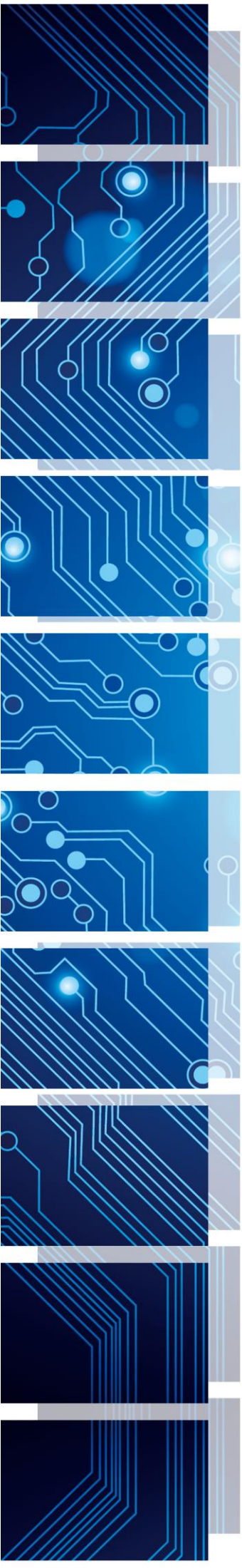


УВЕРЕННОСТЬ В КАЖДОМ РЕШЕНИИ

ГАРАНТ

ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

СБОРНИК ТЕХНИЧЕСКИХ ИНСТРУКЦИЙ ПО УСТАНОВКЕ И ОБСЛУЖИВАНИЮ ЭПС «СИСТЕМА ГАРАНТ» («ГАРАНТ-ПРОКСИМА»)

Москва, 2022 г.

Оглавление

СИСТЕМА ГАРАНТ ПРОКСИМА. ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Технические требования

Виды поставки

Система ГАРАНТ ПРОКСИМА поставляется в следующих вариантах:

1) инсталляционная локальная версия,
2) инсталляционная сетевая клиент-серверная версия, работающая по технологии тонкого web-клиента,
3) локальная мобильная версия (USB флеш-накопитель), Мобильный ГАРАНТ онлайн.

Требования к серверу:

- 64-х разрядная ОС MS Windows 7, 8, 10, 2008R2, 2012, 2016, 2019; Astra Linux Special Edition, Astra Linux Common Edition; Альт Сервер, Альт 8 СП Сервер.
- процессор: 4-8 ядер. Количество ядер зависит от количества одновременно работающих пользователей в системе. Ориентировочно можно считать 2-4 ядра на 10-20 одновременно работающих пользователей.
- Оперативная память от 8 Гб. Объем оперативной памяти так же зависит от количества одновременно работающих пользователей.
- 237 Мб для исполняемых файлов системы. Дисковое пространство, занимаемое информационным банком, определяется его наполнением. Желательно устанавливать ГАРАНТ ПРОКСИМА на быстрые диски в RAID-массиве или SSD. При этом SSD предпочтительнее, так как происходит одновременный поиск нескольких пользователей по сотням Гб информации.

Требования к клиентским местам:

1. При работе с инсталляционной сетевой клиент-серверной версией (то есть с версией, установленной на сервере) операционная система на рабочих станциях может быть любая.
2. Должен быть установлен браузер из списка, не ниже версии поддерживаемых:
   - Chrome 33+
   - Firefox 29+
   - Opera 20+
   - Yandex 21+
   - IE 10+
   - Edge
   - Safari 10+ (MacOS)
   - браузеры мобильных устройств (в этом случае открывается мобильная версия ГАРАНТ ПРОКСИМА)
3. Для полнофункциональной работы в браузере должны быть:
   - разрешены прием cookies (как минимум – с адреса, на котором будет развернута Интранет-версия),
   - разрешены JavaScript,
   - разрешены всплывающие окна,
   - выставлены корректные настройки даты, времени и часового пояса.

Важно! *Приложения, блокирующие рекламу, а также антивирусы могут блокировать работу Javascript, поэтому может потребоваться добавление адреса Интранет-версии в исключения этих приложений.*

Требования к клиентским местам для инсталляционной локальной версии или Мобильный ГАРАНТ онлайн:

- 64-х разрядная ОС MS Windows 7, 8, 10; Astra Linux Special Edition, Astra Linux Common Edition; Альт Workstation.

Краткое техническое описание

ГАРАНТ ПРОКСИМА – кроссплатформенная версия системы, открывающая доступ к информационному банку пользователя в двух режимах – онлайн и оффлайн в единой оболочке через браузер.

При наличии на компьютере пользователя доступа в Интернет при запуске системы ГАРАНТ ПРОКСИМА автоматически открывается актуальная Интернет-версия комплекта, обновляемая три раза в день. При отсутствии Интернета – оффлайн-комплект, который устанавливается на компьютер пользователя или в локальную сеть.

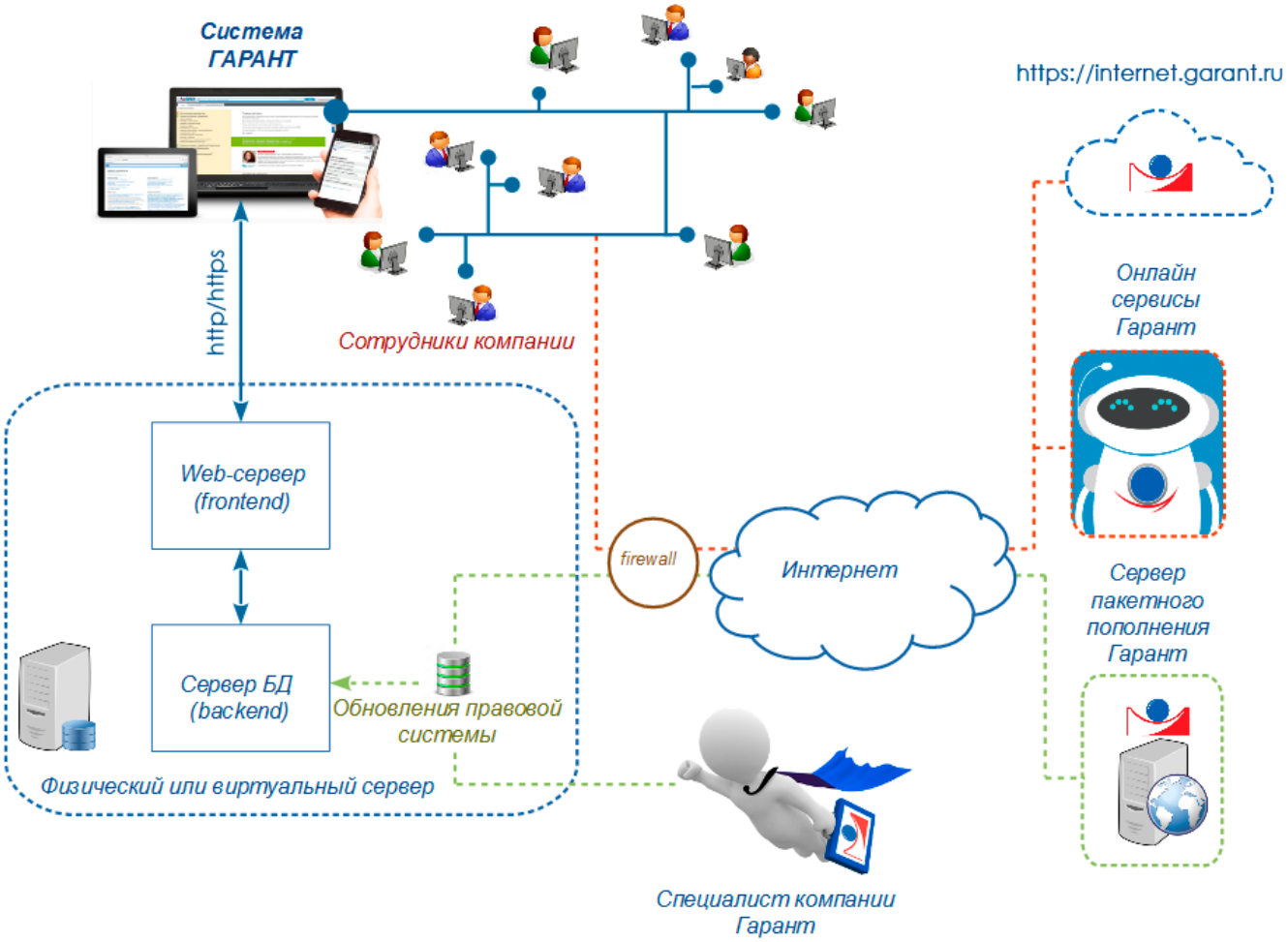
Информационный банк системы может быть распределен: можно установить только часть блоков локально для экономии дискового места и времени для обновления комплекта, а полный комплект использовать только в онлайн-доступе.

ГАРАНТ ПРОКСИМА обеспечивает работу всех онлайн-сервисов при наличии Интернета на локальном компьютере пользователя. При отсутствии Интернета онлайн-сервисы, включая Горячую линию, из системы будут недоступны.

ГАРАНТ ПРОКСИМА является кроссплатформенным решением и работает как на компьютерах под управлением семейства операционных систем Windows, так и в наиболее распространенных дистрибутивах операционных систем Linux.

Интерфейс Интранет-версии системы ГАРАНТ предусматривает работу с разрешением экрана не менее 1024*768.

Пример функциональной схемы работы ГАРАНТ ПРОКСИМА в локальной вычислительной сети компании.



ГАРАНТ ПРОКСИМА НА ОС WINDOWS

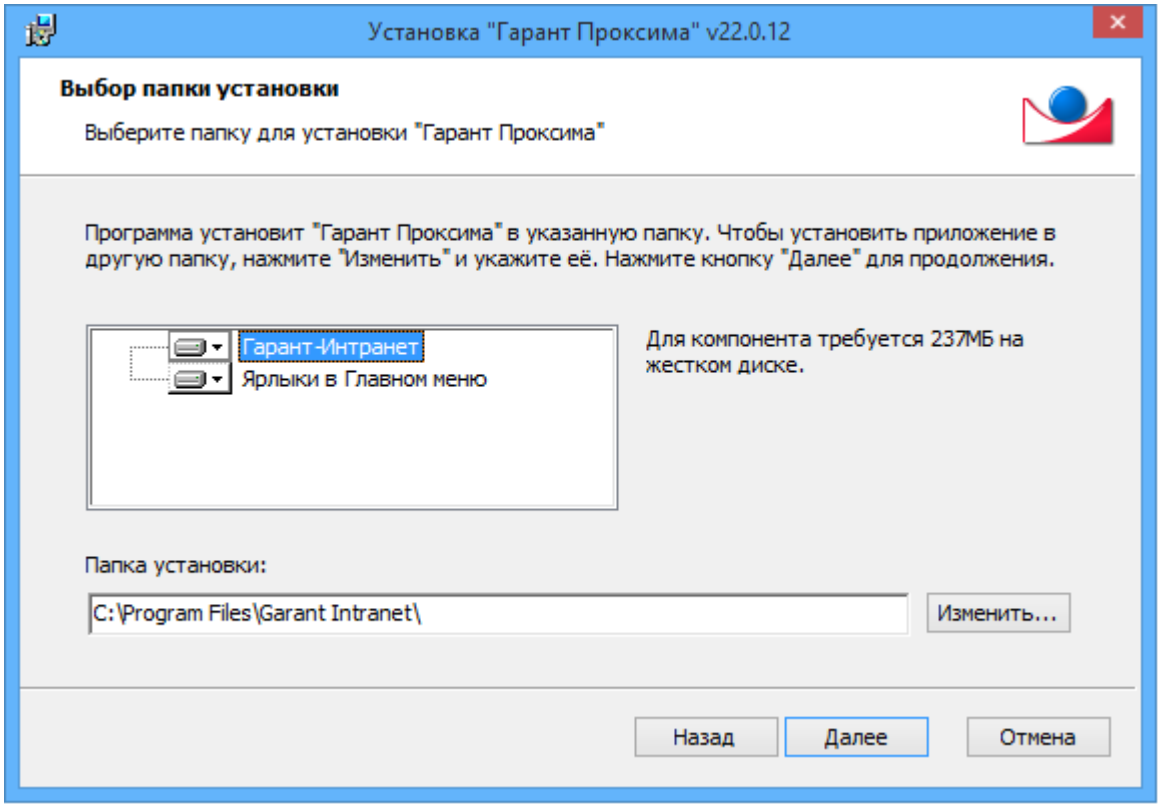
Установка ГАРАНТ ПРОКСИМА на ОС Windows

Шаг 1. С установочного дистрибутива запустите файл **intranet-xx.x.xx.exe**. Подтвердите запуск установки.

Шаг 2. Выберите папку для установки и нажмите «Далее».

Важно!	*Путь для установки ГАРАНТ ПРОКСИМА должен отличаться от каталога установки старой Интранет-версии, которая устанавливалась по умолчанию в каталог C:\Program Files\Garant-Intranet (отличается наличием знака "-").* *Путь для установки ГАРАНТ ПРОКСИМА должен содержать только латинские буквы (кириллица не допускается).*

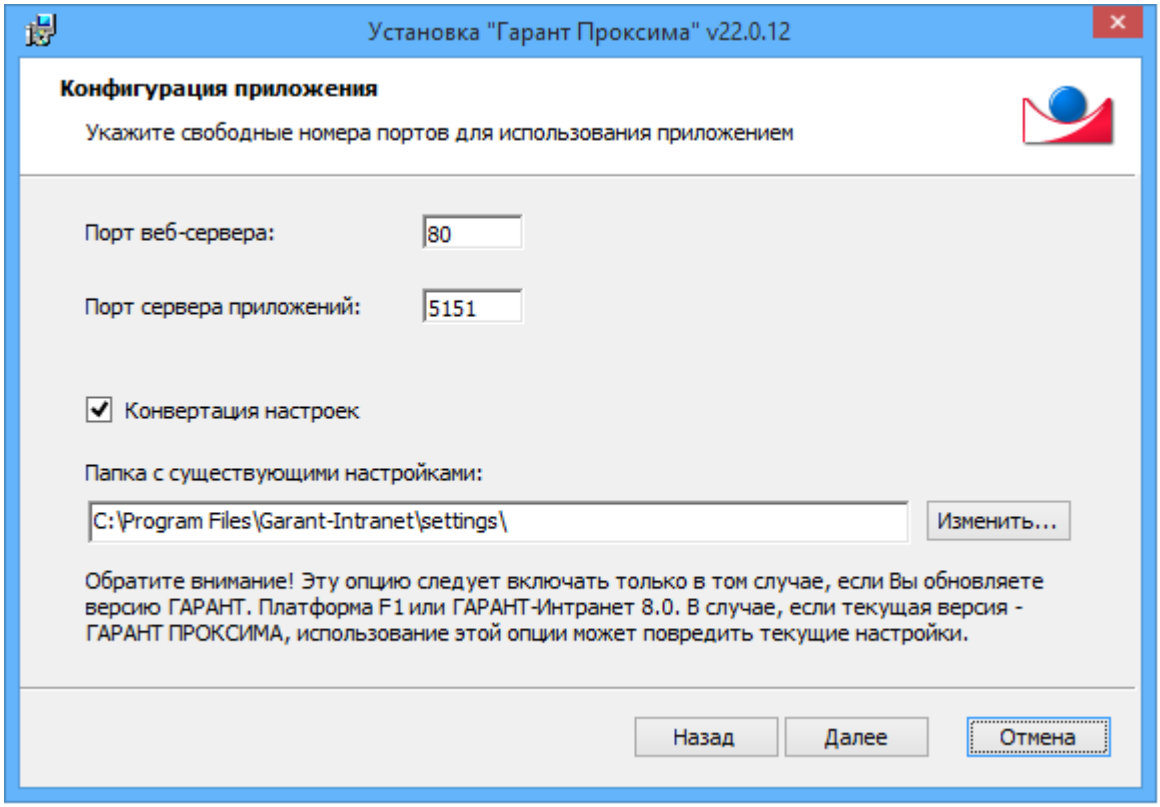
Если ОС на сервере относительно старая, то может потребоваться Microsoft Visual C++ (https://www.microsoft.com/en-gb/download/details.aspx?id=26368) — показателем этого будет остановка web службы.



Шаг 3. Установите свободные номера портов для использования приложением. По умолчанию порт web-сервера: 80, порт сервера приложений: 5151.

***Примечание**:* Иногда порт 80 может быть занят другим приложением, например IIS. Посмотреть список портов, занятых в данный момент соединением, можно следующим образом: в командной строке наберите команду **netstat -a** (если выданный на экран результат не уместится на одну страницу – наберите **netstat -a | more** – результат будет выдаваться поэкранно; следующий экран – после нажатия на пробел).

В том случае, если на сервере установлена старая версия Интранет, инсталлятор произведет ее поиск по пути C:\Program Files\Garant-Intranet для конвертации настроек пользователей. Еслипредыдущая версия установлена в другом каталоге, - укажите его вручную. Путь необходимо указывать до каталога settings (см. рисунок ниже). Это относится и к системе ГАРАНТ Платформа F1, при этом службы предыдущих версий должны быть остановлены. Конвертация настроек возможна только для старых версий, у которых в файле version.txt строчка выглядит как 8.00.xxxxx. Конвертация настроек более свежих версий, например 10.0.32 или 2.06.3.119, запрещена, поскольку при конвертации повредятся настройки пользователей. При наличии данных версий, ГАРАНТ ПРОКСИМА установится поверх в ту же папку. Перед установкой ГАРАНТ ПРОКСИМЫ рекомендуется сделать резервную копию папки settings старой версии при остановленных службах.



После установки порт веб-сервера можно будет поменять в **config.py** в строчке wsgi_port=80. После изменения требуется перезапуск службы веб-сервера.

Порт сервера приложений (БД) настраивается в **garant.ini** в строчке - *GCMServerPort=5151*. При изменении порта сервера приложений соответствующие изменения необходимо внести в **config.py** в строчку *servers=['corbaloc:iiop:localhost:5151/NameService']*. После изменения требуется перезапуск службы сервера приложений.

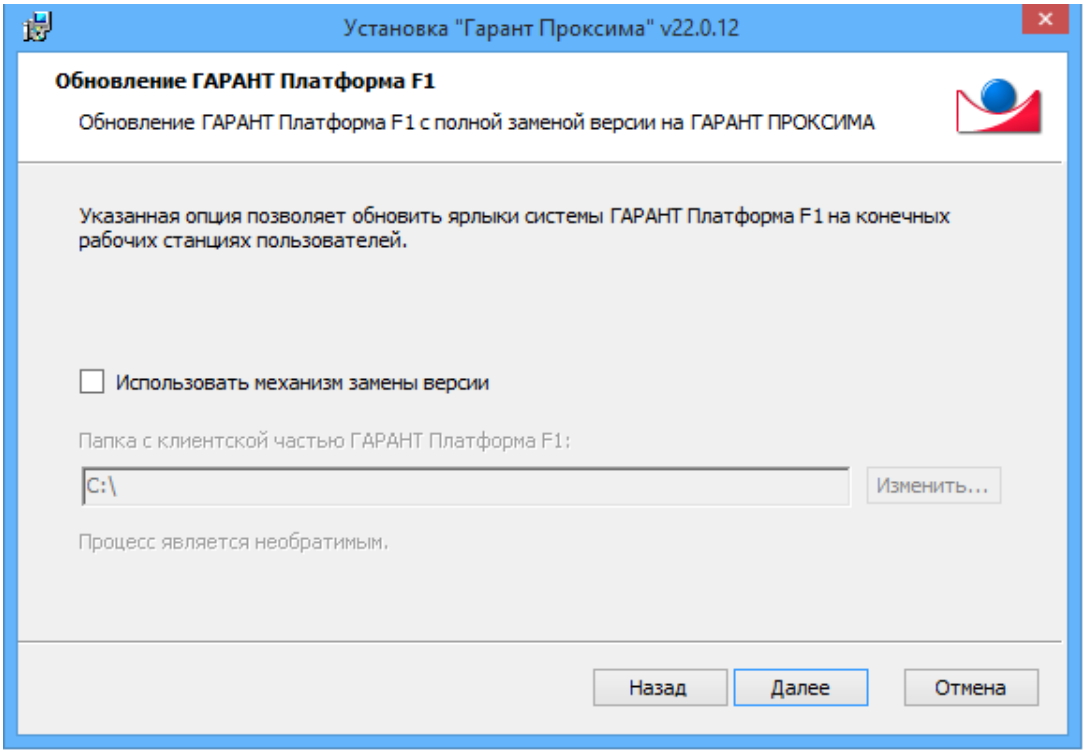
Для изменения портов в Linux ОС рекомендуется запустить утилиту реконфигурации.

Шаг 4. Обновите пользовательский ярлык системы ГАРАНТ Платформа F1 для входа в ГАРАНТ ПРОКСИМА.

В случае, если ранее была установлена система ГАРАНТ Платформа F1, и клиентская часть запускалась не с пользовательских компьютеров, а с единого сетевого ресурса, вы можете использовать механизм замены версии.

При его активации исполняемый файл в расшаренной клиентской оболочке будет заменен на ГАРАНТ ПРОКСИМА, а пользователи со своих рабочих станций войдут по «старому» ярлыку в новую версию. При этом ввод логинов и паролей для входа не потребуется.

