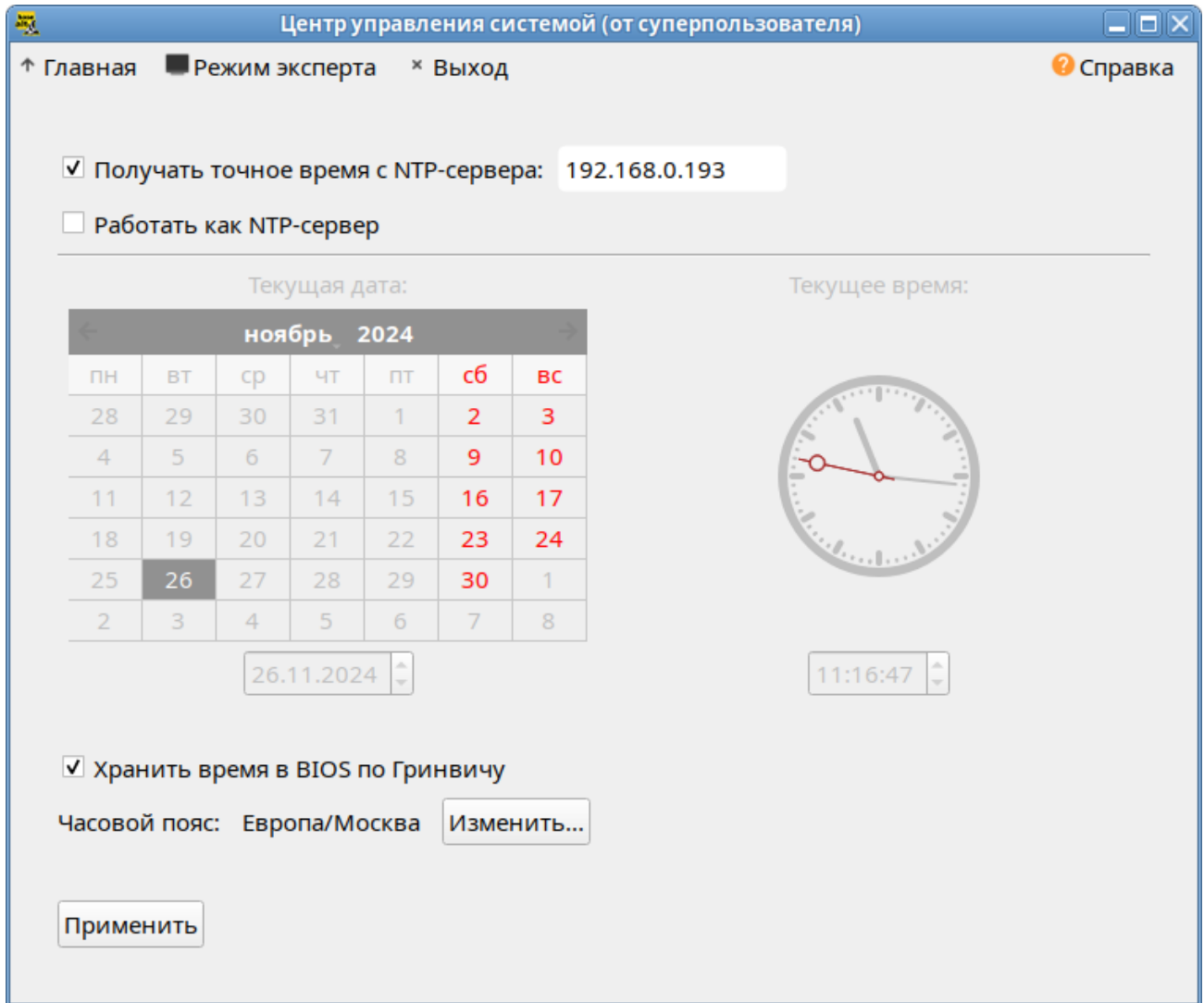


Рис. 197 – Настройка модуля «Дата и время» на рабочей станции

Проверить текущие источники времени:

```
$ chronyc sources
```

```
MS Name/IP address    Stratum Poll Reach LastRx Last sample
=====
^? 192.168.0.193      0  6    0    -    +0ns[  +0ns] +/-  0ns
```

Проверить статус источников NTP:

```
$ chronyc activity
```

```
200 OK
1 sources online
0 sources offline
```

```
0 sources doing burst (return to online)
0 sources doing burst (return to offline)
0 sources with unknown address
```

14.14.4. HTTP(S)

14.14.4.1. Настройка HTTP-сервера

Установить пакет `apache2-base`:

```
# apt-get install apache2-base
```

Запустить `httpd2`:

```
# systemctl start httpd2
```

Убедиться, что служба `httpd2` запущена:

```
# systemctl status httpd2
```

Создать стартовую страницу для веб-сервера:

```
# echo "Hello, World" >/var/www/html/index.html
```

14.14.4.2. Проверка настройки на рабочей станции

Запустить веб-браузер, перейти по адресу `http://<IP-сервера>:>` (рис. 198).

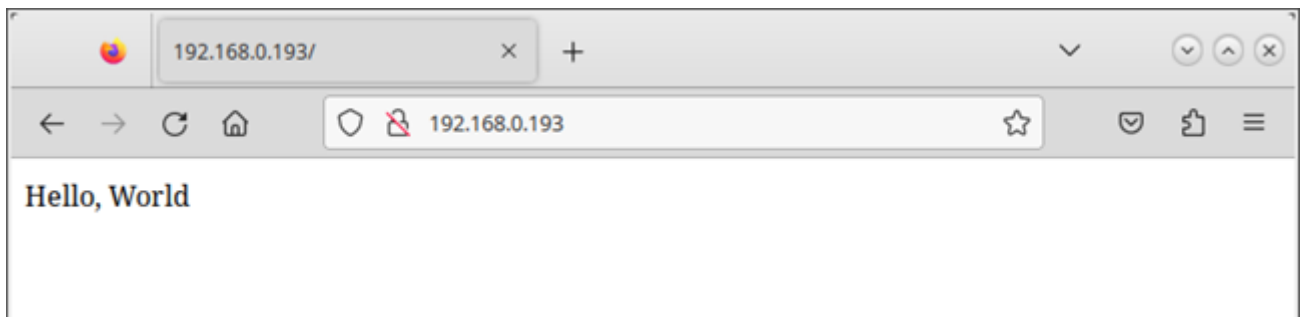


Рис. 198 – Обращение к серверу и получение данных по протоколу http

Можно также выполнить команду:

```
$ curl http://192.168.0.193
Hello, World
```

Происходит обращение к серверу и получение данных по протоколу http.

14.15. Управление печатью

В ОС Альт СП используется система печати CUPS, которая позволяет выполнять следующие действия:

- управляет заданиями на печать;
- исполняет административные команды;

- предоставляет информацию о состоянии принтеров локальным и удаленным программам;
- информирует пользователей, если это требуется.

Система печати CUPS решает задачу монопольной постановки задания в очередь на печать. Данная функция предполагает невозможность вывода документа на печать в обход системы печати.

Существует два способа настройки принтера:

- утилита «Настройка принтера» (пакет `system-config-printer`);
- веб-интерфейс CUPS (Common UNIX Printing System) (пакет `cups`).

14.15.1. Устройство CUPS

В состав файлов конфигурации CUPS входят следующие файлы:

- файл конфигурации сервера CUPS (`/etc/cups/cupsd.conf`);
- файлы определения принтеров и классов (`/etc/cups/printers.conf`, `/etc/cups/classes.conf`);
- файлы типа MIME и файлы правил преобразования;
- файлы описания PostScript-принтеров (PPD).

14.15.1.1. Файл конфигурации сервера CUPS

Конфигурационный файл сервера очень похож на файлы конфигурации веб-сервера и определяет все свойства управления доступом. Настраивать CUPS можно либо непосредственно редактируя файл конфигурации `/etc/cups/cupsd.conf`, либо в веб-интерфейсе CUPS (рис. 199).

Веб-интерфейс CUPS можно запустить следующими способами:

- в графической среде MATE: выбрать на панели инструментов MATE «Меню» → «Приложения» → «Системные» → «Настройка печати»;
- в веб-браузере: `http://localhost:631`.

Если файл `cupsd.conf` редактируется в консоли для применения изменений, нужно перезапустить службу `cups`, выполнив команду:

```
# systemctl restart cups
```

Если файл `cupsd.conf` редактируется в веб-интерфейсе, то служба `cups` автоматически перезапускается после нажатия на кнопку «Сохранить изменения».

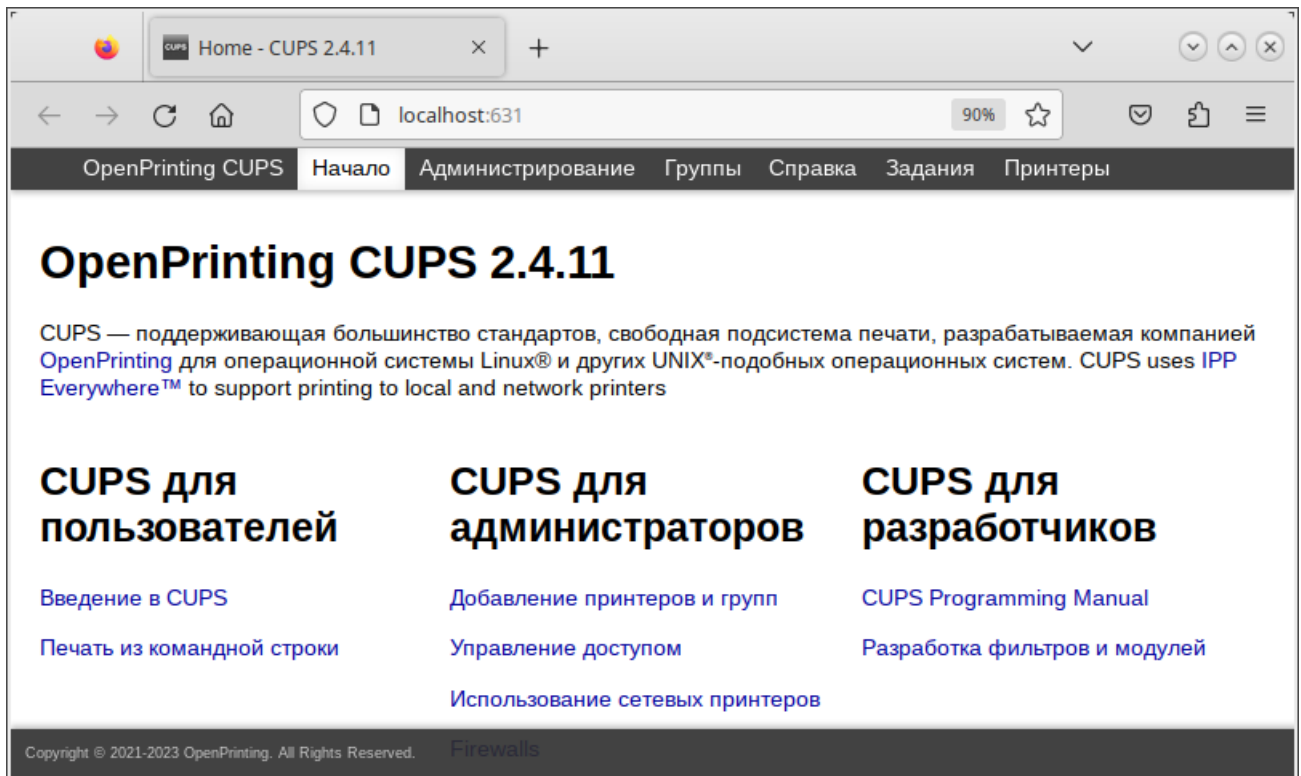


Рис. 199 – Веб-интерфейс CUPS

Файл конфигурации `cupsd.conf` начинается с ряда глобальных директив, которые оформлены в виде пар имя – значение.

`LogLevel` указывает подробность журналирования. Доступные значения: `none` (не записывать логи), `emerg`, `alert`, `crit`, `error`, `warn` (по умолчанию), `notice`, `info`, `debug`, `debug2` (подробный вывод).

`PageLogFormat` определяет формат строк журнала печати (файл `/var/log/cups/page_log`). Последовательности, начинающиеся со знака процента (%), заменяются соответствующей информацией:

- % {name} – значение указанного атрибута IPP;
- % C – количество копий для текущей страницы;
- % P – номер текущей страницы;
- % T – текущую дату и время в общий формат журнала;
- % j – идентификатор задания;
- % p – имя принтера;
- % u – имя пользователя.

По умолчанию строка `PageLogFormat` пустая (журнал печати не пишется). Для ведения журнала печати можно изменить эту строку:

```
PageLogFormat "%p %u %j %T %P %C %{job-billing}
%{job-originating-host-name} %{job-name} %{media} %{sides}"
```

`MaxLogSize` задает максимальный размер журналов до их ротации. Значение 0 отключает ротацию.

`Listen` позволяет указать, на каком IP-адресе будет доступен веб-интерфейс (по умолчанию `localhost:631`), а также прослушиваемый сокет.

Параметры `Browsing` задают настройки возможности 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. `Browsing` — указывает CUPS предоставлять свои серверы в общий доступ, либо нет. Значения может принимать `Yes` или `No` соответственно.

Директива `DefaultAuthType` указывает механизм аутентификации, который будет использоваться для организации доступа (по умолчанию `Basic` — использовать логины/пароли от локальной системы).

`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.

Директива `Order` определяет порядок предоставления доступа к CUPS по умолчанию. Значение `allow,deny` определяет что доступ запрещен, если право на доступ не указано явно. Если директива имеет значение `deny,allow`, то доступ будет разрешен, если явно не запрещен.

Далее идут параметры, сгруппированные в разделы `<Location /...>`. Такие директивы определяют доступ к определенным функциям сервера:

- `<Location />` – доступ к серверу;
- `<Location /admin>` – доступ к странице администрирования;
- `<Location /admin/conf>` – доступ к конфигурационным файлам;
- `<Location /jobs>` – доступ к заданиям;
- `<Location /printer>` – доступ к принтерам.

14.15.1.2. Управление политиками операций

Политики операций – это правила, используемые для каждой операции IPP в CUPS. Правила могут включать такие опции, как «пользователь должен предоставить пароль», «пользователь должен находиться в системной группе», «разрешать только из локальной системы» и т. д.

CUPS позволяет полностью переопределить правила для каждой операции и (или) принтера. Каждая политика имеет название и определяет правила контроля доступа для каждой операции IPP.

Политики операций используются для всех запросов IPP, отправленных в планировщик заданий, и оцениваются после правил управления доступом на основе местоположения. Таким образом, политики операций могут только добавлять дополнительные ограничения безопасности к запросу, а не ослаблять их. Для ограничений на уровне сервера нужно использовать правила управления доступом на основе местоположения, а для ограничений на отдельные принтеры, задачи или службы – политики операций.

Политики хранятся в файле `cupsd.conf` в разделах `Policy`. Каждая политика имеет название, которое используется для ее выбора. Внутри раздела политики находятся один или несколько подразделов `Limit`, в которых перечислены операции, на которые влияют правила внутри него.

Каждая политика имеет название. В названии политики можно использовать те же символы, что и в названии принтера, в частности все печатные символы, кроме пробела, слэша (/) и решетки (#).

В разделах < Limit ...> определяется, какие ограничения должна содержать политика. Директивы внутри подраздела Limit могут использовать любую из директив ограничения: Allow, AuthType, Deny, Encryption, Require и Satisfy. В таблице 15 перечислены основные примеры для разных правил контроля доступа.

Т а б л и ц а 15 – Правила контроля доступа

Уровень доступа	Директива
Разрешить всем	Order allow,deny Allow from all
Разрешить всем в локальной сети	Order allow,deny Allow from @LOCAL
Запретить всем/Отклонить операции	Order allow,deny
Требовать аутентификацию пользователя (Логин, Пароль)	AuthType Basic
Требовать CUPS аутентификацию CUPS (lppasswd) Password	AuthType BasicDigest
Требовать Kerberos	AuthType Negotiate
Только владелец	Require user @OWNER
Только администратор	Require user @SYSTEM
Члены группы foogroup	Require user @foogroup
Пользователи test или test1	Require user test test1
Требовать шифрование	Encryption Required

Пример политики, которая разрешает доступ только из подсети 10.110.1.x:

```
<Policy mypolicy>
# Операции, связанные с заданиями доступны только владельцам
# членам группы lab999 и администратору...
  <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job
Purge-Jobs      Set-Job-Attributes      Create-Job-Subscription      Renew-
Subscription    Cancel-Subscription    Get-Notifications    Reprocess-Job
Cancel-Current-Job  Suspend-Current-Job  Resume-Job      Cancel-My-Jobs
Close-Job CUPS-Move-Job>
    Require user @OWNER @lab999 @SYSTEM
    Order allow,deny
    Allow from 10.110.1.0/24
  </Limit>

# Все административные операции доступны только администратору
и членам группы lab999, также необходима процедура аутентификации...
  <Limit Pause-Printer Resume-Printer Set-Printer-Attributes
Enable-Printer      Disable-Printer      Pause-Printer-After-Current-Job
Hold-New-Jobs Release- Held-New-Jobs      Deactivate-Printer      Activate-
Printer Restart-Printer Shutdown-Printer Startup-Printer Promote-Job
Schedule-Job-After CUPS- Accept-Jobs CUPS-Reject-Jobs CUPS-Set-Default>
    AuthType Default
    Require user @lab999 @SYSTEM
```

```
Order allow,deny
Allow from 10.110.1.0/24
</Limit>
```

Все остальные операции доступны из подсети 10.110.1.0/24 с обязательной аутентификацией пользователей...

```
<Limit All>
AuthType Default
Order allow,deny
Allow from 10.110.1.0/24
</Limit>
</Policy>
```

После создания политики ее можно использовать двумя способами.

Первый способ – назначить ее в качестве политики по умолчанию для всей системы, используя директиву `DefaultPolicy` в файле `cupsd.conf`. Например:

```
DefaultPolicy mypolicy
```

Второй способ – связать политику с одним или несколькими принтерами. Для этого можно воспользоваться командой `lpadmin` (8) или веб-интерфейсом для изменения политики операций для каждого принтера. Например:

```
# lpadmin -p HP_LaserJet_M1536dnf_MFP -o printer-op-policy=mypolicy
```

14.15.1.3. Файлы описания принтеров и классов

Файлы описания принтеров и классов перечисляют доступные очереди печати и классы. Классы принтеров – наборы принтеров. Задания, посланные классу принтеров, направляются к первому доступному принтеру данного класса. Для редактирования файлов `/etc/cups/printers.conf` и `/etc/cups/classes.conf` можно использовать утилиту `lpadmin`.

Пример настройки для локального принтера:

```
<DefaultPrinter laserjet>
UUID urn:uuid:7efaaede-819d-3d9a-6270-3fe957597756
Info laserjet
Location host-15.localdomain
MakeModel HP LaserJet m1537dnf MFP pcl3, hpcups 3.19.1
DeviceURI
usb://HP/LaserJet%20M1536dnf%20MFP?serial=00CND9D8YC9C&interface=1
State Idle
StateTime 1553167952
ConfigTime 1553167952
Type 36892
Accepting Yes # принтер принимает задания
```



```
Shared Yes
JobSheets none none
QuotaPeriod 0
PageLimit 0
KLimit 0
OpPolicy default
ErrorPolicy stop-printer # остановить принтер при ошибке
Option job-hold-until indefinite
</DefaultPrinter>
```

14.15.1.4. Очередь печати

Очередь печати – механизм, который позволяет буферизовать и организовать задания, посылаемые на принтер. Необходимость организации такого механизма обуславливается тем, что принтер является медленно действующим устройством, и задания не могут быть распечатаны мгновенно.

Очевидно, что в многопользовательской среде возникает конкуренция со стороны пользователей при доступе к принтерам, поэтому задания нужно располагать в очереди. Для этого используется буферный каталог `/var/spool/cups/`.

Файлы типов MIME перечисляют поддерживаемые MIME-типы (`text/plain`, `application/postscript`) и правила для автоматического обнаружения формата файла. Они используются сервером для определения поля `Content-Type` для GET- и HEAD-запросов и обработчиком запросов протоколов сетевой печати IPP (Internet Printing Protocol), чтобы определить тип файла.

Правила преобразования MIME перечисляют доступные фильтры. Фильтры используются, когда задание направляется на печать, таким образом, приложение может послать файл удобного (для него) формата системе печати, которая затем преобразует документ в требуемый печатный формат. Каждый фильтр имеет относительную «стоимость», связанную с ним, и алгоритм фильтрации выбирает набор фильтров, который преобразует файл в требуемый формат с наименьшей общей «стоимостью».

Файлы PPD описывают возможности всех типов принтеров. Для каждого принтера имеется один PPD-файл. Файлы PPD для не-PostScript-принтеров определяют дополнительные фильтры посредством атрибута cupsFilter для поддержки драйверов принтеров.

В ОС стандартным языком описания страниц является язык PostScript. Большинство прикладных программ (редакторы, веб-браузеры) генерируют программы печати на этом языке.

Когда нужно напечатать ASCII-текст, программа печати может быть ASCII-текстом. Имеется возможность управления размером шрифтов при печати ASCII-текста.

Управляющая информация используется для контроля доступа пользователя к принтеру и аудита печати. Также имеется возможность печати изображений в форматах GIF, JPEG, PNG, TIFF и документов в формате PDF.

Фильтр – программа, которая читает из стандартного входного потока или из файла, если указано его имя. Все фильтры поддерживают общий набор опций, включающий имя принтера, идентификатор задания, имя пользователя, имя задания, число копий и опции задания. Весь вывод направляется в стандартный выходной поток.

Фильтры предоставлены для многих форматов файлов и включают, в частности, фильтры файлов изображения и растровые фильтры PostScript, которые поддерживают принтеры, не относящиеся к типу PostScript. Иногда несколько фильтров запускаются параллельно для получения требуемого формата на выходе.

Программа backend – это специальный фильтр, который отправляет печатаемые данные устройству или через сетевое соединение. В состав системы печати включены фильтры для поддержки устройств, подключаемых с помощью параллельного и последовательного интерфейсов, а также шины USB.

Клиентские программы используются для управления заданиями и сервером печати.

Управление заданиями включает выполнение следующих действий:

- формирование;
- передачу серверу печати;
- мониторинг и управление заданиями в очереди на печать.

Управление сервером включает выполнение следующих действий:

- запуск/остановку сервера печати;
- запрещение/разрешение постановки заданий в очередь;
- запрещение/разрешение вывода заданий на принтер.

Основные пользовательские настройки содержатся в файлах конфигурации

`client.conf` и `~/.cups/lpoptions`.

Для удаленного использования сервера печати нужно от имени пользователя с идентификатором `root` выполнить следующие команды:

```
cupscctl --remote-admin --remote-printers --remote-any  
cupscctl ServerAlias=*
```

В случае использования сервера печати в едином пользовательском пространстве (далее – ЕПП) нужно задание соответствующего типа аутентификации: для работы в ЕПП значение параметра должно быть `DefaultAuthType Negotiate`, без использования ЕПП значение параметра должно быть `DefaultAuthType Basic`.

В файле конфигурации клиента `client.conf` должен быть задан один параметр `ServerName`, определяющий имя сервера печати, например:

```
ServerName computer.domain
```

В общем случае вывод данных на принтер происходит следующим образом:

- 1) программа формирует запрос на печать задания к серверу печати;
- 2) сервер печати принимает подлежащие печати данные, формирует в буферном каталоге файлы с содержимым задания и файлы описания задания, при этом задание попадает в соответствующую очередь печати;
- 3) сервер печати просматривает очереди печати для незанятых принтеров, находит в них задания и запускает конвейер процессов, состоящий из фильтров и заканчивающийся выходным буфером, информация из которого поступает в принтер посредством драйверов ОС;

4) контроль и мониторинг процесса печати выполняется с помощью программ `lpq`, `lpc`, `lprm`, `lpstat`, `lpmove`, `cancel`.

14.15.2. Установка принтера

Перед началом установки нужно убедиться в том, что в случае локального подключения принтер присоединен к соответствующему порту компьютера и включен, а в случае сетевого подключения принтер корректно сконфигурирован для работы в сети.

Окно «Настройки принтера» можно запустить следующими способами:

- в графической среде: выбрать на панели инструментов МАТЕ «Меню» → «Приложения» → «Администрирование» → «Параметры печати»;
- из командной строки: командой `system-config-printer`.

Примечание. Если возникает ошибка «Служба печати недоступна», следует нажать кнопку «Запустить службу». Потребуется ввести пароль пользователя `root`.

Можно также в терминале от имени системного администратора `root` выполнить команду:

```
# systemctl restart cups
```

После этого следует вернуться к окну «Настройки принтера» и нажать на кнопку «Обновить».

Для добавления принтера в диалоговом окне «Настройки принтера» нужно нажать кнопку «Добавить» (рис. 200).

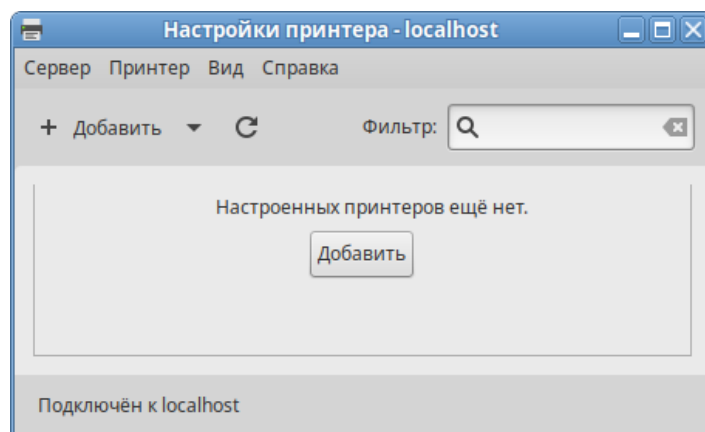


Рис. 200 – Настройки принтера

Далее в открывшемся окне нужно нажать на кнопку «Добавить» и выбрать принтер, который нужно подключить и нажать на кнопку «Далее» (рис. 201).

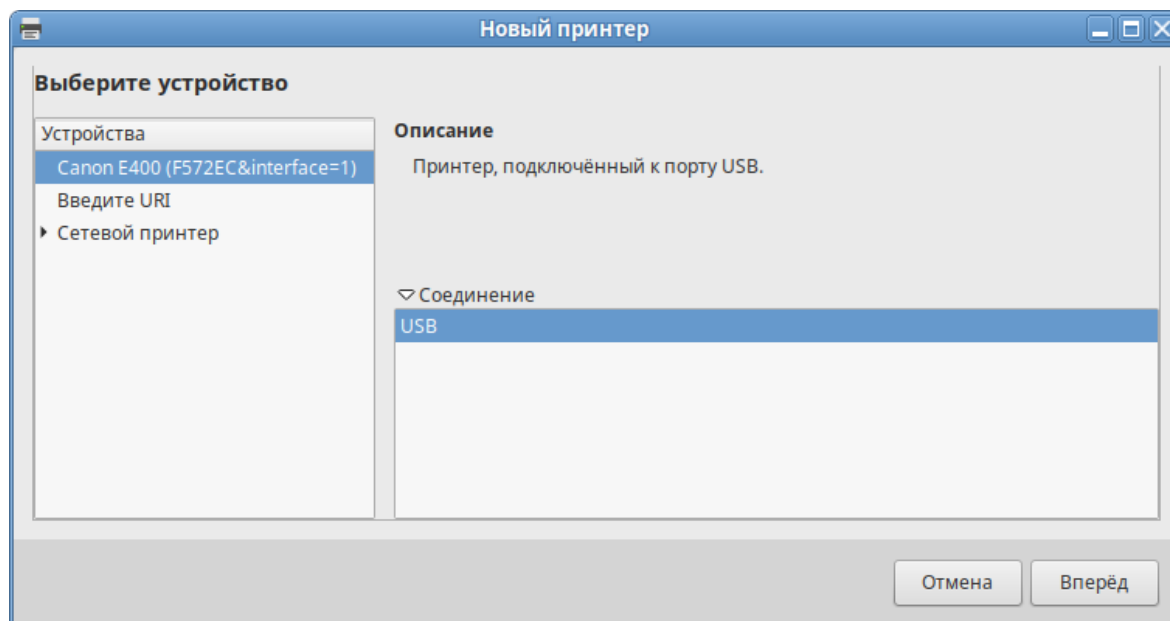


Рис. 201 – Выбор принтера

На следующих шагах настройки принтера нужно выбрать драйвер для принтера. Драйвер можно выбрать из базы данных, содержащей различные файлы описания принтеров (PPD-файлы) от производителей или предоставить файл описания PostScript-принтера (рис. 202).

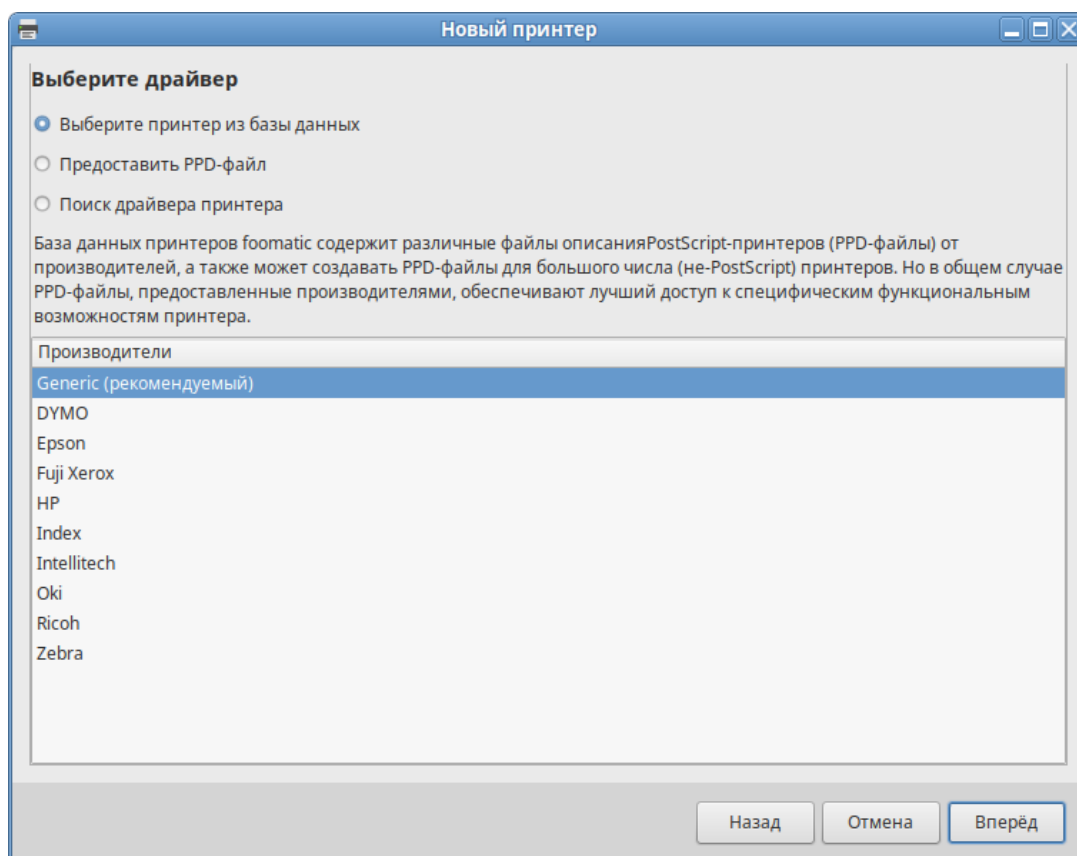


Рис. 202 – Выбор источника драйвера принтера

После выбора драйвера в окне «Новый принтер» можно изменить название и описание принтера (рис. 203).

После нажатия кнопки «Применить» установка принтера завершена, принтер станет доступным для печати (рис. 204).