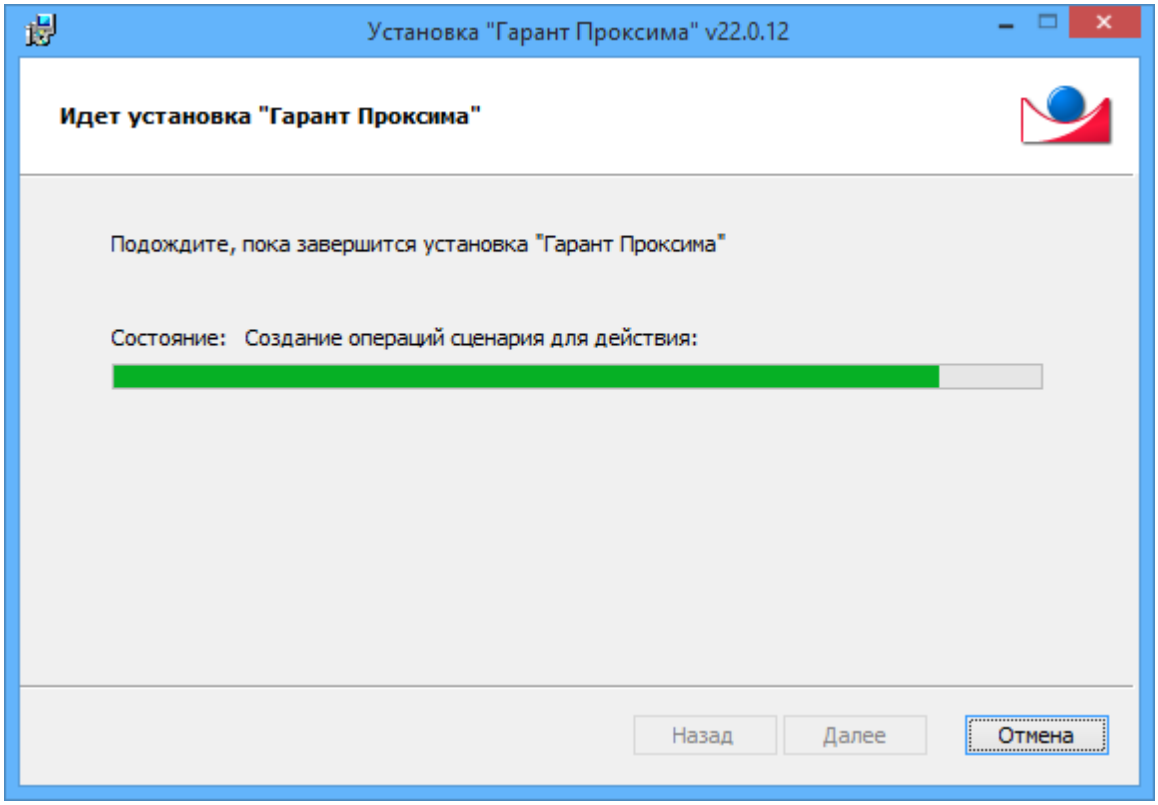
Обратите внимание: использование этой опции а) требует обязательного переноса настроек, б) необратимо, то есть использование клиентской части системы ГАРАНТ Платформа F1 после отработки инсталлятора станет невозможным (перед использованием механизма можно сделать копию клиентской части).



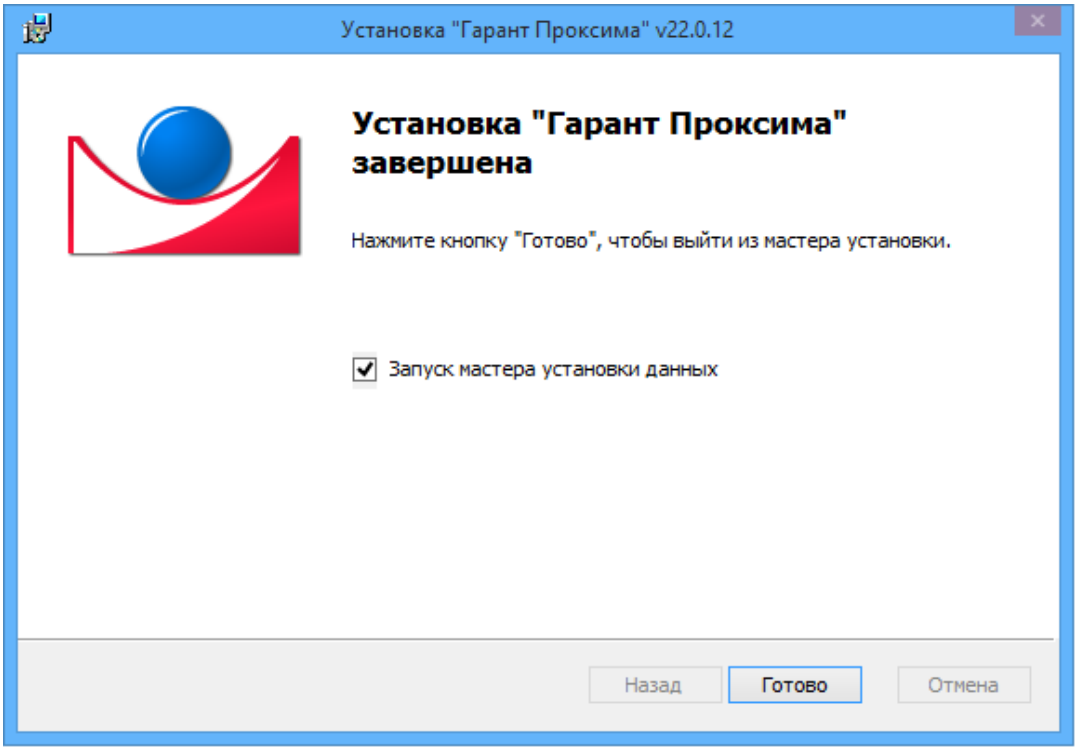
ГАРАНТ ПРОКСИМА может быть установлена и работать параллельно с системой ГАРАНТ Платформа F1. В ряде случаев имеет смысл не удалять старую версию сразу после установки ГАРАНТ ПРОКСИМА, предоставив пользователям возможность убедиться, что все их настройки перенесены. Желательно перед установкой новой версии сохранить папку settings от старой версии, перед сохранением остановить службы ГАРАНТа.

Следует помнить, что если Вы решили оставить старую необновляемую версию на некоторое время, может возникнуть ситуация, при которой места для установки данных двух версий на сервере будет недостаточно.

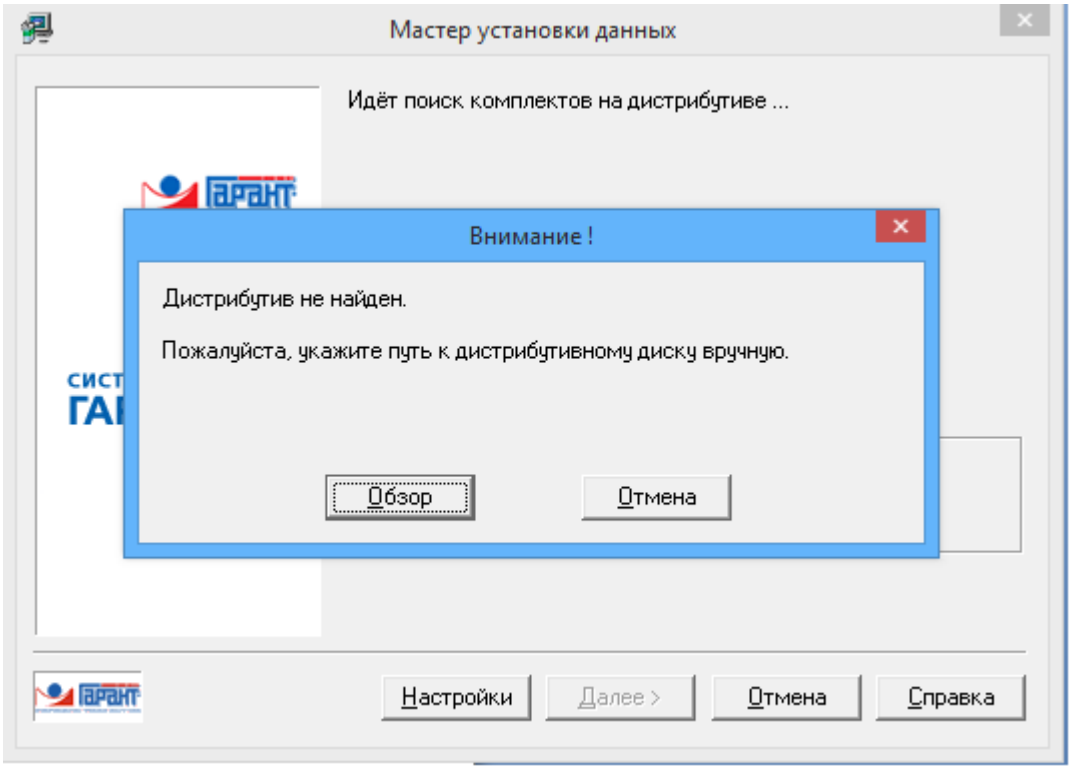
Шаг 5. После выполнения шага 4 начнется установка ГАРАНТ ПРОКСИМА.



Шаг 6. Запустите мастер установки данных. Чтобы запустить его, нажмите «**Готово»**. Если вы откажетесь от запуска мастера установки, вы сможете запустить его вручную позднее (ярлык в меню Пуск\ Программы\ Гарант Проксима\ Информационный банк\ Установка данных, либо %Garant Intranet%\apps\win64\datasetup.exe). Справочную информацию по Мастеру установки данных можно получить, нажав на кнопку «Справка» в окне этой программы, а также в файле %Garant Intranet%\apps\help\F1DataTools.chm.



После запуска мастера установки данных от вас может потребоваться вручную указать путь к каталогу данных, находящемуся на дистрибутиве. Для этого на появившемся окне с заголовком «Внимание!» нажмите кнопку «**Обзор»**, в диалоге выбора папки укажите каталог данных на дистрибутиве и нажмите «**ОК»**.



Шаг 7. Для окончания установки системы ГАРАНТ ПРОКСИМА завершите процесс установки данных. Если мастер установки данных сообщит вам о нехватке свободного места на диске, то на данном этапе можно удалить каталог с предыдущей версией.

Шаг 8. После завершения установки и проверки работоспособности системы ГАРАНТ ПРОКСИМА каталог с предыдущей версией системы Гарант-Интранет или Платформа F1 можно удалить.

Обновление информационного банка системы

Для обновления информационного банка через Интернет предназначены:

- программа загрузки файлов пакетного пополнения (%GarantIntranet%\apps\win64\download.exe)
- программа пакетного пополнения (%Garant Intranet%\apps\win64\dataupd.exe)

Подробное описание этих программ смотрите во встроенном файле справки (%Garant Intranet%\apps\Help\F1DataTools.chm).

Настройка автоматического обновления через Интернет

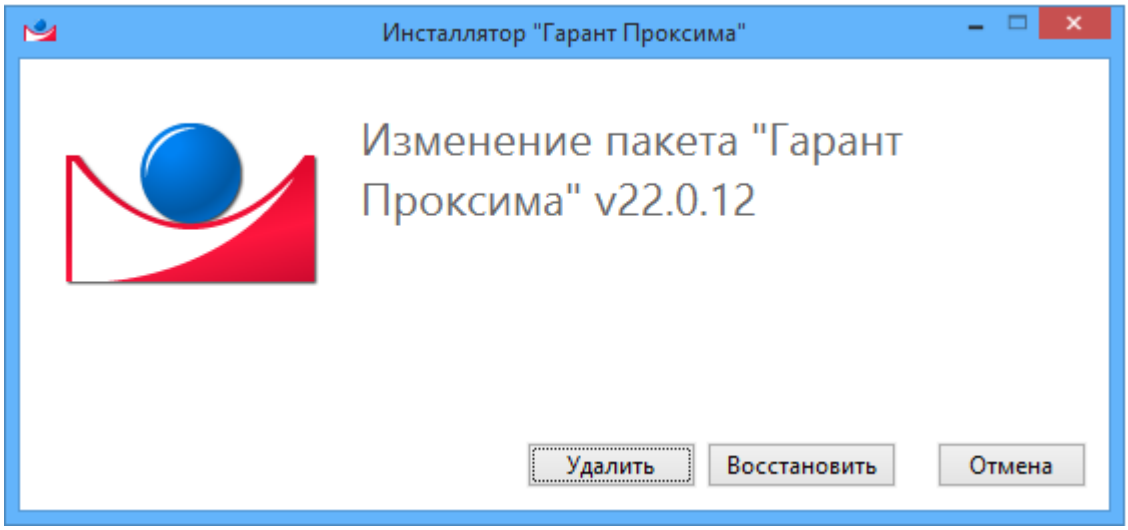
Удобнее всего использовать пакетное обновление в автоматическом режиме (автоматическое скачивание и применение файлов обновления, запускаемое в заданное время, например, по ночам). Для включения и настройки параметров автоматического обновления предназначена программа %Garant Intranet%\apps\F1EasyUpdate.exe.

Подробнее смотрите встроенную справку к программе F1EasyUpdate (%Garant Intranet%\apps\Help\F1EasyUpdate.chm).

Удаление ГАРАНТ ПРОКСИМА

Порядок удаления системы следующий:

1. Откройте панель управления ОС MS Windows.
2. Запустите «Программы и Компоненты».
3. Найдите в списке программ «ГАРАНТ ПРОКСИМА» и нажмите «Изменить».
4. В появившемся окне нажмите «Удалить».

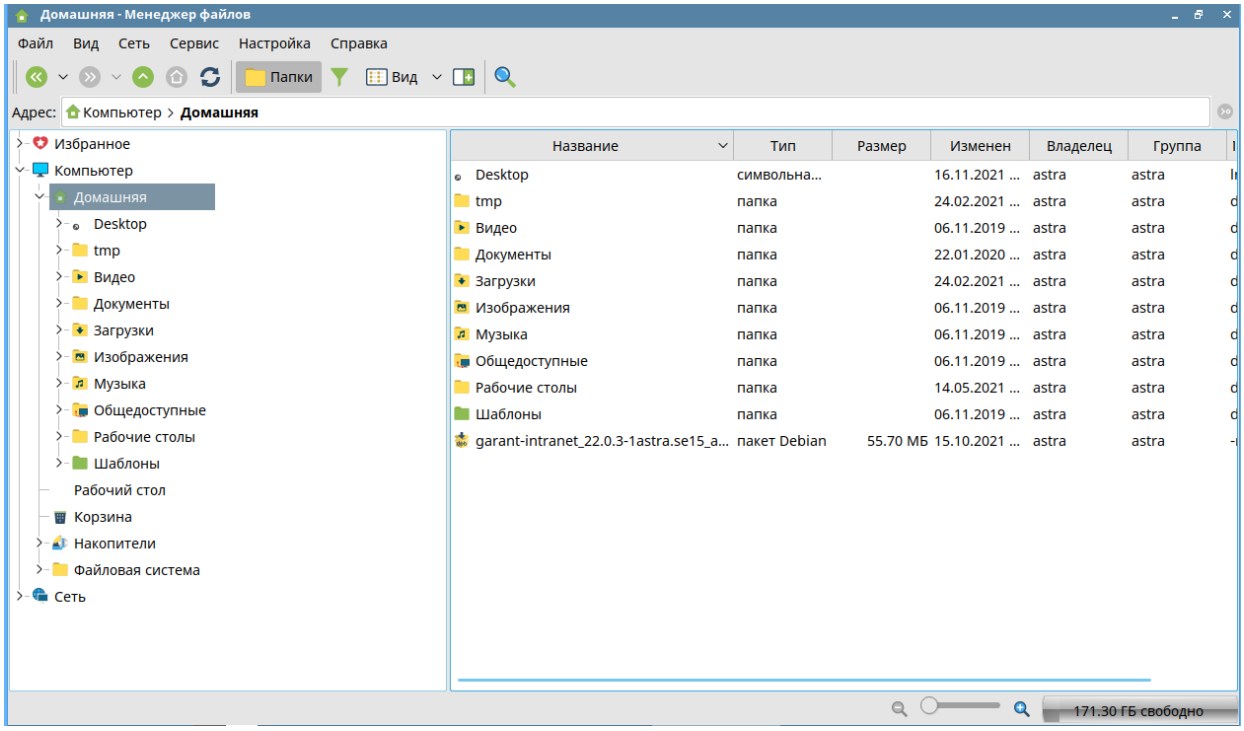


ГАРАНТ ПРОКСИМА НА ОС ASTRALINUX

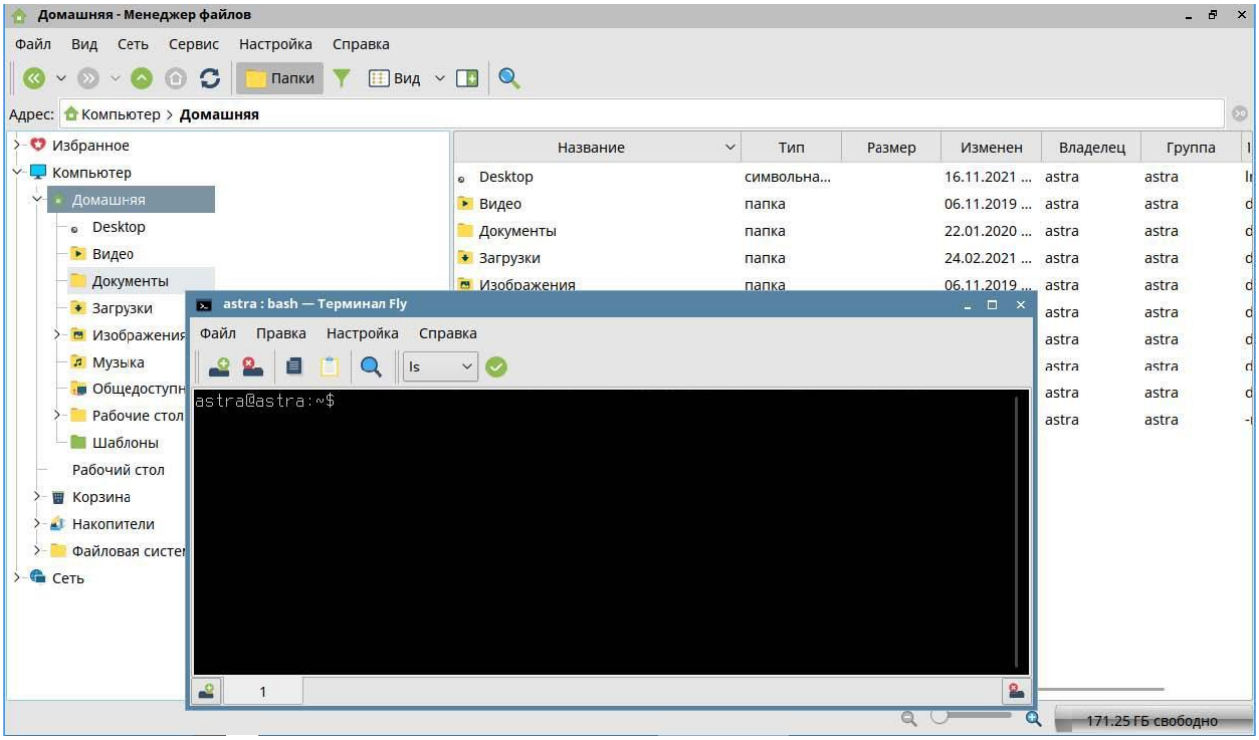
Перед изучением данного раздела рекомендуем изучить раздел Приложение 1. КРАТКАЯ СПРАВКА ПО РАБОТЕ С ОС LINUX.

Установка ГАРАНТ ПРОКСИМА на ОС AstraLinux

Шаг 1. Файл дистрибутива ***garant-intranet-xx.x-x-astra.deb*** необходимо скопировать в домашний каталог (На рабочем столе необходимо найти ярлык «Мой Компьютер»).



Шаг 2. Необходимо запустить терминал. Для этого выберите меню «Сервис - Открыть терминал» (или сочетание клавиш Alt+T). В связи с тем, что на сервере может не быть графического интерфейса, весь процесс установки и настройки производится в терминале (командной строке).



Шаг 3. Далее необходимо запустить установку оболочки с помощью команды в терминале:

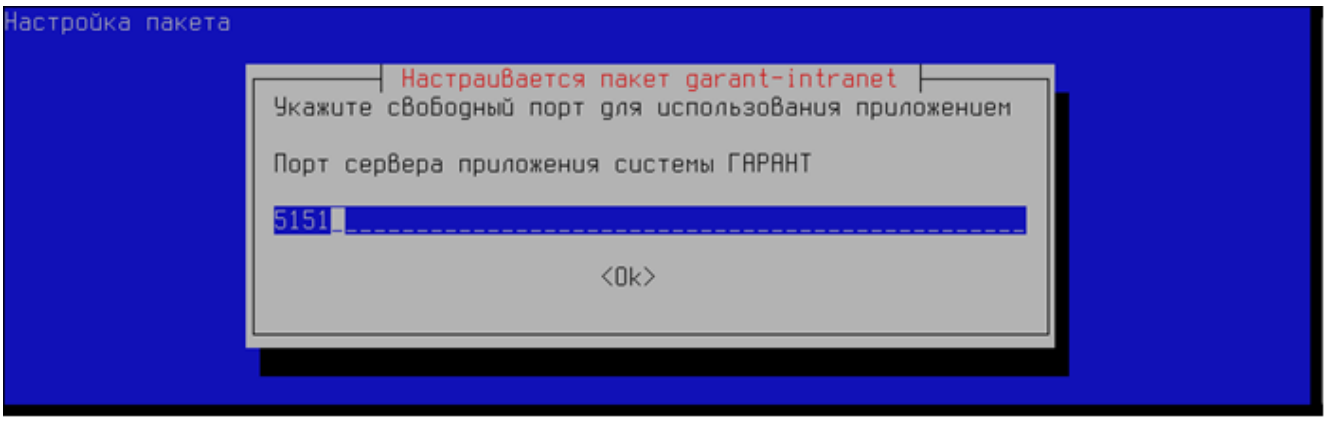
sudo dpkg -i garant-intranet-xx.x-x-astra.deb

При условии, что дистрибутив оболочки лежит в домашнем каталоге, и в терминале мы тоже находимся в домашнем каталоге, иначе надо указать путь к дистрибутиву оболочки относительно корня (можно инсталлировать сразу с переносного носителя). Для ввода названия файла дистрибутива достаточно набрать первые несколько символов и нажать кнопку Tab.

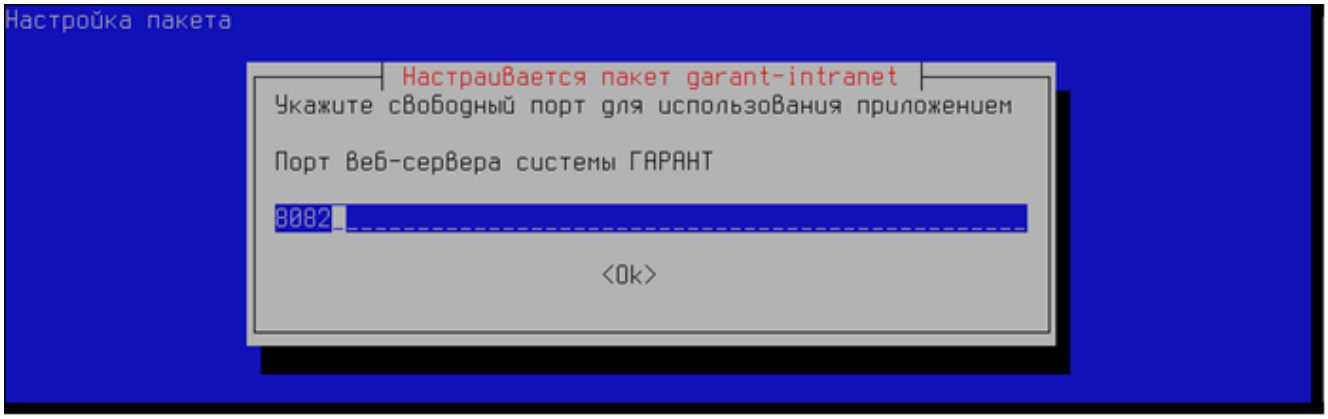
Дистрибутив локальной версии имеет название garant-**desktop**-xx.x-x-astra.deb.

Шаг 4. После запуска установки пакета будет предложено ввести необходимые настройки:

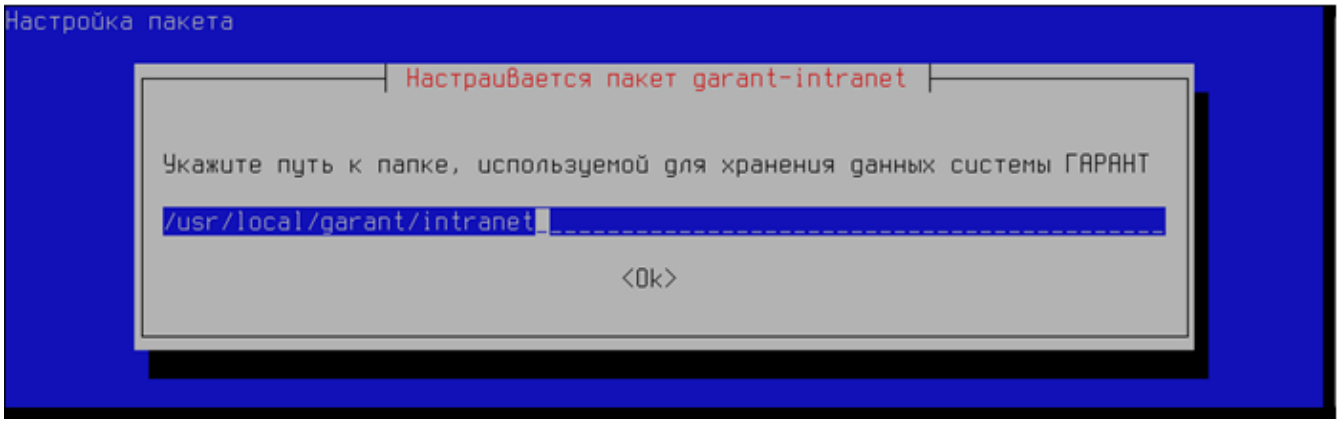
Порт сервера приложений (БД) ГАРАНТ ПРОКСИМА: 5151 (по умолчанию)



Порт Веб-сервера ГАРАНТ ПРОКСИМА: 8082 (по умолчанию)

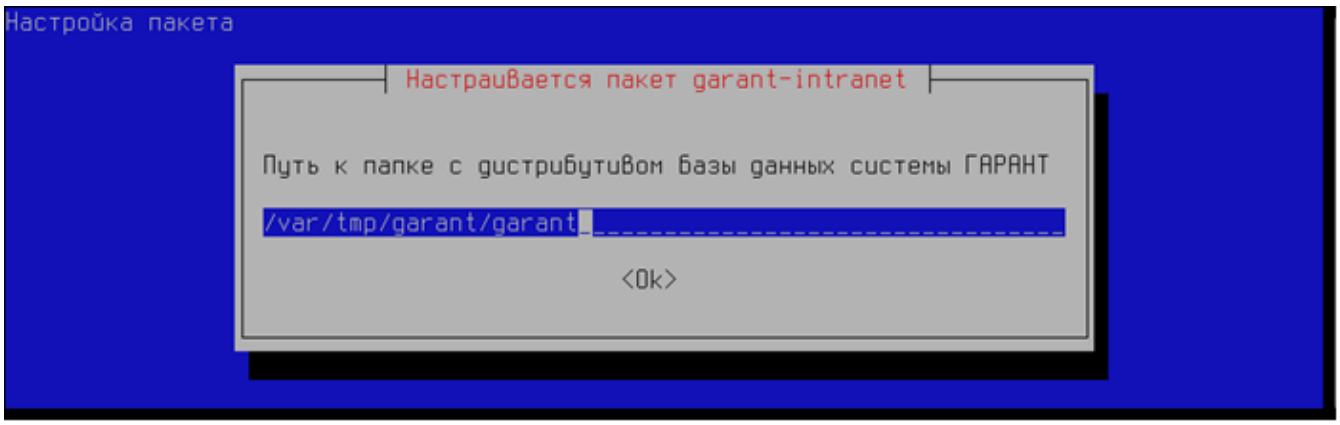


Путь к папке, куда будет установлена по умолчанию система ГАРАНТ ПРОКСИМА: ***/usr/local/garant/intranet***. В этой папке при установке создадутся каталоги data1, data2,delta и т.д.



Для локальной версии путь установки по умолчанию ***/usr/local/garant/desktop***. В дальнейшем учитывайте отличие в пути к папке с установленной версией и необходимым утилитам.

Путь к папке с дистрибутивом базы данных ГАРАНТ ПРОКСИМА (по умолчанию путь указан к приводу CDROM):



В данном примере папка garant с дистрибутивом скопирована на сервер и лежит в папке /var/tmp/garant.

> ***Важно!*** *Путь к папке с дистрибутивом базы данных должен быть указан в виде пути до каталога, где находится папка data.*

Обновление информационного банка системы

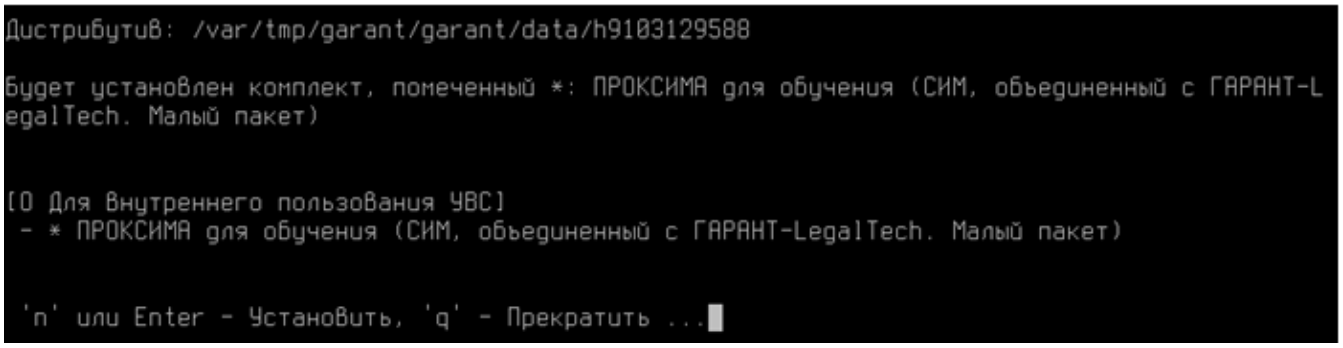
Шаг 5. После успешной установки оболочки ГАРАНТ ПРОКСИМА необходимо выполнить установку базыданных.

Для запуска установки базы данных ГАРАНТ ПРОКСИМА запустите файл datasetup, выполнив следующую команду:

/usr/local/garant/intranet/bin/datasetup

Для локальной версии команда будет: **/usr/local/garant/desktop/bin/datasetup**

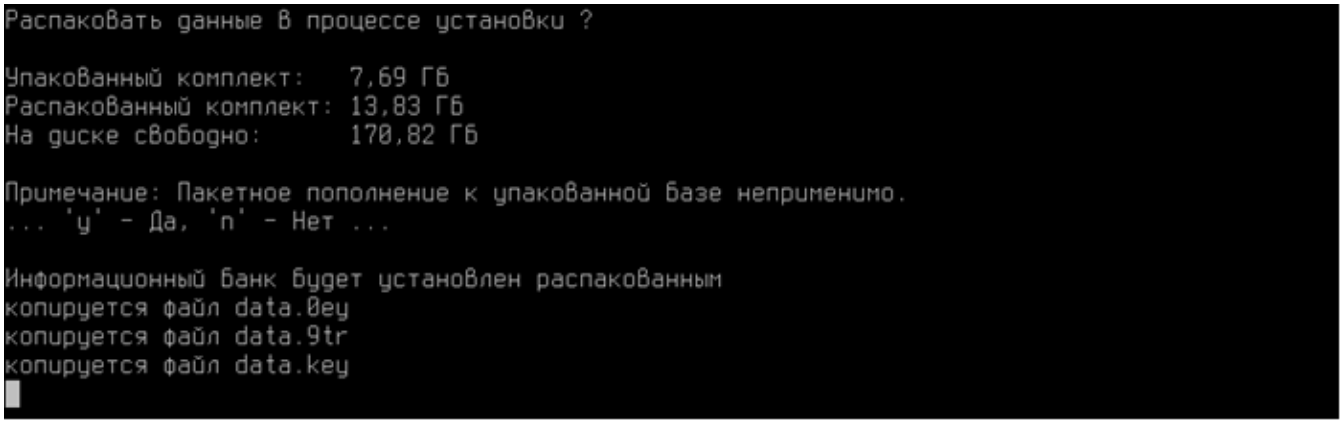
Далее следуйте указаниям мастера установки базы данных. На вопрос о продолжении установки введите **n** или **«Enter»** для продолжения, или **q** для прекращения установки.



Система запросит пароль-отзыв, введите код ответа и нажмите «Enter».

Далее введите **y** или **n** для продолжения установки данных в упакованном или распакованном виде и нажмите «Enter» (распаковывать данные необходимо, если планируется обновление дельтой).

Важно! *Для успешной установки на диске должно быть достаточно свободного места.*



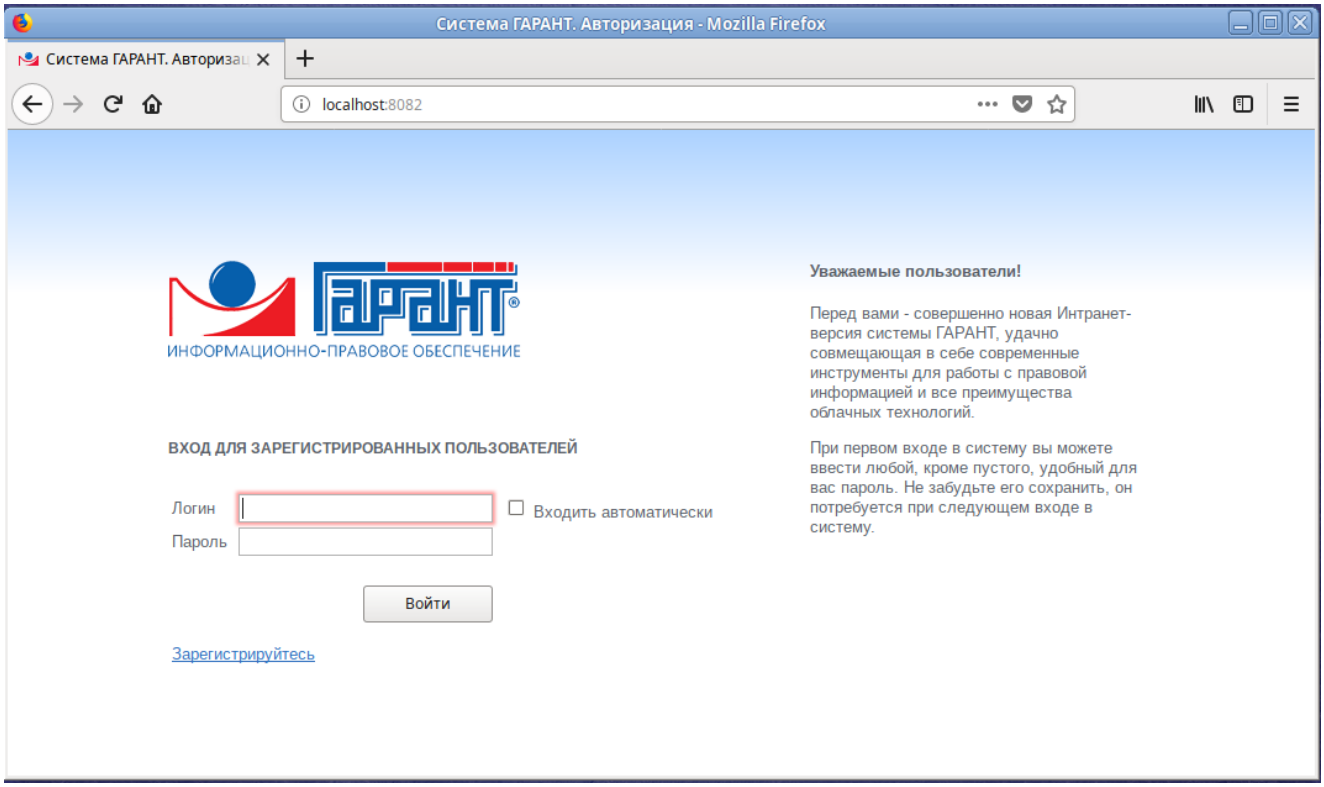
Дождитесь окончания установки базы данных, время установки зависит от производительности ПК и размера базы данных. Процесс установки базы данных показан строчками копирования файлов базы.

Примечание: Если при установке данных появляется ошибка доступа (access denied), необходимо поменять владельца на каталог с дистрибутивом, командой:

sudo chown -R ru-garant:ru-garant /var/tmp/garant/garant

где /var/tmp/garant/garant — каталог, где хранится дистрибутив с базой данных. В случае, если дистрибутив находится на внешнем носителе (USB, DVD), необходимо сменить владельца точки монтирования.

Шаг 6. После завершения установки необходимо проверить работу системы ГАРАНТ ПРОКСИМА, для этого запустите браузер и введите в адресной строке **http://адрес_сервера:8082**



Администрирование учетных записей пользователей происходит в интерфейсе администратора ГАРАНТ ПРОКСИМА. Для перехода в него необходимо ввести в адресной строке браузера **http://адрес_сервера:8082/admin** (Логин – ADMIN, пароль – ADMIN)

При этом пользователь может зарегистрироваться самостоятельно, нажав на странице приветствия «**Зарегистрируйтесь**» и введя требуемые учетные данные.

Настройка автоматического обновления через Интернет

Важно! *Для работы механизма обновления необходимо хотя бы раз запустить /usr/local/garant/intranet/bin/download в ручном режиме, поскольку системе необходимо зафиксировать логин/пароль для доступа к серверу пакетного пополнения (СПП) и комплект. После запуска введите логин и пароль от СПП и укажите номер комплекта в списке, подождите, пока сформируется и скачается дельта для комплекта (процесс занимает некоторое время).*

```
administrator@UVS-ASTRALINUX:~$ /usr/local/garant/intranet/bin/download
Thu Mar 24 2022 16:58:45.633653[2707, 126429265737088] -LM_DEBUG: LD_LIBRARY_PATH: /usr/loca
l/garant/intranet/tools/../lib:/usr/local/lib:/usr/lib:/lib
log file /usr/local/garant/intranet/logs/download.log created
Login: 77-00002-000792
Password: nAAAAAAA
Выберите комплект, для которого требуется скачать дельты
1: СИМ, объединенный с ГАРАНТ-LegalTech. Малый пакет(ПРОКСИМА для обучения)
call getch(): press key to read, then press ENTER: 1

full_path = /usr/local/garant/intranet/delta/54122976.zip
Loading 54122976.zip (2632.39 Mb)
administrator@UVS-ASTRALINUX:~$
```

Для настройки автоматического обновления необходимо создать скрипт, в котором прописать выполнение необходимых утилит, и настроить его запуск в планировщике

задач на заданное время. Например, в примере, прописанном ниже, обновления будут скачиваться с сервера пакетного пополнения и применяться ежедневно в 2 часа ночи. Если требуется только скачивать или только применять обновления, то необходимо указать только соответствующую утилиту.

Пример настройки автоматического обновления.

1. Переходим в каталог с установленным ГАРАНТом:

cd /usr/local/garant/intranet

2. Создаём скрипт:

sudo nano garupd, где garupd - название скрипта. Вместо тестового редактора nano можно использовать редактор vi (основы работы с данным редактором можно прочитать в разделе Приложение 1. КРАТКАЯ СПРАВКА ПО РАБОТЕ С ОС LINUX Текстовый редактор vi).

3. Откроется текстовый редактор nano, в который необходимо вписать следующие строки:

#!/bin/bash

/usr/local/garant/intranet/bin/download -auto -revision

/usr/local/garant/intranet/bin/dataupd

Сохраняем путем нажатия клавиш Ctrl+O и потом Enter, затем выходим путем нажатия клавиш Ctrl+X.

Для обновления без резервной копии – dataupd необходимо запустить с ключом -nobackup (не рекомендуется).

4. Делаем файл исполняемым:

sudo chmod +x garupd

5. Меняем владельца этого файла:

sudo chown ru-garant:ru-garant garupd

6. Для настройки запуска по расписанию нужно выполнить команду:

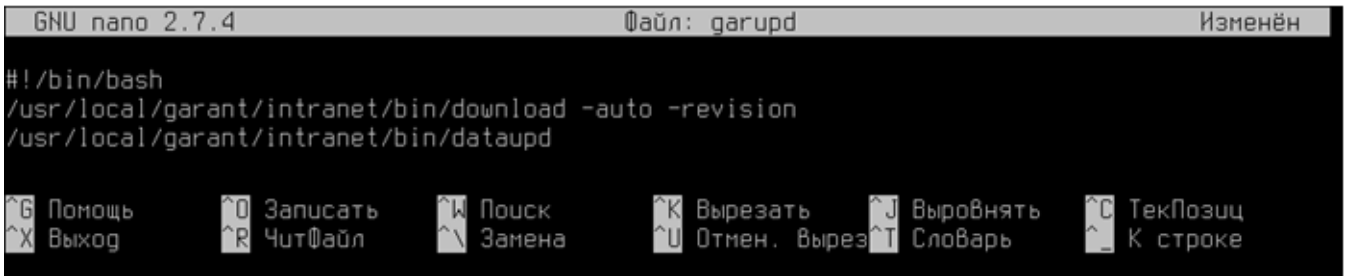
sudo crontab -u ru-garant -e

7. Откроется текстовый редактор планировщика задач cron, куда необходимо добавить следующую строку для выполнения скрипта:

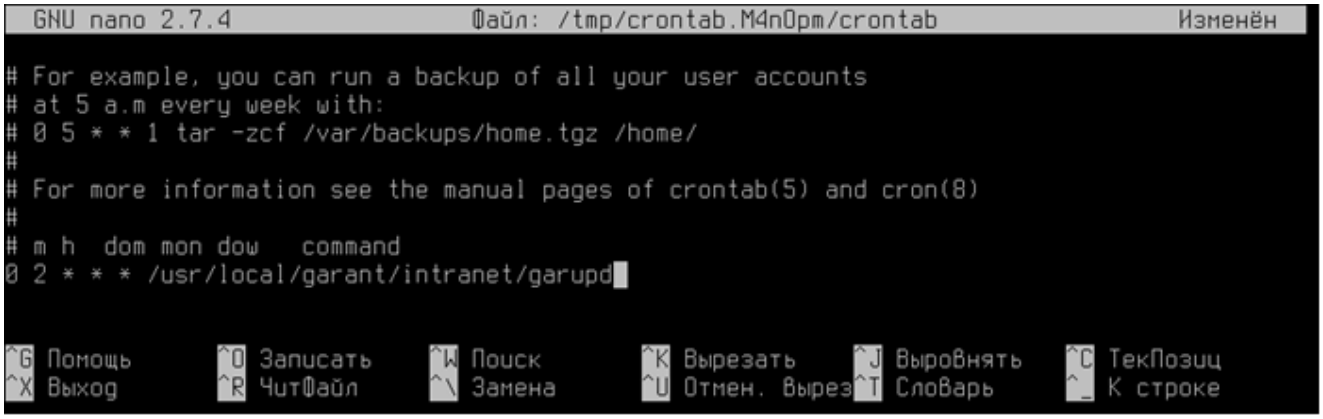
0 2 * * * /usr/local/garant/intranet/garupd

Получается, что скрипт запускается в 02:00 каждую ночь, каждого месяца, каждую неделю.