Изменить настройки принтера (разрешение, размер используемой по умолчанию бумаги, принтер по умолчанию и т. д.) можно в любой момент, выбрав в контекстном меню принтера пункт «Свойства».

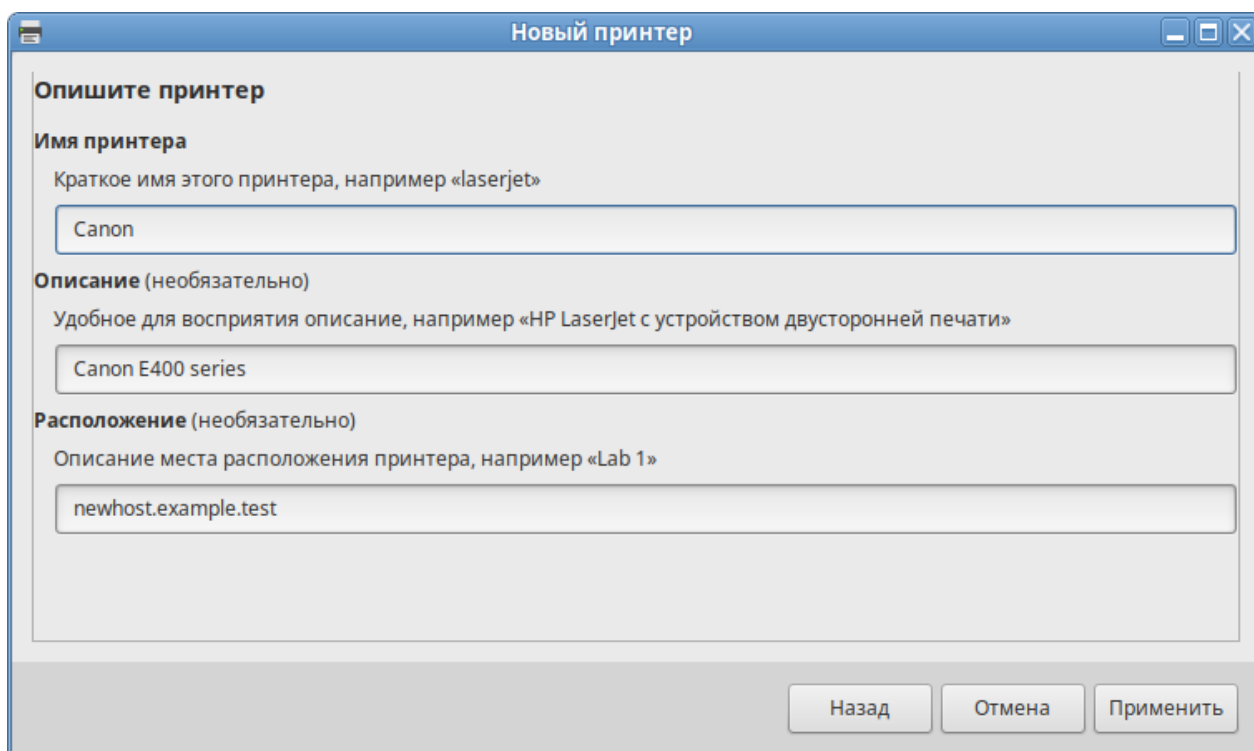


Рис. 203 – Название и описание принтера

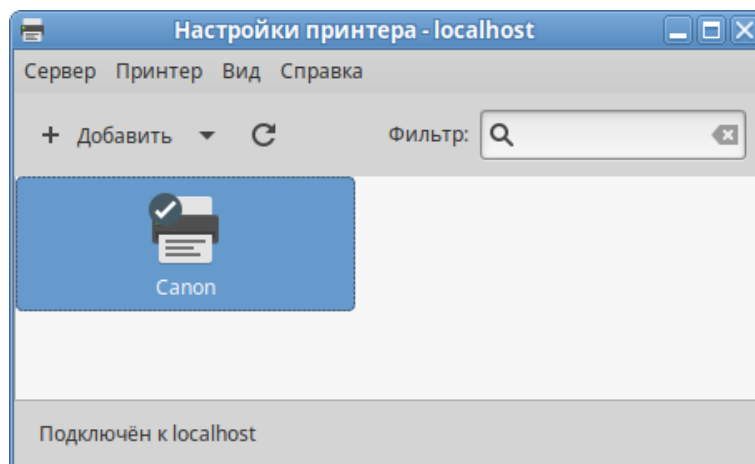


Рис. 204 – Выбор принтера

14.15.3. Настройка сервера печати для сети

Если в сети имеются несколько принтеров или, когда принтеры не подключены непосредственно к тому компьютеру, на котором работает главный сервер CUPS, то целесообразно настроить сервер cupsd, так, чтобы он мог принимать задания на печать из сети.

По умолчанию сервер CUPS работает с локально установленными принтерами, для того, чтобы он мог обрабатывать задания из сети, в конфигурационный файл `/etc/cups/cupsd.conf` нужно внести следующие изменения:

- разрешить доступ к серверу – добавить в секцию Location директиву

```
Allow from:
<Location />
    Order allow,deny
    Allow localhost
    Allow from ip-address/netmask
</Location>
```

- включить отображение (обнаружение) общего принтера:

```
Browsing On
BrowseOrder allow,deny
BrowseAllow 192.168.1.* #локальная сеть
BrowseAddress 192.168.1.*:631#локальная сеть
```

Примечание. Включить отображение (обнаружение) общего принтера можно также отметив пункт «Разрешить совместный доступ к принтерам, подключенным к этой системе» в веб-интерфейсе на вкладке «Администрирование».

После внесения изменений нужно перезапустить службу cups:

```
# systemctl restart cups
```

На клиентах также должен быть установлен CUPS. После установки системы печати на клиенте, CUPS-принтеры, присутствующие в сети, автоматически находятся менеджерами принтеров. В качестве альтернативы, можно воспользоваться веб-интерфейсом CUPS на клиентской машине по адресу `http://localhost:631`. Если принтер не был обнаружен автоматически, введите IPP или HTTP-адрес (URI) сетевого CUPS принтера:

```
ipp://server-name-or-ip/printers/printername
или
http://server-name-or-ip:631/printers/printername
```

Если CUPS клиент не находит в сети принтеры, доступные через сервер CUPS, то иногда может помочь создание или изменение файла `/usr/local/etc/cups/client.conf` с добавлением записи, подобной следующей:

```
ServerName server-ip
```

В этом случае `server-ip` нужно заменить на IP-адрес сервера CUPS в сети.

14.15.4. Команды управления печатью

При печати через локальный сервер печати данные сначала формируются на локальном сервере, как для любой другой задачи печати, после чего посылаются на принтер, подключенный к данному компьютеру.

Вся информация, которая требуется для драйвера принтера (используемое физическое устройство, удаленный компьютер и принтер для удаленной печати), содержится в файлах `/etc/cups/printers.conf` и `/etc/cups/ppd/<имя_очереди>.ppd`.

Примечание. Далее термин «принтер» в этом разделе используется для обозначения принтера, соответствующего одной записи в файле `/etc/cups/printers.conf`. Под термином «физический принтер» подразумевается устройство, с помощью которого производится печать на бумаге. В файле `/etc/cups/printers.conf` может быть несколько записей, описывающих один физический принтер различными способами.

В системе печати CUPS приняты следующие команды для управления печатью:

- `/usr/bin/lpr` – постановка заданий в очередь, совместима с командой `lpr` системы печати BSD UNIX;
- `/usr/bin/lp` – постановка заданий в очередь, совместима с командой `lp` системы печати System V UNIX;
- `/usr/bin/lpq` – просмотр очередей печати;
- `/usr/sbin/lpc` – управление принтером, является частичной реализацией команды `lpc` системы печати BSD UNIX;
- `/usr/bin/lprm` – отмена заданий, поставленных в очередь на печать;
- `/usr/sbin/cupsd` – сервер печати;
- `/usr/sbin/lpadmin` – настройка принтеров и классов принтеров;

- `/usr/sbin/lpmove` – перемещение задания в другую очередь;
- `/usr/bin/fly-admin-printer` – настройка системы печати, установка и настройка принтеров, управление заданиями.

CUPS предоставляет утилиты командной строки для отправления заданий и проверки состояния принтера. Команды `lpstat` и `lpc status` также показывают сетевые принтеры (принтер@сервер), когда разрешен обзор принтеров.

С помощью команды `lp` выполняется передача задачи принтеру, то есть задача ставится в очередь на печать. В результате выполнения этой команды файл передается серверу печати, который помещает его в каталог `/var/spool/cups/`.

Остановить работу сервиса печати можно с помощью команды:

```
# systemctl stop cups
```

Запустить сервис печати можно с помощью команды:

```
# systemctl start cups
```

14.15.4.1. Настройка принтера

Настроить принтер в ОС можно также с помощью команды `lpadmin`. Ее запуск с опцией `-p` выполняется для добавления или модификации принтера:

```
/usr/sbin/lpadmin -p printer [опции]
```

Для `lpadmin` существуют также опции по регулированию политики лимитов и ограничений по использованию принтеров и политики доступа к принтерам.

Для удаления принтера нужно выполнить `lpadmin` с опцией `-x`:

```
/usr/sbin/lpadmin -x printer
```

14.15.4.2. Проверка очереди печати

Команда `lpq` предназначена для проверки очереди печати (используемой `lpd`) и вывода состояния заданий на печать, указанных при помощи номера задания, либо системного идентификатора пользователя, которому принадлежит задание.

`lpq` выводит для каждого задания имя его владельца, текущий приоритет задания, номер задания и размер задания в байтах, без параметров выводит состояние всех заданий в очереди.

14.15.4.3. Удаление задания из очереди печати

Команда `lprm` предназначена для удаления задания из очереди печати. Для определения номера задания нужно использовать команду `lpq`. Для удаления задания нужно быть его владельцем или пользователем с идентификатором `root`.

Системные каталоги, определяющие работу системы печати ОС, также содержат файлы, которые не являются исполняемыми:

- `/etc/cups/printers.conf` – содержит описания принтеров в ОС;
- `/etc/cups/ppd/<имя_очереди>.ppd` – содержит описания возможностей принтера, которые используются при печати заданий и при настройке принтеров;
- `/var/log/cups/error_log` – содержит протокол работы принтера, в этом файле могут находиться сообщения об ошибках сервера печати или других программ системы печати;
- `/var/log/cups/access_log` – содержит все запросы к серверу печати;
- `/var/log/cups/page_log` – содержит сообщения, подтверждающие успешную обработку страниц задания фильтрами и принтером.

14.15.4.4. Настройка сетевого принтера из консоли

Для настройки принтера из консоли нужно выполнить следующие действия:

- 1) получить права администратора;
- 2) просмотреть содержимое каталога `model` на наличие драйверов:

```
ls /usr/share/cups/model
```

Примечание. Для работы с дополнительными драйверами доступных устройств установите пакет `printer-driver-splix`.

- 3) если драйвер устройства присутствует перейти к шагу 7) (настройка нового устройства);
- 4) найти нужное устройство:

```
lpinfo -m | grep название_модели
```

- 5) просмотреть данные о драйвере устройства:

```
foomatic-ppdfilter -A | grep название_модели
```

6) сформировать файл .ppd:

```
foomatic-ppdfile -p 'имя_ppd_драйвера' >
/usr/share/cups/model/имя_ppd_файла.ppd
```

7) произвести настройку нового устройства:

- если принтер подключен по сети:

```
lpadmin -p название_принтера -D еще_одно_название -m
название_ppd_файла.ppd -v socket://ip_принтера -E
```

- если принтер подключен по USB:

```
lpadmin -p название_принтера -D еще_одно_название -m
название_ppd_файла.ppd -v "usb://адрес_принтера" -E
```

8) печать документа:

```
lp -d название_принтера /путь_документ
```

Примечание. Список доступных устройств можно просмотреть, выполнив команду: `lpinfo -v`

Пример вывода:

```
usb://Samsung/M262x%20282x%20Series?serial=ZD1UBJCD5000LVW
```

Список установленных принтеров: `lpstat -p -d`

Пример настройки сетевого принтера Kyocera Ecosys P2235dn:

1) получить права администратора;

2) просмотреть содержимое каталога `/usr/share/cups/model` на наличие драйверов:

```
ls /usr/share/cups/model
```

3) если драйвер устройства присутствует произвести настройку нового устройства (перейти к шагу 7));

4) найти нужное устройство:

```
lpinfo -m | grep Kyocera-P-2
```

5) просмотреть данные о драйвере устройства:

```
foomatic-ppdfile -A | grep Kyocera-P-2
```

6) сформировать файл .ppd:

```
foomatic-ppdfile -p 'Kyocera-P-2000' >
/usr/share/cups/model/Kyocera.ppd
```

7) создать новое устройство:

```
lpadmin -p Kyocera -D Kyocera-P-2000 -m Kyocera.ppd -v
socket://10.120.70.90 -E
```

14.16. Организация терминального доступа XRDP

Для организации и реализации терминального доступа для обработки информации в ОС Альт СП возможно использование XRDP (Remote Desktop Protocol). Программа предоставляет рабочий стол X, обеспечивает графический вход с использованием протокола удаленного рабочего стола RDP. XRDP поддерживает удаленное управление графикой, двустороннюю передачу буфера обмена, перенаправление звука, диска. Передача RDP шифруется с использованием TLS по умолчанию.

14.16.1. Базовая настройка сервера терминалов

Примечание. В настройках сети сервера должен быть указан способ получения IP-адреса: «Вручную», указаны статические настройки сети: IP-адрес, маска, шлюз.

Для настройки сервера терминалов нужно установить пакет `xrdp`:

```
# apt-get install xrdp
```

Включить и добавить в автозагрузку сервисы:

```
# systemctl enable --now xrdp xrdp-sesman
```

Рекомендуется отключить эффекты рабочего стола. Это можно сделать, установив пакет `mate-reduced-resource`.

14.16.2. Настройка сервера

Параметры настройки сервера хранятся в файле `/etc/xrdp/sesman.ini`. Файл конфигурации содержит разделы:

- «Globals» – определяет некоторые глобальные параметры конфигурации;
- «Security» – определяет параметры безопасности;
- «Sessions» – определяет параметры подключения, управление сеансами;
- «Session» definitions – определяет поддерживаемые типы сеансов. Конфигурация каждого типа сеанса определяется как отдельный раздел по имени типа сеанса Xorg, Xvnc;
- «Logging» – определяет параметры подсистемы логирования;
- «Chansrv» – определяет параметры подключения диска, которые поддерживает RDP.

Некоторые настройки сервера, установленные по умолчанию:

- `ListenPort=3389` — порт, который прослушивает `xrdp-sesman` (если настроен межсетевой экран нужно включить этот порт в разрешенные);
- `TerminalServerUsers=tsusers` — группа, в которую нужно добавить пользователей для организации доступа к серверу. Данная группа создается локально при установке сервера, если рассматривать доменную авторизацию, то нужно внести изменения в файл конфигурации `/etc/sss/sss.conf` и в настройках `sesman.ini` вместо локальной группы указать доменную;
- `TerminalServerAdmins=tsadmins` — группа, в которую нужно добавить пользователей для организации административного доступа к серверу;
- `MaxLoginRetry=4` — максимальное количество попыток подключения;
- `MaxSessions=50` — максимальное количество подключений к серверу;
- `KillDisconnected=false` — разрыв сеанса при отключении пользователя;
- `AllowRootLogin=false (true/false)` — управление авторизацией под учетной записью `root`;
- `FuseMountName=thinclient_drivers` — название монтируемого каталога.

Конфигурацию сервера возможно настроить в соответствии с требованиями безопасности.

14.16.3. Настройки доступа пользователей

Для доступа к терминальному сеансу пользователь должен быть включен в группу `tsusers`:

```
# gpasswd -a <пользователь> tsusers
```

Для разрешения монтирования папки пользователь должен быть включен в группу `fuse`:

```
# gpasswd -a <пользователь> fuse
```

14.16.4. Подключение звука

Для возможности прослушивания звука из терминального сеанса локально нужно установить на терминальный сервер пакет `pulseaudio-module-xrdp`:

```
# apt-get install pulseaudio-module-xrdp
```

14.16.5. Подключение USB-устройств

Для организации инфраструктуры перенаправления USB-устройств на сеанс сервера XRDP нужно установить пакет `xrdp-usb`, который состоит из двух пакетов:

- терминальный сервер – `xrdp-usb-session`;
- терминальный клиент – `xrdp-usb-terminal`.

Пакет `xrdp-usb-session` позволяет добавлять подключение разрешенных администратором USB-устройств с клиента.

Установка пакета `xrdp-usb-session` на сервер:

```
# apt-get install xrdp-usb-session
```

Перезапустить службу `xrdp-sesman`:

```
# systemctl restart xrdp-sesman.service
```

Выполнить настройку клиента:

1) установить пакет `xrdp-usb-terminal`:

```
# apt-get install xrdp-usb-terminal
```

2) добавить пользователя клиентского компьютера в группу `disk`:

```
# gpasswd -a <пользователь> disk
```

3) перезагрузить систему (чтобы загрузились все модули и запустилась служба `usbipd`);

4) убедиться, что служба `usbipd` запущена:

```
# systemctl status usbipd
```

5) подключить USB-устройства и просмотреть идентификаторы подключенных устройств:

```
# lsusb
```

```
Bus 004 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 003 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 090c:1000 Silicon Motion, Inc. - Taiwan
(formerly Feiya Technology Corp.) Flash Drive
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

6) из полученного вывода выбрать ID устройства, которое нужно передать при подключении к терминальной сессии, скопировать нужный идентификатор и прописать его в файле `/etc/xrdp-usb`:

```
# Config file for xrdp-usb-terminal
# Add redirected usb ids one per line
```

```
# Example
#072f:90cc      # Advanced Card Systems, Ltd : ACR38 SmartCard
Reader (072f:90cc)
#072f:*         # All devices from specified vendor
090c:1000      # ID устройства
```

14.16.6. Настройка клиента для подключения к серверу терминалов

Примечание. Следует избегать одновременных сеансов RDP и обычных для одного и того же пользователя. Systemd не позволит полноценно работать в сеансе RDP.

Для подключения к серверу терминалов, на клиентском компьютере должен быть установлен клиент удаленного доступа. Для подключения к серверу терминалов можно использовать программы удаленного доступа FreeRDP, Remmina, Connector и т. д.

Перед подключением нужно на клиенте выполнить команду:

```
$ usbip-export
```

Для подключения можно использовать xfreerdp (должен быть установлен пакет xfreerdp):

```
$ xfreerdp [файл] [параметры] [/v:<сервер>[:порт]]
```

Описание некоторых параметров:

- /v:<server>[:port] – ip-адрес или имя сервера;
- /u:<user> – пользователь;
- /p:<password> – пароль;
- /w:<width> – ширина окна;
- /h:<height> – высота окна;
- /f – полноэкранный режим.

Например:

```
$ xfreerdp /v:192.168.0.148 /u:user /p:password
```

Примечание. Если не указывать пользователя или пароль, появится окно входа.

На рис. 205 показано подключение к терминальной сессии с использованием xfreerdp.

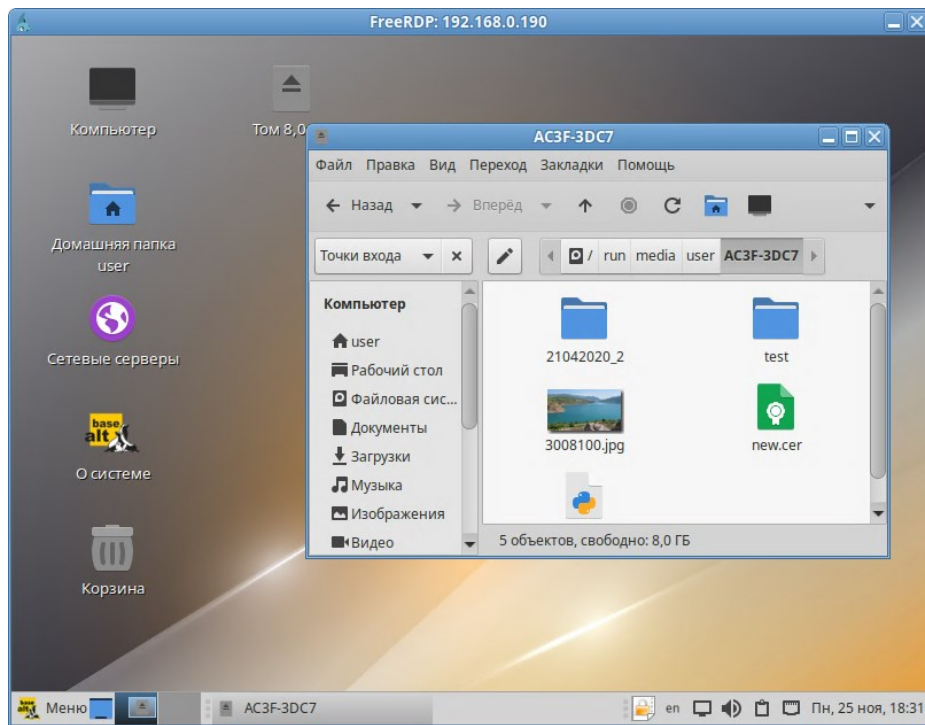


Рис. 205 – FreeRDP. Подключение к удаленному рабочему столу

В качестве клиента удаленного доступа также можно использовать программу Remmina:

- 1) установить пакеты `remmina` и `remmina-plugins-rdp`:
`# apt-get install remmina remmina-plugins-rdp`
- 2) запустить Remmina, выбрав в меню «Приложения» → «Интернет» → «Remmina»;
- 3) в окне Remmina нажать кнопку создания нового подключения (рис. 206) и в открывшемся окне (рис. 207) указать настройки RDP-подключения (IP-адрес терминального сервера, имя пользователя, пароль и т. д.), нажать кнопку «Сохранить и подключить». В результате будет создано подключение (рис. 208).

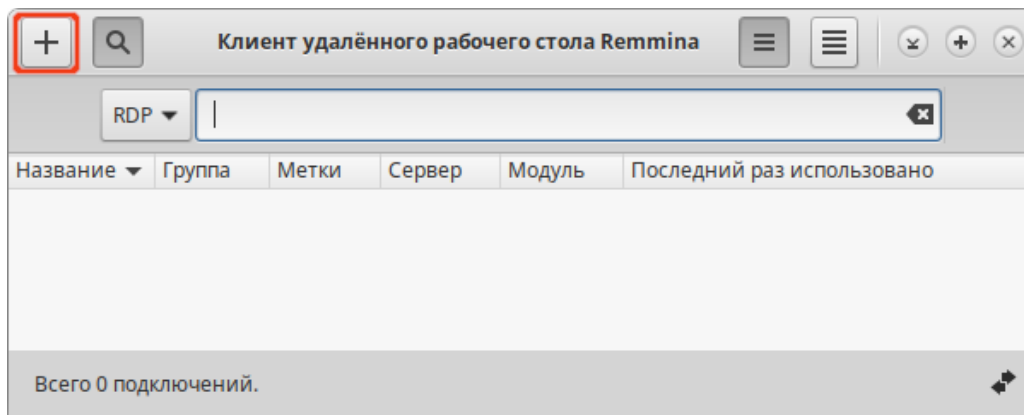


Рис. 206 – Кнопка создания нового подключения

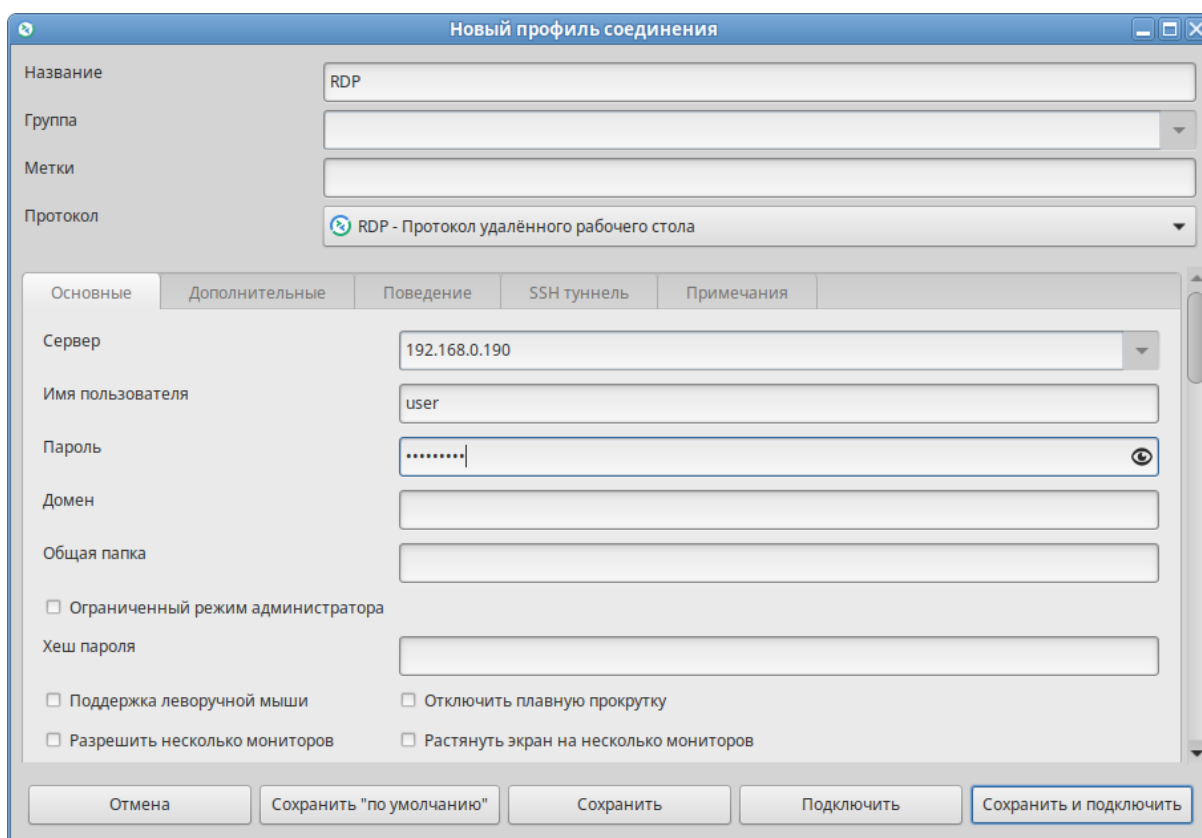


Рис. 207 – Настройки RDP-подключения

Примечание. Если автоматического монтирования не происходит, следует выполнить команду:

```
$ udiskctl mount -b /dev/sdb1
```

где /dev/sdb1 – USB-устройство (можно посмотреть в выводе команды lsblk).

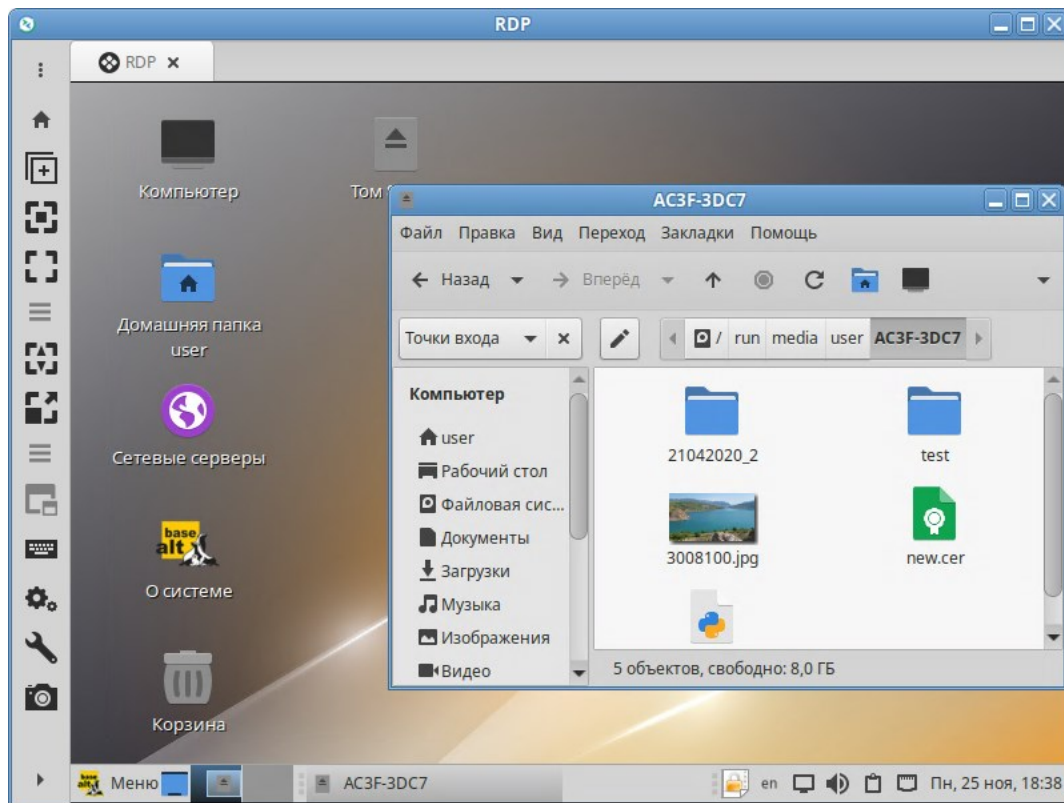


Рис. 208 – Remmina. Подключение к удаленному рабочему столу

В качестве клиента удаленного доступа можно использовать программу MyConnector. MyConnector позволяет осуществлять удаленный доступ к компьютерам с различными ОС с использованием распространенных типов подключений, таких как RDP, VNC, NX, XDMCP, SSH, SFTP. MyConnector реализует интерфейс для пользователя к предустановленным программам для запуска их с введенными параметрами.

Подключение с помощью MyConnector:

- 1) установить пакет myconnector на клиентский компьютер:

```
# apt-get install myconnector
```

- 2) запустить Myconnector, выбрав в меню «Приложения» → «Интернет» → «MyConnector»;
- 3) в окне подключения (рис. 209) указать IP-адрес терминального сервера. Нажать на кнопку «Дополнительные параметры» и в открывшемся окне (рис. 210) указать настройки RDP-подключения. Нажать на кнопку «Подключение» для подключения к терминальной сессии (рис. 211).

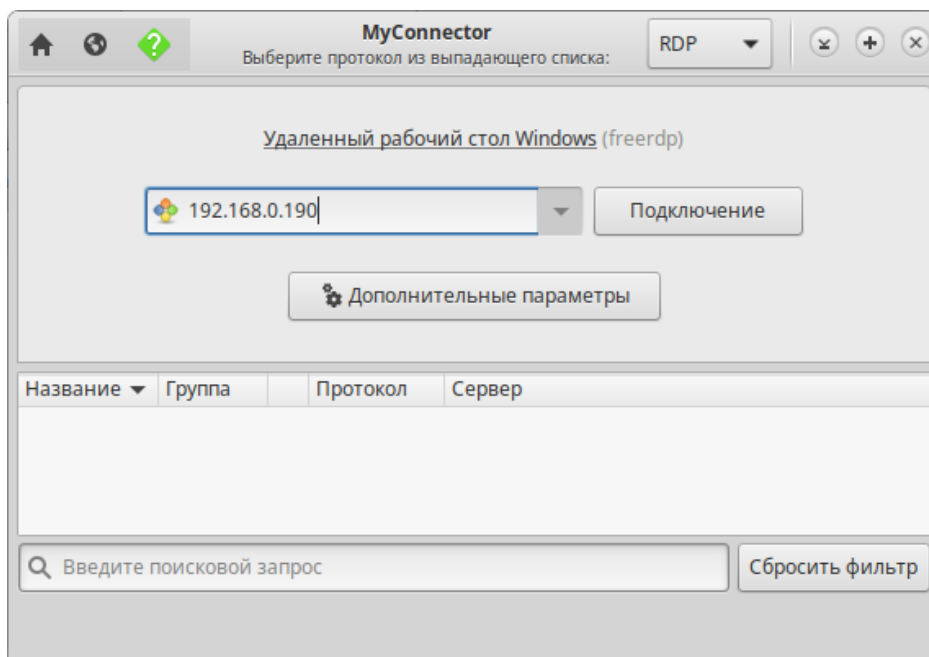


Рис. 209 – MyConnector. Окно подключения

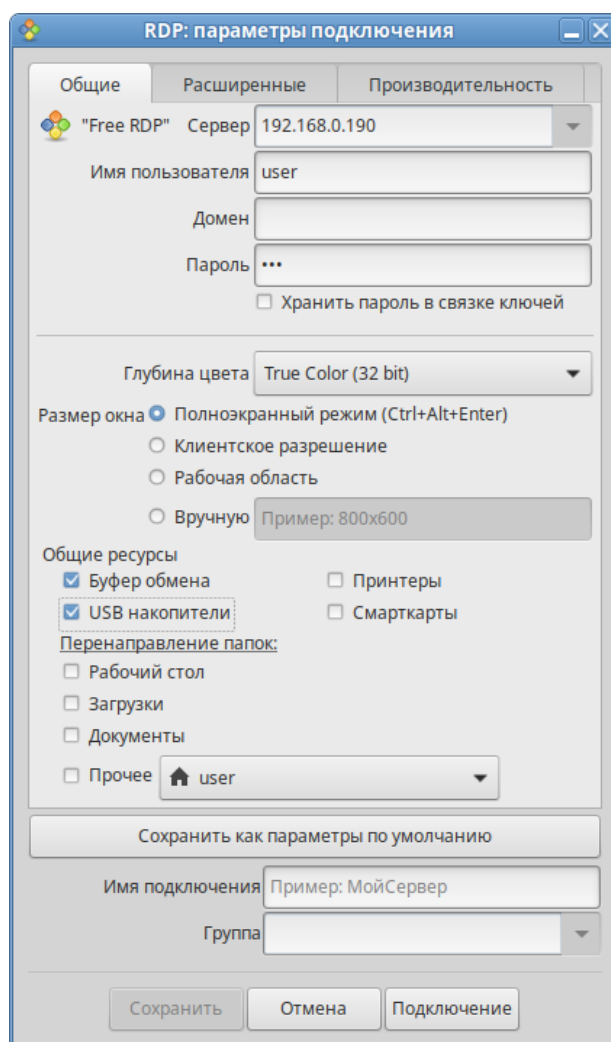


Рис. 210 – Настройки RDP-подключения

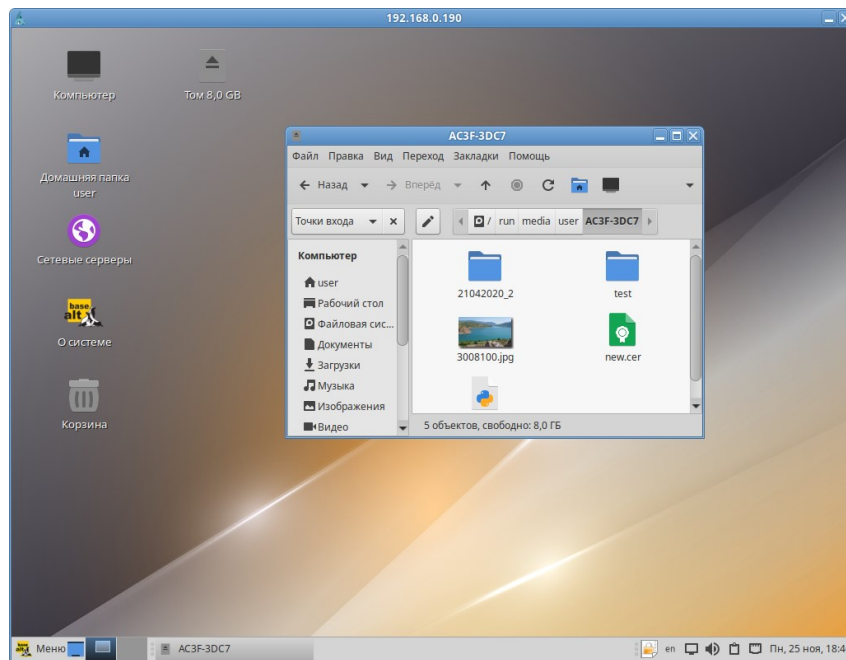


Рис. 211 – MyConnector. Подключение к удаленному рабочему столу

14.16.7. Управление XRDP

Просмотр информации об активных пользователях:

```
# ps aux |grep xrdp |grep xorg
user          5689   0.6   2.5  943524 100112 ?        Ssl   17:48   0:09
Xorg :10 -auth .Xauthority -config xrdp/xorg.conf -noreset -nolisten tcp -
logfile .xorgxrdp.%s.log
```

В выводе команды видно, что подключен пользователь user и его PID 5689.

Следующая команда отключит пользователя user и завершит все его процессы:

```
# pkill -9 -u user
```

14.17. Timeshift

Timeshift – программа для автоматического периодического создания копий системы (снимков/snapshots).

Timeshift предназначен, прежде всего, для сохранения системных файлов и настроек. Пользовательские данные по умолчанию не архивируются, поэтому в случае сбоя системы, восстанавливаются системные файлы, а данные пользователей остаются в актуальном состоянии (конечно, если они не были повреждены).

Резервные копии не могут быть восстановлены на уровне отдельных файлов, восстановление всегда происходит в полном объеме настроек Timeshift.

Запустить Timeshift можно из МАТЕ «Меню» → «Приложения» → «Системные» → «Timeshift» или из командной строки:

```
$ timeshift-launcher
```

Запуск Timeshift требует прав администратора, поэтому необходимо ввести пароль администратора (рис. 212).

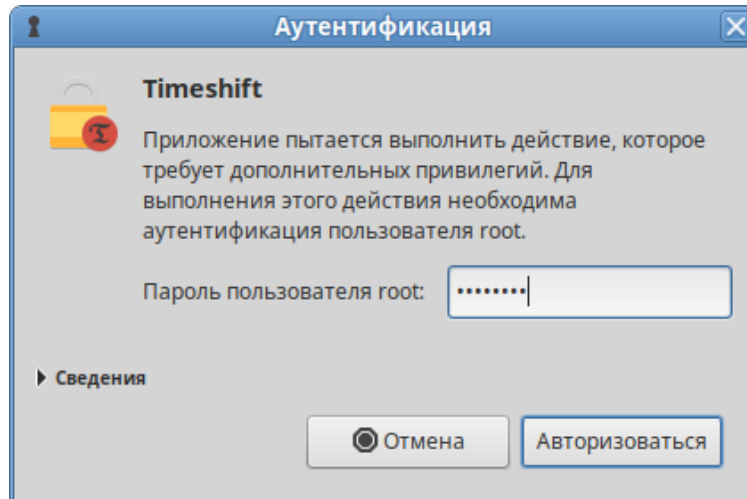


Рис. 212 – Запрос пароля для запуска Timeshift

При первом запуске Timeshift будет запущен «Мастер установки». Запустить мастер установки или открыть окно настроек резервного копирования также можно, нажав соответствующую кнопку на панели инструментов в окне Timeshift (рис. 213).

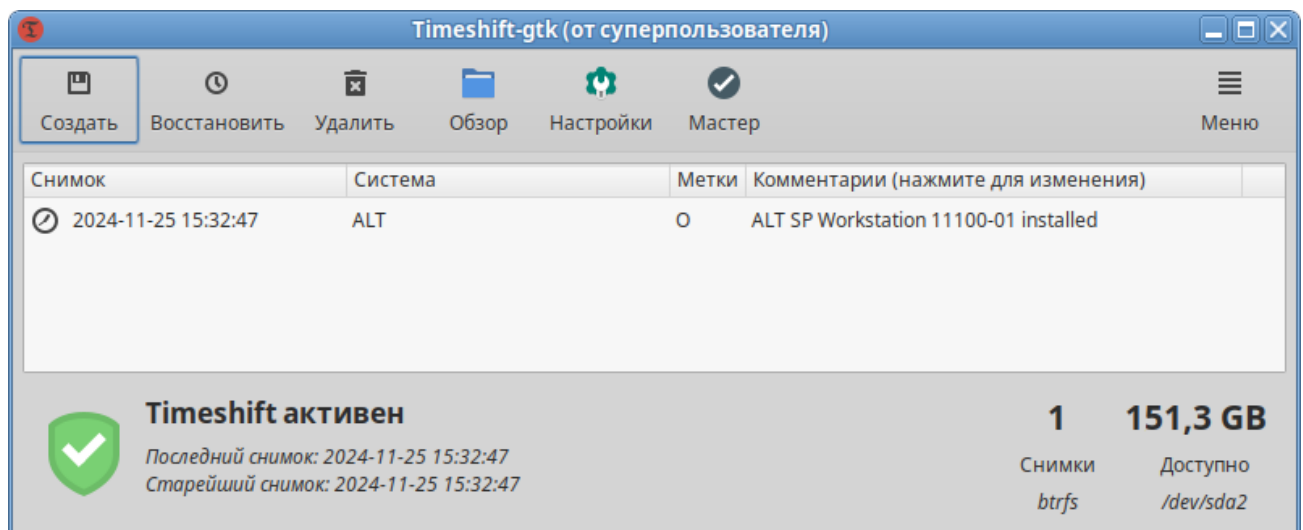


Рис. 213 – Окно программы Timeshift

14.17.1. Настройка резервного копирования

14.17.1.1. Режим RSYNC

Особенности режима RSYNC:

- снимки создаются путем копирования системных файлов при помощи rsync и создания жестких ссылок на неизмененные файлы из предыдущего снимка;
- все файлы копируются при создании первого снимка. Последующие снимки являются инкрементальными. Неизменные файлы будут связаны с предыдущим снимком, если он доступен;
- создание первого снимка может занять до 10 минут;
- системный раздел может быть отформатирован в любой файловой системе. Резервный раздел может быть отформатирован в любой файловой системе Linux, поддерживающей жесткие ссылки. Сохранение снимков на несистемный или внешний диск позволяет восстановить систему, даже если системный диск поврежден;
- можно задать исключения для файлов и каталогов для экономии дискового пространства;
- систему нужно перезагрузить после восстановления снимка.

Тип снимков можно выбрать на вкладке «Тип» окна настроек Timeshift (рис. 214) или на первом шаге работы мастера установки.

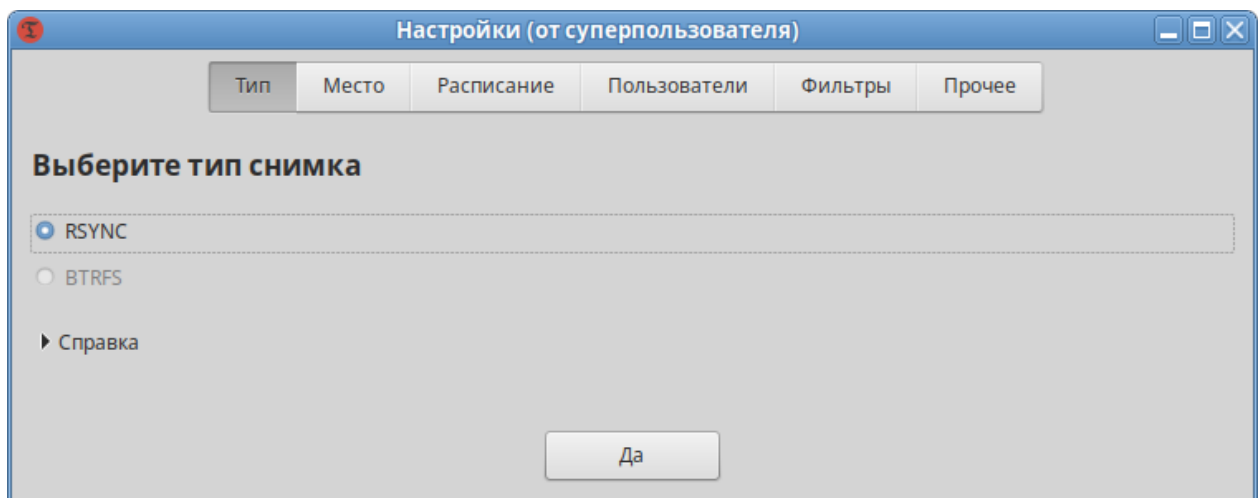


Рис. 214 – Выбор режима RSYNC

На вкладке «Место» можно выбрать диск, где будут храниться снимки (рис. 215). RSYNC снимки имеют большой размер, поэтому желательно хранить их на другом (не системном) диске или разделе. По умолчанию снимки сохраняются в системном (корневом) разделе в /timeshift, также можно выбрать другие разделы Linux.

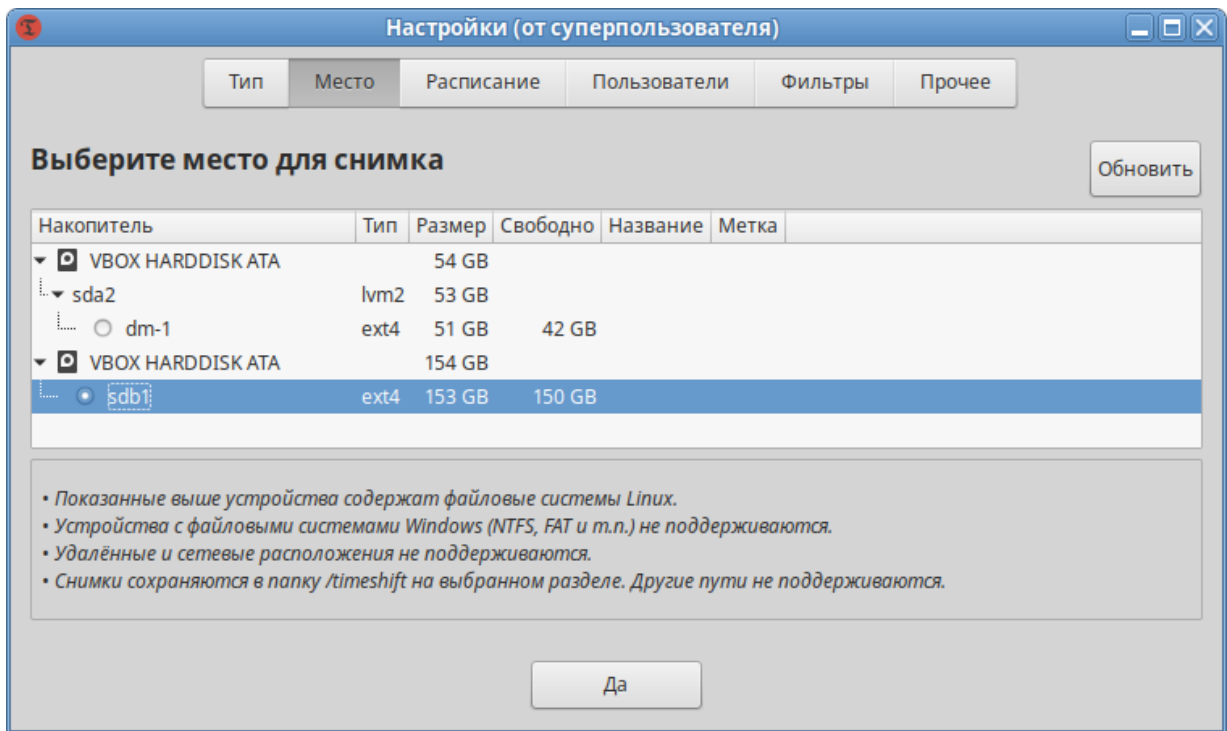


Рис. 215 – Выбор места хранения снимков RSYNC

На вкладке «Расписание» (рис. 216) следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня.

Примечание. Снимки уровня «Загрузка» создаются при каждом запуске системы (с задержкой в 10 минут). Они выполняются в фоне и не влияют на скорость загрузки системы.

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение. Например, если выбрать опцию «Включить только скрытые файлы» (рис. 217), будет выполнено резервное копирование и восстановление скрытых файлов и каталогов в домашнем каталоге пользователя (эти каталоги содержат пользовательские файлы конфигурации).

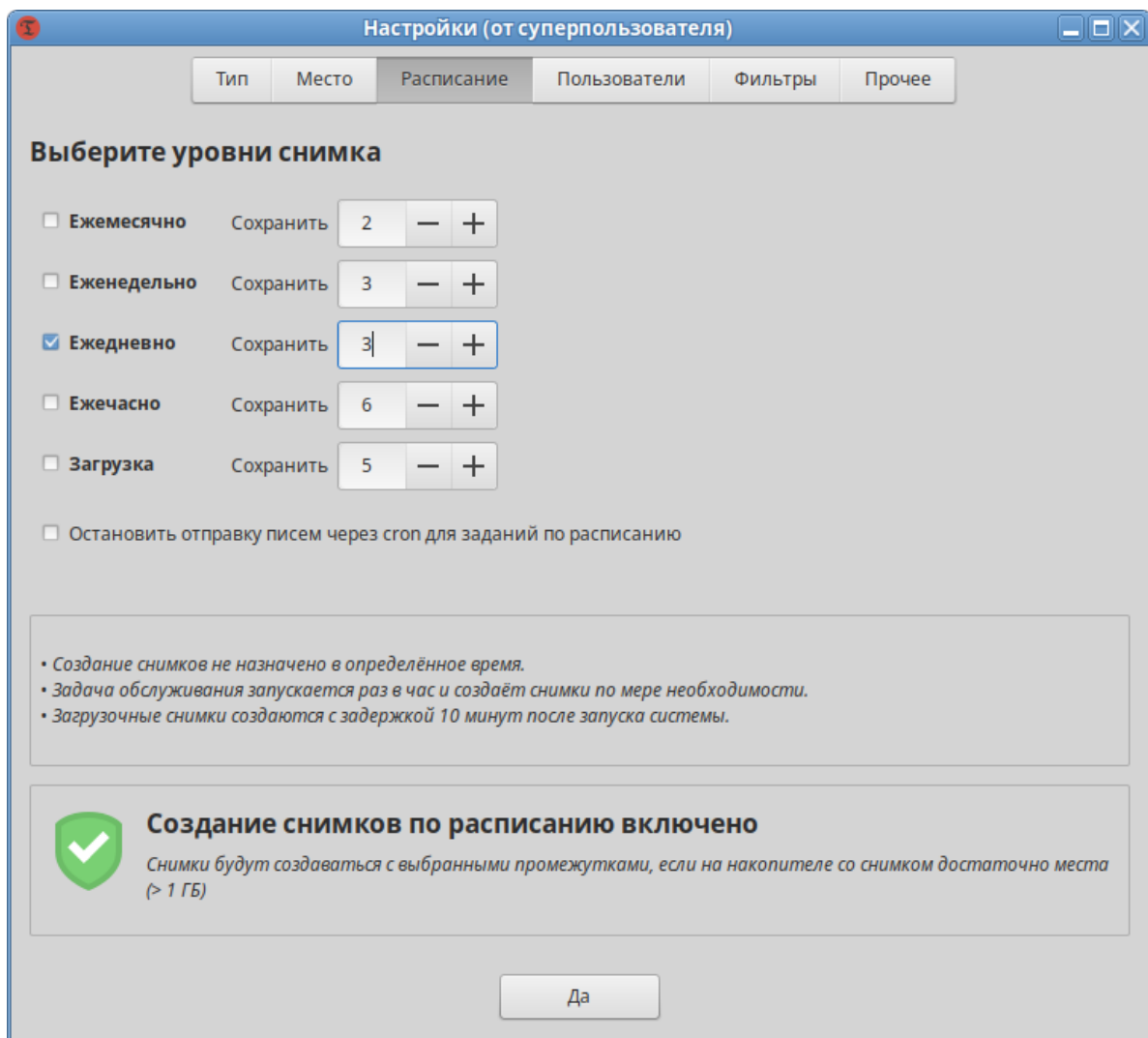


Рис. 216 – Расписание для снимков RSYNC

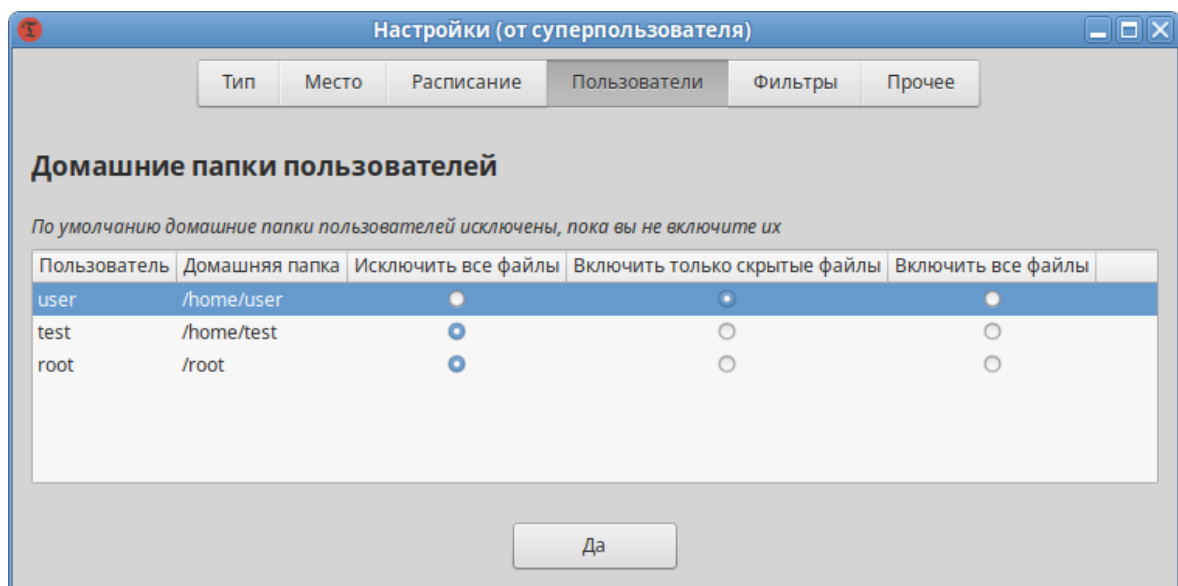


Рис. 217 – Вкладка «Пользователи»

На вкладке «Фильтры» (рис. 218) можно указать, какие файлы/каталоги включать/исключать из резервного копирования (динамические каталоги исключаются по умолчанию: /dev, /proc, ...).

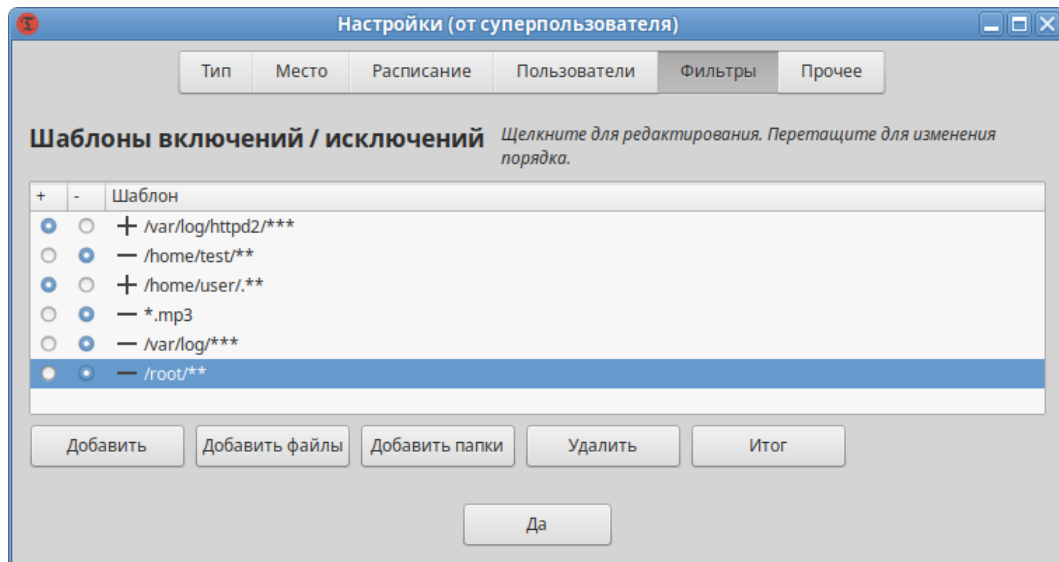


Рис. 218 – Timeshift. Вкладка «Фильтры»

В данном примере из резервной копии будут исключены все файлы mp3, все системные журналы, кроме журналов веб-сервера Apache. Просмотреть итоговый список исключений (рис. 219) можно, нажав кнопку «Итог» на вкладке «Фильтры». Отредактировать шаблон можно, дважды щелкнув левой кнопкой мыши по строке шаблона.

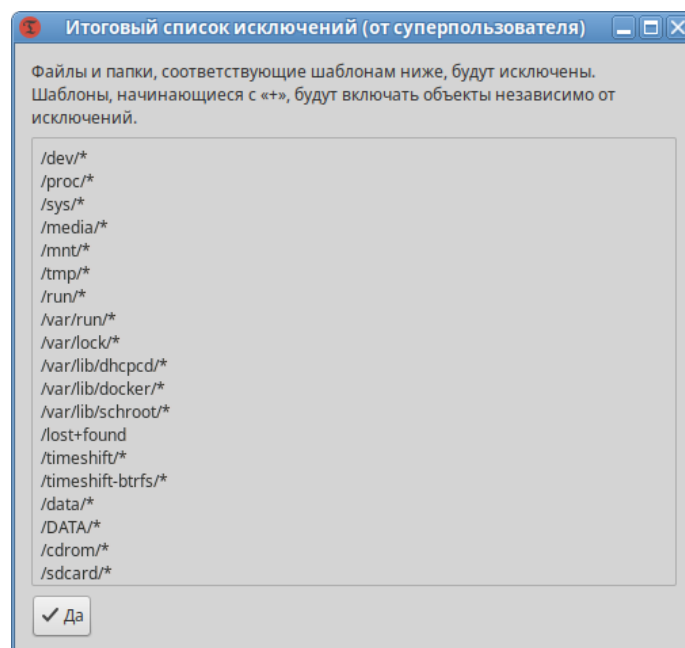


Рис. 219 – Итоговый список исключений

На вкладке «Прочее» (рис. 220) можно выбрать формат даты.

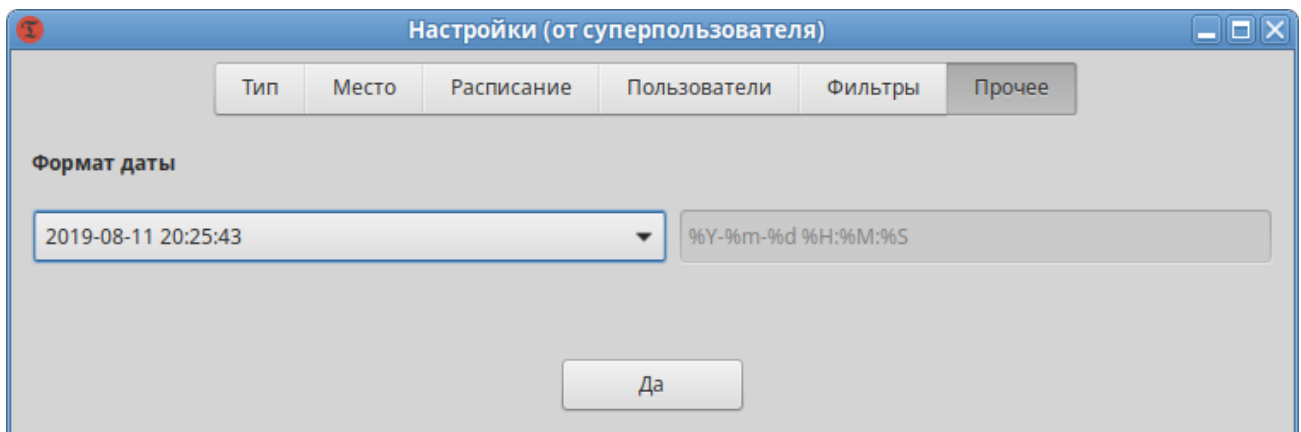


Рис. 220 – Итоговый список исключений

14.17.1.2. Режим BTRFS

Особенности режима BTRFS:

- снимки создаются с использованием встроенных средств файловой системы BTRFS;
- снимки создаются и восстанавливаются мгновенно (создание снимков – это атомарная транзакция на уровне файловой системы);
- снимки восстанавливаются путем замены системных подразделов. Поскольку файлы никогда не копируются, не удаляются и не перезаписываются, риск потери данных отсутствует. Существующая система сохраняется как новый снимок после восстановления;
- снимки сохраняются на том же диске, с которого они созданы (системном диске). Хранение на других дисках не поддерживается. Если системный диск выйдет из строя, снимки, хранящиеся на нем, будут потеряны вместе с системой;
- нет возможности исключать файлы и каталоги;
- размер снимков BTRFS изначально равен нулю. При изменении системных файлов, данные записываются в новые блоки данных, которые занимают дисковое пространство (копирование при записи). Файлы в снимке продолжают указывать на исходные блоки данных;

- снимки можно восстановить без немедленной перезагрузки запущенной системы;
- ОС должна быть установлена на раздел BTRFS с разбивкой на подразделы @ и @home. Другие виды разделов не поддерживаются.

Примечание. Для установки ОС на раздел BTRFS с разбивкой на подразделы @ и @home можно при установке системы, на этапе «Подготовка диска» создать следующие подтома (рис. 221):

- подтом @ с точкой монтирования в /;
- подтом @home с точкой монтирования в /home.

Тип снимков BTRFS можно выбрать на вкладке «Тип» окна настроек Timeshift (рис. 221) или на первом шаге работы мастера установки.

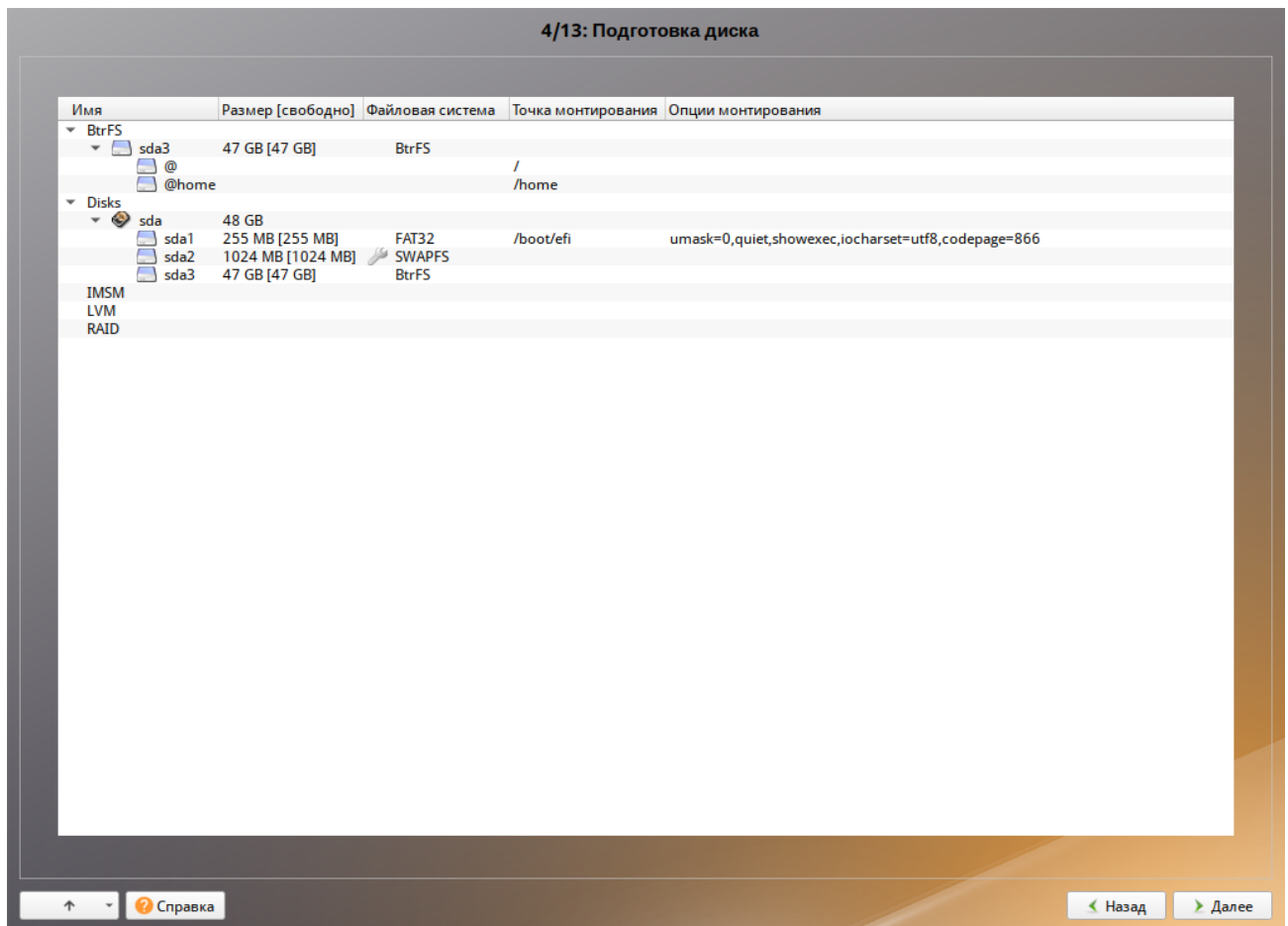


Рис. 221 – Корень системы с файловой системой BTRFS

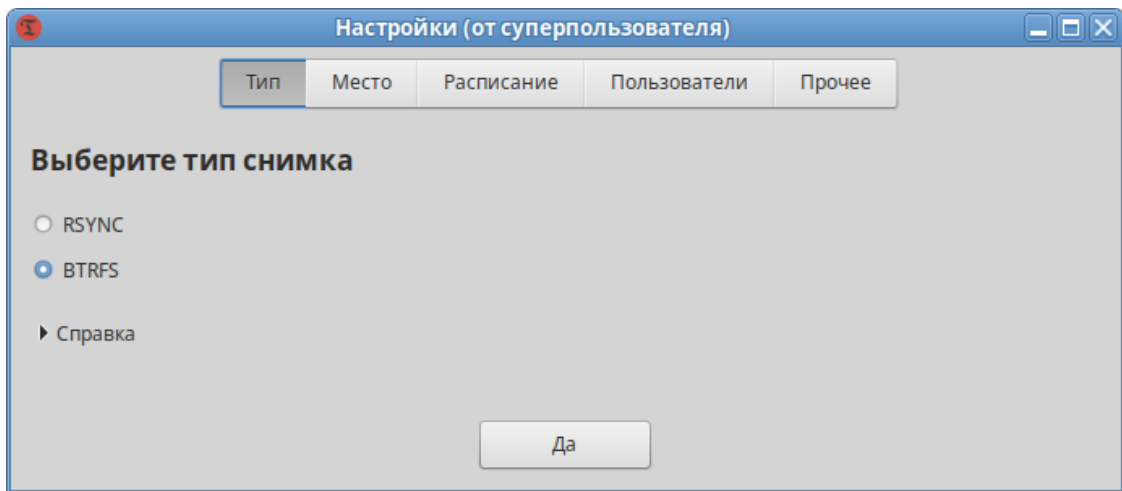


Рис. 222 – Выбор режима BTRFS

Снимки BTRFS сохраняются в системном разделе, другие разделы не поддерживаются (рис. 223).

На вкладке «Расписание» следует выбрать уровни создания снимков (ежемесячно, еженедельно, ежедневно, ежечасно, при загрузке) и указать количество сохраняемых снимков для каждого уровня (рис. 224).

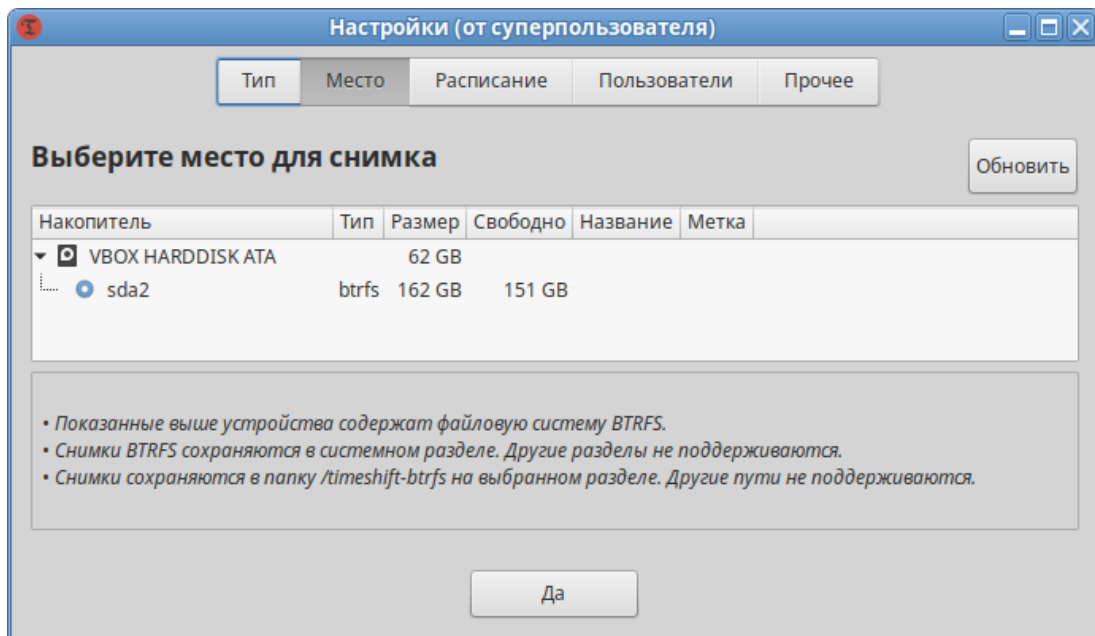


Рис. 223 – Выбор места хранения снимков BTRFS

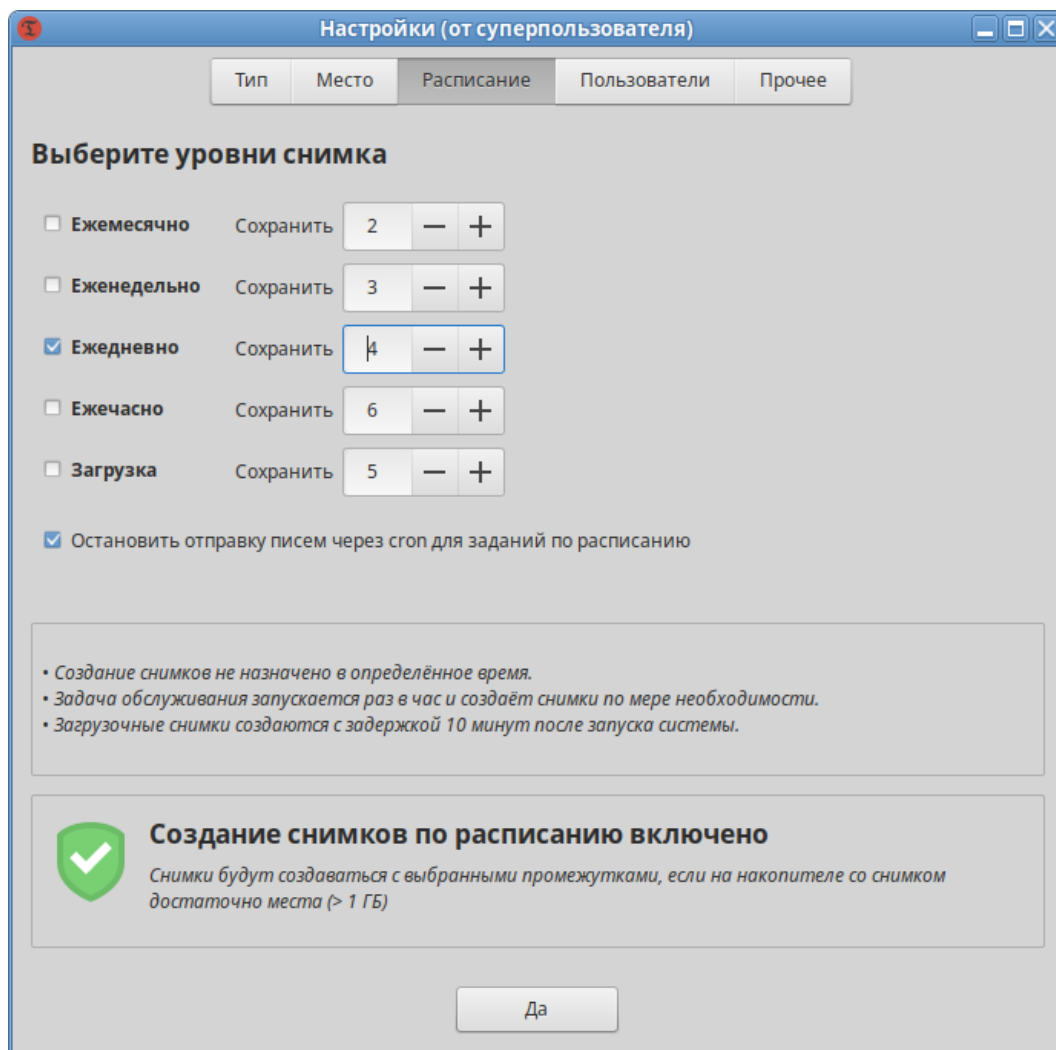


Рис. 224 – Расписание для снимков BTRFS

По умолчанию домашние каталоги пользователей не включаются в резервную копию. На вкладке «Пользователи» можно изменить это поведение и включить подраздел @home в создаваемые снимки (рис. 225).

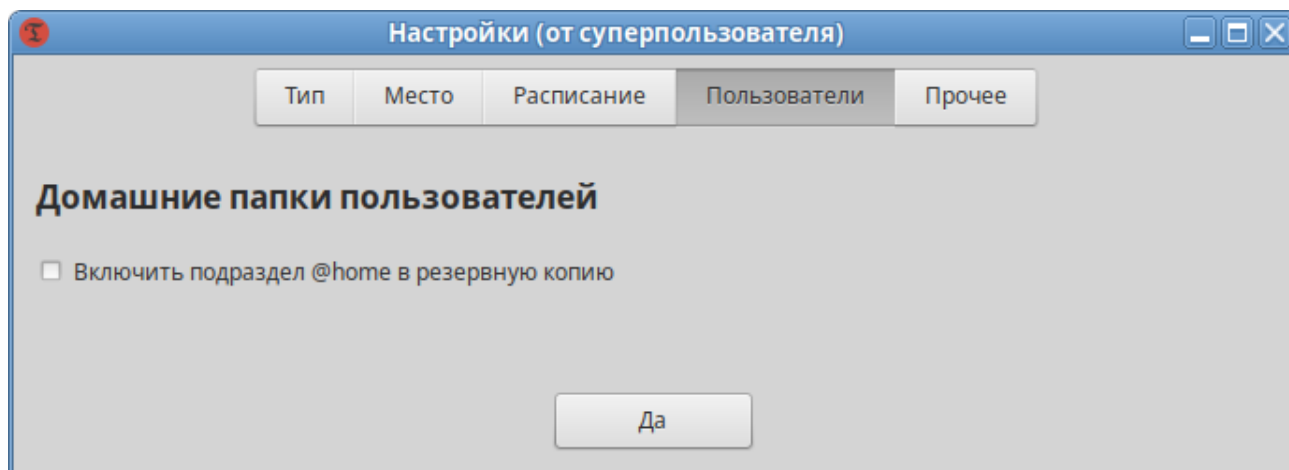


Рис. 225 – Включить подраздел @home в создаваемые снимки

На вкладке «Прочее» можно выбрать формат даты.

14.17.2. Создание снимков

Снимки будут создаваться автоматически согласно настроенному расписанию.

Для создания снимка в ручном режиме следует нажать кнопку «Создать» на панели инструментов (рис. 226). Резервная копия будет создана на устройстве хранения, который был указан в настройках.

14.17.3. Восстановление системы

Снимки можно восстановить как из работающей системы (оперативное восстановление), так и из другой системы, на которой установлен Timeshift (автономное восстановление).

Для восстановления снимка следует выбрать снимок в главном окне и нажать кнопку «Восстановить» (рис. 227).

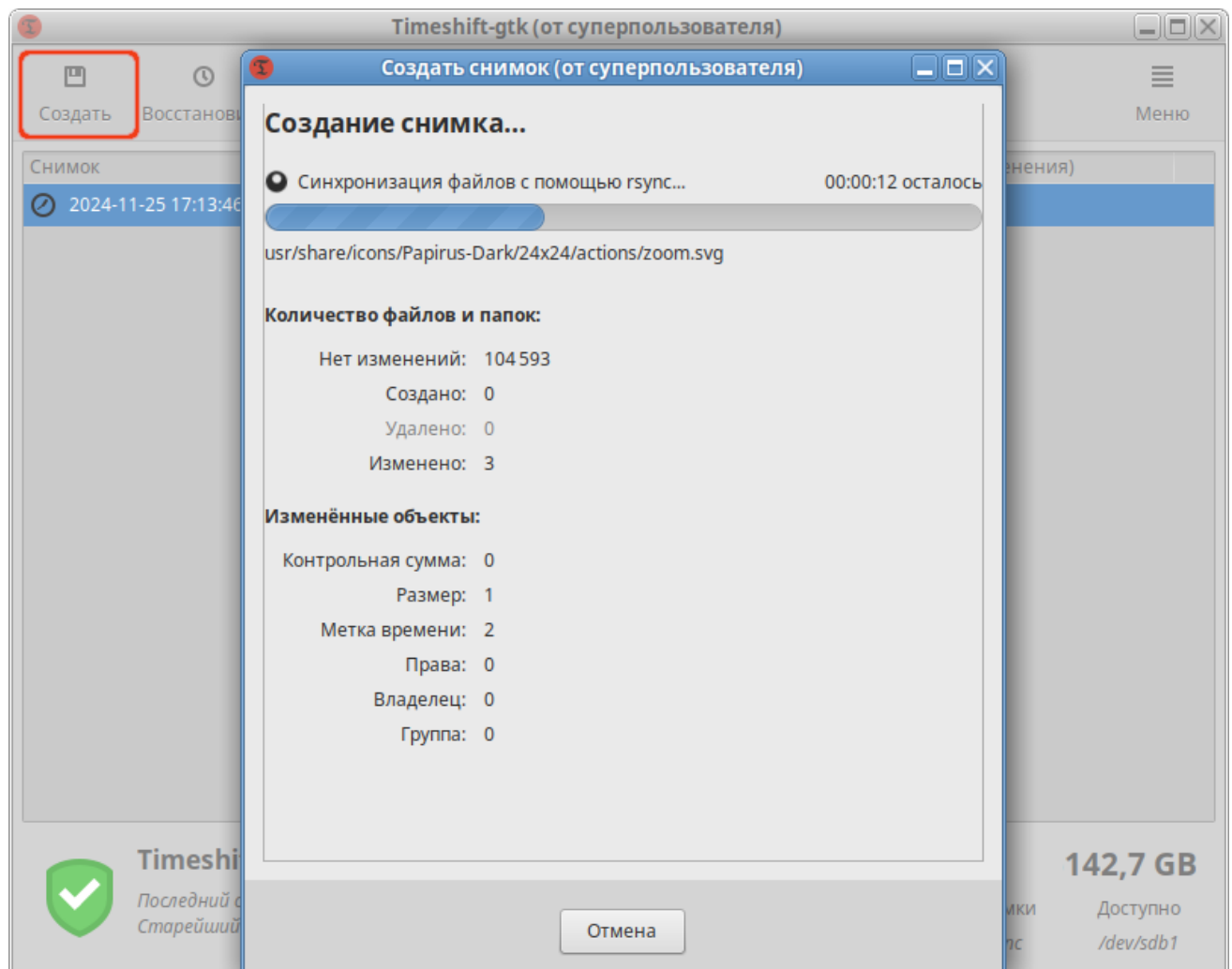


Рис. 226 – Создание снимка в режиме RSYNC

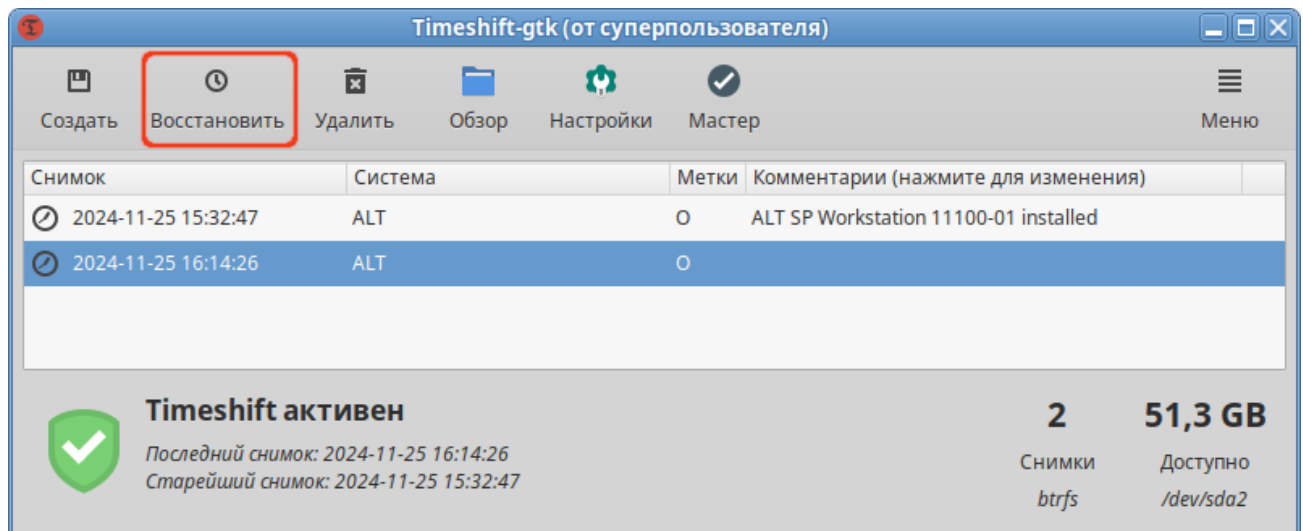


Рис. 227 – Снимки системы и кнопка «Восстановить»

При восстановлении снимка в режиме RSYNC после нажатия кнопки «Восстановить» можно выбрать устройство, куда будут восстановлены файлы (рис. 228), указать нужно ли переустанавливать GRUB, нажав кнопку «Настройки загрузчика (дополнительные)». На следующем шаге будут показаны файлы, которые будут созданы/восстановлены/удалены в процессе восстановления снимка (рис. 229).

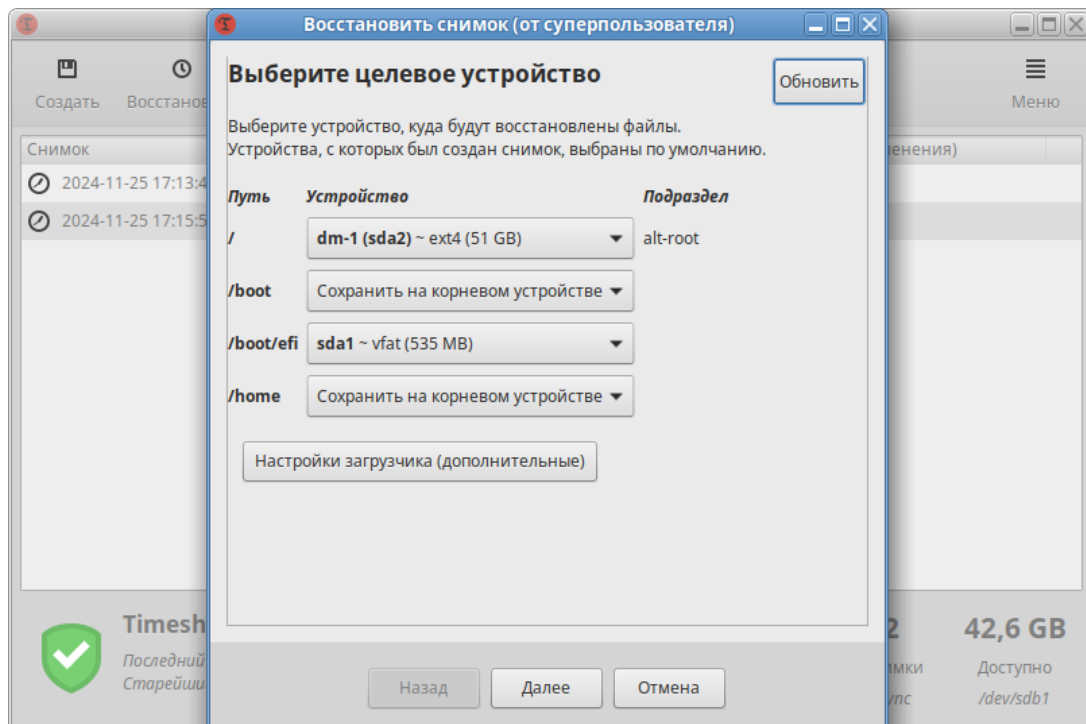


Рис. 228 – Выбор целевого устройства

Примечание. Если основная система не загружается, то можно загрузиться в режиме восстановления и развернуть снимок в командной строке.

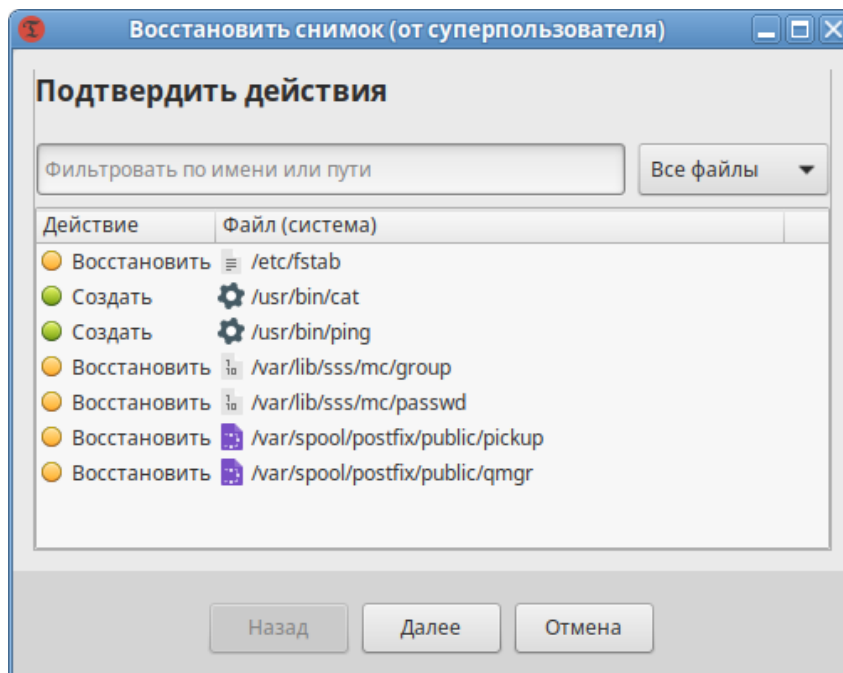


Рис. 229 – Восстановление снимка в режиме RSYNC

14.17.4. Работа с Timeshift в командной строке

Примечание. Одновременно может работать только один экземпляр Timeshift, поэтому для работы с Timeshift из командной строки необходимо закрыть окно программы Timeshift.

Вывод справки о команде:

```
$ timeshift
```

Если параметры не указаны, например, при создании снимка, значения по умолчанию будут загружены из конфигурации приложения.

Просмотр списка снимков:

```
# timeshift --list
```

```
Mounted '/dev/sdb1' at '/run/timeshift/6683/backup'
Device : /dev/sdb1
UUID   : 136a6133-f354-4d84-b4d1-07a52b7d8203
Path    : /run/timeshift/6683/backup
Mode    : RSYNC
Status  : OK
2 snapshots, 42.6 GB free
```

Num		Name	Tags	Description
0	>	2024-11-25_17-13-46	0	
1	>	2024-11-25_17-15-52	0	

Пример создания снимка (в режиме RSYNC):

```
# timeshift --create --comments "after update" --tags D

Mounted '/dev/sdb1' at '/run/timeshift/6727/backup'
-----
Creating new snapshot...(RSYNC)
Saving to device: /dev/sdb1, mounted at path:
/run/timeshift/6727/backup
Linking from snapshot: 2024-11-25_17-15-52
Syncing files with rsync...
Created control file:
/run/timeshift/6727/backup/timeshift/snapshots/2024-11-25_17-31-45/info.json
RSYNC Snapshot saved successfully (14s)
Tagged snapshot '2024-11-25_17-31-45': ondemand
-----
```

Пример создания (в режиме BTRFS):

```
# timeshift --create --comments "after update" --tags D

Using system disk as snapshot device for creating snapshots in BTRFS
mode
Mounted '/dev/sda2' at '/run/timeshift/5005/backup'
btrfs: Quotas are not enabled
Creating new backup...(BTRFS)
Saving to device: /dev/sda2, mounted at path:
/run/timeshift/5005/backup
Created directory: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28
Created subvolume snapshot: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28/@
Created control file: /run/timeshift/5005/backup/timeshift-
btrfs/snapshots/2024-11-25_16-32-28/info.json
BTRFS Snapshot saved successfully (0s)
Tagged snapshot '2024-11-25_16-32-28': ondemand
-----
```

Создание снимка, если он запланирован (есть в расписании):

```
# timeshift --check
```

Восстановить снимок (параметры будут запрошены в интерактивном режиме):

```
# timeshift --restore
```

Восстановить снимок:

```
# timeshift --restore --snapshot '2024-11-25_17-13-46'
```

Восстановить определенный снимок в раздел:

```
# timeshift --restore --snapshot '2024-11-25_17-15-52' --target /dev/sdb1
```

Удалить снимок:

```
# timeshift --delete --snapshot '2024-11-25_17-15-52'
```

Если основная система не загружается, то нужно загрузиться в режиме восстановления и выполнить следующие действия (на примере режима RSYNC):

1) установить timeshift:

```
# apt-get update && apt-get install timeshift
```

2) посмотреть список снимков на устройстве:

```
# timeshift --list --snapshot-device /dev/sdb1
```

3) запустить восстановление:

```
# timeshift --restore --snapshot-device /dev/sdb1 --snapshot  
'2024-11-25_17-13-46' --target /dev/sda2 --grub-device /dev/sda
```

4) перезагрузить систему.

14.18. Информация о системе и об аппаратной части компьютера

14.18.1. Команда inxi

inxi – это инструмент командной строки, который позволяет отображать информацию о системе и об аппаратной части компьютера. Часто используется в качестве инструмента отладки для технической поддержки, чтобы быстро определить конфигурации системы и оборудование пользователей.

Установка пакета inxi:

```
# apt-get install inxi
```

Команда:

```
inxi [-AbBCdDEfFGhiIjJlLmMnNopPrRsSuUVwyYzZ]
```

```
inxi [-c <целое число>] [--sensors-exclude SENSORS] [--  
sensors-use SENSORS] [-t [c|m|cm|mc][целое число]] [-v <целое  
число>] [-W LOCATION] [--weather-unit {m|i|mi|im}] [-y WIDTH]
```

```
inxi [--edid] [--memory-modules] [--memory-short] [--recommends]  
[--sensors-default] [--slots]
```