Пример скрипта:

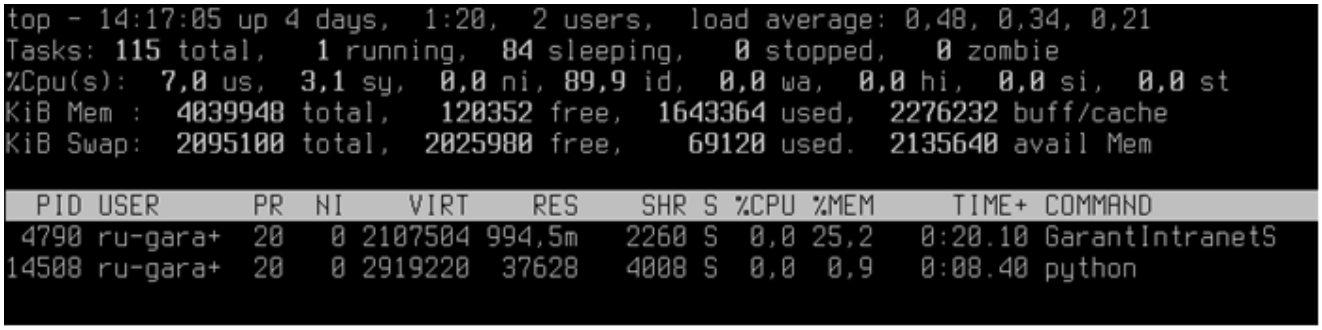


Пример запуска скрипта через планировщик cron:



Службы ГАРАНТ ПРОКСИМА

Для работы сетевой клиент-серверной версии ГАРАНТ ПРОКСИМА на сервере должны быть запущены два процесса: сервер приложений для работы с базами данных и веб-сервер для отображения интерфейса пользователя. Оба процесса запускаются от пользователя ru-garant. Убедиться в их работе можно через диспетчер задач. Для этого в командной строке необходимо выполнить команду: **top -U ru-garant**. В результате мы увидим список процессов пользователя ru-garant:



Для перезапуска служб ГАРАНТ ПРОКСИМА необходимо выполнить в терминале команду **/usr/local/garant/intranet/bin/restart.sh** (может потребоваться запуск с правами sudo):

Или перезапуск служб ГАРАНТ ПРОКСИМА можно сделать отдельными командами:

/usr/local/garant/intranet/bin/stop.sh

/usr/local/garant/intranet/bin/start.sh

В случае, если процесс GarantIntranetServer не закрывается (например, из-за конфликта прав), то его можно закрыть при помощи команды **kill**, указав PID процесса. Для примера выше команда будет выглядеть следующим образом:

sudo kill 4790

Важно! *В случае перезагрузки сервера служба приложений системы ГАРАНТ ПРОКСИМА автоматически не запустится, а в случае выхода из всех сессий на сервере служба приложений будет остановлена. Для того, что бы этого не происходило, необходимо в файле /etc/systemd/logind.conf раскомментировать и исправить строку KillUserProcesses=no, либо в случае ее отсутствия — добавить.*

В локальной версии данные процессы появляются только при запуске ГАРАНТ ПРОКСИМА. При выходе из ГАРАНТ ПРОКСИМА процессы закрываются.

Изменение настроек установки

В случае, если производится переустановка оболочки или обновление оболочки на более свежую версию, то экраны настроек установки (порты, расположение дистрибутива базы данных) отображаться не будут. Для изменения данных настроек ГАРАНТ ПРОКСИМА выполните команду в терминале (для применения новых настроек потребуется перезагрузка сервисов /usr/local/garant/intranet/bin/restart.sh):

sudo dpkg-reconfigure garant-intranet

```
administrator@UVS-ASTRALINUX:~$ sudo dpkg-reconfigure garant-intranet
```

Для локальной версии команда будет выглядеть следующим образом:

sudo dpkg-reconfigure garant-desktop

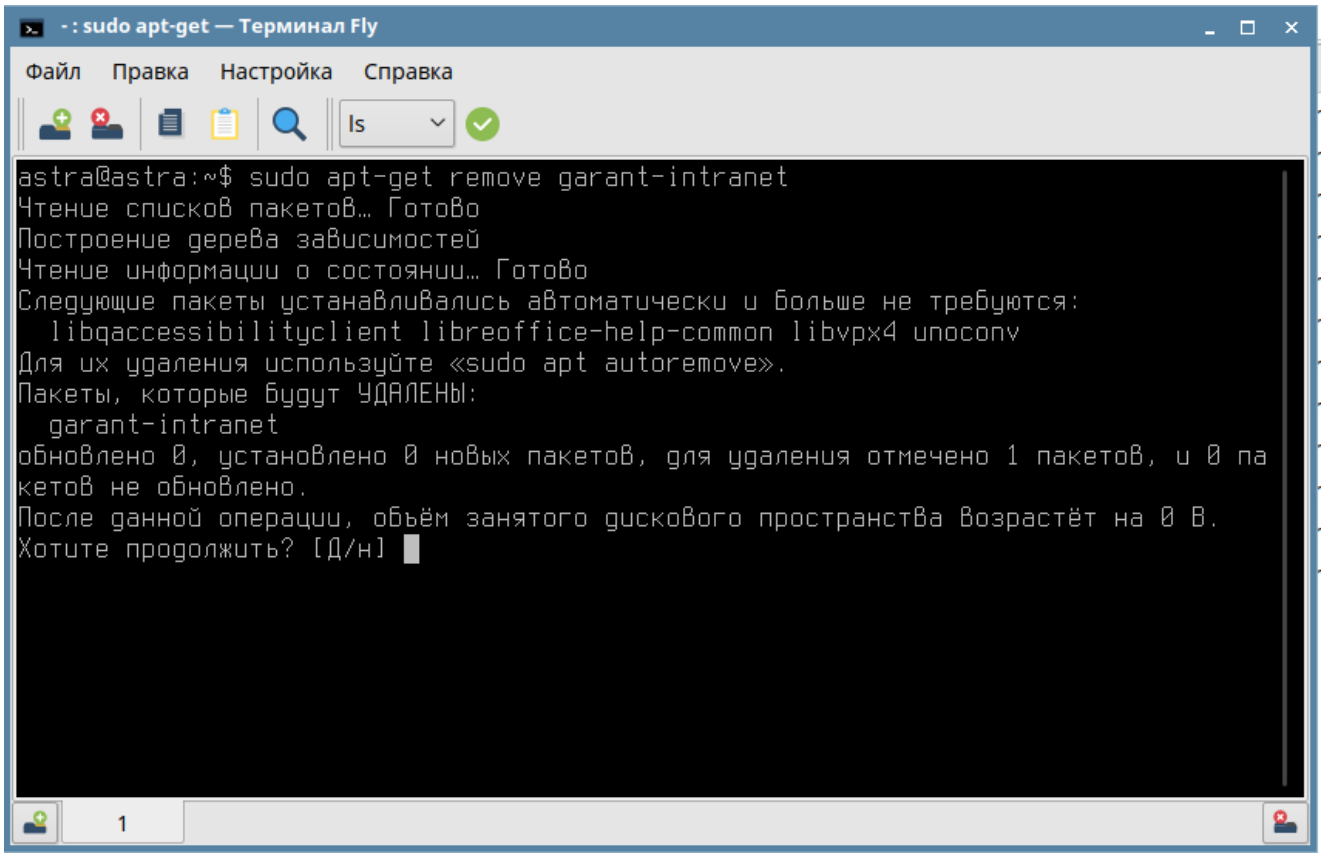
В результате выполнения данной команды будет предложено изменить настройки, которые устанавливались при первоначальной установке на Шаге 4.

Удаление ГАРАНТ ПРОКСИМА

7. Для удаления ГАРАНТ ПРОКСИМА используйте команду в терминале:

sudo apt-get remove garant-intranet

Подтвердите удаление нажатием Y и «ENTER»



По завершению удаления пакета **garant-intranet** удалите содержимое папки **garant**, которая находится в каталоге **/usr/local/garant**.

Для локальной версии команда будет выглядеть следующим образом:

sudo apt-get remove garant-desktop

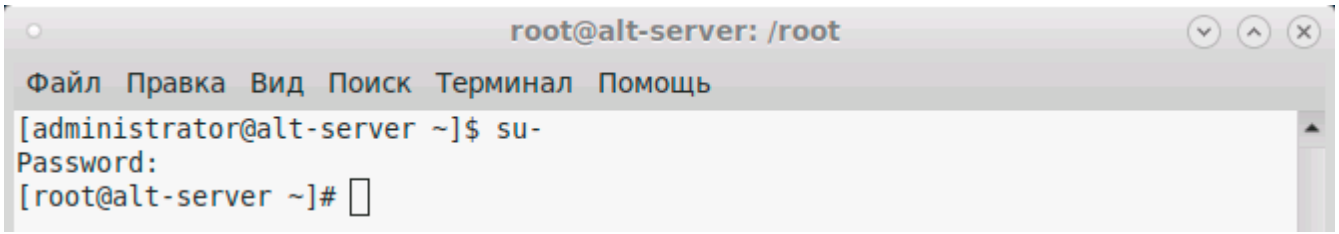
ГАРАНТ ПРОКСИМА НА ОС ALTLINUX

Перед изучением данного раздела рекомендуем изучить раздел Приложение 1. КРАТКАЯ СПРАВКА ПО РАБОТЕ С ОС LINUX

Установка ГАРАНТ ПРОКСИМА на ОС AltLinux

Шаг 1. Устанавливаем пакет ***garant-intranet-xx.x-x-alt.rpm*** с предоставленного дистрибутива.

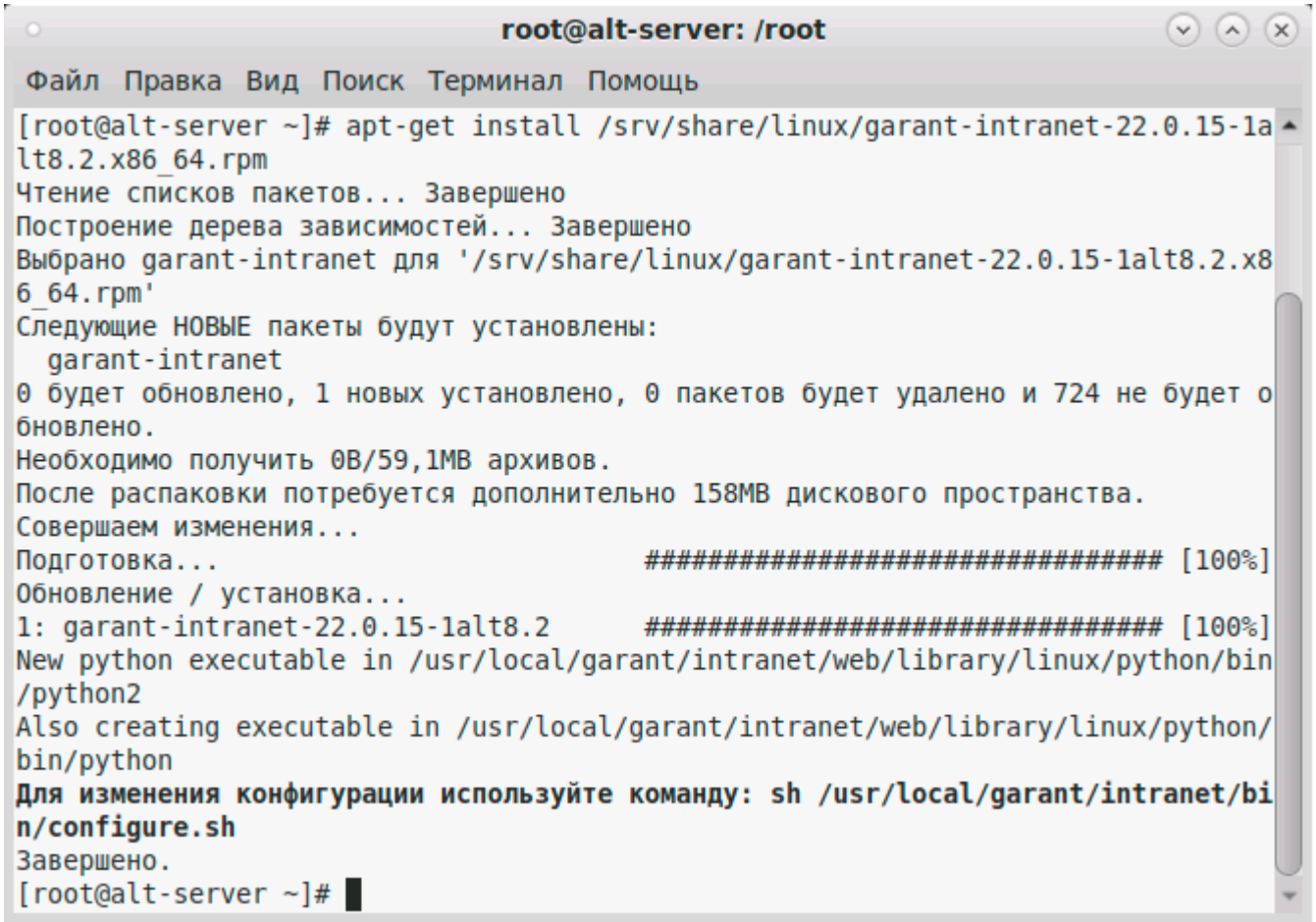
Для этого необходимо запустить «Терминал» и перейти в режим суперпользователя командой **su-** (минус на конце важен).



Шаг 2. Запускаем установку с помощью команды в терминале:

apt-get install /media/ALTLinux/garant/linux/*garant-intranet-xx.x-x-alt.rpm*

(путь необходимо указать к rpm пакету, в случае локальной установки пакет будет называться garant-desktop-xx.x-x-alt.rpm).



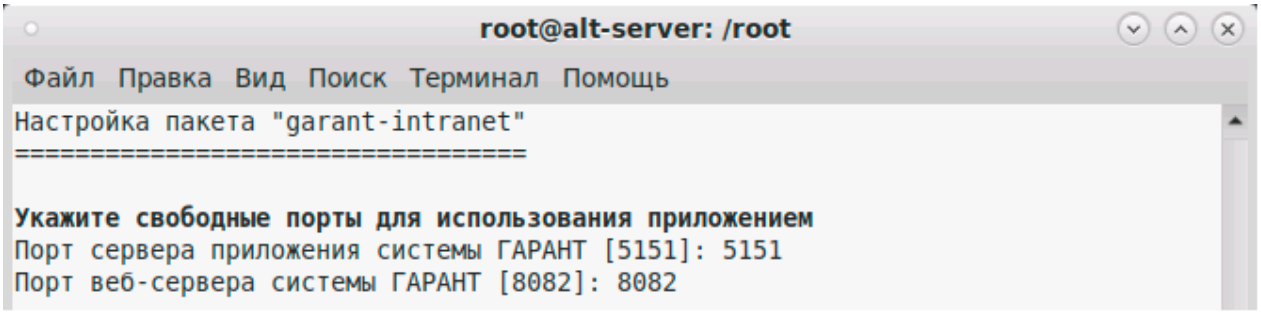
Шаг 3. Для настройки конфигурации установки используйте команду:

sh /usr/local/garant/intranet/bin/configure.sh

```
[root@alt-server ~]# sh /usr/local/garant/intranet/bin/configure.sh
```

Далее необходимо указать параметры установки:

- порт сервера **ГАРАНТ: 5151** (В квадратных скобках указана подсказка по умолчанию, если не планируется указывать какое-то другое значение, то указываем значение из квадратных скобок),
- порт Веб-сервера **ГАРАНТ 8082** (по умолчанию),



Если вы решите изменить порты по умолчанию, то выберите свободные порты, руководствуясь списком часто используемых портов (список портов можно посмотреть командой **cat /etc/services**).

- путь к папке, используемой для хранения данных ГАРАНТ:

  /usr/local/garant/intranet (по умолчанию), в ней при установке создадутся каталоги data1, data2, delta

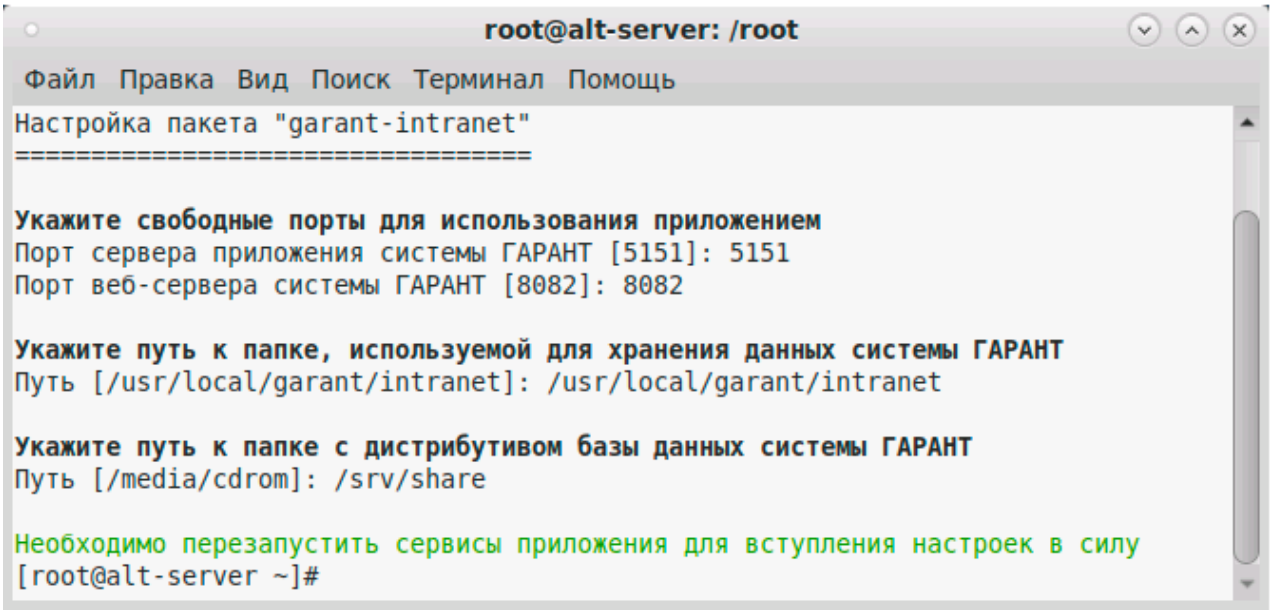
```
Укажите путь к папке, используемой для хранения данных системы ГАРАНТ
Путь [/usr/local/garant/intranet]: /usr/local/garant/intranet
```

Для локальной версии путь будет ***/usr/local/garant/desktop***

Указываем свой путь к папке с дистрибутивом базы данных ГАРАНТ (в данном примере дистрибутив находится в папке /srv/share/garant)

```
Укажите путь к папке с дистрибутивом базы данных системы ГАРАНТ
Путь [/media/cdrom]: /srv/share/garant
```

Важно! *Путь к папке с дистрибутивом базы данных должен быть указан в виде пути до каталога, в котором находится папка data..*



Обновление информационного банка системы

Шаг 5. После успешной установки оболочки ***garant-intranet*** необходимо выполнить установку базы данных ГАРАНТ ПРОКСИМА.