```
inxi [-x|-xx|-xxx|-a] -OPTION(s)
```

В таблице 16 приведены некоторые стандартные опции команды inxi.

Т а б л и ц а 16 – Стандартные опции команды inxi

Ключ	Описание
-A	Выводит информацию об аудио/звуковых устройствах, включая драйвер устройства. Для отображения всех обнаруженных звуковых API/серверов, включая неактивные, нужно использовать ключ -Ax: <pre>\$ inxi -Ax</pre> Audio: <pre>Device-1: Intel Alder Lake PCH-P High Definition Audio vendor: Lenovo driver: sof-audio-pci-intel-tgl bus-ID: 00:1f.3 API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api Server-1: JACK v: 1.9.22 status: off Server-2: PulseAudio v: 16.1 status: active</pre>
-b	Выводит общую информацию в краткой форме. Аналогично выводу <code>\$ inxi -v 2</code> .
-B	Выводит данные батареи системы (при наличии батареи): (ID-х), заряд, состояние, а также дополнительную информацию. <pre>\$ inxi -B</pre> Battery: <pre>ID-1: BAT0 charge: 54.5 Wh (100.0%) condition: 54.5/57.0 Wh (95.6%)</pre>
-c	Задаёт цветовую тему для стилизации выводимой информации. Предусмотрено 43 темы (0-42): <pre>\$ inxi -c 5</pre> Просмотреть все предустановленные темы можно, выполнив команду: <pre>\$ inxi -c 94</pre>
-C	Выводит данные о процессоре (дополнительные данные доступны с ключами -x, -xxx и -a): <pre>\$ inxi -C</pre> CPU: <pre>Info: 10-core (2-mt/8-st) model: 12th Gen Intel Core i7-1255U bits: 64 type: MST AMCP cache: L2: 6.5 MiB Speed (MHz): avg: 2480 min/max: 400/4700:3500 cores: 1: 2873 2: 3438 3: 1903 4: 2600 5: 1787 6: 2600 7: 2600 8: 2316 9: 2600 10: 2600 11: 2600 12: 1853</pre>
-d	Выводит данные накопителей на оптических дисках
-D	Выводит информацию о жестких дисках: идентификатор диска, тип (FireWire, съемный, USB), производитель (если обнаружен), модель и размер. Также показывает общее пространство на дисках и занятое место: <pre>\$ inxi -D</pre> Drives: <pre>Local Storage: total: 1.4 TiB used: 426.1 GiB (29.8%) ID-1: /dev/nvme0n1 vendor: Micron model: MTFDKCD512TFK size: 476.94 GiB ID-2: /dev/nvme1n1 vendor: Western Digital model: WD PC SN740 SDDPTQD- 1T00 size: 953.87 GiB</pre>
-E	Выводит информацию об устройствах bluetooth: <pre>\$ inxi -E</pre> Bluetooth: <pre>Device-1: Intel AX201 Bluetooth driver: btusb type: USB Report: hciconfig ID: hci0 state: up address: 3C:21:9C:AE:28:B4 bt-v: 3.0</pre>

Продолжение таблицы 16

Ключ	Описание
-F	Выводит общую информацию. Включает все буквы верхнего регистра, а также -s и -n. Не выводит дополнительные подробные данные, такие как -d -f -l -m -o -p -r -t -u -x, если эти ключи не используются в команде, например: \$ inxi -Frmxx
-G	Выводит информацию о графических устройствах, включая сведения о драйверах устройств и дисплеев. При использовании ключей -Gxx также выводится информация о мониторах. \$ inxi -G Graphics: Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v: kernel Device-2: Syntek Integrated Camera driver: uvcvideo type: USB Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz 2: 1920x1080~60Hz API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)
-i	Отображает локальные и WAN IP-адреса. По соображениям безопасности, эти данные не отображаются в выводе с -F
-I	Выводит следующую информацию: процессы, время бесперебойной работы, память, оболочка: \$ inxi -I Info: Processes: 338 Uptime: 3h 15m Memory: available: 38.88 GiB used: 9.91 GiB (25.5%) Shell: Bash inxi: 3.3.27 Для получения дополнительной информации, можно использовать параметры -Ix, -Ixx и -Ia: \$ inxi -Ia Info: Processes: 337 Uptime: 3h 16m wakeups: 4 Memory: available: 38.88 GiB used: 9.94 GiB (25.6%) Init: systemd v: 252 target: graphical (5) default: graphical tool: systemctl Compilers: gcc: 12 Packages: pm: rpm pkgs: N/A note: see --rpm Shell: Bash v: 4.4.23 running-in: xfce4-terminal inxi: 3.3.27
-j	Показывает все активные типы подкачки (раздел, файл, zram). Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с -l или -u. \$ inxi -ju Swap: ID-1: swap-1 type: partition size: 7.46 GiB used: 0 KiB (0.0%) dev: /dev/nvme0n1p2 uuid: 3cee8elf-494c-4622-90d9-5f3da9ab2082
-J	Выводит данные USB для подключенных концентраторов и устройств. Концентраторы также показывают количество портов
-l	Выводит метки разделов. Следует использовать с ключами -j, -o, -p и -P. Если ни один из этих ключей не указан, ничего не выводит
-L	Выводит информацию о логическом томе для LVM, LUKS, bcache и т. д.

Продолжение таблицы 16

Ключ	Описание
-m	Выводит информацию о памяти (RAM). Не отображается с ключами -b или -F, если -m не указывается явно. Данный ключ использует dmidecode, который должен запускаться от имени пользователя root: # inxi -m Memory: System RAM: available: 38.88 GiB used: 9.95 GiB (25.6%) Array-1: capacity: 256 GiB slots: 8 EC: None Device-1: Controller0-ChannelA-DIMM0 type: DDR4 size: 32 GiB speed: 3200 MT/s Device-2: Controller0-ChannelB-DIMM0 type: no module installed ...
-M	Выводит информацию о машине: устройство, материнская плата, BIOS.
-n	Выводит расширенную информацию о сетевом устройстве.
-N	Выводит информацию о сетевых устройствах, включая драйвер устройства. С ключом -x показывает идентификатор шины, номер порта. \$ inxi -N Network: Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi Device-2: Intel Ethernet I219-V driver: e1000e
-o	Выводит информацию о несмонтированном разделе (включая UUID и LABEL, если они доступны)
-p	Выводит полную информацию о всех смонтированных разделах. Чтобы отобразить метки разделов или UUID (если они доступны и уместны), следует использовать с ключами -l или -u.
-P	Выводит основную информацию о разделах (показывает, если обнаружено: / /boot /boot/efi /home /opt /tmp /usr /usr/home /var /var/tmp /var/log): \$ inxi -P Partition: ID-1: / size: 460.79 GiB used: 426.1 GiB (92.5%) fs: ext4 dev: /dev/nvme0nlp3 ID-2: swap-1 size: 7.46 GiB used: 0 KiB (0.0%) fs: swap dev: /dev/nvme0nlp2
-r	Выводит информацию о репозиториях
-R	Выводит данные RAID. Показывает устройства RAID, состояния, уровни, размер устройства/массива и компоненты
-s	Выводит данные от датчиков (если эти датчики установлены/настроены): температура материнской платы/процессора/графического процессора; скорость вентилятора: \$ inxi -s Sensors: System Temperatures: cpu: 48.0 C mobo: N/A Fan Speeds (RPM): fan-1: 1800 fan-2: 1800
-S	Выводит информацию о системе: имя хоста, ядро, окружение рабочего стола, дистрибутив. С ключами -xx также показывает DM

Окончание таблицы 16

Ключ	Описание
-t	Выводит процессы: -t c – только процессор; -t m – только память; -t cm – процессор/память (по умолчанию). Если указано число, показывает данное количество процессов для каждого типа (по умолчанию 5). <pre>\$ inxi -t cm3</pre> Processes: CPU top: 3 of 348 1: cpu: 27.6% command: virtualboxvm pid: 7152 2: cpu: 17.3% command: virtualboxvm pid: 5544 3: cpu: 7.3% command: x pid: 2700 System RAM: available: 38.88 GiB used: 10.21 GiB (26.3%) Memory top: 3 of 348 1: mem: 1376.0 MiB (3.4%) command: virtualboxvm pid: 5544 2: mem: 1306.8 MiB (3.2%) command: virtualboxvm pid: 7152 3: mem: 808.8 MiB (2.0%) command: telegram pid: 5163
-u	Выводит UUID разделов. Для отображения меток разделов следует использовать с ключами -j, -o, -p и -P. Если ни один из этих ключей не указан, ничего не выводит
-v	Задаёт уровень детализации. Если номер уровня детализации не указан, предполагается значение 0. Не следует использовать с -b или -F. Поддерживаются уровни 0 – 8: 0 – вызов inxi без параметров; 1 – базовый уровень, включает: -s + базовая информация о центральном процессоре (ЦП) + -G + базовая информация о дисках + -I; 2 – включает информацию: о сетевых устройствах (-N), информацию о машине (-M), данные батареи (-B). То же самое, что и inxi -b; 3 – включает: данные о ЦП (-C), данные батареи (-B), сетевые устройства (-n) (тоже, что и -x); 4 – включает основную информацию о разделах (-P) для /, /home, /var/, /boot. Показывает полную информацию о жестких дисках (-D); 5 – включает: информацию об аудиоустройствах (-A), данные от датчиков (-s), RAM (-m), информацию о bluetooth, метки разделов (-l), все активные типы подкачки (-j), UUID (-u), информацию об оптических устройствах, данные RAID; 6 – включает полную информацию о всех смонтированных (-p) и не смонтированных разделах (-o), оптических устройствах (-d), USB (-J), RAID (тоже, что и -xx); 7 – включает локальные и WAN IP-адреса (-i), информацию о bluetooth, информацию о логических томах (-L), RAID, все данные CPU (тоже, что и -xxx); 8 – включает всю доступную информацию, репозитории (-r), процессы (-tcm), слоты PCI (--slots). <pre>\$ inxi -v 7</pre>

Ключи можно комбинировать, если они не конфликтуют. Например:

```
$ inxi -AG
```

Graphics:

```
Device-1: Intel Alder Lake-UP3 GT2 [Iris Xe Graphics] driver: i915 v:
kernel
```

```
Device-2: Syntek Integrated Camera driver: uvcvideo type: USB
```

```
Display: x11 server: X.Org v: 1.21.1.8 driver: X: loaded: modesetting
```

```

unloaded: fbdev,vesa dri: iris gpu: i915 resolution: 1: 1920x1080~60Hz
2: 1920x1080~60Hz
API: OpenGL v: 4.6 Mesa 23.0.4 renderer: Mesa Intel Graphics (ADL GT2)
Audio:
Device-1: Intel Alder Lake PCH-P High Definition Audio
driver: sof-audio-pci-intel-tgl
API: ALSA v: k6.1.12-un-def-alt1 status: kernel-api
Server-1: PulseAudio v: 16.1 status: active

```

Для получения более подробных данных о различных параметрах можно использовать один или несколько ключей `-x` (всего три дополнительных уровня данных: `-x`, `-xx`, `-xxx`). Эти ключи можно добавить в любой список опций, например: `-bxx` или `-Sxxx`.

Для получения более технических параметров (параметров администратора) используется ключ `--admin` или `-a`.

Чтобы обеспечить базовую конфиденциальность и безопасность, `inxi` позволяет отфильтровывать такие данные, как MAC-адрес сетевой карты, серийные номера, IP-адрес WAN и LAN, домашний каталог пользователя. Для активации фильтрации используется ключ `-z`, например:

```

$ inxi -iz
Network:
Device-1: Intel Alder Lake-P PCH CNVi WiFi driver: iwlwifi
IF: wlp0s20f3 state: up mac: <filter>
IP v4: <filter> type: dynamic noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: link
Device-2: Intel Ethernet I219-V driver: e1000e
IF: enp0s31f6 state: up speed: 1000 Mbps duplex: full mac: <filter>
IP v4: <filter> type: dynamic noprefixroute scope: global
IP v6: <filter> type: noprefixroute scope: global
Message: Output throttled. IPs: 4; Limit: 10; Override: --limit [1-x;-1
all]
WAN IP: <filter>

```

Следующая команда проверяет зависимости и программы, которые требуются для работы `inxi`, а затем показывает, какие пакеты нужно установить, чтобы добавить поддержку каждой функции:

```
$ inxi --recommends
```

Пример использования цветовой темы с выводом детальной информации в файл для анализа, команда выполняется от администратора, так как не вся информация доступна пользователю:

```
# inxi -c2 -v8 > inxi.txt
```

14.18.2. Команда `glxinfo`

Команда `glxinfo` позволяет получить информацию о OpenGL и реализации GLX в Xwindows.

Установка пакета:

```
# apt-get install glxinfo
```

Примеры:

- краткий вывод:

```
$ glxinfo -B
```

- показать информацию об активной видеокарте:

```
$ glxinfo -B | grep 'Device:'  
Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)
```

- получить информацию о поддержке OpenGL renderer:

```
$ glxinfo | grep rendering  
direct rendering: Yes
```

- посмотреть информацию по графике intel (NVIDIA):

```
$ glxinfo | grep OpenGL
```

- узнать версию сервер/клиент, версию драйвера:

```
$ glxinfo | grep version
```

- просмотреть количество памяти, доступное видеокарте:

```
$ glxinfo | egrep -i 'device|memory'  
egrep: warning: egrep is obsolescent; using grep -E  
Device: Mesa Intel(R) Graphics (ADL GT2) (0x46a8)  
Video memory: 39808MB  
Unified memory: yes
```

14.19. Xpra

Xpra – это инструмент, который запускает программы X11, обычно на удаленном хосте, и направляет их отображение на локальный компьютер без потери состояния (позволяет отключение и повторное подключение без прерывания перенаправленного приложения).

Xpra может предоставить удаленный доступ, как к отдельным приложениям, так и к новым/существующим сеансам рабочего стола.

Хгра не имеет root-доступа: т.е. приложения, перенаправленные хгра, отображаются на локальном рабочем столе как обычные окна, управляемые локальным оконным менеджером. Хгра также использует собственный протокол, который самонастраивается и относительно нечувствителен к задержкам.

На сервере утилита Хгра запускает в режиме демона нужную программу с заданным идентификатором сеанса, а на клиенте происходит присоединение к сеансу с этим идентификатором.

Доступ к сеансам можно получить по SSH или через защищенные паролем сокеты TCP (с SSL или без).

14.19.1. Установка

Для установки на сервере и на клиенте выполните команду:

```
# apt-get install xpra
```

Можно использовать клиент html5, и в этом случае на клиенте ничего устанавливать не нужно. А на сервере, начиная с хгра версии 4.4.4, нужно дополнительно установить пакет xpra-html5:

```
# apt-get install xpra-html5
```

14.19.2. Режимы работы

14.19.2.1. Запуск приложения

Запуск приложения или бесшовный режим (seamless) – позволяет пересылать клиенту отдельные окна приложений, эти окна появляются на рабочем столе клиента так же, как и другие локальные приложения.

Все операции по управлению окнами выполняются непосредственно клиентской ОС или оконным менеджером, поэтому любые задержки между клиентом и сервером не мешают действиям по управлению окнами (сворачивание, перемещение, изменение размера окна).

Пример запуска приложения xterm удаленно, через SSH, без предварительного запуска хгра на сервере:

```
$ xpra start ssh://user@192.168.0.101 --start="xterm"
```

Примечание. Хгра и запускаемое приложение должны быть установлены на сервере.

Вместо параметра `--start=команда`, можно использовать параметр `--start-child=команда`, позволяющий учитывать параметр `--exit-with-children`. Если параметр `--exit-with-children=yes`, то сервер `xpra` будет отслеживать состояние дочерних элементов, запущенных `--start-child`, и автоматически завершится, когда последний из них завершит работу.

Запуск приложения, с предварительным запуском сервера `xpra`:

- 1) на сервере: запустить экземпляр сервера `xpra`, автоматически выбрать дисплей и запустить программу (например, `xterm`) на этом виртуальном дисплее:

```
$ xpra start --start=xterm
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/1/server.log'
```

- 2) с клиента подключиться к этому экземпляру сервера:

```
$ xpra attach ssh://user@192.168.0.101/1
```

Локальное подключение:

- запустить экземпляр сервера `xpra` на дисплее 101 (или автоматически выбрать дисплей) и запустить программу (например, `firefox`) на этом виртуальном дисплее:

```
$ xpra start :101 --start=firefox
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/101/server.log'
```

- подключиться к этому экземпляру сервера:

```
$ xpra attach :101
```

Подключение с использованием сокетов TCP:

- запустить экземпляр сервера `xpra`:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000
Entering daemon mode; any further errors will be reported to:
'/run/user/500/xpra/S9454/server.log'
Actual display used: :1
Actual log file name is now: '/run/user/500/xpra/1/server.log'
```

- подключиться к серверу, используя выбранный порт:

```
$ xpra attach tcp://192.168.0.109:10000
```

ВНИМАНИЕ!

Использование параметра `--bind-tcp` без использования параметра `tcp-auth` не рекомендуется и представляет серьезную угрозу безопасности (особенно при 0.0.0.0), т. к. кто угодно может подключиться к этому порту и получить доступ к сеансу. Доступ к сеансам Xpra в режиме TCP и websocket можно защитить, используя аутентификацию и шифрование.

14.19.2.2. Запуск новой графической сессии

Режим рабочего стола (desktop) позволяет запустить вложенный сервер X11.

Запуск приложения:

```
$ xpra start-desktop --start=firefox
```

Та же команда, но с запуском сеанса и подключением к нему со стороны клиента:

```
$ xpra attach ssh://user@10.81.1.130/2
```

Где 2 номер дисплея.

Чтобы запустить оконный менеджер (WM) или среду рабочего стола (DE) достаточно в примере выше заменить команду `xterm` командой, которая запускает WM или DE, например:

```
$ xpra start-desktop ssh://user@192.168.0.99 --exit-with-children --start-child=mate-session
```

Подключение:

```
$ xpra attach ssh://user@192.168.0.154:101 --min-size=1200x800 --clipboard-direction=both --clipboard=yes --opengl=no
```

Примечание. Чтобы сеанс завершался при выходе из WM, следует использовать `--start-child` и `--exit-with-children`.

14.19.2.3. Получение управления запущенной графической сессией (shadow режим)

Этот режим позволяет использовать xpra для удаленного доступа к существующему сеансу рабочего стола (обычно подключенному к реальному физическому дисплею).

Примечание. Shadow режим поддерживается на всех платформах, включая MS Windows и Mac OS X, но не на Wayland. В некоторых случаях, использование этого режима, может вызвать высокую нагрузку на процессор как на сервере, так и на клиенте. На большинстве платформ затеняемый дисплей должен быть активен: не заблокирован и не выключен.

Если к машине, к дисплею X11 которой нужно получить удаленный доступ, есть SSH-доступ, можно на клиенте запустить команду:

```
$ xpra shadow ssh://user@HOST/
```

В результате выполнения этой команды будет произведено подключение по SSH к HOST, запущен теневой сервер xpra и произведено подключение к нему. Теневой сервер будет остановлен после отключения.

При этом на сервере в трее появится значок («Exit» – остановить сервер, «Read Only» – запретить управление, только просмотр рабочего стола) (Рис. 230).

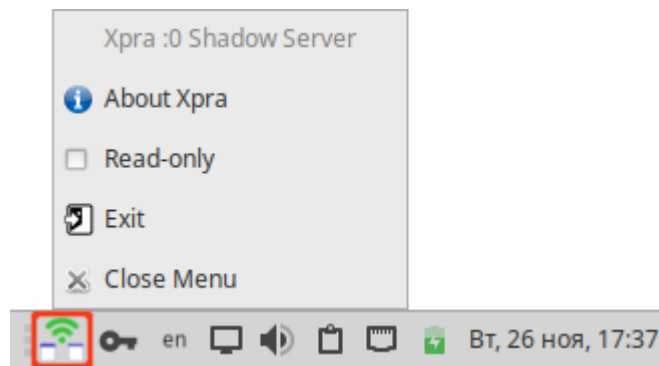


Рис. 230 – Значок Xpra

Если запуск через SSH не поддерживается или нужно запустить теневой сервер вручную и, возможно, настроить дополнительные параметры, можно запустить его из оболочки. Пример запуска управления запущенной графической сессией через TCP-сокеты:

```
$ xpra shadow :0 --bind-tcp=0.0.0.0:9876
```

14.19.3. Использование

14.19.3.1. Некоторые команды xpra

Некоторые команды xpra приведены в таблице 17.

Т а б л и ц а 17 – Команды xpra

Команда	Описание	Пример
xpra start	Запустить новый сервер xpra (при запуске удаленного сервера со строкой подключения <code>ssh://HOST/DISPLAY</code> новый сеанс также будет присоединен)	<pre>\$ xpra start :7 \$ xpra start -- start=gimp</pre>
xpra start-desktop	Запустить вложенный сервер X11, все дочерние команды будут запускаться на вложенном сервере X11	<pre>\$ xpra start-desktop -- start=xfce4-session</pre>
xpra attach	Подключиться к работающему серверу xpra. Любые приложения, использующие этот сервер, будут перенаправляться на текущий экран	<pre>\$ xpra attach :7 \$ xpra attach ssh://user@test/7</pre>
xpra detach	Отсоединить данный дисплей xpra	<pre>\$ xpra detach :7</pre>
xpra screenshot	Сделать снимок экрана и сохранить его в файле с указанным именем (снимки экрана можно делать только при подключенном клиенте)	<pre>\$ xpra screenshot my.jpg</pre>
xpra version	Вывести версию сервера	<pre>\$ xpra version 4.4.4-r0</pre>
xpra info	Вывести версию, статус и статистику	
xpra top	Отобразить ключевые атрибуты работоспособности сервера	
xpra control	Изменить параметры запущенного сервера. Список команд можно получить, указав «help» в качестве команды (например, <code>xpra control :1 help</code>)	<pre>\$ xpra control :1 min- quality 20</pre>
xpra stop	Подключиться к работающему серверу xpra и запросить его немедленное завершение. Обычно это приводит к тому, что любые приложения, использующие этот сервер, также прекращают работу	
xpra exit	Подключиться к работающему серверу xpra и запросить его немедленное завершение. В отличие от команды <code>xpra stop</code> , процесс <code>Xvfb</code> и его клиенты X11 (если таковые имеются) останутся запущенными	
xpra showconfig	Вывести конфигурацию xpra. В качестве дополнительных аргументов можно указать определенные параметры, или использовать специальное значение <code>all</code> , чтобы отобразить все параметры	<pre>\$ xpra showconfig clipboard-direction clipboard-direction = 'both'</pre>
xpra list	Вывести список всех серверов xpra, запущенные текущим пользователем на текущей машине	
xpra shadow	Предоставить доступ к рабочему столу (существующему дисплею X11). Если активен только один дисплей X11 и его номер меньше 10, он может быть обнаружен автоматически. Для этого режима работы настоятельно рекомендуется использовать видеокодек (h264 или vp8)	

Окончание таблицы 17

Команда	Описание	Пример
xpra проху	Позволяет одному серверу проксировать соединения для нескольких других, потенциально выступая в качестве точки входа для балансировки нагрузки или аутентификации для многих сеансов. Прокси-сервер будет создавать новый процесс для каждого прокси-соединения, этот прокси-процесс создаст неаутентифицированный новый сокет домена unix, который можно использовать с подкомандами info, version и stop	

14.19.3.2. Строка подключения

Локальный дисплей (только для локальных дисплеев локального пользователя):

:DISPLAY

Подключение с использованием SSH:

ssh://[USERNAME[:PASSWORD]@]HOST[:SSH_PORT]/[DISPLAY][?QUERYSTRING]

QUERYSTRING можно использовать для указания прокси-сервера

ssh: ?proxy=ssh://[ИМЯ ПОЛЬЗОВАТЕЛЯ[:ПАРОЛЬ]@]HOST[:SSH_PORT].

В этом случае xpra установит SSH-соединение с указанным «прокси-сервером» и с этого хоста xpra установит SSH-соединение с сервером xpra.

Для обратной совместимости режим SSH также поддерживает синтаксис:

ssh:[USERNAME[PASSWORD]@HOST:DISPLAY

Пароль нужно указывать только тогда, когда он требуется модулю аутентификации сервера.

Примечание. При подключении по ssh может потребоваться указать системный ssh-клиент:

```
$ xpra start --ssh=ssh ssh://user@192.168.0.101 --start=scratch-desktop
```

Или дописать в файл ~/.xpra/xpra.conf строку:

```
ssh = ssh
```

В режиме TCP используются номера портов, а не номера дисплеев. Если через один TCP-порт доступно несколько дисплеев (например, при использовании прокси-сервера), то можно также указать номер дисплея:

tcp://[USERNAME@]HOST:PORT[/DISPLAY]

Режим SSL (добавляет безопасный уровень сокетов поверх режима TCP):

```
ssl://[USERNAME@]HOST:PORT[/DISPLAY]
```

Подключиться по протоколу websocket:

```
ws://[USERNAME[:PASSWORD]@]HOST:PORT[/DISPLAY]
```

Подключиться по защищенному протоколу websocket (websocket с SSL):

```
wss://[USERNAME[:PASSWORD]@]HOST:PORT[/DISPLAY]
```

14.19.3.3. Дисплей

При запуске хгра сервера (`xpra start`) можно не использовать номер дисплея, в этом случае он будет выбран автоматически. Номер дисплея будет указан в выводе команды, также его можно увидеть, выполнив команду `xpra list`.

В противном случае, при запуске сервера хгра может потребоваться указать номер дисплея. Для этого можно выбрать любое число и поставьте перед ним двоеточие (например, `:7`, `:12` и `:3117`). Нужно учитывать, что:

- каждый X или хгра сервер, работающие на одном хосте должны использовать уникальный номер дисплея;
- первые несколько цифр (0, 1, 2) обычно используются реальными X серверами.

При указании сервера хгра в клиентской программе (`xpra attach`, `xpra detach`, `xpra stop`, `xpra exit`, `xpra version`, `xpra info`, `xpra list`, `xpra screenshot`) можно использовать указание дисплея в формате `:DISPLAY` при подключении к локальному узлу или одну из форм `ssh://[USER@]HOST/DISPLAY` при подключении к удаленному узлу. Если на узле запущен только один сеанс хгра, то номер дисплея можно не указывать.

Если при запуске сервера был указан параметр `--bind-tcp`, `--bind-ssl` `--bind-udp=[HOST]:PORT`, `--bind-ws`, `--bind-wss` или `--bind-vsock`, то к нему можно подключаться используя следующие строки:

```
tcp://HOST:PORT[/DISPLAY],
udp://HOST:PORT[/DISPLAY],
ssl://HOST:PORT[/DISPLAY],
ws://HOST:PORT[/DISPLAY],
wss://HOST:PORT[/DISPLAY] или vsock://HOST:PORT[/DISPLAY].
```

14.19.3.4. Сеть и аутентификация

Хрга поддерживает разные типы сетевых подключений (`tcp`, `ssl`, `ws`, `wss`, `vnc`, `ssh`, `vsock`, `quic` и т.д.), и большинство из них можно шифровать и мультиплексировать через один порт.

Безопасность зависит от типа подключения клиента хрга (`ssl`, `quic` и `ssh` считаются самыми безопасными, поскольку они обеспечивают проверку хоста и шифрование в одном протоколе).

Доступ к сеансам хрга через сокеты TCP можно защитить с помощью модулей аутентификации, но так как они не защищают само сетевое соединение от атак «человек посередине», то для защиты от таких атак можно использовать один из трех вариантов:

- шифрование AES;
- SSL;
- SSH.

14.19.3.4.1. Модули аутентификации

Примечание. При использовании для подключения к серверу SSH разделы шифрование и аутентификация можно пропустить (по умолчанию сокеты, используемые `ssh`, не используют аутентификацию).

Модули аутентификации приведены в таблице 18.

Т а б л и ц а 18 – Модули аутентификации

Модуль	Описание	Примечание
allow	Аутентификация всегда успешна (используется имя пользователя, предоставленное клиентом)	Небезопасно, и должно использоваться только для тестирования
none	Аутентификация всегда успешна (используется имя пользователя, под которым работает сервер)	Небезопасно, и должно использоваться только для тестирования
fail	Аутентификация всегда не успешна (пароль не запрашивается)	Полезно для тестирования
reject	Аутентификация всегда не успешна (пароль запрашивается)	Полезно для тестирования

Продолжение таблицы 18

Модуль	Описание	Примечание
env	Пароль сопоставляется с указанной переменной среды (по умолчанию XPRA_PASSWORD).	--auth=env:name=SOME_OTHER_ENV_VAR_NAME
password	Пароль сопоставляется с паролем, указанным с помощью опции value	--auth=password:value=mysecret
file	Сравнивает пароль с паролем, записанным в файле, указанным с помощью опции filename	--auth=file:filename=./password.txt Содержимое файла пароля будет рассматриваться как двоичные данные, ограничений на кодировку символов или размер файла нет. Следует остерегаться завершающих символов новой строки, которые будут включены в данные пароля (пример создания файла с паролем: echo -n "mypassword" > password.txt)
multifile	Сопоставляет имя пользователя и пароль с содержимым файла аутентификации, указанным с помощью опции filename	Файл аутентификации должен содержать учетные данные пользователей в формате: username password uid gid displays env_opts session_opts Имя пользователя и пароль не должны содержать символ вертикальной черты (), который используется в качестве разделителя. Этот модуль устарел, вместо него следует использовать sqlite
ram	Проверяет имя пользователя и пароль с помощью системы RAM	Аутентификация ОС Linux
win32	Проверяет имя пользователя и пароль с помощью win32security	Аутентификация MS Windows
sys	Системная аутентификация	Автоматически выбирает соответствующий системный модуль аутентификации (либо ram, либо win32)
sqlite, mysql, sql	Сверяет имя пользователя и пароль с файлом базы данных sqlite, указанным с помощью параметра filename (sqlite), или с базой данных, указанной с помощью параметра uri (mysql и sql)	Аутентификация будет обработана с использованием следующего запроса (настраивается с помощью параметра password_query): SELECT password FROM users WHERE username=(?) Сеансы, доступные для каждого пользователя, будут запрашиваться с помощью запроса (настраивается с помощью параметра session_query): SELECT uid, gid, displays, env_options, session_options FROM users WHERE username=(?)
exec	Делегирует процедуру аутентификации внешней команде. Команда указывается с помощью атрибута command	Команда должна вернуть 0, чтобы разрешить доступ, любое другое значение будет запрещать доступ
peercred	Аутентификация SO_PEERCREDS	

Окончание таблицы 18

Модуль	Описание	Примечание
hosts	Проверяет хост с помощью системной библиотеки tcp-wrappers	Подробнее см. в hosts.allow и hosts.deny
kerberos-password	Проверяет имя пользователя и пароль с помощью проверки подлинности Kerberos	Модуль не использует билеты Kerberos, и пароль будет отправлен на сервер в виде открытого текста. Следует использовать только для тестирования
kerberos-ticket	Проверяет билет Kerberos, полученный клиентом	
gss	Проверяет билет GSS, полученный клиентом	
u2f	Запрашивает у клиента токен U2F	
ldap	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap	
ldap3	Проверяет имя пользователя и пароль на сервере LDAP, используя библиотеку python-ldap3	

Предпочтительный способ указания аутентификации – в опции сокета.

Примеры:

```
$ XPRA_PASSWORD=mysecret
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000,auth=env

$ SOME_OTHER_ENV_VAR_NAME=mysecret
$ xpra start --bind-
tcp=0.0.0.0:10000,auth=env:name=SOME_OTHER_ENV_VAR_NAME

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=password:value=mysecret

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=file:filename=/path/to/mypasswordfile.txt

$ xpra start --bind-
tcp=0.0.0.0:10000,auth=sqlite:filename=/path/to/userlist.sdb
```

Разные сокеты могут использовать разные модули аутентификации:

```
$ xpra start --start=xterm -d auth \
--bind-
tcp=0.0.0.0:10000,auth=hosts,auth=file:filename=password.txt --bind \
--bind-tcp=0.0.0.0:10001,auth=sys
```

14.19.3.5. Журналирование

Журналирование управляется опцией `--debug (-d)`.

Например, запуск сервера `xpra` с включенной отладкой фокуса:

```
$ xpra start -d focus --start=xterm
```

Список возможных категорий журналов можно получить, выполнив команду:

```
$ xpra -d help
```

Для записи в журнал событий всех категорий используется значение `all` (следует избегать применение этого значения, так как вывод будет очень подробным и сложным для восприятия).

Добавление к категории знака «-» отключает для данной категории ведение журнала. Например, регистрировать все категории, кроме `window` и `focus`:

```
$ xpra start :10 -d all,-window,-focus
```

Категорию журналирования также можно включить с помощью переменных среды. Это может потребоваться, если нет возможности изменить командную строку, или если регистрация должна происходить очень рано.

Например, включить отладку «геометрии» с помощью подкоманды `attach`:

```
XPRA_GEOMETRY_DEBUG=1 xpra attach
```

У запущенного сервера `xpra` можно изменить параметры журналирования с помощью подкоманды `control` (эту команду можно использовать как на сервере, так и на клиенте):

```
$ xpra control :DISPLAY debug enable CATEGORY
```

Сервер также может пересылать команды управления отладкой подключенным к нему клиентам:

```
$ xpra control :DISPLAY client debug enable geometry
```

Можно включить сразу несколько категорий:

```
$ xpra control :2 debug enable window geometry screen
```

Включить только регистраторы, которые соответствуют категориям с `+`:

```
$ xpra control :2 debug disable focus+grab
```

Конфиденциальная информация, такая как пароли и ключи обычно не отображается в журнале, но все же, используя журнал можно собрать достаточно данных, чтобы представлять реальную угрозу.

Хорошей превентивной мерой является отключение удаленного ведения журнала и выключение канала управления сервером.

`xpra shell` — это очень мощная функция отладки, которая обеспечивает полный доступ ко всем структурам данных, хранящимся на клиенте и сервере. По умолчанию эта функция отключена.

14.19.4. Клиент HTML5

Пример запуска экземпляра сервера:

```
$ xpra start --start=xterm --bind-tcp=0.0.0.0:10000 --html=on
```

Или:

```
$ xpra start --start=xterm --bind-ws=0.0.0.0:10000
```

Теперь можно получить доступ к этому сеансу в веб-браузере (рис. 231).

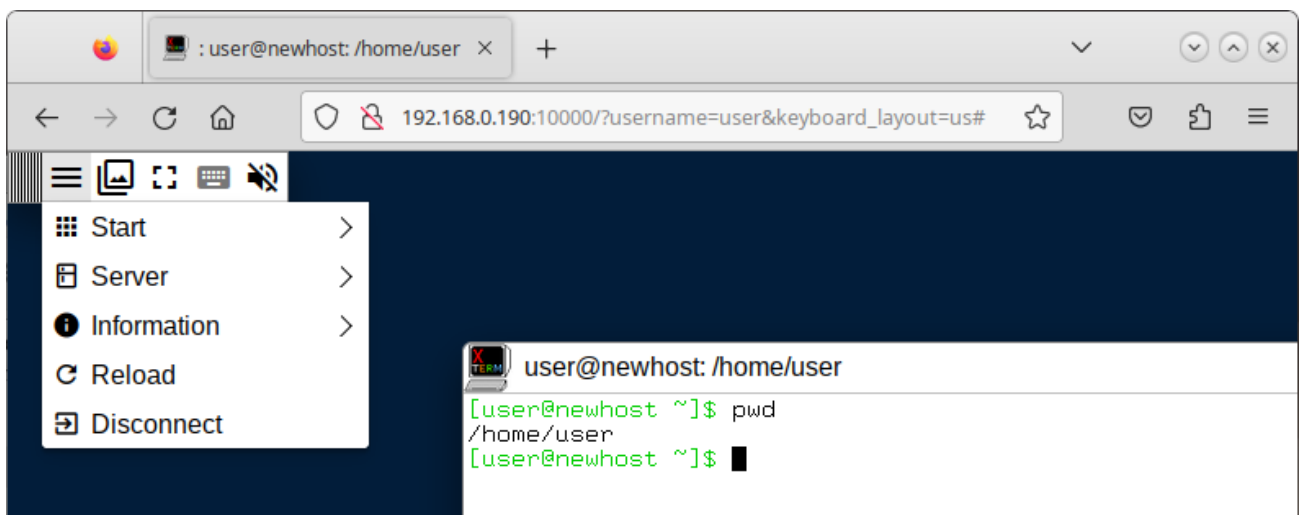


Рис. 231

Параметры подключения можно указать с помощью диалоговой формы подключения (`http://host:port/connect.html`) или указать как параметры URL, например: `http://192.168.0.99:10000/?username=user&keyboard_layout=us`.