Для запуска установки базы данных ГАРАНТ ПРОКСИМА выполните команду:

sh /usr/local/garant/intranet/bin/datasetup

```
[root@alt-server ~]# sh /usr/local/garant/intranet/bin/datasetup
Mon Apr  4 2022 18:21:01.056603[3364, 140161045418176] -LM_DEBUG: LD_LIBRARY_PAT
H: /usr/local/garant/intranet/tools/../lib:/usr/local/lib:/usr/lib:/lib

Дистрибутив данных ищется в каталоге /srv/share, подождите...
```

Далее следуйте указаниям мастера установки базы данных. На вопрос о продолжении установки введите **n** или **Enter** для продолжения, или **q** для прекращения установки.

```
Дистрибутив: /srv/share/data/h9105129588

Будет установлен комплект, помеченный *: Проксима для ТЕСТОВ (СИМ)


[0 Для внутреннего пользования УВС]
 - * Проксима для ТЕСТОВ (СИМ)


 'n' или Enter - Установить, 'q' - Прекратить ...
```

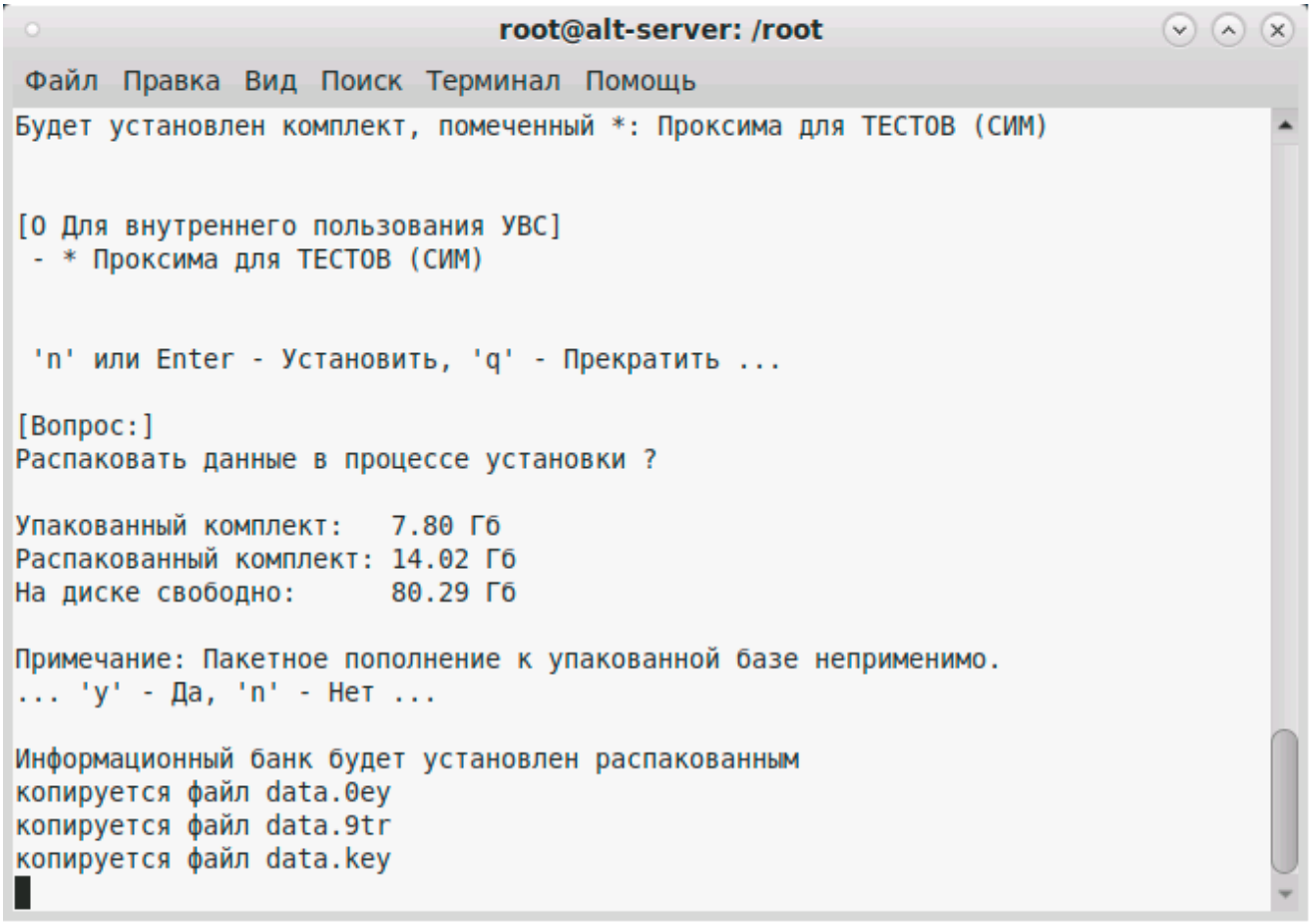
Система запросит пароль-отзыв, введите код ответа и нажмите «Enter».

Далее введите **y** или **n** для продолжения установки данных в упакованном или распакованном виде и нажмите **Enter** (распаковывать данные необходимо, если планируется обновление дельтой).

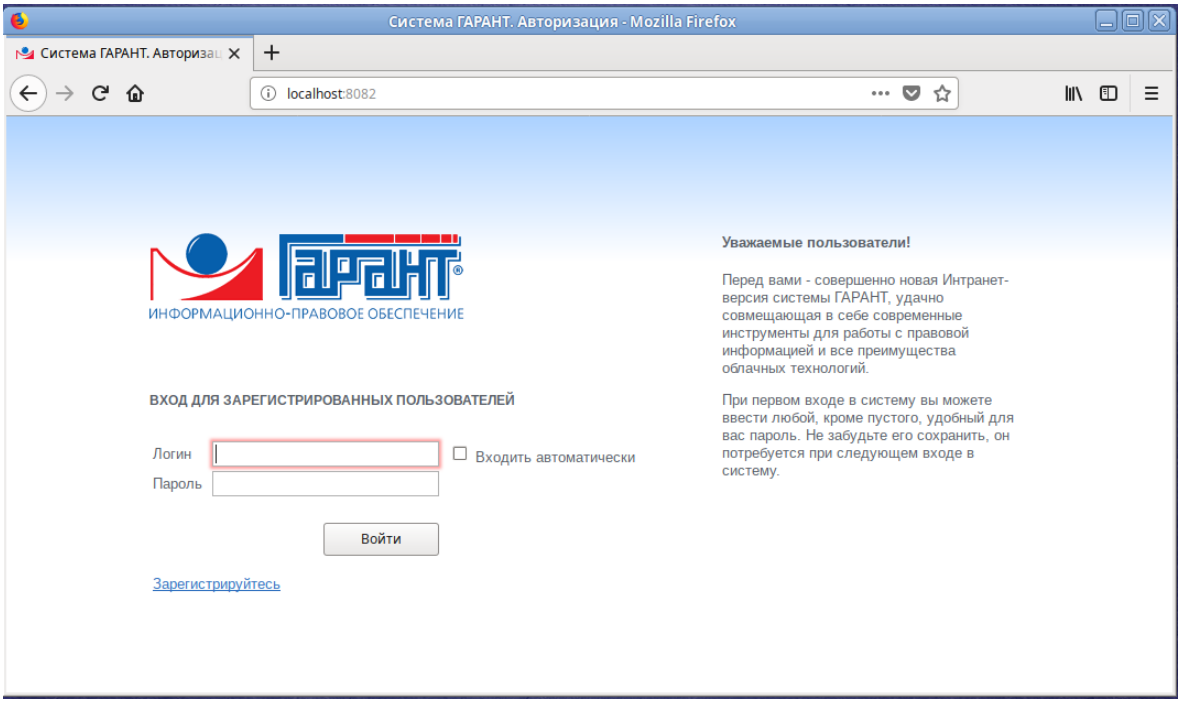
Важно! *Для успешной установки на диске должно быть достаточно свободного места*

```
[Вопрос:]
Распаковать данные в процессе установки ?

Упакованный комплект:   7.80 Гб
Распакованный комплект: 14.02 Гб
На диске свободно:      80.29 Гб

Примечание: Пакетное пополнение к упакованной базе неприменимо.
... 'y' - Да, 'n' - Нет ...
```

Дождитесь окончания установки базы данных. Время установки зависит от производительности ПК и размера базы данных. Процесс установки базы данных показан строчками копирования файлов базы.



Шаг 6. После завершения установки необходимо проверить работу системы ГАРАНТ ПРОКСИМА. Для этого необходимо запустить браузер и ввести в адресной строке **http://адрес_сервера:8082**



Администрирование учетных записей пользователей происходит в интерфейсе администратора ГАРАНТ ПРОКСИМА, для перехода в него необходимо ввести в адресной строке браузера **http://адрес_сервера:8082/admin** (Логин – ADMIN, пароль – ADMIN).

Пользователь может зарегистрироваться самостоятельно, нажав на странице приветствия «**Зарегистрируйтесь**» и введя требуемые учетные данные.

Настройка автоматического обновления через Интернет

Важно! *Для работы механизма обновления необходимо хотя бы раз запустить /usr/local/garant/intranet/bin/download в ручном режиме, поскольку системе необходимо зафиксировать логин/пароль для доступа к серверу пакетного пополнения (СПП) и комплект. После запуска введите логин и пароль от СПП, укажите номер комплекта в списке, затем подождите, пока сформируется и скачается дельта для комплекта (процесс занимает некоторое время).*

Для настройки автоматического обновления необходимо создать скрипт, в котором прописать выполнение необходимых утилит, и настроить его запуск в планировщике задач на заданное время. В приведенном ниже примере обновления будут скачиваться с сервера пакетного пополнения и применяться ежедневно в 2 часа ночи. Если требуется только скачивать или только применять обновления, то необходимо указать только соответствующую утилиту.

Пример настройки автоматического обновления:

1. Перейдите в режим суперпользователя командой su- и введите пароль.

2. Перейдите в каталог с установленным ГАРАНТом:

cd /usr/local/garant/intranet

3. Создайте скрипт:

vi garupd, где garupd - название скрипта.

4. Откроется текстовый редактор **vi**, в который необходимо вписать следующие строки (для этого надо перейти в режим редактирования, нажав на клавиатуре клавишу **i**, после этого вводить текст):

#!/bin/bash

/usr/local/garant/intranet/bin/download -auto -revision

/usr/local/garant/intranet/bin/dataupd

Сохраните введенное (для этого надо выйти из режима ввода текста клавишей **Esc**, далее набрать **:x** и нажать «Enter»).

5. Делаем файл исполняемым:

chmod +x garupd

6. Измените владельца этого файла:

chown ru-garant:ru-garant garupd

7. Настройте запуск по расписанию, для чего выполните команду:

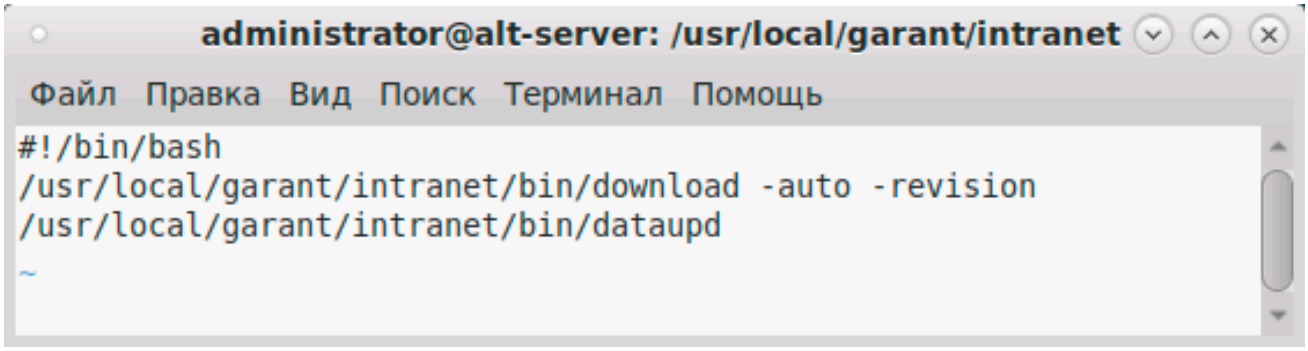
crontab -e

8. Откроется текстовый редактор планировщика задач cron, куда необходимо добавить следующую строку, для выполнения скрипта:

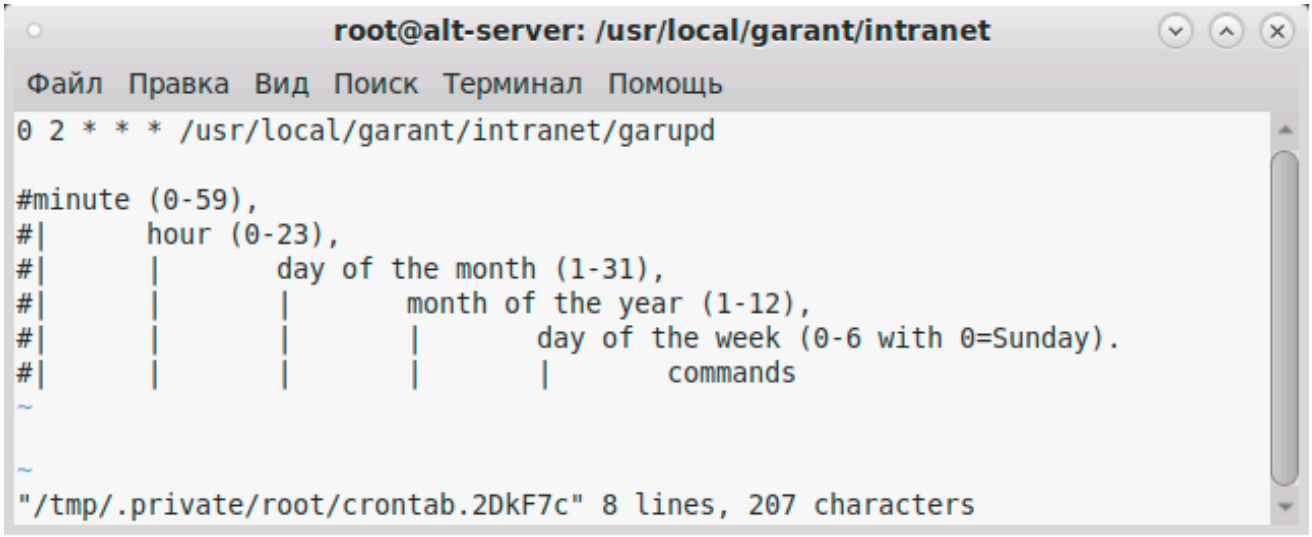
0 2 * * * /usr/local/garant/intranet/garupd

Получается, что скрипт запускается в 02:00 каждую ночь, каждого месяца, каждую неделю.

Пример скрипта:



Пример запуска скрипта через планировщик cron:



Редактор vi требует определенных навыков в работе, в связи с этим рекомендуется изучить основы работы с данным редактором (см. раздел «Приложение 1. КРАТКАЯ СПРАВКА ПО РАБОТЕ С ОС LINUX Текстовый редактор vi»).

После выхода из cron вы должны увидеть только строчку **crontab: installing new crontab**.

Если вы видите какие-то другие сообщения, значит возникли проблемы. Например, если появилось собщение: crontab: warning, cron does not appear to be running — это значит, что планировщик не запущен, его надо включить в автозагрузку и запустить командами:

systemctl enable crond

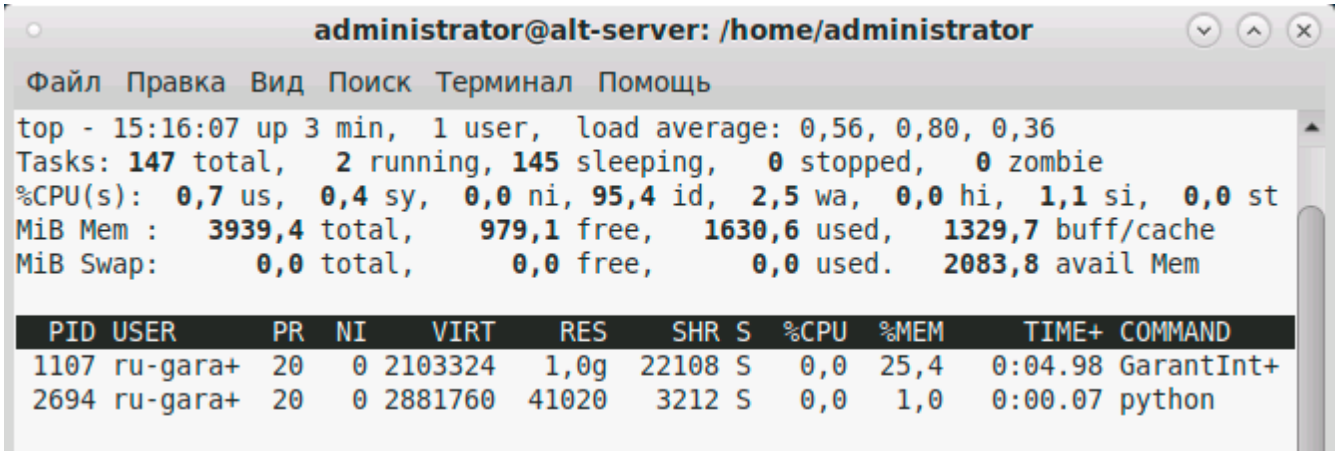
systemctl start crond

Важно! *Обратите внимание, cron требует обязательную пустую строку в конце файла или после всех записей планировщика.*

Службы ГАРАНТ ПРОКСИМА

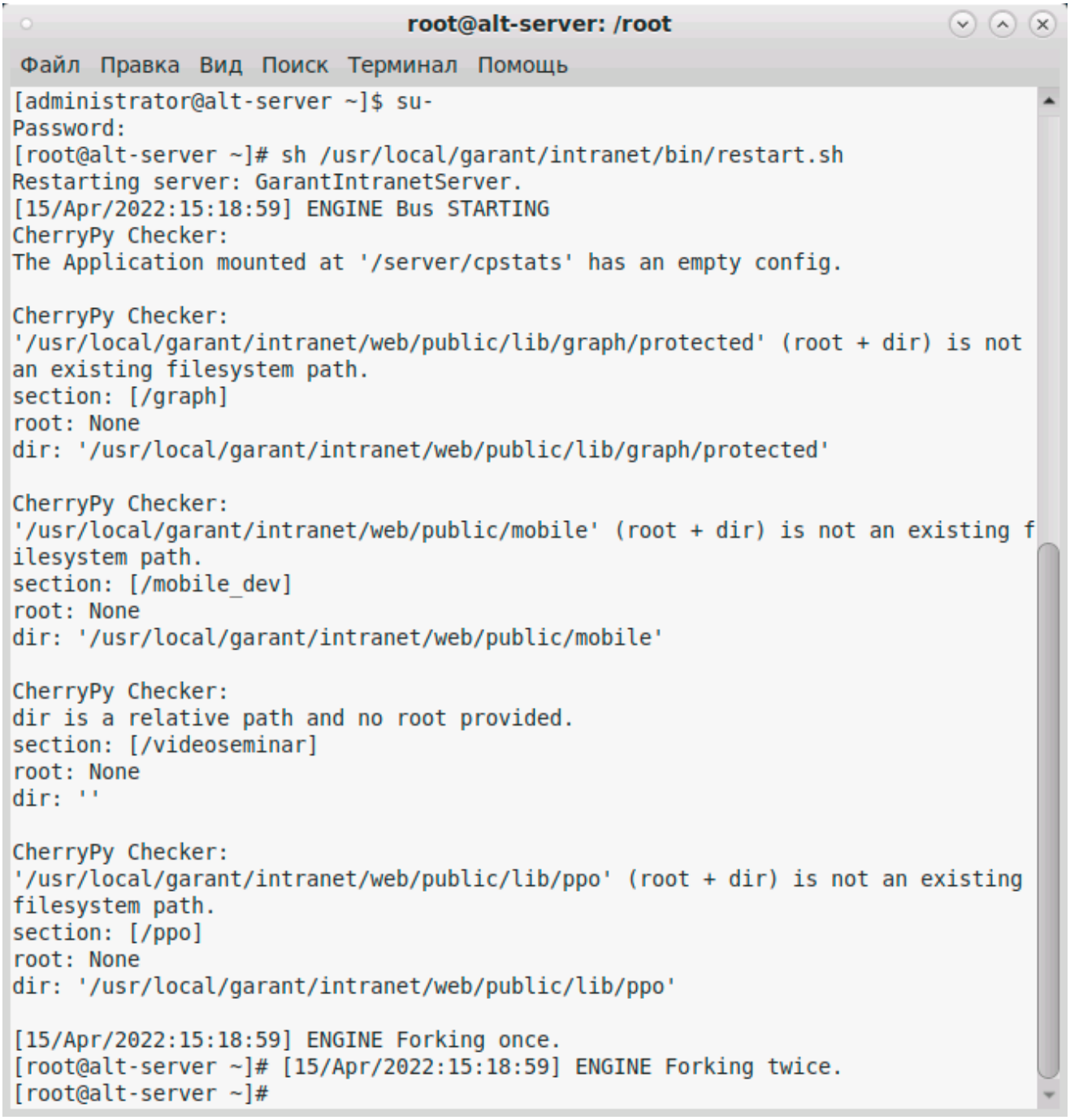
Для работы сетевой клиент-серверной версии ГАРАНТ ПРОКСИМА на сервере должны быть запущены два процесса: сервер приложений для работы с базами данных и веб-сервер для отображения интерфейса пользователя. Оба процесса запускаются от пользователя ru-garant.

Убедиться в их работе можно через диспетчер задач. Для этого в командной строке необходимо выполнить команду: **top -U ru-garant**. В результате выполнения команды вы увидите список процессов пользователя ru-garant:



Для одновременного перезапуска служб ГАРАНТ ПРОКСИМА необходимо запустить под правами суперпользователя следующий скрипт:

sh /usr/local/garant/intranet/bin/restart.sh

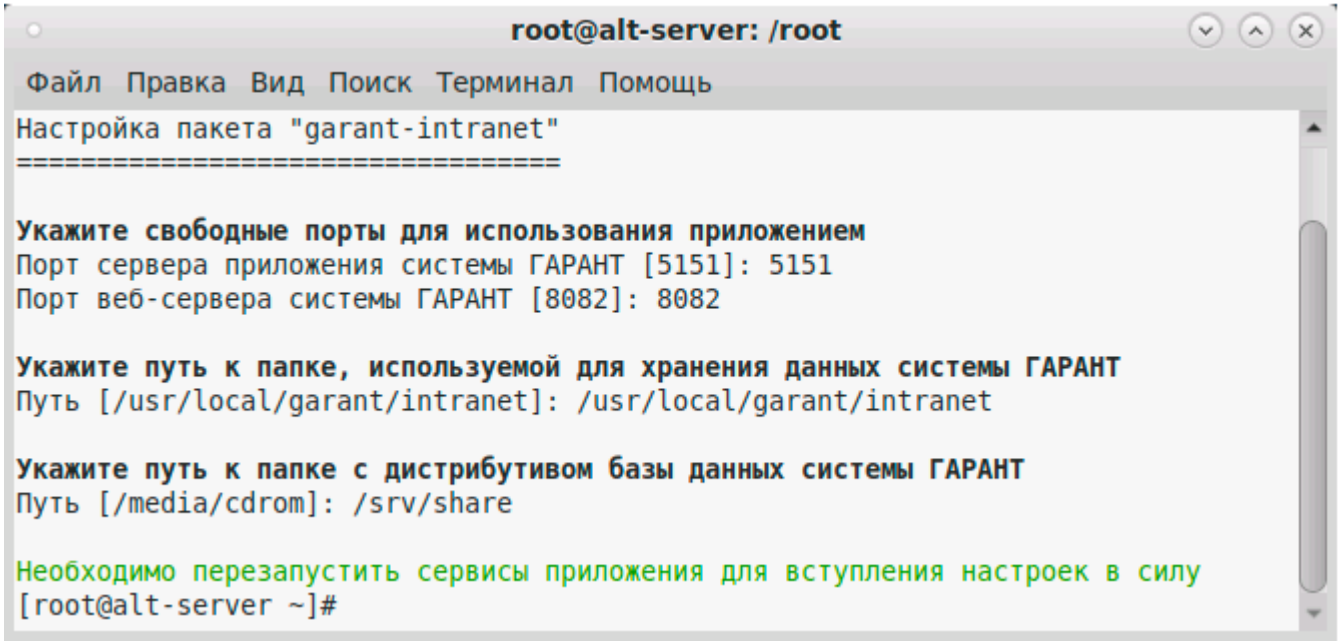


В локальной версии данные процессы появляются только при запуске ГАРАНТ ПРОКСИМА. При выходе из ГАРАНТ ПРОКСИМА процессы закрываются.

Изменение настроек установки

Для внесения изменений в настройки ГАРАНТ ПРОКСИМА выполните под правами суперпользователя команду в терминале (потребуется перезагрузка сервисов приложения):

sh /usr/local/garant/intranet/bin/configure.sh



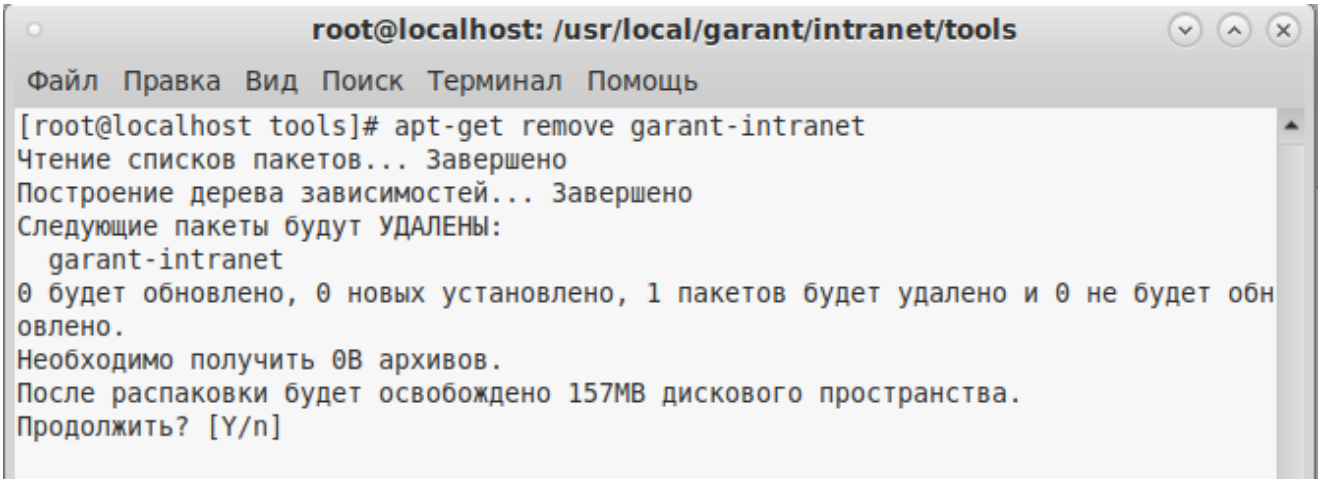
В результате выполнения данной команды на экране будут отображены окна настроек из Шага 3.

Удаление ГАРАНТ ПРОКСИМА

Для удаления ГАРАНТ ПРОКСИМА используйте команду в терминале с правами суперпользователя:

apt-get remove garant-intranet

Подтвердите удаление нажатием **Y** и «**ENTER»**.



По завершении удаления пакета **garant-intranet** удалите содержимое папки **garant**, которая находится в каталоге **/usr/local/garant**.

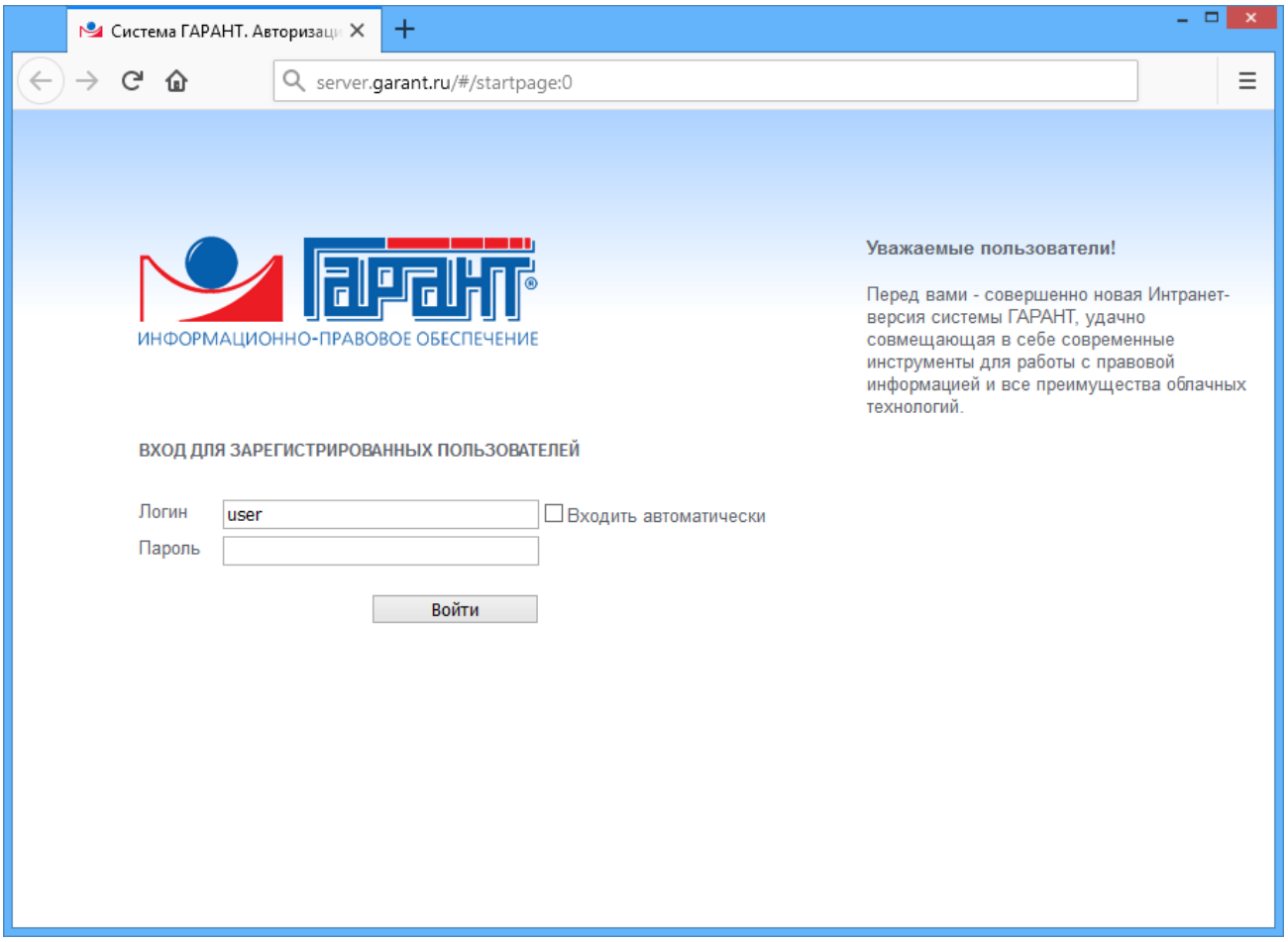
Для локальной версии команда будет следующая: **apt-get remove garant-desktop**

ЗАПУСК СИСТЕМЫ ГАРАНТ ПРОКСИМА.

Запуск системы ГАРАНТ ПРОКСИМА

Для ОС Windows запуск системы ГАРАНТ ПРОКСИМА осуществляется из меню Пуск «Перейти на главную страницу».

Также можно запустить систему из браузера. Для этого необходимо в адресной строке браузера ввести адрес сервера и порт веб-сервера. Например: http://server.garant.ru:80



В том случае, если ГАРАНТ ПРОКСИМА ставилась взамен ГАРАНТ Платформа F1, и при установке использовался механизм замены версии, то ранее созданные ярлыки на ГАРАНТ Платформа F1 также будут работать.

Альтернативный запуск на сервере возможен посредством выполнения файла **browse.cmd** (данный файл располагается в коре папки Garant Intranet и содержит необходимую минимальную информацию для запуска системы).

Для ОС Линукс запуск сетевой версии осуществляется переходом на адрес http://server.garant.ru:8082 через браузер.

Отключение онлайн-части

Система ГАРАНТ ПРОКСИМА в момент запуска проверяет наличие доступа в Интернет и, в случае если он есть, автоматически открывает в браузере актуальную обновляемую три раза в день версию системы ГАРАНТ в Интернете.

В случае, если Интернет отсутствует, открывается комплект, установленный на локальном компьютере либо в сети компании, с предупреждением о том, что работа идет в локальном комплекте.

Иногда бывает необходимо запустить ГАРАНТ ПРОКСИМА в оффлайн-режиме, несмотря на наличие Интернета. Это можно сделать двумя способами:

- отключить запуск онлайн-части для всех пользователей и навсегда,
- отключить онлайн-часть на время одной сессии и для конкретного пользователя.

Для того чтобы отключить онлайн-часть для всех пользователей и навсегда, необходимо в файл **%Garant Intranet%/config.py** добавить строчку **is_proxima_disabled=True** и перезапустить службы ГАРАНТа. После этого система ГАРАНТ будет работать только с оффлайн-частью информационного банка. Мы рекомендуем включать данный режим только при крайней необходимости, так как в данном случае актуальность информационного банка будет «отставать» от онлайн-части и требовать установки полного информационного банка на сервере компании. При включенной онлайн-части можно устанавливать в оффлайн-часть меньший по объему информационный банк, а полным пользоваться в онлайн-части.

Для того чтобы временно отключить онлайн-часть для конкретного пользователя, ему необходимо при запуске ГАРАНТ ПРОКСИМА в адресной строке браузера после имени сервера добавить **/noproxima** (можно сразу создать ярлык с адресом http://server.garant.ru/noproxima), тогда система откроет оффлайн-часть комплекта.

СИСТЕМА АДМИНИСТРИРОВАНИЯ ПОЛЬЗОВАТЕЛЕЙ.

Система Администрирования – это специальный интерфейс администратора, позволяющий централизованно (без привлечения пользователей и использования их персональных компьютеров):

- создавать, удалять, редактировать учетные записи пользователей,
- отключать пользователей от работы,
- запрещать самостоятельную регистрацию пользователей,
- создавать группы пользователей,
- предоставлять возможность работы с информационными блоками комплекта ЭПС «Система ГАРАНТ»,
- выбрать способ идентификации пользователя, в том числе под именем учетной записи Windows или Linux (возможность автоматической регистрации пользователя без необходимости введения пользователем данных в регистрационную форму) при первом входе в ЭПС «Система ГАРАНТ» с присвоением логина, совпадающего с логином этого пользователя в операционной системе,
- интегрировать систему с Active Directory и другими службами каталогов под учётными данными пользователя LDAP-каталога, под учётными данными пользователя keycloak.

Переход в систему Администрирования учетных записей

Переход в систему Администрирования учетных записей осуществляется из меню «Пуск» / «Перейти на страницу администратора» или непосредственно в браузере, для чего необходимо ввести адрес сервера, порт веб-сервера и текст **/admin**.

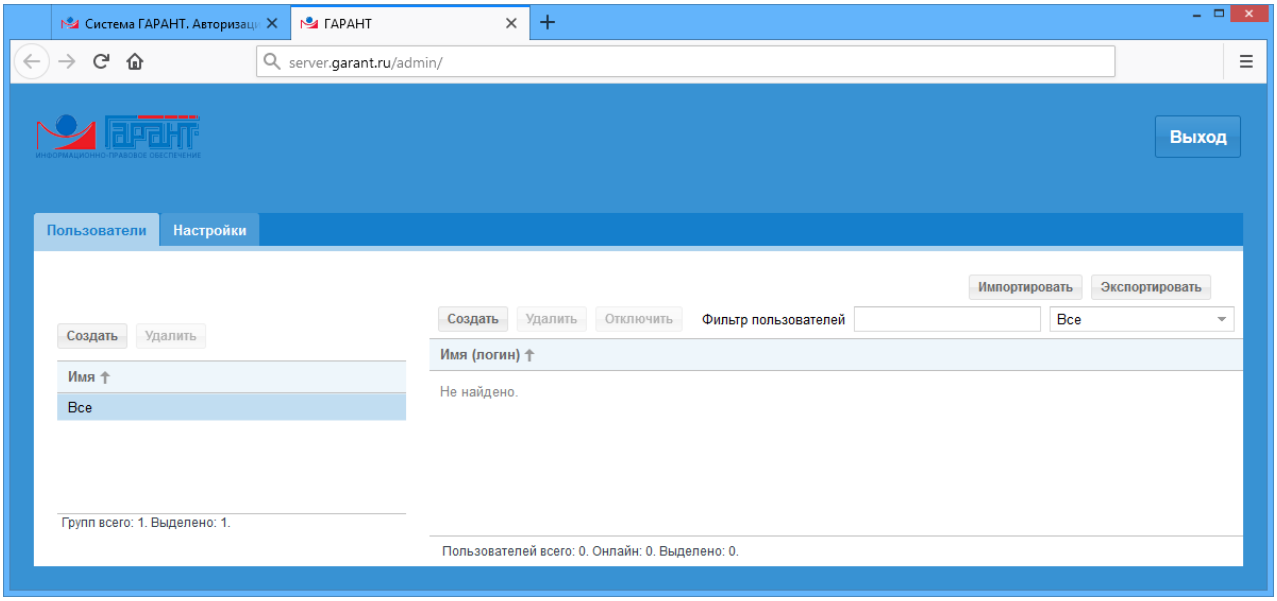
Например: **http://server.garant.ru:80/admin/**

Альтернативный вариант запуска системы Администрирования можно осуществлять при помощи запуска файла **browse_admin.cmd**, который находится в корне папки Garant Intranet.

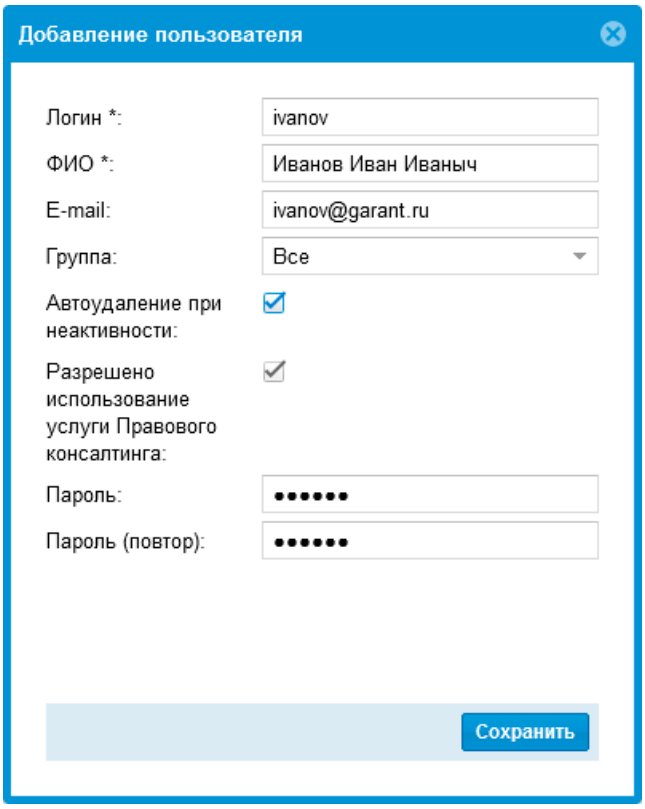
Логин и пароль для доступа к Администрированию учетных записей – **ADMIN/ADMIN**.

Создание пользователей

Для работы многих важных функций системы ГАРАНТ необходима авторизация пользователей в системе. Добавление новых пользователей возможно в ручном и автоматическом режиме.



Для добавления нового пользователя в ручном режиме нажмите кнопку «Создать», заполните все необходимые поля и подтвердите, нажав «Сохранить».



Импорт пользователей

Кроме самостоятельной регистрации пользователей существует еще один способ добавления, удаления и редактирования учетных записей пользователей – операция пакетного импорта пользователей из файла специального формата. Для этого в интерфейсе администратора есть кнопки «Импортировать» и «Экспортировать».

Файл для импорта должен соответствовать формату csv, кодировка файла – utf-8.

Для получения файла в нужной кодировке (utf-8) воспользуйтесь одним из вариантов:

- Если для формирования списка пользователей вы используете программу Calc из пакета OpenOffice или LibraOffice, то при сохранении в csv программа позволяет выбрать кодировку, – вам нужно выбрать utf-8.

- Если вы используете Excel или другой редактор текстовых документов, то после сохранения в файл вам нужно открыть его в программе Блокнот из стандартной поставки ОС Windows, выбрать «Сохранить как» и в появившемся окне внизу в поле «Кодировка» указать utf-8.

Создайте хотя бы одного пользователя в системе вручную и нажмите кнопку «Экспортировать», – сохраненный файл будет в нужной кодировке.

Допустимые в файле разделители:

«;» (точка с запятой)

«,» (запятая)

«|» (вертикальная черта)

«(0x09)» (символ табуляции)

Использование разных разделителей в одном файле не допускается, выбранный (первый упомянутый с начала файла) разделитель не может быть использован в значениях параметров.

Список и порядок полей:

Действие	Логин	Фамилия	Имя	Отчество	Пароль	Консалтинг	Email	Группа	Автоудаление
+	ivanov	Иванов	Иван	Иванович	pass	0	ivanov@garant.ru	Все	1
=	petrov	Петров	Петр	Петрович	pass	0	petrov@garant.ru	Группа 1	1
-	sidorov	Сидоров	Иван	Сидорович	pass	0	ivanov@garant.ru	Группа 2	1

<Действие> – тип действия, производимого с пользователем:

«+» – добавление пользователя (по умолчанию),

«=» – изменение данных пользователя,

«-» – удаление пользователя.

<Логин> – логин пользователя (обязательное и уникальное поле).

<Фамилия> – фамилия пользователя, max 85 знаков (обязательное поле).

<Имя> – имя пользователя, max 85 знаков (опциональное поле).

<Отчество> – отчество пользователя, max 85 знаков (опциональное поле).

<Пароль> – пароль пользователя (опциональное поле).

<Консалтинг> – параметр, позволяющий дать доступ пользователю к Правовому консалтингу.

<Email> – адрес электронной почты пользователя (опциональное поле).

<Группа> – группа пользователя (опциональное поле).

<Автоудаление> – параметр отвечает за автоматическое удаление пользователя при неактивности (0 – нет, 1 – да) (опциональное поле).

Если при добавлении («+») пользователя такая запись уже существует в системе, то она полностью перезаписывается данными из файла (включая пустые поля). В статистике это учитывается как изменение.

При изменении («=») данных пользователя все поля, указанные в файле, будут переписаны поверх имеющихся, а все поля, значения которых не будут указаны, не поменяют своего состояния.

Если явно указано «изменить» («=»), а пользователя с таким логином нет в системе, такой пользователь добавляется. В статистике это учитывается, как добавление.

Если явно указано «удалить» («-»), а пользователя с таким логином нет в системе, то строка игнорируется.

Если для одного логина во входном файле задано больше одной операции, все такие записи игнорируются. Если строка не удовлетворяет формату (не все обязательные поля указаны, есть лишние столбцы, значения полей содержат неверные типы или превышают ограничения), то строка игнорируется.

Пример рабочей строки в файле импорта пользователей:

+;test_user;Иванов;Иван;Иванович;pass;0;test_user@garant.ru;Все;0;

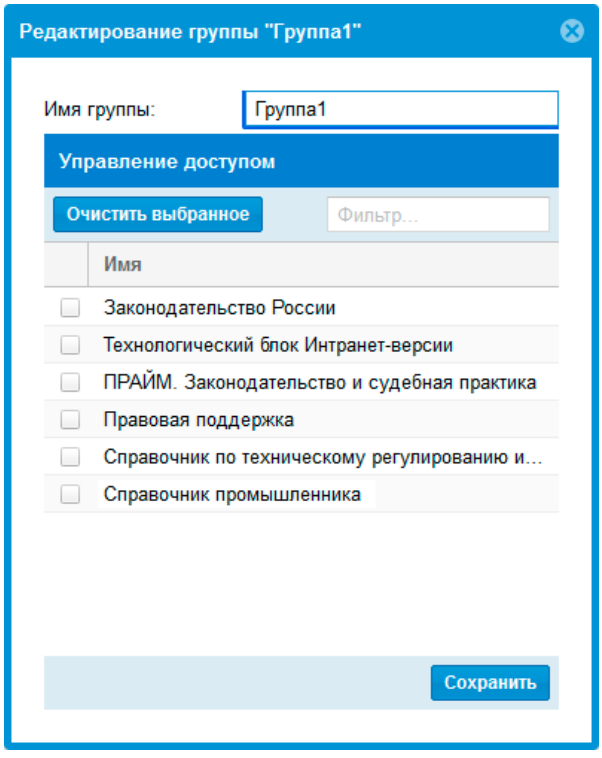
Экспорт пользователей

Экспорт пользователей происходит по нажатию кнопки «Экспортировать» в интерфейсе администратора. Экспорт пользователей происходит в файл users.csv.