Значения по умолчанию можно указать в файле:

```
/etc/xpra/html5-client/default-settings.txt.
```

Описание параметров подключения приведены в таблице 19.

Т а б л и ц а 19 – Описание параметров подключения

Параметр	Описание
Параметры подключения	
server	Имя хоста или IP-адрес хрга-сервера
port	Номер порта хрга-сервера
username	Аутентификация на сервере
password	Аутентификация на сервере
ssl	Включить SSL-соединение с сервером хрга
insecure	Разрешить отправку паролей по незашифрованным соединениям (No)
path	Путь WebSocket для подключения (обычно не требуется)
display	Дисплей для подключения (для прокси-серверов)
password	Аутентификация на сервере
encryption	Для включения шифрования, следует указать AES-CBC, AES-CTR или AES-CFB
key	Ключ шифрования AES
sharing	Разрешить другим клиентам подключаться к тому же сеансу (No)
steal	Взять на себя управление сеансом и отключить всех существующих клиентов (Yes)
reconnect	Автоматически переподключаться при обрыве соединения (Yes)
bandwidth_limit	Бюджет пропускной способности в битах в секунду (0 – без ограничений)
override_width	Ширина рабочего стола клиента, ширина окна веб-браузера в пикселях (по умолчанию – ширина окна веб-браузера)
Функции	
keyboard	Включить ввод с клавиатуры
keyboard_layout	Раскладка клавиатуры, которую будет использовать клиент (по умолчанию язык веб-браузера)
clipboard	Включить общий доступ к буферу обмена.
printing	Включить переадресацию принтера
file_transfer	Включить передачу файлов
swap_keys	Поменять местами клавиши Command и Control
scroll_reverse_x	Реверс оси X указателя мыши
floating_menu	Показывать плавающее меню
toolbar_position	Положение панели инструментов по умолчанию (например, top, top-right)
autohide	Скрыть большую часть панели инструментов до наведения на нее указателя
sound	Переадресация звука с сервера («выход динамика»)
video	Разрешить использование программного декодирования видео
Дополнительные параметры	
audio_codec	Используемый аудиоформат (detected)
encoding	Кодировка изображения, например, png, jpeg, webp и т. д. (auto)
remote_logging	Отправлять важные события на сервер
action	Режим подключения, например, start, shadow (connect)
shadow_display	Дисплей, если action=shadow
submit	Показать диагностику при отключении
start	Запустить сервер
exit_with_children	Завершить сессию, когда завершается последняя команда запуска (при запуске нового сеанса)
exit_with_client	Завершить сеанс при закрытии соединения (при запуске нового сеанса)

Значения параметров `server`, `port` и `ssl` отражают соединение, которое использовалось для загрузки клиента HTML5 (то, что указано в строке URL-адреса веб-браузера), и эти значения обычно не нужно изменять.

Примечание. Если в окне клиента при вводе с клавиатуры ничего не происходит, попробуйте изменить раскладку клавиатуры (параметр `keyboard_layout`).

14.19.5. Графический интерфейс

Графический интерфейс `xpra` («Меню» → «Приложения» → «Интернет» → «Xpra») (рис. 232).

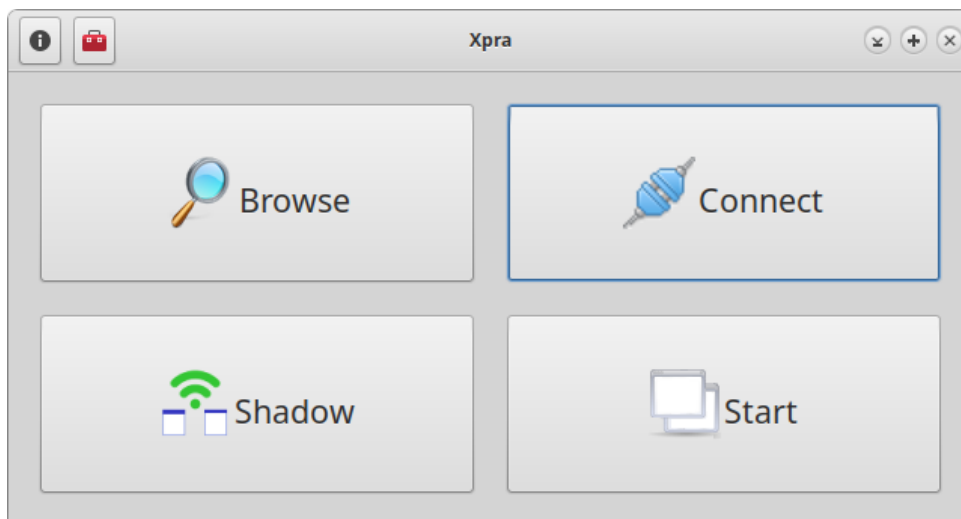


Рис. 232

«Browse» – просмотреть список и подключиться к локальному дисплею (рис. 233).

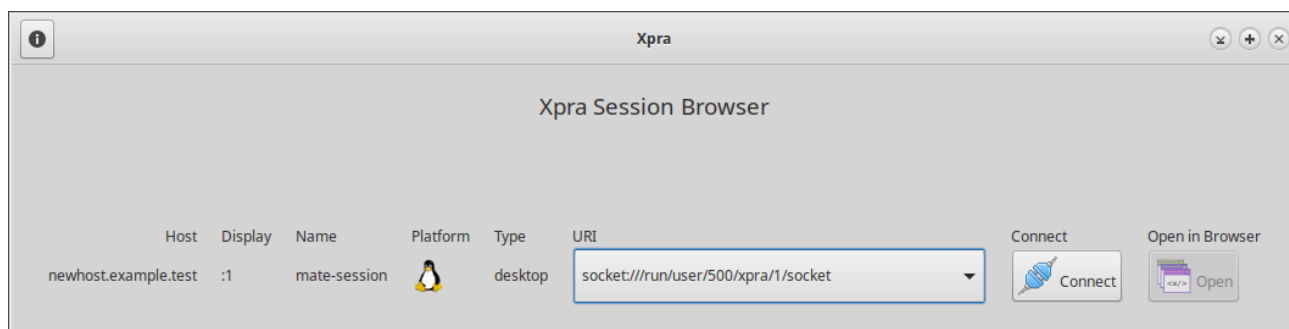


Рис. 233

«Connect» – подключиться к удаленному серверу (рис. 234).

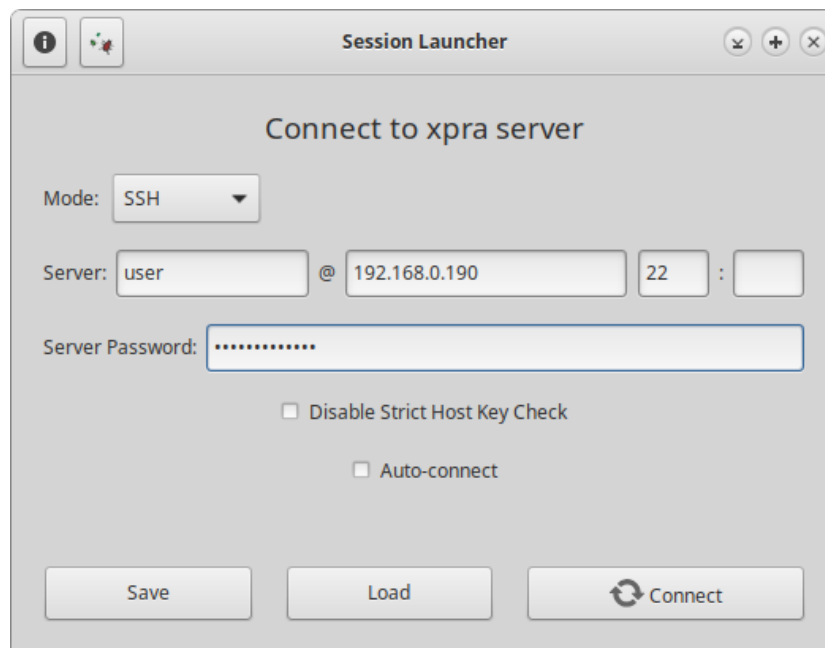


Рис. 234

«Shadow» – предоставить доступ к рабочему столу.

«Start» – запустить сервер xpra (рис. 235).

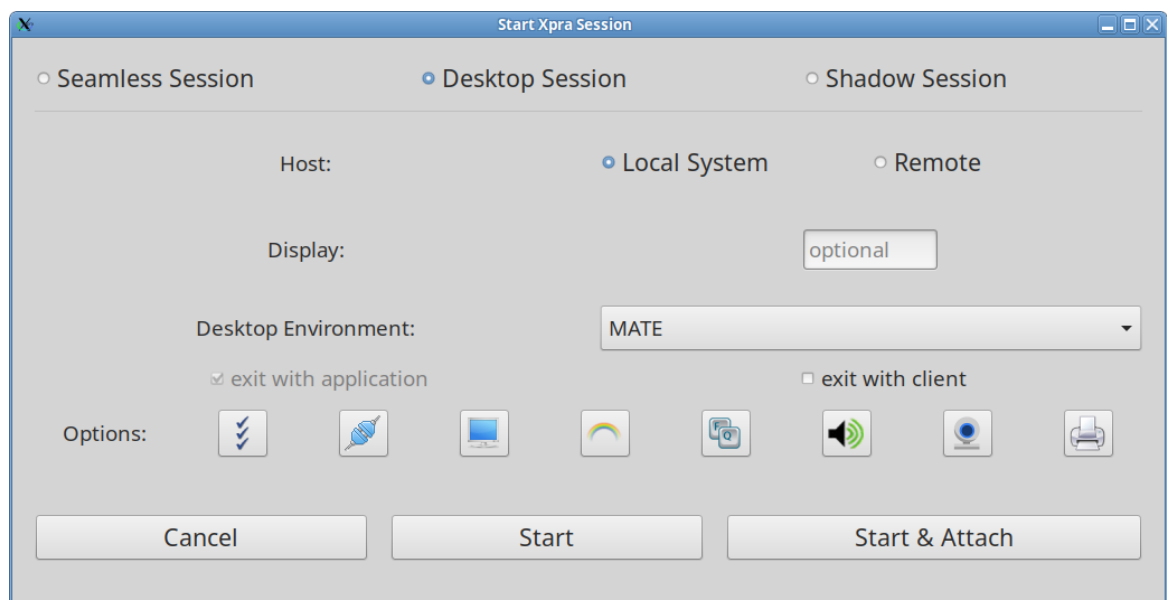


Рис. 235

14.20. Установка корневого сертификата

Для поддержки работы сайтов с российскими сертификатами и установки комплекта корневых сертификатов СА России достаточно установить пакет `ca-certificates-digital.gov.ru`:

```
# apt-get install ca-certificates-digital.gov.ru
```

В результате в хранилище доверенных сертификатов должны появиться сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA»:

```
$ trust list |grep "Russian Trusted" -B 2 -A 2

pkcs11:id=%E1%D1%81%E5%CE%5A%5F%04%AA%D2%E9%B6%9D%66%B1%C5%FA%AC%2C%87;
type=cert
  type: certificate
  label: Russian Trusted Root CA
  trust: anchor
  category: authority
--
pkcs11:id=%D1%E1%71%0D%0B%2D%81%4E%6E%8A%4A%8F%4C%23%B3%4C%5E%AB%69%0B;
type=cert
  type: certificate
  label: Russian Trusted Sub CA
  trust: anchor
  category: authority
```

Сертификаты «Russian Trusted Root CA» и «Russian Trusted Sub CA» в Firefox (рис. 236).

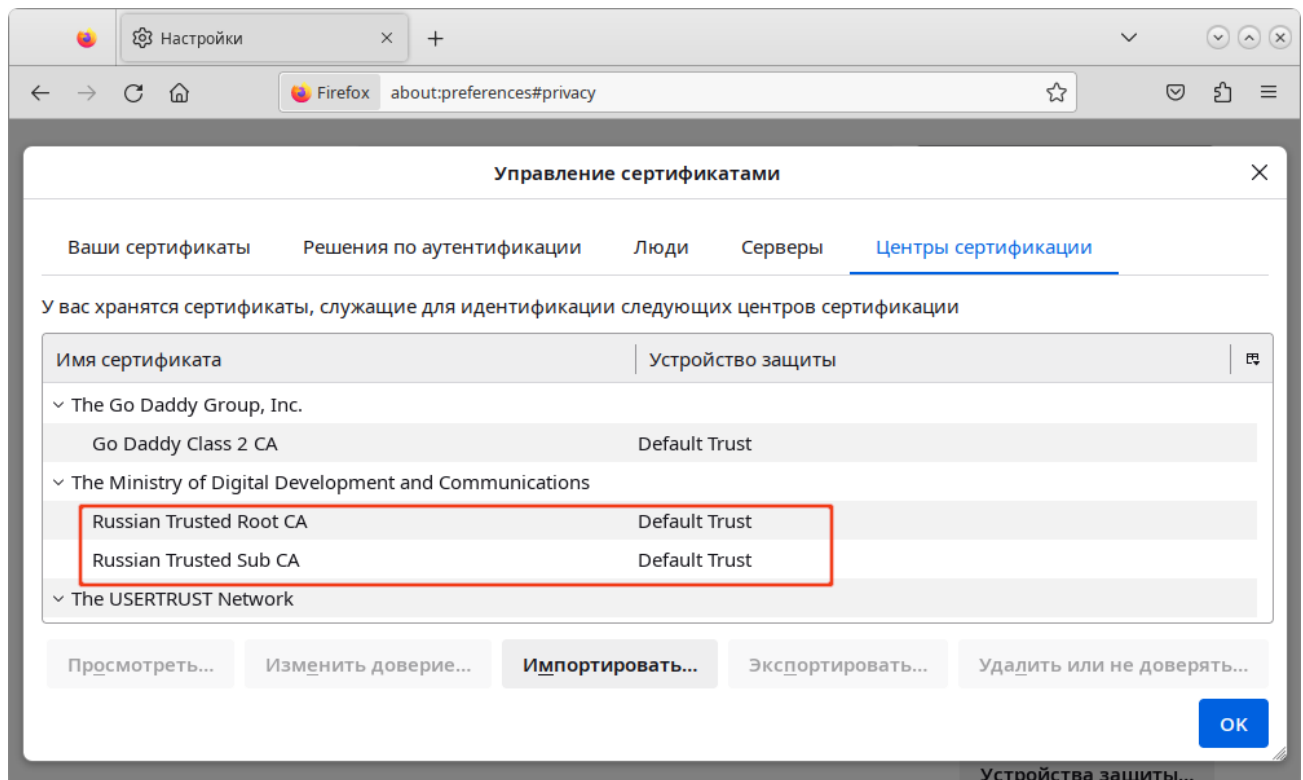


Рис. 236 – Корневые сертификаты СА России в Firefox

15. УПРАВЛЕНИЕ ПРОГРАММНЫМИ ПАКЕТАМИ

После установки ОС Альт СП при первом запуске доступен тот или иной набор ПО. Количество предустановленных программ зависит от набора программ конкретного дистрибутива или от выбора, сделанного при установке системы. Если интересующие программы не были обнаружены в системе, то имеется возможность доустановить их из разных источников.

Дополнительное ПО может находиться на установочном диске и (или) в специальных банках программ (репозиториях), расположенных в сети Интернет и (или) в локальной сети. Программы, размещенные в указанных источниках, имеют вид подготовленных для установки пакетов.

Для установки, удаления и обновления программ и поддержания целостности системы в ОС семейства Linux используются менеджеры пакетов типа «rpm». Для автоматизации этого процесса и применяется усовершенствованная система управления программными пакетами APT (Advanced Packaging Tool).

⚠ Перед установкой программ внимательно ознакомьтесь с п. 15.4 «Управление установкой (инсталляцией) компонентов программного обеспечения».

Автоматизация достигается созданием одного или нескольких внешних репозиториев, в которых хранятся пакеты программ и относительно которых производится сверка пакетов, установленных в системе. Репозитории могут содержать как официальную версию дистрибутива, обновляемую его разработчиками по мере выхода новых версий программ, так и локальные наработки, например, пакеты, разработанные внутри компании.

Таким образом, в распоряжении APT находятся две базы данных: одна описывает установленные в системе пакеты, вторая – внешний репозиторий. APT отслеживает целостность установленной системы и, в случае обнаружения противоречий в зависимостях пакетов, руководствуется сведениями о внешнем репозитории для разрешения конфликтов и поиска корректного пути их устранения.

Система АРТ состоит из нескольких утилит. Чаще всего используется утилита управления пакетами `apt-get`, которая автоматически определяет зависимости между пакетами и строго следит за их соблюдением при выполнении любой из следующих операций: установка, удаление или обновление пакетов.

15.1. Источники программ (репозитории)

15.1.1. Репозитории для АРТ

Репозитории, с которыми работает АРТ, отличаются от обычного набора пакетов наличием мета информации – индексов пакетов, содержащихся в репозитории, и сведений о них. Поэтому, чтобы получить всю информацию о репозитории, АРТ достаточно получить его индексы.

АРТ может работать с любым количеством репозиториях одновременно, формируя единую информационную базу обо всех содержащихся в них пакетах. При установке пакетов АРТ обращает внимание только на название пакета, его версию и зависимости, а расположение в том или ином репозитории не имеет значения. Если потребуется, АРТ в рамках одной операции установки группы пакетов может пользоваться несколькими репозиториями.

Подключая одновременно несколько репозиториях, нужно следить за тем, чтобы они были совместимы друг с другом по пакетной базе – отражали один определенный этап разработки. Совместимыми являются основной репозиторий дистрибутива и репозиторий обновлений по безопасности к данному дистрибутиву. В то же время смешение среди источников АРТ репозиториях, относящихся к разным дистрибутивам, или смешение стабильного репозитория с нестабильной веткой разработки (*Sisyphus*) чревато различными неожиданными трудностями при обновлении пакетов.

АРТ позволяет взаимодействовать с репозиторием с помощью различных протоколов доступа. Наиболее популярные – HTTP и FTP, однако существуют и некоторые дополнительные методы.

Для того чтобы АРТ мог использовать тот или иной репозиторий, информацию о нем нужно поместить в файл.

Файлы описания источников находятся в каталоге `/etc/apt/sources.list.d/` и имеют расширение `.list`, например:

```
altsp.list
sources.list
```

Так же, есть файл с предопределенным именем: `/etc/apt/sources.list`.

Утилита `apt-get`, в момент работы, просматривает одновременно все эти файлы.

Описания репозиториев заносятся в этот файл в следующем виде:

```
rpm [подпись] метод: путь база название
rpm-src [подпись] метод: путь база название
```

где:

- `rpm` или `rpm-src` – тип репозитория (скомпилированные программы или исходные тексты);
- `[подпись]` – необязательная строка-указатель на электронную подпись разработчиков. Наличие этого поля подразумевает, что каждый пакет из данного репозитория должен быть подписан соответствующей электронной подписью. Подписи описываются в файле `/etc/apt/vendors.list`;
- `метод` – способ доступа к репозиторию: `ftp`, `http`, `file`, `rsh`, `ssh`, `cdrom`, `copy`;
- `путь` – путь к репозиторию в терминах выбранного метода;
- `база` – относительный путь к базе данных репозитория;
- `название` – название репозитория.

Пример синтаксиса, описывающего источники приведен в п. 15.1.2.2.

Если первым символом идет символ комментария – строка считается простым текстом, а не описанием источника. У активной записи, в начале строки этот символ отсутствует.

Описание источника состоит из ключевых элементов:

- тип репозитория – применяется пакетная система `rpm` (все источники описывают `rpm`-репозитории);
- ключ подписи – пакеты в репозитории подписаны и могут быть проверены, если указать ключ. Списки доступных ключей хранятся в каталоге `/etc/apt/vendors.list` в файлах с расширением `.list`. Так же, есть файл `/etc/apt/vendors.list`. В примере использован ключ `[cert8]`;

- адрес – адрес расположения репозитория. Репозитории доступны несколькими способами (ftp://, http:// и rsync://). После описания способа доступа прописан адрес;
- тип данных – репозиторий может содержать как исполняемые пакеты, так и пакеты для разработчиков или пакеты с данными общего характера. Например, тип x86_64-i586 показывает, что в данном репозитории находятся исполняемые программы и библиотеки, собранные для 32-х разрядных систем (32bit). При использовании дистрибутива для 64-х разрядных процессоров, тип содержимого будет x86_64. В общем случае, запись источника с выполняемыми программами и библиотеками дополняет источник с типом noarch. Этот источник предоставляет пакеты, идентичные для различных платформ. Как правило, это данные, небинарные библиотеки к Perl, Python и т. п.;
- название – название репозитория.

Для добавления в `sources.list` репозитория на CD/DVD-носителе информации в АРТ предусмотрена специальная утилита – `apt-cdrom`. Чтобы добавить запись о репозитории на носителе, достаточно вставить его в привод, например, для чтения (записи) CD (DVD)-носителей информации и выполнить команды создания директории, монтирования устройства, добавления носителя, указав актуальное имя устройства:

```
# mkdir /media/ALTLinux
# mount /dev/носитель /media/ALTLinux/
# apt-cdrom -m add
```

После этого в `sources.list` появится запись о подключенном диске примерно такого вида:

```
rpm cdrom:[ALT SP Workstation 10.2 11102-01 e2kv4]/ ALTLinux main
```

После того как список репозитория в `sources.list` будет отредактирован, нужно обновить локальную базу данных АРТ о доступных пакетах, выполнив команду:

```
# apt-get update
```

В случае если в `sources.list` присутствует репозиторий, содержимое которого может изменяться, то прежде чем работать с АРТ, нужно синхронизировать локальную базу данных с удаленным сервером. Обновление данных осуществляется командой:

```
# apt-get update
```

Так происходит с любым постоянно разрабатываемым репозиторием, например, появляются обновления по безопасности (`updates`).

Локальная база данных создается заново каждый раз, когда в репозитории происходит изменение: добавление, удаление или переименование пакета. Для репозитория, находящегося на извлекаемых носителях информации и подключенных командой `apt-cdrom add`, синхронизация производится единожды в момент подключения.

При установке определенного пакета АРТ производит поиск самой новой версии этого пакета во всех известных ему репозиториях вне зависимости от способа доступа к ним.

Так, если в репозитории, доступном в сети Интернет, обнаружена более новая в сравнении с компакт-диском версия программы, то АРТ начнет загружать соответствующий пакет из сети Интернет.

Поэтому, если подключение к сети Интернет отсутствует или ограничено низкой пропускной способностью канала или высокой стоимостью, то следует закомментировать строчки (добавить в начало строки символ `#`) в `/etc/apt/sources.list`, относящиеся к ресурсам в сети Интернет.

15.1.2. Добавление репозитория с использованием терминала

15.1.2.1. Скрипт `apt-repo`

Для добавления репозитория можно воспользоваться скриптом `apt-repo`. Для выполнения большинства команд требуются права администратора.

Просмотреть список активных репозитория можно, выполнив команду:

```
apt-repo list
```

Для добавления репозитория в список активных репозиториях используется команда:

```
apt-repo add репозиторий
```

Для удаления или выключения репозитория используется команда:

```
apt-repo rm репозиторий
```

Для обновления информации о репозиториях необходимо выполнить команду:

```
apt-repo update
```

Для получения более подробной справки о команде можно выполнить команду:

```
man apt-repo
```

```
или apt-repo --help
```

15.1.2.2. Добавление репозитория вручную

Для редактирования списка репозиториях можно отредактируйте в любом текстовом редакторе файлы из каталога `/etc/apt/sources.list.d/` (см. п. 15.1.1). Нужны права администратора для изменения этих файлов.

В файле `altsp.list` может содержаться примерно такая информация:

```
$ cat /etc/apt/sources.list.d/altsp.list
# update.altsp.su (IVK, Moscow)

# ALT Certified 8
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f/branch/x86_64-i586 classic
#rpm [cert8] ftp://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/noarch classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/x86_64-i586 classic
rpm [cert8] http://update.altsp.su/pub/distributions/ALTlinux
c10f2/branch/noarch classic
```

⚠ В файле `/etc/apt/sources.list.d/altsp.list` перечислены официальные источники программ для обновления ПИ, которые можно использовать для установки дополнительных программных пакетов с учетом ограничений лицензии на продукт.

По сути, каждая строка соответствует некому репозиторию. Не активные репозитории – строки, начинающиеся с `#rpm`.

Для выключения репозитория достаточно закомментировать соответствующую строку (дописать символ решетки перед строкой). Для добавления нового репозитория необходимо дописать его вниз этого или любого другого файла.

После добавления репозитория необходимо обновить информацию о них, выполнив команду `apt-get update` или `apt-repo update`. Для выполнения этих команд нужны права администратора.

15.1.3. Программа управления пакетами Synaptic

Программа Synaptic также может использоваться для выбора репозитория, совместимого с дистрибутивом (рис. 237). Для указания конкретного репозитория в меню «Параметры» → «Репозитории» нужно отметить один из предлагаемых вариантов и нажать кнопку «ОК». К предложенному списку можно добавить репозитории, нажав на кнопку «Создать» и введя данные.

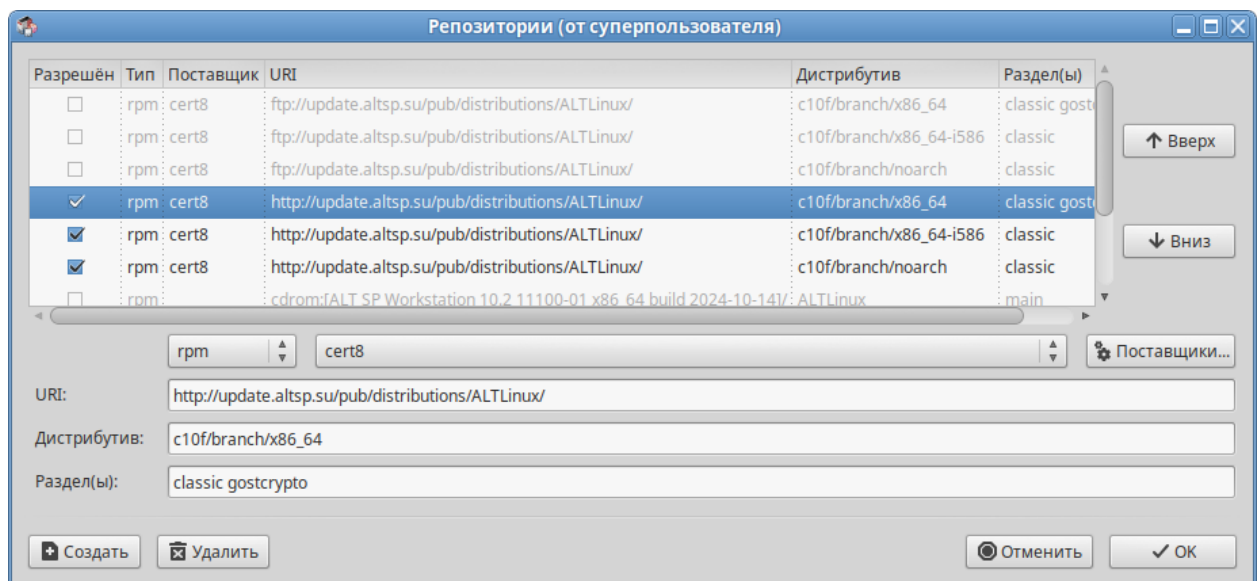


Рис. 237 – Пример списка репозитория

После выбора и добавления репозитория необходимо получить сведения о находящихся в них пакетах (кнопка «Получить сведения» или меню «Правка» → «Получить сведения о пакетах»). В противном случае, список доступных для установки программ будет не актуален.

15.2. Обновление информации о репозиториях в АРТ

Практически любое действие с системой АРТ начинается с обновления данных от активированных источников. Список источников нужно обновлять при поиске новой версии пакета, установке пакетов или обновлении установленных пакетов новыми версиями.

Обновление данных осуществляется командой:

```
# apt-get update
```

Программа загрузит данные с активированных источников в свой кеш.

Пример:

```
# apt-get update
Получено: 1 http://update.altsp.su c10f/branch/x86_64 release [3578B]
Получено: 2 http://update.altsp.su c10f/branch/x86_64-i586 release
[1033B]
Получено: 3 http://update.altsp.su c10f/branch/noarch release [2199B]
Получено 6810B за 5s (1292B/s).
Найдено http://update.altsp.su c10f/branch/x86_64/classic pkglist
Найдено http://update.altsp.su c10f/branch/x86_64/classic release
Найдено http://update.altsp.su c10f/branch/x86_64/gostcrypto pkglist
Найдено http://update.altsp.su c10f/branch/x86_64/gostcrypto release
Найдено http://update.altsp.su c10f/branch/x86_64-i586/classic pkglist
Найдено http://update.altsp.su c10f/branch/x86_64-i586/classic release
Найдено http://update.altsp.su c10f/branch/noarch/classic pkglist
Найдено http://update.altsp.su c10f/branch/noarch/classic release
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
```

После выполнения этой команды, apt обновит свой кеш новой информацией.

15.3. Поиск пакетов (apt-cache)

Утилита apt-cache предназначена для поиска программных пакетов в репозитории, и позволяет искать не только по имени пакета, но и по его описанию.

Команда apt-cache search <подстрока> позволяет найти все пакеты, в именах или описании которых присутствует указанная подстрока. Пример поиска может выглядеть следующим образом:

```
$ apt-cache search ^gimp
gimp - The GNU Image Manipulation Program
libgimp - GIMP libraries
libgimp-devel - GIMP plugin and extension development kit
gimp-help-en - English help files for the GIMP
gimp-help-ru - Russian help files for the GIMP
gimp-plugin-separateplus - Improved version of the CMYK Separation
plug-in [...]
gimp-script-ISONoiseReduction - Gimp script for reducing sensor noise
```



```
[...]
gimp-plugin-gutenprint - GIMP plug-in for gutenprint
gimp-plugin-ufraw - GIMP plugin for opening and converting RAW files
[...]
```

Символ «^» в поисковом выражении, указывает на то, что нужно найти совпадения только в начале строки (в данном случае – в начале имени пакета).

Для того чтобы подробнее узнать о каждом из найденных пакетов и прочитать его описание, можно воспользоваться командой `apt-cache show`, которая покажет информацию о пакете из репозитория:

```
$ apt-cache show gimp-help-ru

Package: gimp-help-ru
Section: Graphics
Installed Size: 62888647
Maintainer: Valery Inozemtsev <shrek@altlinux.ru>
Version: 2.10.0-alt1:p10+286245.100.1.1@1633083328
Pre-Depends: rpmlib(PayloadIsXz)
Provides: gimp-help-ru (= 2.10.0-alt1:p10+286245.100.1.1)
Obsoletes: gimp-help-common (< 2.10.0-alt1)
Architecture: noarch
Size: 45251404
MD5Sum: 04b5c9d3b5bb3f33822761497f58c7cf
Filename: gimp-help-ru-2.10.0-alt1.noarch.rpm
Description: Russian help files for the GIMP
 Russian help files for the GIMP.
```

Команда `apt-cache` позволяет осуществлять поиск по русскому слову, однако в этом случае будут найдены только те пакеты, у которых есть описание на русском языке.