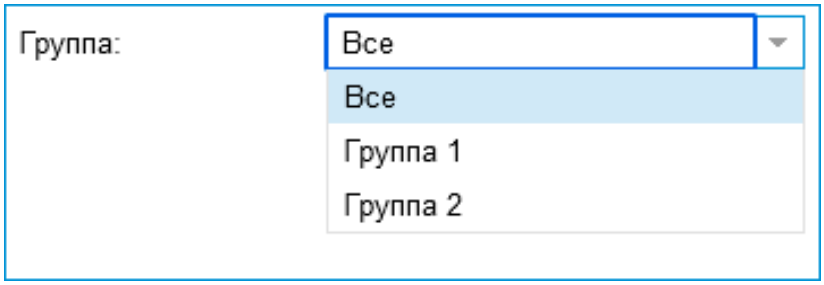
Ограничение доступа к информационным блокам

Существует возможность уменьшать состав комплекта для отдельных пользователей. Эта возможность может быть использована в случае, если документы, принадлежащие к определенным информационным блокам, входящим в состав установленного комплекта, не интересны этому пользователю (например, региональные документы) или считаются по каким-то причинам недопустимыми для просмотра этим пользователем. В результате включения ограничения из списков, полученных любым поиском, будут исключены документы, содержащиеся только в запрещенных блоках (если документ принадлежит как запрещенным, так и разрешенным блокам, он будет по-прежнему доступен пользователю). Перейти на документы, содержащиеся только в запрещенных блоках, по ссылке из других документов будет также невозможно.

Для включения ограничения видимых пользователю баз нужно зайти в интерфейс Администратора. В Администраторе пользователей нужно создать (или выбрать имеющуюся) группу пользователей, двойным нажатием по группе открыть окно редактирования группы, где отметить блоки, которые мы хотим сделать невидимыми для выбранной группы пользователей, и нажать кнопку «Сохранить».

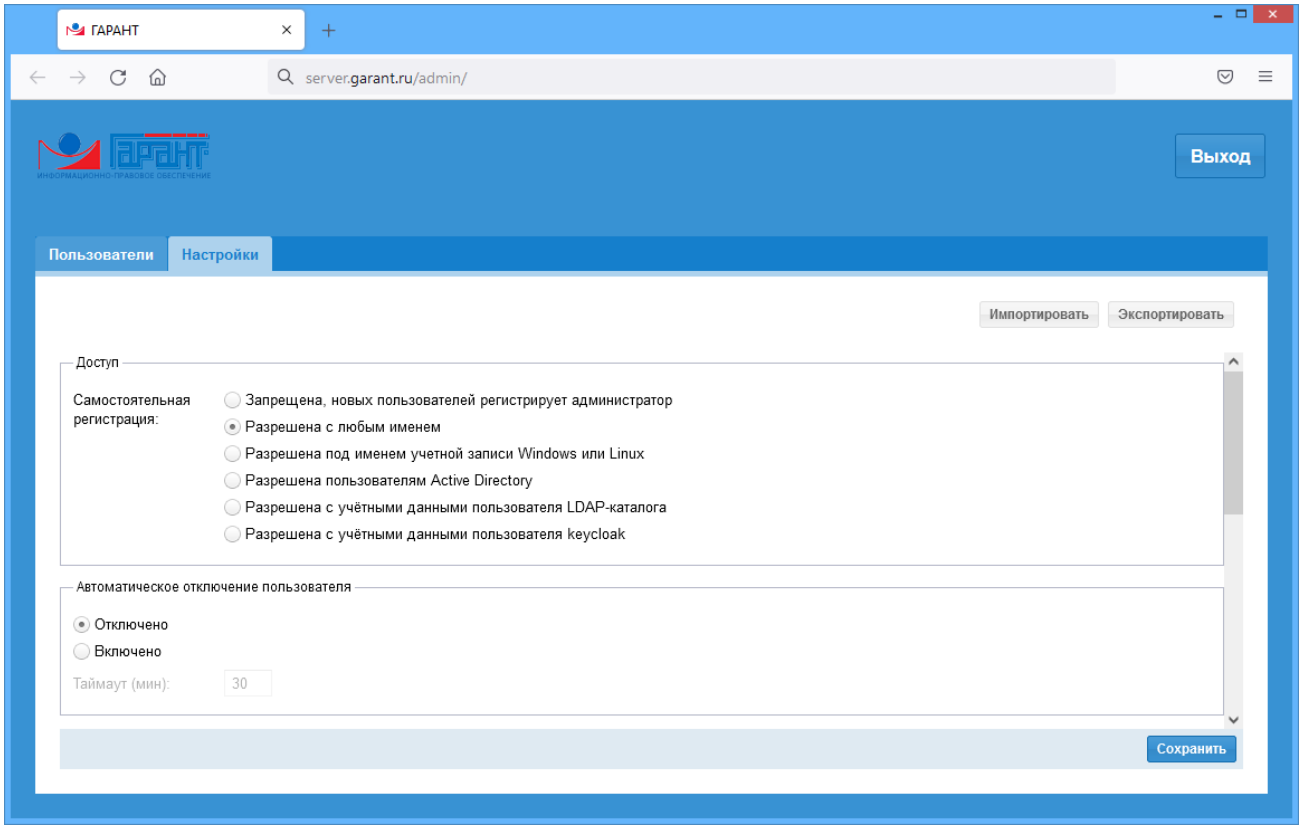


Для того чтобы поместить пользователя в требуемую группу, нужно два раза нажать на пользователя и выбрать группу, к которой он будет принадлежать. В списке всех пользователей с помощью специального фильтра «Не сгруппированные» можно посмотреть пользователей, которые еще не были присоединены к какой-либо группе. Для массового изменения пользователей рекомендуется воспользоваться механизмом «Экспорт/Импорт пользователей».



Способы авторизации

Выбор способа авторизации в системе осуществляется на вкладке «Настройки» в интерфейсе администратора:



Система предусматривает различные возможности регистрации пользователей:

- Пользователей может регистрировать только Администратор.

  В разделе «Доступ» необходимо выбрать пункт «Запрещена, новых пользователей регистрирует администратор».

  В этом случае работать с системой смогут только пользователи, зарегистрированные администратором системы вручную или импортированные описанным выше способом. Пользователи смогут зайти в систему только при наличии у них пары логин/пароль (пароль может быть пустым).

- Пользователи регистрируются сами.

  В разделе «Доступ» необходимо выбрать пункт «Разрешена с любым именем».

  Процедура регистрации максимально упрощена для того, чтобы пользователи прошли ее самостоятельно. При обращении к системе будет отображаться форма авторизации и ссылка «Зарегистрироваться», при нажатии на которую отобразится дополнительная форма регистрации нового пользователя. В ней требуется ввести логин, пароль, имя пользователя, его электронную почту (не обязательно) и нажать кнопку «Начать работу». После этого откроется интерфейс системы. В

дальнейшем, при вводе логина и пароля рекомендуется поставить галочку «Входить автоматически», - это позволит не вводить каждый раз пароль при входе.

- Автоматический вход под учетной записью Windows или Linux.

  В разделе «Доступ» необходимо выбрать пункт «Разрешена под именем учетной записи Windows или Linux».

  Пользователи могут проходить автоматическую регистрацию в системе под именем учетной записи Windows. Для этого необходимо в интерфейсе Администратора включить данный функционал:

  Пользователи смогут автоматически регистрироваться в системе по запуску скрипта logon.wsf (скрипт расположен в корне папки Garant Intranet). Данный скрипт является Windows Script File, который определяет логин пользователя в Windows при помощи функции wshNetwork.userName, запускает браузер по умолчанию и передает адресной строке специальный url, где содержится адрес сервера с Системой ГАРАНТ и имя пользователя. Рекомендуется разместить данный скрипт на общем сетевом ресурсе, а пользователям вывести ярлыки на этот скрипт. При этом иконку для ярлыка можно скачать по ссылке https://disk.yandex.ru/d/MhSjN64ohc-Khw (иконку тоже необходимо разместить на общем сетевом ресурсе). Данный способ можно использовать на внутреннем портале компании, если есть возможность уникально идентифицировать каждого пользователя. В этом случае для каждого пользователя необходимо формировать уникальную ссылку, в которой будет содержаться уникальное имя пользователя на портале.

  Пример url находится в самом скрипте logon.wsf. В ближайшей сборке в папке support можно взять исполняемый файл, который будет запускать браузер по умолчанию и регистрировать пользователя, если его еще нет.

  Для использования данного способа регистрации пользователей на Linux-системах есть свой sh-скрипт, который так же определяет имя пользователя в Linux и подставляет его в url. Скрипт находится в папке support.

- Интеграция с Active Directory.

  В разделе «Доступ» необходимо выбрать пункт «Интеграция с Active Directory (Windows)».

  Перед включением данной интеграции необходимо определиться, нужно ли кому-то ограничивать доступ к системе ГАРАНТ или части информационных блоков (как описывалось выше) или необходимо пускать всех, кто есть в домене.

  Если необходимо пускать в систему ГАРАНТ всех, кто есть в домене, то для настройки автоматического входа в систему необходимо:

  1. Включить опцию «разрешена пользователям Active Directory» в интерфейсе администратора и нажать «Сохранить». При этом поле «Organization unit» должно быть пустым.

  2. Настроить браузеры пользователей на передачу имени пользователя через групповые политики Active Directory (см. ниже).

  После применения данных настроек и групповых политик система ГАРАНТ будет пускать всех пользователей, которые есть в Active Directory.

  Важно! *Обращаться к системе ГАРАНТ необходимо по полному доменному имени! Если ярлык (закладка) будет вести на короткое имя или IP-адрес, то система пользователя не пустит.*

  Примечание: на самом сервере, где установлена ГАРАНТ ПРОКСИМА, при включении интеграции с Active Directory в систему ГАРАНТ не пустит (только в панель Администратора), для проверки работоспособности нужно использовать любую рабочую станцию в домене.

В случае, если необходимо ограничить доступ к системе ГАРАНТ (например, доступ дать только юристам и бухгалтерам) или к части информационных блоков (например, скрыть часть региональных блоков), то настраиваем все так же, но в поле «Organization unit» необходимо указать путь к OU, в котором будут группы пользователей, которым можно настроить доступ к информации.

В Active Directory администратор создает Organization unit - Garant, в которой он может заводить группы пользователей (например, юристы, кадры, бухгалтерия и т.д.), куда и помещает соответствующих пользователей (список групп внутри OU может быть только одноуровневым). В интерфейсе администратора ГАРАНТ ПРОКСИМА в поле Organization unit необходимо указать путь этому OU. Если Organization unit Garant создано в корне домена, то в системе ГАРАНТ поле будет выглядеть следующим образом OU=Garant. Если Organization unit Garant создается внутри дерева домена, то в поле Organization unit необходимо указать полный путь, например, OU=Garant,OU=Other,OU=Service. В нашем примере Organization unit Service будет располагаться в корне домена, то есть путь указывается справа налево. Если в Active Directory используется лес доменов, то данный путь должен быть одинаковым для всех доменов, и в таком случае администратор каждого домена сможет управлять своим списком групп пользователей, кому будет разрешен доступ к ГАРАНТу.

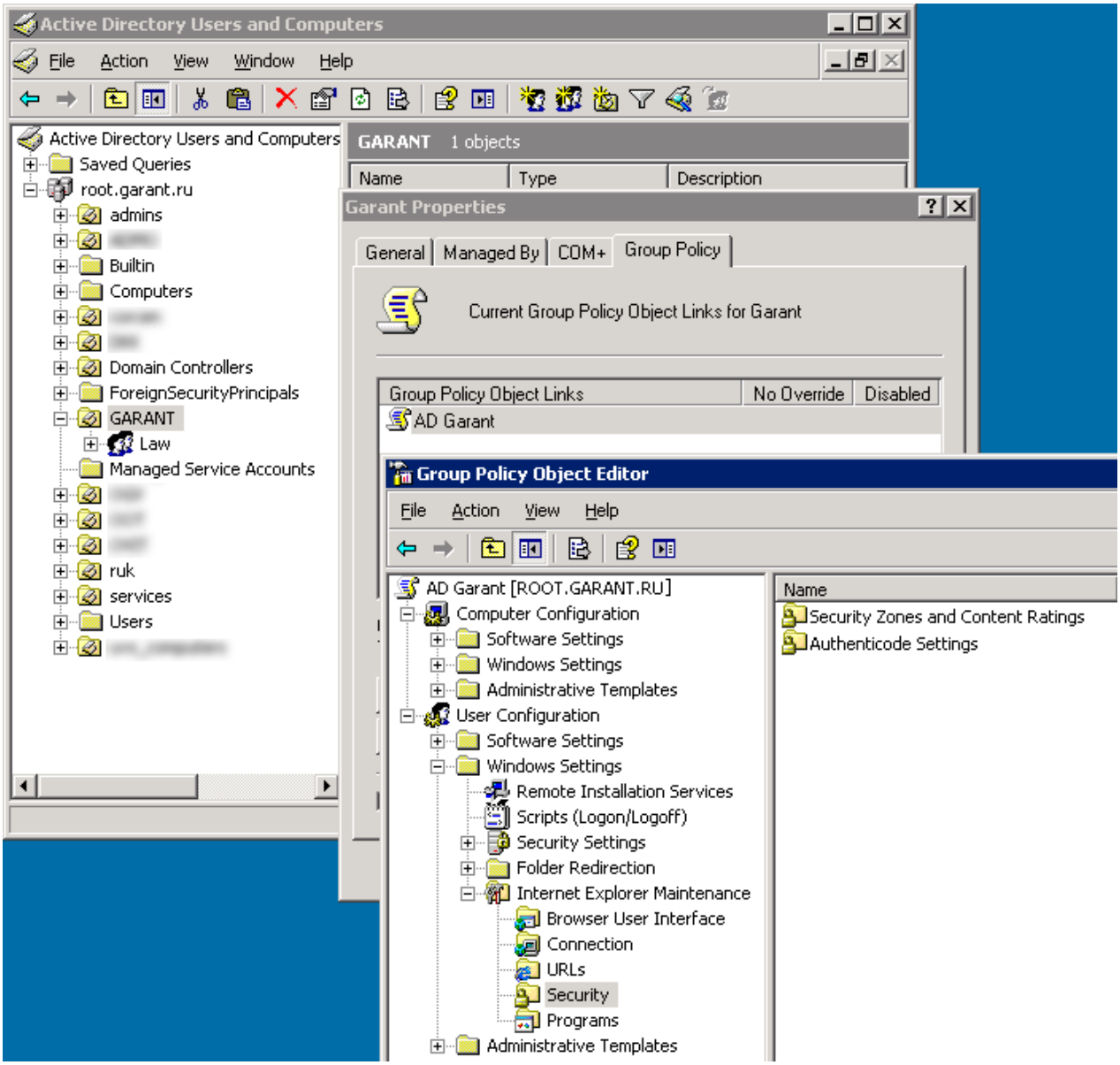
После того, как пользователь, принадлежащий к той или иной группе в Active Directory, зайдет в систему ГАРАНТ, в панели Администратора ГАРАНТ ПРОКСИМА появится группа с таким же именем, которой можно настроить доступ к информационным блокам, способом, описанным ранее. Если пользователь не входит ни в одну из групп в OU=Garant, и при этом в панели Администратора поле Organization unit заполнено, то такой пользователь в систему войти не сможет. Данный способ используется, если надо дать доступ в ГАРАНТ только определенным группам пользователей. В большинстве случаев поле Organization unit необходимо оставлять пустым, и тогда система будет пускать всех пользователей, заведенных в Active Directory.

Для настройки браузеров пользователей необходимо использовать групповые политики Active Directory:

- для IE на серверах до Windows Server 2012:

1. Создаём GPO для Organisation Unit GARANT

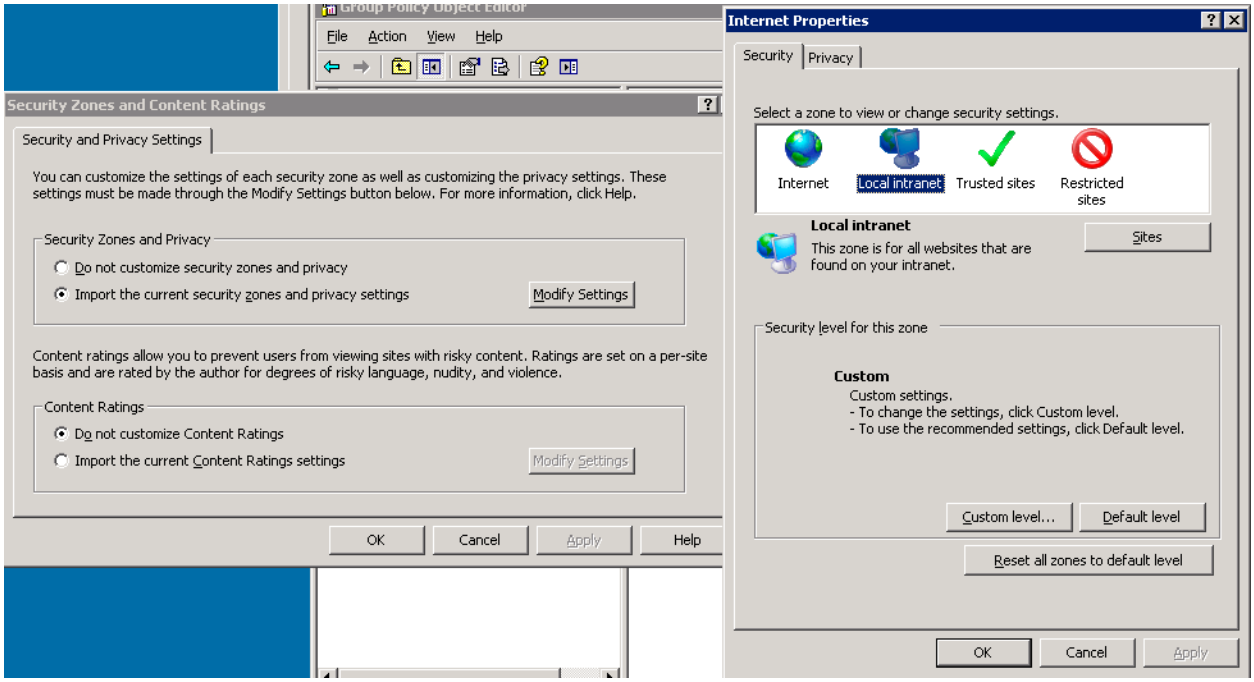
В ней: User Configuration — Windows Settings — Internet Explorer Maintance — Security — Security Zones and Content Ratings



2. Меняем Security Zones and Privacy на Import the current security zones and privacy settings

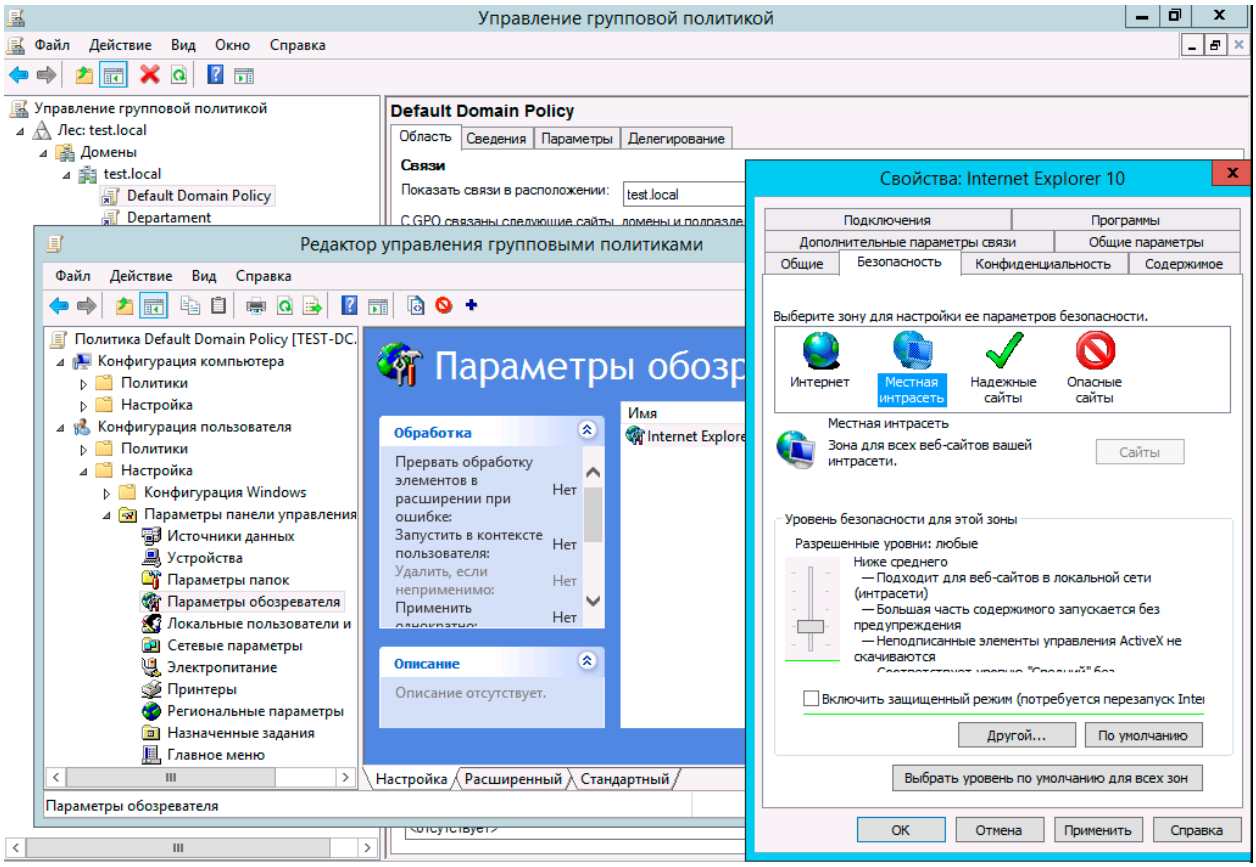
В ней: Modify Settings — Local Intranet — Sites — Добавляем путь к серверу с интранетом

Custom level — user Authentication — Logon — Automatic logon only in Intranet Zones/ Automatic logon with current user name and password (либо/либо)



3. В завершении необходимо выполнить команду ***gpupdate /force*** либо перезагрузить ПК.