15.4. Управление установкой (инсталляцией) компонентов программного обеспечения

Установку пакетов может производить только администратор.

ВНИМАНИЕ!

Обновление пакетов выполняется при отсутствии нарушений целостности системы. Проверка целостности системы выполняется:

1) с помощью команды:

```
# integalert
```

При отсутствии изменений вывод команды: `integrity check OK`

2) или просмотром записей `ossec` в системном журнале с помощью команды:

```
# journalctl | grep ossec
```

При отсутствии изменений в записях журнала присутствует:
`No changes[ossec]`

ВНИМАНИЕ!

Если в системе инициализированы средства контроля целостности IMA/EVM (должны быть инициализированы), то установка/обновление пакетов должны происходить с использованием команды `integrity-applier` (см. п. 15.4.1).

Подробнее информацию о контроле целостности см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01».

Если средства контроля целостности не используются, то обновление пакетов нужно производить в следующем порядке:

- 1) если используется `control++` (черные/белые списки), нужно выключить черные/белые списки, выполнив сброс текущего режима (просмотреть установленный режим можно, выполнив команду `control++ list`, активный режим будет дополнительно отмечен *):

```
# control++ --reset
```

- 2) установить пакеты/обновить систему при помощи `apt-get`;

- 3) включить установленный ранее режим черного/белого списка, выполнив команду (в зависимости от вывода в шаге 1)):

```
# control++ blacklist
```

или

```
# control++ wl
```

- 4) выполнить команду:

```
# integalert fix
```

15.4.1. Команда `integrity-applier`

Для того чтобы система сохранила все настройки безопасности установку/обновление пакетов нужно производить в следующем порядке:

- 1) войти в ОС и от администратора (`root`), выполнить команду отключения подсистемы IMA/EVM (если активирована):

```
# integrity-remover
```

Система будет перезагружена;

- 2) установить пакеты при помощи `apt-get` (см. п. 15.5) или обновить пакеты:

```
# apt-get update
```

```
# apt-get dist-upgrade
```

3) запустить инициализацию средств контроля целостности:

```
# integrity-applier -i
```

после выполнения данной команды будет запущен первый этап инициализации подсистемы IMA/EVM, в результате выполнения команды, система будет перезагружена;

4) после перезагрузки системы выполните авторизацию в терминале и получите права суперпользователя (root);

5) запустить второй этап инициализации подсистемы IMA/EVM – выполнить команду:

```
# integrity-applier -s
```

в результате выполнения команды, система будет перезагружена;

6) переименовать файл записи аудита /var/log/audit/audit.log:

```
# mv /var/log/audit/audit.log /var/log/audit/audit_old.log
```

7) выполнить запуск аудита:

```
# service auditd start
```

15.5. Установка или обновление пакета командой apt

Установка пакета с помощью АРТ выполняется командой:

```
# apt-get install имя_пакета
```

Перед установкой и обновлением пакетов нужно выполнить команду обновления индексов пакетов:

```
# apt-get update
```

Если пакет уже установлен и в подключенном репозитории нет обновлений для данного пакета, система сообщит об уже установленном пакете последней версии. Если в репозитории присутствует более новая версия или новое обновление – программа начнет процесс установки.

apt-get позволяет устанавливать в систему другие, пока еще не установленные пакеты, требуемые для работы. Он определяет, какие пакеты нужно установить, и устанавливает их, пользуясь всеми доступными репозиториями.

Установка пакета gimp командой apt-get install gimp приведет к следующему диалогу с АРТ:

```
# apt-get install gimp
```

```
Чтение списков пакетов... Завершено
```

```

Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2 libopenraw
libspiro libwebkitgtk2 libwmf
Следующие НОВЫЕ пакеты будут установлены:
gimp icc-profiles libbabl libgegl libgimp libjavascriptcoregtk2
libopenraw libspiro libweb-kitgtk2 libwmf
0 будет обновлено, 10 новых установлено, 0 пакетов будет удалено и 0 не
будет обновлено.
Нужно получить 0В/24,6МВ архивов.
После распаковки потребуется дополнительно 105МВ дискового
пространства.
Продолжить? [Y/n] y
. . .
Получено 24,6МВ за 0s (44,1МВ/s).
Совершаем изменения...
Preparing... ##### [100%]
1: libbabl ##### [ 10%]
2: libwmf ##### [ 20%]
3: libjavascriptcoregtk2 ##### [ 30%]
4: libwebkitgtk2 ##### [ 40%]
5: icc-profiles ##### [ 50%]
6: libspiro ##### [ 60%]
7: libopenraw ##### [ 70%]
8: libgegl ##### [ 80%]
9: libgimp ##### [ 90%]
10: gimp ##### [100%]
Running /usr/lib/rpm/posttrans-filetriggers
Завершено.

```

Команда `apt-get install имя_пакета` используется и для обновления уже установленного пакета или группы пакетов. В этом случае `apt-get` дополнительно проверяет, не обновилась ли версия пакета в репозитории по сравнению с установленным в системе.

При помощи АРТ можно установить и отдельный бинарный rpm-пакет, не входящий ни в один из репозиториев. Для этого достаточно выполнить команду `apt-get install путь_к_файлу.rpm`. При этом АРТ проведет стандартную процедуру проверки зависимостей и конфликтов с уже установленными пакетами.

В результате операций с пакетами без использования АРТ может нарушиться целостность ОС Альт СП, и `apt-get` в таком случае откажется выполнять операции установки, удаления или обновления.

Для восстановления целостности ОС Альт СП нужно повторить операцию, задав опцию `-f`, заставляющую `apt-get` исправить нарушенные зависимости, удалить или заменить конфликтующие пакеты. Любые действия в этом режиме обязательно требуют подтверждения со стороны пользователя.

При установке пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета installed
```

15.6. Удаление установленного пакета командой apt

Для удаления пакета используется команда `apt-get remove <имя_пакета>`.

Удаление пакета с сохранением его файлов настройки производится при помощи следующей команды:

```
# apt-get remove <значимая_часть_имени_пакета>
```

В случае, если при этом нужно полностью очистить систему от всех компонент удаляемого пакета, то применяется команда:

```
# apt-get remove --purge <значимая_часть_имени_пакета>
```

Для того чтобы не нарушать целостность системы, будут удалены и все пакеты, зависящие от удаляемого.

В случае удаления с помощью `apt-get` базового компонента системы появится запрос на подтверждение операции:

```
# apt-get remove filesystem
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие пакеты будут УДАЛЕНЫ:
[...]
ВНИМАНИЕ: Будут удалены важные для работы системы пакеты
Обычно этого делать не следует. Вы должны точно понимать возможные
последствия!
[...]
0 будет обновлено, 0 новых установлено, 1732 пакетов будет удалено и 1
не будет обновлено.
Необходимо получить 0В архивов.
После распаковки будет освобождено 5439МВ дискового пространства.
Вы делаете нечто потенциально опасное!
Введите фразу 'Yes, do as I say!' чтобы продолжить.
```

Каждую ситуацию, в которой АРТ выдает такое сообщение, нужно рассматривать отдельно. Однако, вероятность того, что после выполнения этой команды система окажется неработоспособной, очень велика.

При удалении пакетов происходит запись в системный журнал вида:

```
apt-get: имя-пакета removed
```

15.7. Альтернативная установка дополнительного ПО

Для установки дополнительного ПО можно использовать программу управления пакетами Synaptic.

⚠ Нельзя использовать одновременно два менеджера пакетов, так как это может привести к их некорректной работе.

15.7.1. Программа управления пакетами Synaptic

Запустить программу управления пакетами Synaptic можно, выбрав пункт «Меню MATE» → «Приложения» → «Параметры» → «Программа управления пакетами Synaptic».

При запуске программы необходимо ввести пароль администратора системы.

Для облегчения поиска доступные для установки программы (рис. 238) разделены на группы, выводимые в левой части окна программы. Справа расположен список самих программ с указанием их текущего состояния:

- ☒ синяя метка – пакет уже установлен;
- ☐ белая метка – пакет не установлен;
- ☒ синяя метка с восклицательным знаком – для установленного пакета имеется обновление.

При выборе пакета из списка в нижней части отображаются сведения о нем и его описание.

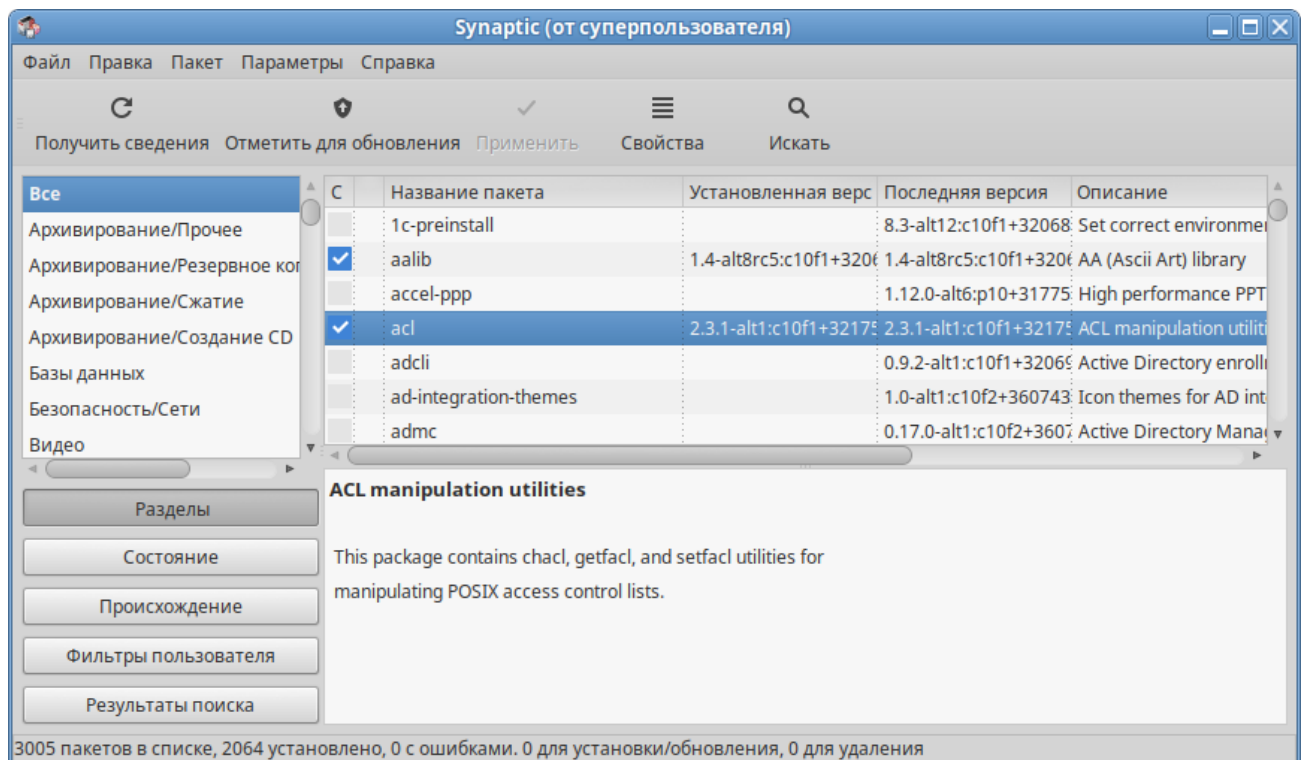


Рис. 238 – Программа управления пакетами Synaptic

Перед тем как устанавливать или обновлять пакет, нужно нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО.

Для начала установки двойным щелчком мыши нужно отметить неустановленный пакет в правой половине окна и нажать на кнопку «Применить».

15.8. Обновление всех установленных пакетов apt-get

Полное обновление всех установленных в системе пакетов производится при помощи команды:

```
# apt-get dist-upgrade
```

Примечание. Команда `apt-get dist-upgrade` обновит систему, но ядро ОС не будет обновлено (см. п. 15.11).

В случае обновления всего дистрибутива АРТ проведет сравнение системы с репозиторием и удалит устаревшие пакеты, установит новые версии присутствующих в системе пакетов, отследит ситуации с переименованиями пакетов или изменения зависимостей между старыми и новыми версиями программ. Все, что потребуется поставить (или удалить) дополнительно к уже имеющемуся в системе, будет указано в отчете `apt-get`, которым АРТ предварит само обновление.

15.9. Обновление всех установленных пакетов Synaptic

Synaptic поддерживает два варианта обновления системы:

- интеллектуальное обновление (рекомендуется) – попытается разрешить конфликты пакетов перед обновлением системы. Действие интеллектуального обновления аналогично действию команды `apt-get dist-upgrade`;
- стандартное обновление – обновление обновит только те пакеты, которые не требуют установки дополнительных зависимостей.

По умолчанию Synaptic использует интеллектуальное обновление. Для того чтобы изменить метод обновления системы, нужно открыть диалоговое окно «Параметры» («Параметры» → «Параметры») и на вкладке «Основные» в списке «Обновить систему» выбрать требуемый способ.

Для обновления системы необходимо (рис. 239):

- 1) нажать на кнопку «Получить сведения» (или комбинацию клавиш <Ctrl>+<R>), для того чтобы скачать список самых последних версий ПО;
- 2) нажать на кнопку «Отметить для обновления» (или комбинацию клавиш <Ctrl>+<G>), для того чтобы Synaptic отметил доступные для обновления пакеты. При этом программа может вывести окно со списком вносимых изменений;
- 3) нажать на кнопку «Применить». Будет показан список изменений, который произойдет при обновлении пакетов. Тут следует обратить внимание на объем данных, который будет скачан из сети. После подтверждения Synaptic начнет загружать файлы, затем начнется непосредственно установка.

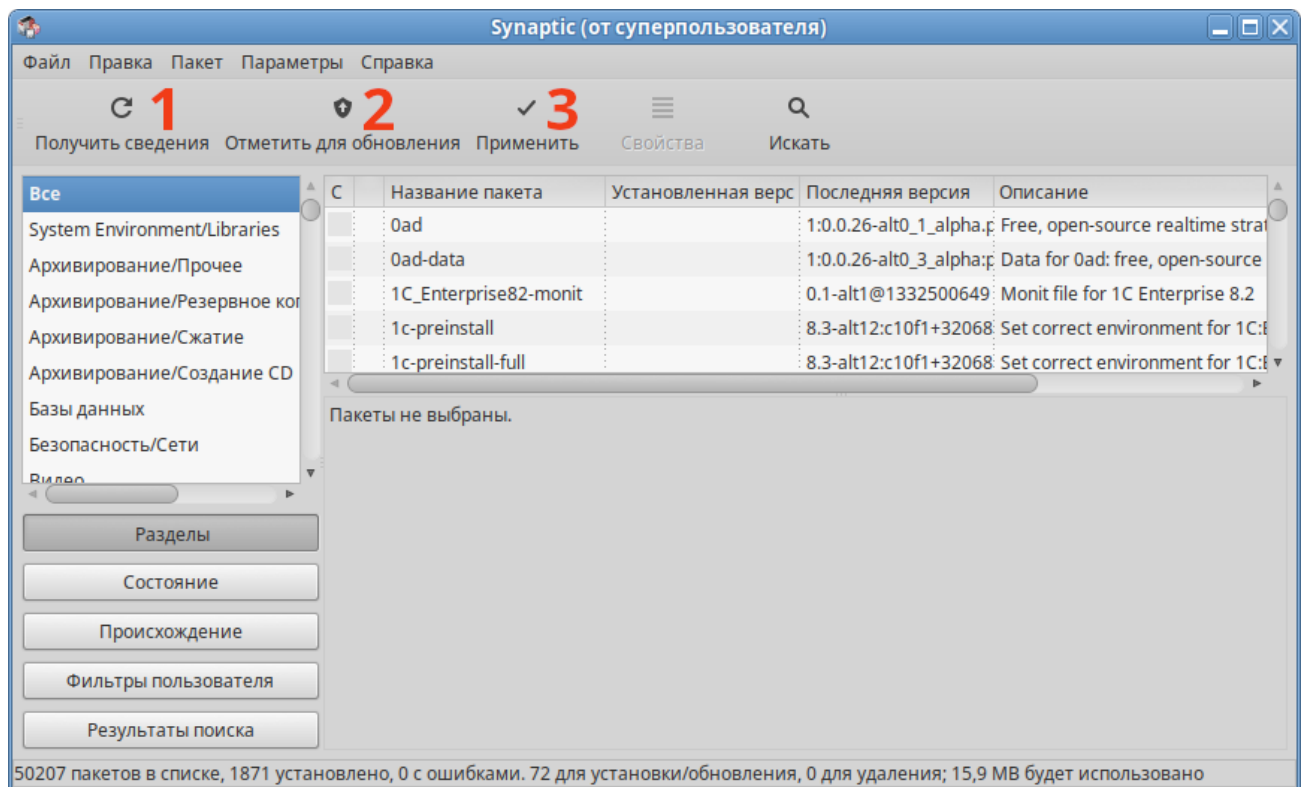


Рис. 239 – Обновление всех установленных пакетов

15.10. Обновление ядра и модулей ядра

15.10.1. В консоли

Для обновления ядра ОС используется команда:

```
# update-kernel
```


Примечание. Если индексы сегодня еще не обновлялись перед выполнением команды `update-kernel` нужно выполнить команду `apt-get update`.

Если нужно обновить/установить другой тип ядра, нужно выполнить команду:
`update-kernel -t <новый тип ядра>`

где <новый тип ядра> – `std-def`, `un-def` и т. п.

Примечание. Ключ `-t` и тип ядра (`std-def`, `un-def` и т. п.) следует указывать, только если нужно обновить ядро другого типа, так как по умолчанию обновляется текущий тип ядра. Узнать версию загруженного ядра можно командой:

```
$ uname -r
```

Новое ядро загрузится только после перезагрузки системы. Если с новым ядром что-то пойдет не так, можно будет вернуться к предыдущему варианту, выбрав его в начальном меню загрузчика.

После успешной загрузки на обновленном ядре можно удалить старые ядра, выполнив команду:

```
# remove-old-kernels
```

Команда `update-kernel` обновит и модули ядра, если в репозитории есть обновления модулей для текущего ядра.

Установка/обновление модулей ядра выполняется командой:

```
apt-get install kernel-modules-<модуль>-<тип ядра>
```

Например, для установки модуля LiME, если текущий тип ядра `un-def`, следует выполнить команду:

```
# apt-get install kernel-modules-LiME-un-def
```

Примечание. Перед установкой модулей ядра необходимо обязательно обновить ядро.

15.10.2. Графический инструмент обновления ядра

Модуль «Обновление ядра» (пакет `alterator-update-kernel`) реализует функционал утилиты `update-kernel`. Данный модуль предоставляет возможность:

- просматривать список установленных ядер;
- устанавливать, обновлять и удалять ядра;
- задавать ядро, загружаемое по умолчанию;
- устанавливать/удалять отдельные модули ядра.

Модуль «Обновление ядра» доступен как в графическом интерфейсе ЦУС (п. 7.1.1) (раздел «Система» → «Обновление ядра» (рис. 240), так и в веб-интерфейсе (п. 7.1.2) <https://ip-address:8080> (рис. 241).

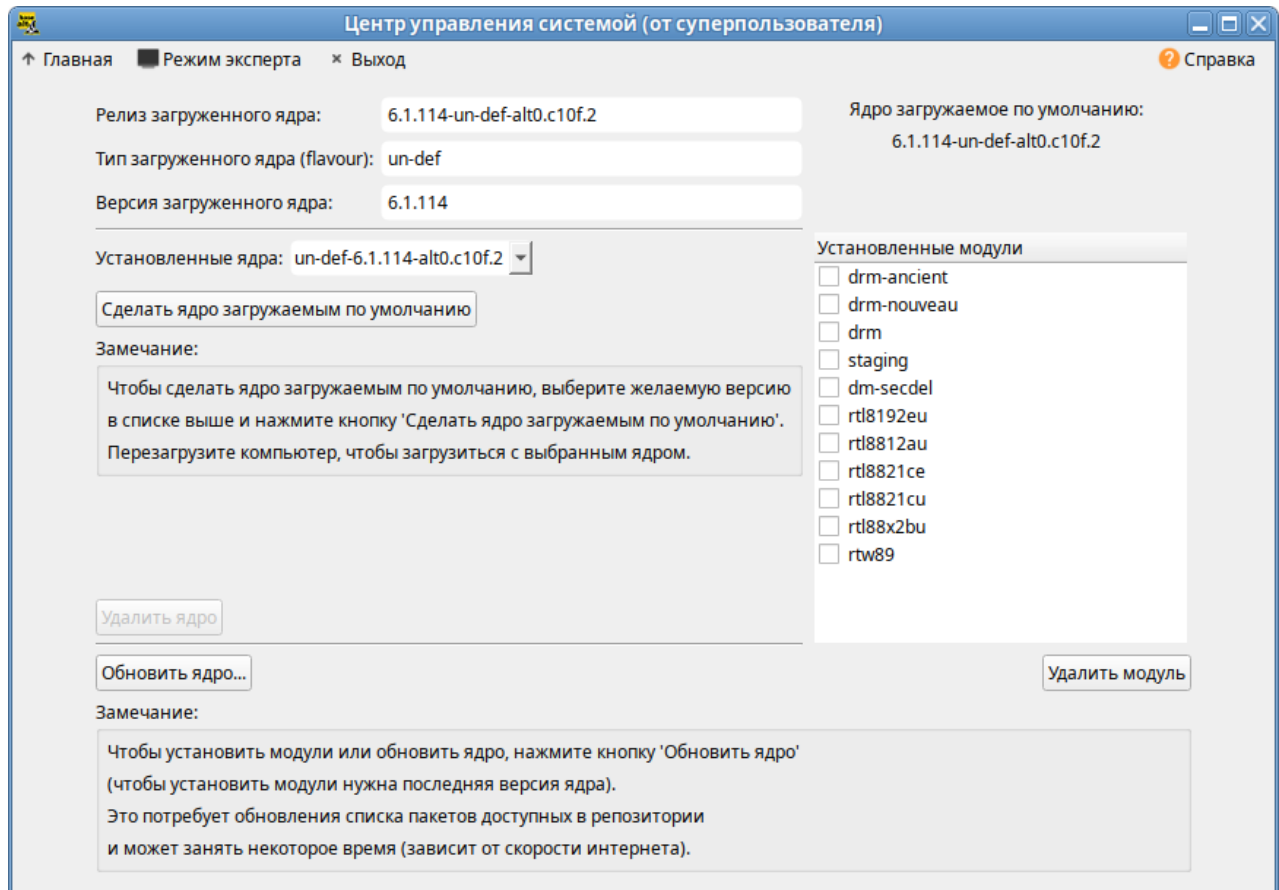


Рис. 240 – Пример интерфейса модуля «Обновление ядра»

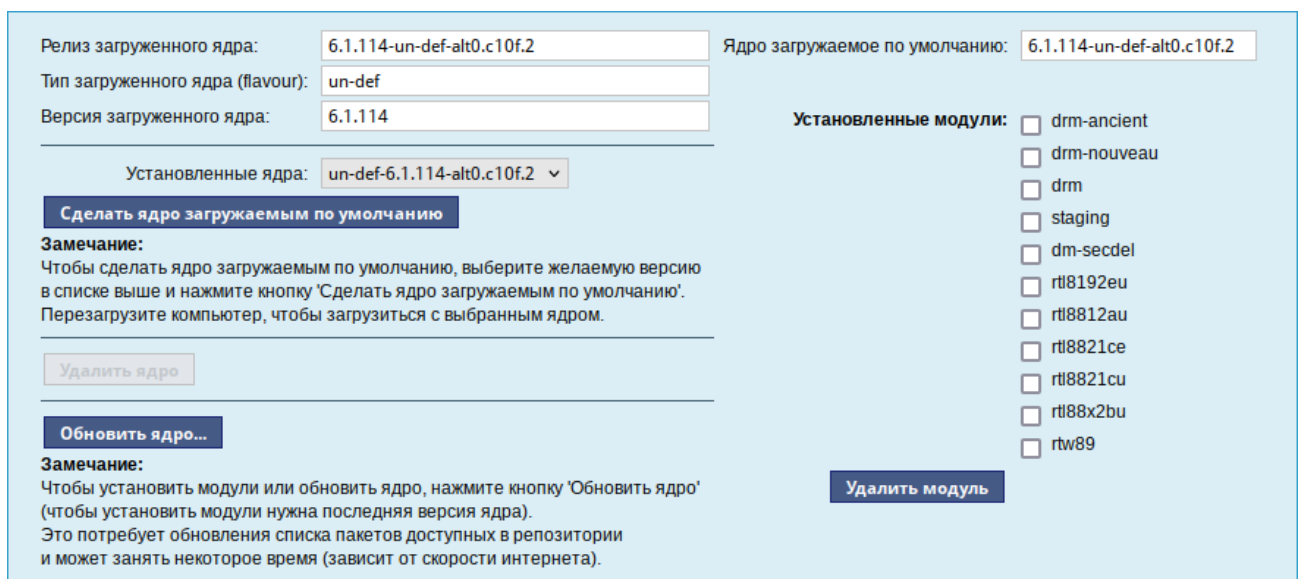


Рис. 241 – Пример веб-интерфейса модуля «Обновление ядра»

В главном окне модуля отображается ядро, загруженное по умолчанию, список установленных ядер (поле «Установленные ядра»), список установленных модулей ядра (поле «Установленные модули»).

15.10.2.1. Установка/обновление ядра и установка модулей ядра

При обновлении ядра, обновляются и модули ядра, но исходя из списка установленных для текущего ядра пакетов.

Примечание. Для установки модулей требуется последняя версия ядра.

Для того чтобы обновить ядро или установить модули ядра, нужно нажать кнопку «Обновить ядро...».

Примечание. При нажатии кнопки «Обновить ядро...» локальная база данных пакетов будет синхронизирована с удаленным репозиторием, это может занять некоторое время.

В открывшемся окне будет показано доступное к установке ядро или сообщение о том, что последнее ядро уже установлено в системе (рис. 242).

В выпадающем списке можно выбрать тип ядра. В окне «Доступные модули» отмечаются модули, которые будут установлены.

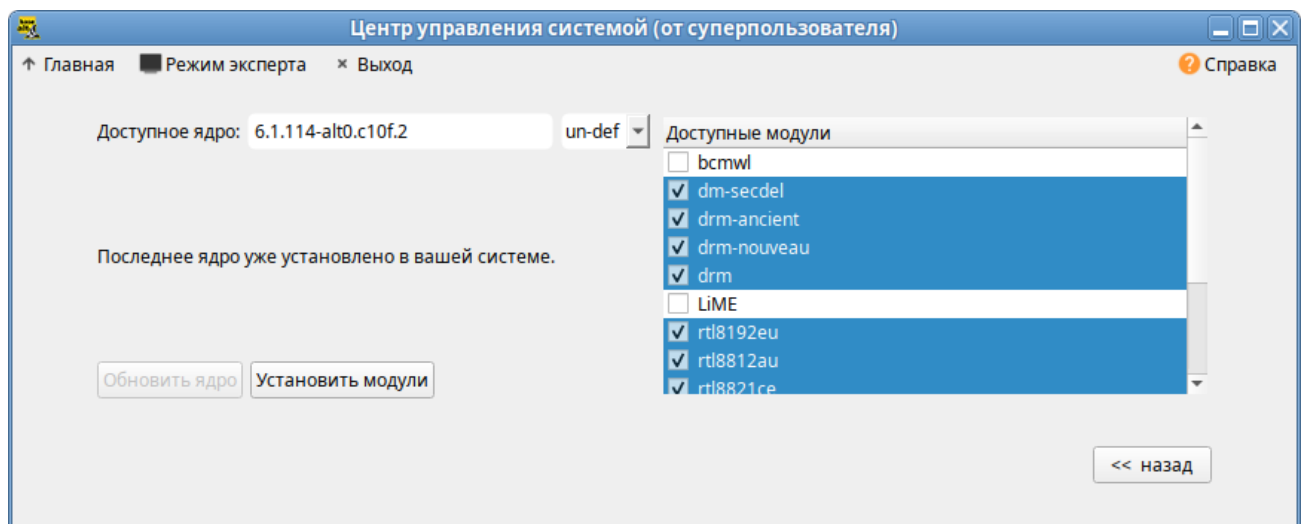


Рис. 242 – Доступное к установке ядро

Чтобы обновить ядро, нужно нажать кнопку «Обновить ядро». Откроется окно, в котором следует нажать кнопку «Да» для того, чтобы обновить ядро, или «Нет», чтобы отказаться от данного действия.

Установленное ядро станет загружаемым по умолчанию.

Если ядро не требует обновления, в окне «Доступные модули» можно отметить модули ядра, доступные к установке, и нажать на кнопку «Установить модули».

Новое ядро загрузится только после перезагрузки системы.

15.10.2.2. Сделать ядро загружаемым по умолчанию

В дистрибутиве можно установить несколько версий ядра одного и того же типа одновременно. После установки, или обновления ядра, старые ядра не удаляются. В случае возникновения проблем с новым ядром можно переключиться на ядро, установленное ранее.

Для этого следует выбрать нужное ядро в списке «Установленные ядра» (рис. 243) и нажать кнопку «Сделать ядро загружаемым по умолчанию».

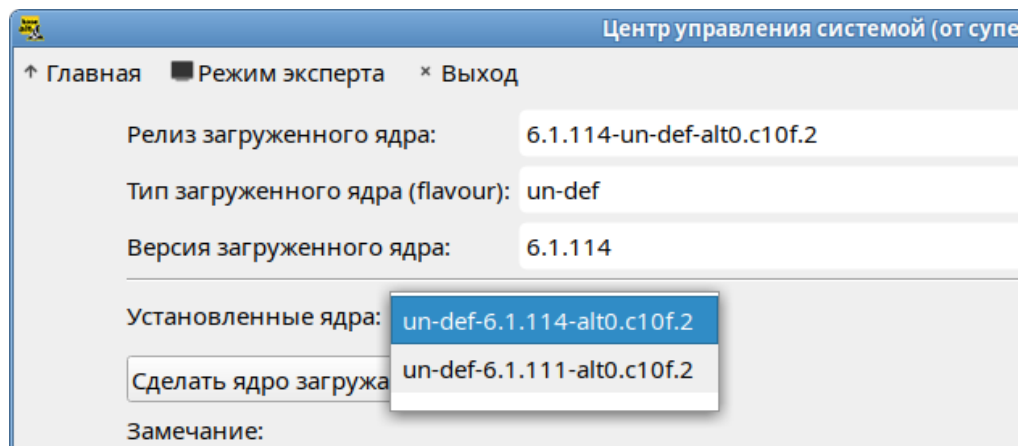


Рис. 243 – Пример выбора ядра. Список «Установленные ядра»

15.10.2.3. Удаление ядра

Накопленный при обновлениях набор ранее установленных ядер можно удалить для освобождения дискового пространства. Для этого следует выбрать нужное ядро в списке «Установленные ядра» и нажать кнопку «Удалить ядро».

15.10.2.4. Удаление модулей ядра

При установке ОС автоматически устанавливаются модули для различных аппаратных средств, включая различные модели видеокарт. Для уменьшения нагрузки при обновлениях неиспользуемые модули можно удалить. Для этого в списке «Установленные ядра» следует выбрать ядро, модули которого нужно

удалить, затем в списке «Установленные модули» (рис. 244) выделить удаляемые модули и нажать на кнопку «Удалить модуль».

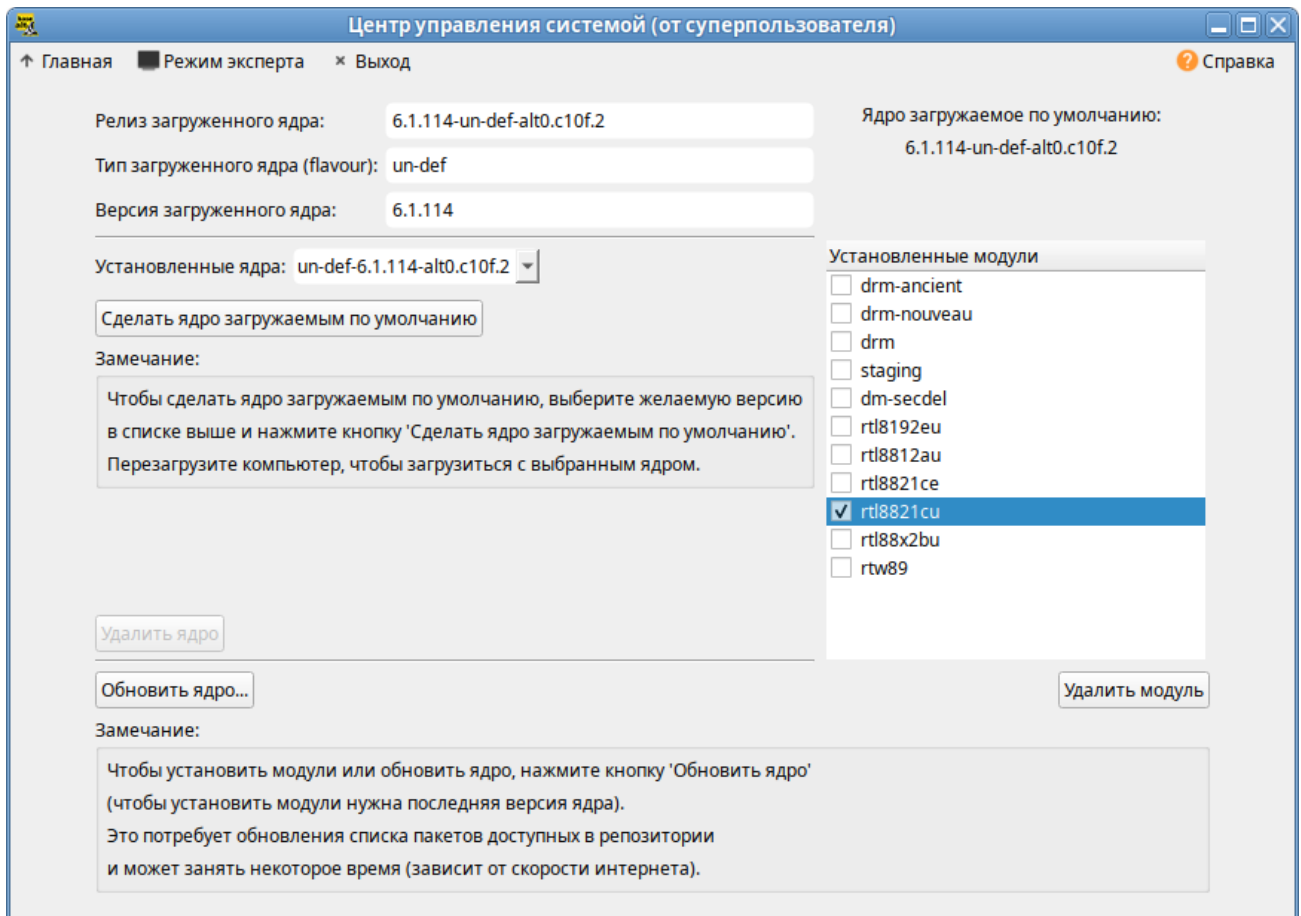


Рис. 244 – Пример выбора модуля в списке «Установленные модули»

15.11. Обновление изолированного окружения (chrooted environment)

Команда `update_chrooted --list` выводит список всех типов модулей для `update_chrooted`, которые установлены в системе:

```
# update_chrooted --list
List of registered types: all conf lib
```

С помощью команды `update_chrooted <имя_типа>` можно выполнить все модули указанного типа.

После изменения общесистемных конфигурационных файлов типа `/etc/resolv.conf`, для того чтобы синхронизировать эти изменения во всех многочисленных `chrooted environments` следует выполнить команду:

```
# update_chrooted conf
```

После изменения системных библиотек следует выполнить команду:

```
# update_chrooted lib
```

Для синхронизации изменений конфигурационных файлов и системных библиотек следует выполнить команду:

```
# update_chrooted all
```

15.12. Проверка подлинности пакетов

Подлинность пакетов при обновлении обеспечивается средствами кодирования, подтверждающих как целостность самих пакетов, так и целостность индексов, описывающих репозитории.

Ключевая информация для проверки подлинности распространяется вместе с дистрибутивом на сертифицированном носителе и защищена от потенциальной подмены при передаче по каналам связи.

Проверить подлинность и целостность пакета можно командой:

```
# rpm -vK имя_пакета
```

15.13. Получение уведомлений о выходе обновлений

Информирование потребителей о мерах, направленных на нейтрализацию выявленных уязвимостей ПИ ОС Альт СП, и выпускаемых обновлениях выполняется путем публикации информации на официальном сайте предприятия-разработчика (<https://altsp.su>) или по электронной почте.

15.14. Обновление систем, не имеющих выхода в Интернет

Обновление систем, не имеющих выхода в Интернет осуществляется в соответствии с п. 8.6.4.

15.15. Единая команда управления пакетами (rpm)

rpm – единая команда управления пакетами. Основное предназначение: унифицировать управление пакетами в дистрибутивах с разными пакетными менеджерами. rpm упрощает процедуру управления пакетами, особенно полезна для тех, кто работает с множеством дистрибутивов, может использоваться в скриптах и установщиках, сервисных программах, в повседневном администрировании различных систем. Кроме того, в rpm добавлены типовые операции, которые, например, в случае использования apt, потребовали бы ввода более одной команды.

Установка выполняется командой:

```
# apt-get install eepm
```

Включает в себя следующую функциональность:

- управление пакетами (установка – удаление – поиск);
- управление репозиториями (добавление – удаление – обновление – список);
- управление системными сервисами (включение – выключение – список).

Список поддерживаемых пакетных менеджеров: rpm, deb, tgz, tbz, tbz2, apk, pkg.gz.

Список команд epm --help представлен в таблице 20.

Т а б л и ц а 20 – Список команд epm --help

Описание операции	Команда epm	Команда ОС Альт СП
Установка пакета по названию в систему	epm -i (package)	apt-get install (package)
Установка файла пакета в систему	epm -i (package file)	apt-get install (package file)
Удаление пакета из системы	epm -e (package)	apt-get remove (package)
Поиск пакета в репозитории	epm -s (text)	apt-cache search (text)
Проверка наличия пакета в системе	epm -q (package)	rpm -qa (pipe) grep (package)
Список установленных пакетов	epm -qa	rpm -qa
Поиск по названиям установленных пакетов	epm -qp <word>	grep <word>
Принадлежность файла к (установленному) пакету	epm -qf (file)	rpm -qf (file)
Поиск, в каком пакете есть указанный файл	epm -sf <file>	
Список файлов в (установленном) пакете	epm -ql (package)	rpm -ql (package)
Вывести информацию о пакете	epm -qi (package)	apt-cache show (package)
Обновить дистрибутив	epm upgrade	apt-get dist-upgrade

Примеры:

```
# epms name subtext – выполняет epms name | grep subtest
```

```
# epms name ^subtext – выполняет epms name | grep -v subtest
```

```
# epms "name1 name2" – выполняет поиск именно такого сочетания.
```

16. КОНТРОЛЬНЫЕ ХАРАКТЕРИСТИКИ РАЗВЕРНУТОЙ ОС АЛЫТ СП

После установки нужно проверить корректность развертывания ОС Алыт СП путем подсчета и сличения контрольных характеристик установленных файлов. Подробнее см. в документе «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01».

В качестве контрольной характеристики файла выступает контрольная сумма.

Подробнее об интегральных контрольных суммах ПИ, расположении пофайловых отчетов подсчета, алгоритме подсчета контрольных сумм приведено в документах «Формуляр. ЛКНВ.11102-01 30 01» и «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01».

Информацию о применении критических обновлений ОС Алыт СП нужно внести в раздел «Особые отметки» документа «Формуляр. ЛКНВ.11102-01 30 01».

17. ОСНОВЫ АДМИНИСТРИРОВАНИЯ LINUX

17.1. Общие принципы работы ОС

17.1.1. Процессы и файлы

ОС Альт СП является многопользовательской интегрированной системой. Это значит, что она разработана в расчете на одновременную работу нескольких пользователей.

Пользователь может либо сам работать в системе, выполняя некоторую последовательность команд, либо от его имени могут выполняться прикладные процессы.

Пользователь взаимодействует с системой через командный интерпретатор. Командный интерпретатор представляет собой прикладную программу, которая принимает от пользователя команды или набор команд и транслирует их в системные вызовы к ядру системы. Интерпретатор позволяет пользователю просматривать файлы, передвигаться по дереву файловой системы, запускать прикладные процессы. Все командные интерпретаторы UNIX имеют развитый командный язык и позволяют писать достаточно сложные программы, упрощающие процесс администрирования системы и работы с ней.

17.1.1.1. Процессы функционирования ОС

Все программы, которые выполняются в текущий момент времени, называются процессами. Процессы можно разделить на два основных класса: системные процессы и пользовательские процессы.

Системные процессы – программы, решающие внутренние задачи ОС, например, организацию виртуальной памяти на диске или предоставляющие пользователям те или иные сервисы (процессы-службы).

Пользовательские процессы – процессы, запускаемые пользователем из командного интерпретатора для решения задач пользователя или управления системными процессами. Linux изначально разрабатывался как многозадачная система.

Он использует технологии, опробованные и отработанные другими реализациями UNIX, которые существовали ранее.

Фоновый режим работы процесса – режим, когда программа может работать без взаимодействия с пользователем. В случае необходимости интерактивной работы с пользователем (в общем случае) процесс будет «остановлен» ядром, и работа его продолжается только после перевода его в «нормальный» режим работы.

17.1.1.2. Файловая система ОС

В ОС использована файловая система Linux, которая, в отличие от файловых систем DOS и Windows, является единым деревом. Корень этого дерева – каталог, называемый root и обозначаемый /.

Части дерева файловой системы могут физически располагаться в разных разделах разных дисков или вообще на других компьютерах – для пользователя это прозрачно. Процесс присоединения файловой системы раздела к дереву называется монтированием, удаление – размонтированием. Например, файловая система CD-ROM в дистрибутиве монтируется по умолчанию в каталог /media/cdrom (путь в дистрибутиве обозначается с использованием /, а не \, как в DOS/Windows).

Текущий каталог обозначается ./.

17.1.1.3. Структура каталогов

Корневой каталог /:

- /bin – командные оболочки (shell), основные утилиты;
- /boot – содержит ядро системы;
- /dev – псевдофайлы устройств, позволяющие работать с устройствами напрямую. Файлы в /dev создаются сервисом udev;
- /etc – общесистемные конфигурационные файлы для большинства программ в системе;
- /etc/rc?.d, /etc/init.d, /etc/rc.boot, /etc/rc.d – каталоги, где расположены командные файлы, выполняемые при запуске системы или при смене ее режима работы;

- `/etc/passwd` –база данных пользователей, в которой содержится информация об имени пользователя, его настоящем имени, личном каталоге, его зашифрованный пароль и другие данные;
- `/etc/shadow` –теневая база данных пользователей. При этом информация из файла `/etc/passwd` перемещается в `/etc/shadow`, который недоступен для чтения всем, кроме пользователя `root`. В случае использования альтернативной схемы управления теневыми паролями (ТСВ), все теневые пароли для каждого пользователя располагаются в каталоге `/etc/tcb/имя пользователя/shadow`;
- `/home` –домашние каталоги пользователей;
- `/lib` –содержит файлы динамических библиотек, которые нужны для работы большей части приложений, и подгружаемые модули ядра;
- `/lost+found` –восстановленные файлы;
- `/media` –подключаемые носители (каталоги для монтирования файловых систем сменных устройств);
- `/mnt` –точки временного монтирования;
- `/opt` –вспомогательные пакеты;
- `/proc` –виртуальная файловая система, хранящаяся в памяти компьютера при загруженной ОС. В данном каталоге расположены самые свежие сведения обо всех процессах, запущенных на компьютере;
- `/root` –домашний каталог администратора системы;
- `/run` –файлы состояния приложений;
- `/sbin` –набор программ для административной работы с системой (системные утилиты);
- `/selinux` –виртуальная файловая система SELinux;
- `/srv` –виртуальные данные сервисных служб;
- `/sys` –файловая система, содержащая информацию о текущем состоянии системы;
- `/tmp` –временные файлы;

- /usr – пользовательские двоичные файлы и данные, используемые только для чтения (программы и библиотеки);
- /var – файлы для хранения изменяющихся данных (рабочие файлы программ, очереди, журналы).

Каталог /usr:

- /usr/bin – дополнительные программы для всех учетных записей;
- /usr/sbin – команды, используемые при администрировании системы и не предназначенные для размещения в файловой системе root;
- /usr/local – место, где рекомендуется размещать файлы, установленные без использования пакетных менеджеров, внутренняя организация каталогов практически такая же, как и корневого каталога;
- /usr/man – каталог, где хранятся файлы справочного руководства man;
- /usr/share – каталог для размещения общедоступных файлов большей части приложений.

Каталог /var:

- /var/log – каталог для регистрации сообщений, системный журнал;
- /var/spool – каталог для хранения файлов, находящихся в очереди на обработку для того или иного процесса (очереди печати, непрочитанные или не отправленные письма, задачи cron и т. д.).

17.1.1.4. Организация файловой структуры

Система домашних каталогов пользователей помогает организовывать безопасную работу пользователей в многопользовательской системе. Вне своего домашнего каталога пользователь обладает минимальными правами (обычно чтение и выполнение файлов) и не может нанести ущерб системе, например, удалив или изменив файл.

Кроме файлов, созданных пользователем, в его домашнем каталоге обычно содержатся персональные конфигурационные файлы некоторых программ.

Маршрут (путь) – это последовательность имен каталогов, представляющая собой путь в файловой системе к данному файлу, где каждое следующее имя отделяется от предыдущего наклонной чертой (слешем). Если название маршрута начинается со слеша, то путь в искомый файл начинается от корневого каталога всего дерева системы. В обратном случае, если название маршрута начинается непосредственно с имени файла, то путь к искомому файлу должен начаться от текущего каталога (рабочего каталога).

Имя файла может содержать любые символы за исключением косой черты (/). Однако следует избегать применения в именах файлов большинства знаков препинания и непечатаемых символов. При выборе имен файлов рекомендуется ограничиться следующими символами:

- строчные и ПРОПИСНЫЕ буквы. Следует обратить внимание на то, что регистр всегда имеет значение;
- символ подчеркивания (_);
- точка (.).

Для удобства работы точку можно использовать для отделения имени файла от расширения файла. Данная возможность может быть нужна пользователям или некоторым программам, но не имеет значение для shell.

17.1.1.5. Имена дисков и разделов

Все физические устройства компьютера отображаются в каталог `/dev` файловой системы дистрибутива. Диски (в том числе IDE/SATA/SCSI/SAS жесткие диски, USB-диски) имеют имена:

- `/dev/sda` – первый диск;
- `/dev/sdb` – второй диск;
- и т. д.

Диски обозначаются `/dev/sdX`, где `X` – a, b, c, d, e, ... в зависимости от порядкового номера диска на шине.

Раздел диска обозначается числом после его имени. Например, `/dev/sdb4` – четвертый раздел второго диска.

17.1.1.6. Разделы для работы ОС

Для работы ОС на жестком диске (дисках) должны быть созданы, по крайней мере, два раздела: корневой (то есть тот, который будет содержать каталог /) и раздел подкачки (swap). Размер последнего, как правило, составляет от однократной до двукратной величины оперативной памяти компьютера. Если на диске много свободного места, то можно создать отдельные разделы для каталогов /usr, /home, /var.

17.1.2. Командные оболочки (интерпретаторы)

Для управления ОС используются командные интерпретаторы (shell).

После входа в систему, увидите приглашение – строку, содержащую символ «\$» (далее этот символ будет обозначать командную строку). Программа ожидает ваших команд. Роль командного интерпретатора – передавать ваши команды операционной системе. По своим функциям он соответствует `command.com` в DOS, но несравненно мощнее. При помощи командных интерпретаторов можно писать небольшие программы – сценарии (скрипты). В Linux доступны следующие командные оболочки:

- `bash` – самая распространенная оболочка под linux. Она ведет историю команд и предоставляет возможность их редактирования;
- `pdksh` – клон `korn shell`, хорошо известной оболочки в UNIX системах.

Проверить, какая оболочка используется в данный момент можно, выполнив команду:

```
$ echo $SHELL
```

Оболочкой по умолчанию является Bash (Bourne Again Shell) – самая распространенная оболочка под Linux, которая ведет историю команд и предоставляет возможность их редактирования.

17.1.3. Командная оболочка Bash

В Bash имеется несколько приемов для работы со строкой команд. Например, можно использовать следующие сочетания клавиш:

- `<Ctrl>+<A>` – перейти на начало строки;

- <Ctrl>+<U> – удалить текущую строку;
- <Ctrl>+<C> – остановить текущую задачу.

Для ввода нескольких команд одной строкой можно использовать разделитель «;». По истории команд можно перемещаться с помощью клавиш ↑ («вверх») и ↓ («вниз»).

Чтобы найти конкретную команду в списке набранных, не пролистывая всю историю, можно нажать <Ctrl>+<R> и начать вводить символы ранее введенной команды.

Для просмотра истории команд можно воспользоваться командой `history`. Команды, присутствующие в истории, отображаются в списке пронумерованными. Чтобы запустить конкретную команду нужно набрать:

```
!номер команды  
Если ввести:  
!!
```

запустится последняя из набранных команд.

В Bash имеется возможность самостоятельного завершения имен команд из общего списка команд, что облегчает работу при вводе команд, в случае, если имена программ и команд слишком длинны. При нажатии клавиши <Tab> Bash завершает имя команды, программы или каталога, если не существует нескольких альтернативных вариантов. Например, чтобы использовать программу декомпрессии `gunzip`, можно набрать следующую команду:

```
gu
```

Затем нажать клавишу <Tab>. Так как в данном случае существует несколько возможных вариантов завершения команды, то нужно повторно нажать клавишу <Tab>, чтобы получить список имен, начинающихся с `gu`.

В предложенном примере можно получить следующий список:

```
$ gu  
guile gunzip gupnp-binding-tool
```

Если набрать: `n` (`gunzip` – это единственное имя, третьей буквой которого является «n»), а затем нажать клавишу <Tab>, то оболочка самостоятельно дополнит имя. Чтобы запустить команду нужно нажать <Enter>.

Программы, вызываемые из командной строки, Bash ищет в каталогах, определяемых в системной переменной `$PATH`. По умолчанию в этот перечень каталогов не входит текущий каталог, обозначаемый `./` (точка слеш) (если только не выбран один из двух самых слабых уровней защиты). Поэтому, для запуска программы из текущего каталога, нужно использовать команду (в примере запускается команда `prog`):

```
./prog
```

17.1.4. Стыкование команд в системе Linux

17.1.4.1. Стандартный ввод и стандартный вывод

Многие команды системы имеют так называемые стандартный ввод (standard input) и стандартный вывод (standard output), часто сокращаемые до `stdin` и `stdout`. Ввод и вывод здесь – это входная и выходная информация для данной команды. Программная оболочка делает так, что стандартным вводом является клавиатура, а стандартным выводом – экран монитора.

Пример с использованием команды `cat`. По умолчанию команда `cat` читает данные из всех файлов, которые указаны в командной строке, и посылает эту информацию непосредственно в стандартный вывод (`stdout`). Следовательно, команда:

```
cat history-final masters-thesis
```

выведет на экран сначала содержимое файла `history-final`, а затем – файла `masters-thesis`.

Если имя файла не указано, программа `cat` читает входные данные из `stdin` и возвращает их в `stdout`.

Пример:

```
cat
Hello there.
Hello there.
Bye.
Bye.
Ctrl-D
```


Каждую строку, вводимую с клавиатуры, программа `cat` немедленно возвращает на экран. При вводе информации со стандартного ввода конец текста сигнализируется вводом специальной комбинации клавиш, как правило, `<Ctrl>+<D>`. Сокращенное название сигнала конца текста – EOT (end of text).

17.1.4.2. Перенаправление ввода и вывода

При необходимости можно перенаправить стандартный вывод, используя символ `>`, и стандартный ввод, используя символ `<`.

Фильтр (filter) – программа, которая читает данные из стандартного ввода, некоторым образом их обрабатывает и результат направляет на стандартный вывод. Когда применяется перенаправление, в качестве стандартного ввода и вывода могут выступать файлы. Как указывалось выше, по умолчанию, `stdin` и `stdout` относятся к клавиатуре и к экрану соответственно. Программа `sort` является простым фильтром – она сортирует входные данные и посылает результат на стандартный вывод. Совсем простым фильтром является программа `cat` – она ничего не делает с входными данными, а просто пересылает их на выход.

17.1.4.3. Использование состыкованных команд

Стыковку команд (pipelines) осуществляет командная оболочка, которая `stdout` первой команды направляет на `stdin` второй команды. Для стыковки используется символ `|`. Направить `stdout` команды `ls` на `stdin` команды `sort`:

```
ls | sort -r
notes
masters-thesis
history-final
english-list
```

Вывод списка файлов частями:

```
ls /usr/bin | more
```

Если нужно вывести на экран последнее по алфавиту имя файла в текущем каталоге, можно использовать следующую команду:

```
ls | sort -r | head -1 notes
```

где команда `head -1` выводит на экран первую строку получаемого ей входного потока строк (в примере поток состоит из данных от команды `ls`), отсортированных в обратном алфавитном порядке.

17.1.4.4. Недеструктивное перенаправление вывода

Эффект от использования символа `>` для перенаправления вывода файла является деструктивным; т. е., команда `ls > file-list` уничтожит содержимое файла `file-list`, если этот файл ранее существовал, и создаст на его месте новый файл. Если вместо этого перенаправление будет сделано с помощью символов `>>`, то вывод будет приписан в конец указанного файла, при этом исходное содержимое файла не будет уничтожено.

Примечание. Перенаправление ввода и вывода и стыкование команд осуществляется командными оболочками, которые поддерживают использование символов `>`, `>>` и `|`. Сами команды не способны воспринимать и интерпретировать эти символы.

17.2. Режим суперпользователя

17.2.1. Пользователи ОС

Linux – система многопользовательская, а потому пользователь – ключевое понятие для организации всей системы доступа в Linux. Файлы всех пользователей в Linux хранятся отдельно, у каждого пользователя есть собственный домашний каталог, в котором он может хранить свои данные. Доступ других пользователей к домашнему каталогу пользователя может быть ограничен.

Суперпользователь в Linux – это выделенный пользователь системы, на которого не распространяются ограничения прав доступа. Именно суперпользователь имеет возможность произвольно изменять владельца и группу файла. Ему открыт доступ на чтение и запись к любому файлу или каталогу системы.

Среди учетных записей Linux всегда есть учетная запись суперпользователя – `root`. Поэтому вместо «суперпользователь» часто говорят «`root`». Множество системных файлов принадлежат `root`, множество файлов только ему доступны для чтения или записи. Пароль этой учетной записи – одна из самых больших драгоценностей системы. Именно с ее помощью системные администраторы выполняют самую ответственную работу.

17.2.2. Назначение режима суперпользователя

Системные утилиты, например, такие, как ЦУС или программа управления пакетами Synaptic, настройки КСЗ ОС требуют для своей работы привилегий суперпользователя, потому что они вносят изменения в системные файлы. При их запуске выводится запрос/диалоговое окно с запросом пароля системного администратора.

17.2.3. Получение прав суперпользователя

Существует два различных способа получить права суперпользователя.

Первый – это зарегистрироваться в системе под именем root в командной строке.

Второй способ – воспользоваться специальной утилитой `su` (shell of user), которая позволяет выполнить одну или несколько команд от лица другого пользователя. По умолчанию эта утилита выполняет команду `sh` от пользователя root, то есть запускает командный интерпретатор. Отличие от предыдущего способа в том, что всегда известно, кто именно запускал `su`, а значит, ясно, кто выполнил определенное административное действие.

В некоторых случаях удобнее использовать не `su`, а утилиту `sudo`, которая позволяет выполнять только заранее заданные команды.

Примечание. Для того чтобы воспользоваться командами `su` и `sudo`, нужно быть членом группы `wheel`. Пользователь, созданный при установке системы, по умолчанию уже включен в эту группу.

17.2.4. Переход в режим суперпользователя

Для перехода в режим суперпользователя наберите в терминале команду `su -`.

Синтаксис:

```
su [-] [name [arg...]]
```

Чтобы вернуться к правам пользователя, нужно ввести следующую команду:

```
exit
```

Если воспользоваться командой `su` без ключа, то происходит вызов командного интерпретатора с правами root. При этом значение переменных

окружения, в частности `$PATH`, остается таким же, как у пользователя: в переменной `$PATH` не окажется каталогов `/sbin`, `/usr/sbin`, без указания полного имени будут недоступны команды `route`, `shutdown`, `mkswap` и другие. Более того, переменная `$HOME` будет указывать на каталог пользователя, все программы, запущенные в режиме суперпользователя, сохраняют свои настройки с правами `root` в каталоге пользователя, что в дальнейшем может вызвать проблемы.

Чтобы избежать этого, следует использовать `su -`. В этом режиме `su` запустит командный интерпретатор в качестве `login shell`, и он будет вести себя в точности так, как если бы в системе зарегистрировался `root`.

17.3. Управление пользователями

Подробнее о средствах управления учетными записями пользователей смотрите в документе «Руководство по комплексу средств защиты. ЛКНВ.11102-01 99 01».

17.4. Система инициализации `systemd` и `sysvinit`

17.4.1. Запуск операционной системы

17.4.1.1. Запуск системы

Алгоритм запуска компьютера:

- 1) БСВВ компьютера;
- 2) загрузчик системы (например, `LILO`, `GRUB` или другой). В загрузчике можно задать параметры запуска системы (см. п. 6.2);
- 3) загрузка ядра `Linux`;
- 4) запускается на выполнение первый процесс в системе – `init`.

Ядром запускается самая первая программа в системе `init`. Ее задачей является запуск новых процессов и повторный запуск завершившихся. Можно посмотреть, где расположился `init` в иерархии процессов системы, введите команду: `ps tree`.

От конфигурации `init` зависит, какая система инициализации будет использована.

17.4.1.2. Система инициализации

Система инициализации – это набор скриптов, которые будут выполнены при старте системы.

Существуют разные системы инициализации, наиболее популярной системой являются `sysvinit` и ее модификации. `systemd` разрабатывается как замена для `sysVinit`.

В ОС Альт СП используется `sysvinit` (от `System V init`).

`System V` – классическая схема инициализации, на которой базируются многие дистрибутивы. Привычна и довольно проста для понимания: `init` описывает весь процесс загрузки в своем конфигурационном файле `/etc/inittab`, откуда вызываются другие программы и скрипты на определенном этапе запуска.

17.4.2. Примеры команд управления службами, журнал в `systemd`

Обратите внимание, что команды `service` и `chkconfig` продолжают работать в `systemd` практически без изменений. Тем не менее, в таблице 21 показано как выполнить те же действия с помощью встроенных утилит `systemctl`.

Т а б л и ц а 21 – Команды управления службами

Команды <code>sysvinit</code>	Команды <code>systemd</code>	Примечания
<code>service frobozz start</code>	<code>systemctl start frobozz.service</code>	Используется для запуска службы (не перезагружает постоянные).
<code>service frobozz stop</code>	<code>systemctl stop frobozz.service</code>	Используется для остановки службы (не перезагружает постоянные).
<code>service frobozz restart</code>	<code>systemctl restart frobozz.service</code>	Используется для остановки и последующего запуска службы.
<code>service frobozz reload</code>	<code>systemctl reload frobozz.service</code>	Если поддерживается, перезагружает файлы конфигурации без прерывания незаконченных операций.

Окончание таблицы 21

Команды sysvinit	Команды systemd	Примечания
<code>service frobozz condrestart</code>	<code>systemctl condrestart frobozz.service</code>	Перезапускает службу, если она уже работает.
<code>service frobozz status</code>	<code>systemctl status frobozz.service</code>	Сообщает, запущена ли уже служба.
<code>ls /etc/rc.d/init.d/</code>	<code>systemctl list-unit-files --type=service (preferred)</code> <code>ls /lib/systemd/system/*.service</code> <code>/etc/systemd/system/*.service</code>	Используется для отображения списка служб, которые можно запустить или остановить. Используется для отображения списка всех служб.
<code>chkconfig frobozz on</code>	<code>systemctl enable frobozz.service</code>	Включает службу во время следующей перезагрузки, или любой другой триггер.
<code>chkconfig frobozz off</code>	<code>systemctl disable frobozz.service</code>	Выключает службу во время следующей перезагрузки, или любой другой триггер.
<code>chkconfig frobozz</code>	<code>systemctl is-enabled frobozz.service</code>	Используется для проверки, сконфигурирована ли служба для запуска в текущем окружении.
<code>chkconfig --list</code>	<code>systemctl list-unit-files --type=service(preferred)</code> <code>ls /etc/systemd/system/*.wants/</code>	Выводит таблицу служб. В ней видно, на каких уровнях загрузки они (не)запускаются.
<code>chkconfig frobozz --list</code>	<code>ls /etc/systemd/system/*.wants/frobozz.service</code>	Используется, для отображения на каких уровнях служба (не)запускается.
<code>chkconfig frobozz --add</code>	<code>systemctl daemon-reload</code>	Используется, когда создается новая служба или модифицируется любая конфигурация.

17.4.3. Журнал в systemd

В systemd включена возможность ведения системного журнала. Для чтения журнала следует использовать команду `journalctl`. По умолчанию, больше не требуется запуск службы `syslog`.

Можно запускать `journalctl` с разными ключами (таблица 22).

Для ознакомления с прочими возможностями, читайте руководство по `journalctl`. Для этого используйте команду `man journalctl`.

Т а б л и ц а 22 – Примеры запуска `journalctl`

Команда	Описание
<code>journalctl -b</code>	Покажет сообщения только с текущей загрузки.
<code>journalctl -f</code>	Покажет только последние сообщения.
<code>journalctl --since "2015-07-20 17:15:00"</code>	Просмотреть все сообщения начиная с 20 июля 2015 года 17:15.
<code>journalctl -k</code>	Просмотр сообщений ядра.
<code>journalctl /usr/lib/systemd/system</code>	Все сообщения конкретной утилиты <code>systemd</code> .
<code>journalctl _PID=1</code>	Просмотр сообщения определенного процесса, покажет сообщения первого процесса (<code>init</code>).
<code>journalctl -u netcfg</code>	Все сообщения конкретного приложения или службы.
<code>journalctl _UID=33</code>	Все сообщения процессов, запущенных от имени конкретного пользователя.

18. СООБЩЕНИЯ АДМИНИСТРАТОРУ

При возникновении проблем в процессе функционирования ОС Альт СП появляются диагностические сообщения трех типов: информационные, предупреждающие и сообщения об ошибках.

Администратор должен проанализировать диагностические сообщения и принять меры по устранению появившихся проблем.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	– база данных;
БСВВ	– базовая система ввода-вывода;
ВК	– вычислительный комплекс;
ГП	– групповая политика;
ЕПП	– единое пользовательское пространство;
ИС	– информационная система;
КСЗ	– комплекс средств защиты;
НЖМД	– накопитель на жестких магнитных дисках;
ОС	– операционная система;
ПИ	– программное изделие;
ПО	– программное обеспечение;
ПНС	– программа начального старта;
ПЭВМ	– персональная электронная вычислительная машина;
СВТ	– средство вычислительной техники;
УЦ	– удостоверяющий центр;
ФС	– файловая система;
ЦУС	– центр управления системой;
AD	– Active Directory;
DC	– Domain Controller;
PDC	– Primary Domain Controller.

[illegible][illegible]