Для серверов начиная с Windows Server 2012 настройка IE находится немного в другом месте.



- для Mozilla

1. Создаём файл all-settings.js со следующим содержимым:

pref("general.config.obscure_value", 0);

pref("general.config.filename", "mozilla.cfg");

2. Создаём файл mozilla.cfg со следующим содержимым:

//

pref("network.negotiate-auth.trusted-uris","*.garant.ru");

pref("network.negotiate-auth.delegation-uris","*.garant.ru");

где *.garant.ru имя сервера Интранет. При этом замечено, что в последних версиях Firefox "*.garant.ru" не работает, необходимо указывать полный путь к серверу в домене.

> ***Важно!*** *Настройки берутся со второй строки в этом файле, из-за чего в первой строке стоят два слеша.*

3. Помещаем эти файлы в сетевую папку, видимую для всех пользователей домена. Например, в \\%DomainName%\NETLOGON

4. В AD создаём политику для ПК. Конфигурация компьютера — Настройка — Конфигурация Windows – Файлы.

Далее создать — файл.

Во вкладке «общие»:

Действие — создать

Исходный файл — \\%путь_к_файлу%\all-settings.js

(Например: \\dc\netlogon\all-settings.js)

Конечный файл — %Путь_на_ПК_к_папке_Mozilla_Firefox%\defailts\pref\all-settings.js

(Например: C:\Program Files\Mozilla Firefox\defaults\pref\all-settings.js)

Ещё раз создать — файл.

Во вкладке «общие»:

Действие — создать

Исходный файл — \\%путь_к_файлу%\mozilla.cfg

(Например: \\uvs-dc\netlogon\mozilla.cfg)

Конечный файл — %Путь_на_ПК_к_папке_Mozilla_Firefox%\mozilla.cfg

(Например: C:\Program Files\Mozilla Firefox\mozilla.cfg)

После требуется перезагрузка клиентского ПК, либо выполнение команды **gpupdate /force**.

- Интеграция с LDAP-протоколом.

  В разделе «Доступ» необходимо выбрать пункт «Разрешена с учётными данными пользователя LDAP-каталога» (позволяет также интегрироваться со службами каталогов в Linux системах).

  При выборе варианта входа в Интранет-версию под учетными данными пользователей из LDAP-каталога необходимо зарегистрировать один или несколько LDAP-серверов. Параметры сервера (все обязательные):

  - «Сервер» - здесь необходимо указать IP-адрес сервера или его доменное имя. В IP-адрес можно добавить порт после двоеточия. Например: 192.168.56.103:8082.

  - «Домен» - домен, в котором находятся пользователи. Например: garant.ru.

  - «OU» - корень дерева каталогов LDAP (base DN), в котором расположены пользователи с необходимостью доступа в Интранет-версию. Например: CN=User или OU=Garant. Обратите внимание, что это не полное DN-имя - из полного удалены данные о домене, который задается в поле выше.

  После настройки LDAP-сервера пользователи могут входить в Интранет-версию под своими учетными данными в LDAP-каталоге. Для этого на форме авторизации необходимо ввести свой логин, пароль и указать домен. Если домен не указывать, то будет задействована функция Автопоиска, которая в момент входа

последовательно опрашивает все зарегистрированные LDAP-каталоги на предмет нахождения в них пользователя с заданным логином.

- Интеграция с протоколом OAuth 2.0

  OAuth 2.0 — протокол авторизации, позволяющий выдавать одному сервису права на доступ к различным ресурсам (в нашем случае системе ГАРАНТ ПРОКСИМА). Таким образом, залогинившись один раз на портале организации, система ГАРАНТ ПРОКСИМА может "узнавать" данного пользователя и пускать в систему ГАРАНТ ПРОКСИМА без дополнительной авторизации. На деле, реализация данного протокола у всех производится по-разному, и возможность интеграции со всеми системами не гарантируется или потребует доработки механизма авторизации со стороны клиента. В тоже время, в системе ГАРАНТ ПРОКСИМА заложена возможность интеграции с данным протоколом, что может позволить пользоваться системой ГАРАНТ ПРОКСИМА без дополнительной регистрации пользователей и их администрирования.

ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

Настройки пользователей

Каждый пользователь может настраивать систему под себя, например, устанавливать профессиональную страницу, может создавать закладки, устанавливать документы на контроле и т.д. Все пользовательские настройки системы ГАРАНТ хранятся на сервере в каталоге **%Garant Intranet%\settings**.

Восстановление настроек пользователей

В системе ГАРАНТ ПРОКСИМА предусмотрен механизм резервного копирования пользовательских настроек. Данный механизм запускается сервером приложений при его старте и создает Backup в виде полной бинарной копии.

Backup'ы складываются в каталог, заданный с помощью опции -BinaryBackupPath секции [F1Server Params] (по умолчанию %Garant Intranet%\settings-backup), в tar gzip архивы с именем файла формата — settings-YYYYMMDD.tar.gz, где YYYYMMDD - дата его создания.

Включение/выключение механизма резервного копирования осуществляется с помощью опции -BinaryBackupEnable в секции [F1Server Params] (ненулевое значение указывает, что необходимо осуществлять резервное копирование). Значение по умолчанию — 1.

Для восстановления настроек из резервной копии необходимо:

1. Выбрать архив с соответствующей датой и распаковать его до структуры папок настроек.
2. Остановить службы ГАРАНТ ПРОКСИМА.
3. Очистить папку settings и скопировать в нее такую же структуру папок из архива.
4. Запустить службы ГАРАНТ ПРОКСИМА.

Для «обнуления» настроек пользователей необходимо:

1. Остановить службы ГАРАНТ ПРОКСИМА.
2. Очистить папку settings.
3. Запустить службы ГАРАНТ ПРОКСИМА.

После запуска служб, сервер приложений создаст «чистые» настройки.

Конвертация настроек из системы ГАРАНТ Платформа F1

Конвертация настроек пользователей системы ГАРАНТ Платформа F1 может быть произведена автоматически при установке системы ГАРАНТ ПРОКСИМА (при выборе соответствующей опции). Для переноса настроек пользователей «вручную» используется утилита **Garant Intranet\settings\F1MigrateSettings.exe**. Конвертация настроек возможна только на ПК с ОС Windows, при этом получившиеся настройки можно использовать в ГАРАНТ ПРОКСИМА для любой ОС.

Важно! *Служба GARANT.Application.Server Платформы F1, а также службы ГАРАНТ ПРОКСИМЫ, во время конвертации настроек, должны быть остановлены.*

Для переноса настроек необходимо запустить утилиту и указать два параметра. Первый параметр - исходные настройки системы ГАРАНТ Платформа F1, второй - папка получения конечных настроек.

Ниже указан пример работы утилиты персона настроек из командной строки:

"C:\Program Files\Garant Intranet\settings\F1MigrateSettings.exe" -ndt "C:\Program Files (x86)\Garant-Server\settings" -leveldb "C:\Program Files\Garant Intranet\settings"

Сброс пароля администратора

Если пароль администратора был изменен и/или забыт, можно вернуть его значение по умолчанию. Для этого в конфигурационный файл **config.py** необходимо добавить опцию **use_default_administrator_password = True** и перезапустить службы ГАРАНТа.

После перезагрузки службы пароль администратора станет ADMIN (пользователь ADMIN). При наличии данной опции в интерфейс администрирования можно войти, используя только пароль ADMIN. В связи с этим, после восстановления пароля данную опцию из config.py необходимо убрать.

Работа по защищенному протоколу HTTPS

При необходимости использовать во внутренней сети организации протокол https (порт 443), в конфигурационный файл **config.py** вносятся следующие изменения:

wsgi_port=443

Также прописываются пути до сертификатов безопасности относительно файла config.py:

ssl_pk_file = './cert/nash.server.key'

ssl_cert_file = './cert/nash.server.crt'

ssl_cert_chain_file = None

Пути выше будут такими, если папка находится в папке %Garant Intranet% для ОС Windows или в папке %Garant Intranet%/web для ОС Линукс.

Установка нескольких копий ГАРАНТ ПРОКСИМА на один сервер

Иногда бывает необходимо установить две или более копий ГАРАНТ ПРОКСИМА на один компьютер, например, на разные порты. На данный момент такая возможность существует только для ОС Windows при помощи механизма клонирования. Данный механизм не поставляется на дистрибутиве, его необходимо запросить у разработчика, например, по адресу hotline@garant.ru. Инструкция по работе с данным механизмом поставляется в комплекте с ним.

Онлайн-сервисы в сети Интернет

В систему ГАРАНТ ПРОКСИМА пользователь заходит на сервер при помощи браузера, поэтому между браузером пользователя и сервером должны быть настроены все необходимые правила для обеспечения сетевого взаимодействия по порту на сервере, который задается в настройках при установке версии (по умолчанию порт 80 в ОС Windows и 8082 в ОС Linux).

Для функционирования пакетного обновления базы данных ГАРАНТа необходимо открыть доступ на сервере к следующим адресам:

- datasetup.garant.ru,
- mirror.garant.ru.

Для работы пользователя с онлайн-сервисами, входящими в комплект, необходимо открыть доступ на компьютерах пользователей к следующим адресам:

- arbitr.garant.ru – для доступа к Онлайн-архиву Судебных Решений,
- municipal.garant.ru – для доступа к Онлайн-архиву муниципальных актов,
- msud.garant.ru – для доступа к Архиву, содержащему практику мировых судей всех субъектов Российской Федерации,

- internet.garant.ru – для доступа к Интернет-версии,
- www.garant.ru – для просмотра Новостей Онлайн,
- mirror2.garant.ru – для просмотра образов и книг,
- service.garant.ru – для просмотра новых сервисов и доступа к Конструктору правовых документов,
- is.garant.ru – для просмотров Интернет-семинаров,
- sutyazhnik.ru – для доступа к Системе «Сутяжник»,
- disk.garant.ru – для доступа к Гарант-диск,
- aero.garant.ru – для доступа к информации по проводимым семинарам, программам повышения квалификации,
- proverka.gardoc.ru – для доступа к сервису «Экспресс проверка контрагентов»,
- *.gartender.ru – для доступа к сервису «Экспресс тендер»,
- visa.gardoc.ru – для доступа к сервису «Экспресс согласование»,
- okpd.garant.ru – для доступа к сервису «Сервис ОКПД2»,
- chat.garant.ru – для доступа к сервису «Чат со специалистами ППО, технология websocket».

Более правильным и удобным является внесение исключения в правила фаерволла для указанных выше доменных имен, лучше по маске ***.garant.ru**.

Если в исключения требуется вносить ip-адреса, то их в любой момент можно получить командой **nslookup** для каждого из указанных доменных имен (для mirror.garant.ru определится два ip-адреса).

Для работы со всеми указанными серверами нужно открыть порты 80 и 443 для работы по протоколам http и https соответственно.

ВЕРСИЯ НА ПЕРЕНОСНОМ НОСИТЕЛЕ. МОБИЛЬНЫЙ ГАРАНТ ОНЛАЙН

Краткое описание

Версия на переносном носителе представляют собой набор программных файлов, записанных на USB флеш-накопитель.

Для использования версии на переносном носителе не требуется никакой установки (ее установка сводится к подключению USB флеш-накопителя), обновление сводится к смене USB флеш-накопителя.

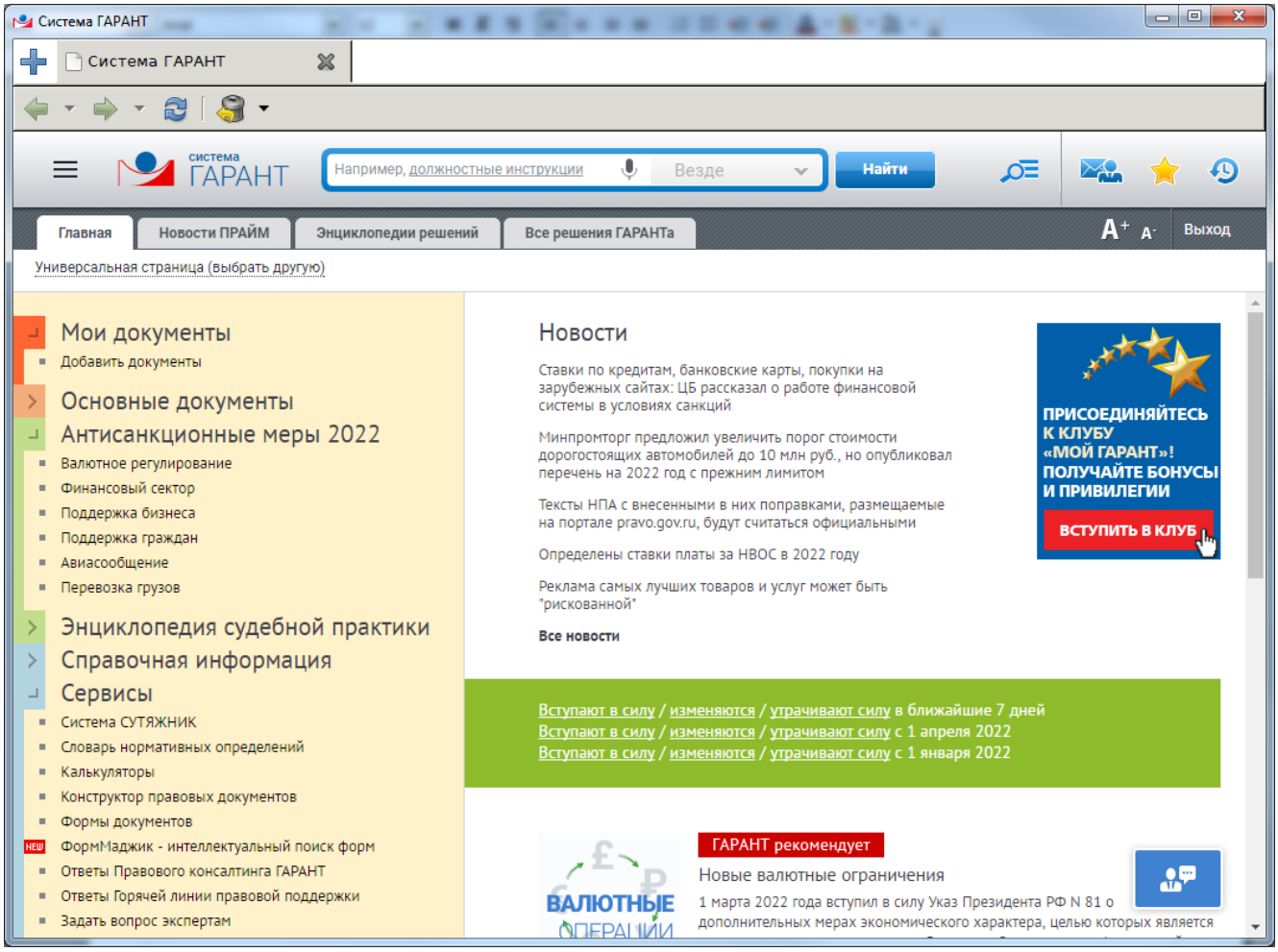
Ограничением рабочей версии является то, что она работает немного медленнее инсталляционной, так как скорость чтения данных с USB флеш-накопителя ниже, чем с жесткого диска. Запуск мобильной версии на USB флеш-накопителе возможен только на том компьютере, к которому подключен носитель (запуск по сети невозможен).

Запуск мобильной версии на ОС WINDOWS

Запуск версии на переносном носителе не требует администраторских или других дополнительных прав на компьютере.

Запуск версии на переносном носителе на рабочих станциях сводится к запуску файла **garant.cmd**, находящегося на USB флеш-накопителе (если в операционной системе выключено отображение расширения файлов, то название файла garant).

После запуска файла откроется интерфейс системы ГАРАНТ ПРОКСИМА:



В случае, если на компьютере доступен Интернет, то откроется онлайн-часть ГАРАНТ ПРОКСИМА. Для принудительного запуска базы с флеш-носителя, не используя Интернет, необходимо запустить файл «ЗАПУСТИТЬ-ГАРАНТ-ЛОКАЛЬНО.cmd».

Запуск мобильной версии на ОС ASTRALINUX

По умолчанию в AstraLinux Special Edition запрещено монтировать незарегистрированные носители. Для разрешения монтирования доверенного носителя всем пользователям и разрешения запуска исполняемых файлов с него потребуется настроить файл **fstab** (/etc/fstab), содержащий инструкции по монтированию блочных устройств.

Важно! *Настройка производится от администратора с высоким уровнем целостности, нулевой меткой безопасности и пустым набором категорий.*

Порядок настройки файла fstab:

1. Подключить USB носитель.

2. Получить UUID устройства – команда **sudo blkid**

```
administrator@UVS-ASTRALINUX:~$ sudo blkid
/dev/sda1: UUID="bbda3775-aae5-471d-9c2a-58e75eca9285" TYPE="ext4" PARTUUID="d3fe6def-01"
/dev/sda5: UUID="6fa0907b-38ae-4084-b709-71878c640649" TYPE="swap" PARTUUID="d3fe6def-05"
/dev/sdb1: LABEL="GARANT" UUID="743fcfc6-2cf4-4843-bf37-c1de38e7e05d" TYPE="ext4" PARTUUID=
"e4feaa0c-01"
administrator@UVS-ASTRALINUX:~$
```

Команда выведет список устройств на компьютере. Флеш-носитель МГО имеет метку LABEL=”GARANT”, необходимо скопировать цифры UUID внутри кавычек из этой строчки. Для того чтобы скопировать текст, в терминале необходимо выделить нужный текст мышкой, зажать кнопку «Shift» и нажать на выделение правой кнопкой мышки и выбрать копировать (чтобы вставить текст, нужно так же зажать «Shift»).

3. Затем добавить строку в конец файла **/etc/fstab**:

UUID=f9497cbb-57b8-4511-b919-0e57d197497e /media/garant auto user,rw,exec,suid,nofail 0 0,

где UUID - это скопированный ранее UUID.

Для этого можно воспользоваться любым редактором, например nano, vi или Midnight Commander(sudo mc) через F4:

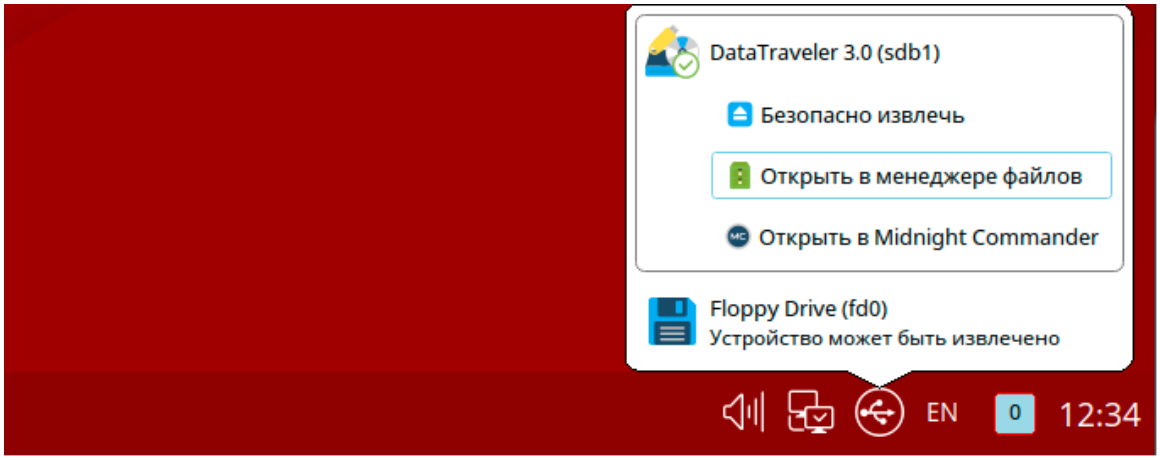
```
administrator@UVS-ASTRALINUX:~$ sudo nano /etc/fstab
```

```
 GNU nano 2.7.4                    Файл: /etc/fstab

# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
# / was on /dev/sda1 during installation
UUID=f9497cbb-57b8-4511-b919-0e57d197497e /media/garant auto user,rw,exec,suid,nofail 0 0

^G Помощь    ^O Записать  ^W Поиск     ^K Вырезать  ^J ВыроВнять  ^C ТекПозиц
^X Выход     ^R ЧитФайл   ^\ Замена    ^U Отмен. Вырез ^T СловарЬ  ^_ К строке
```

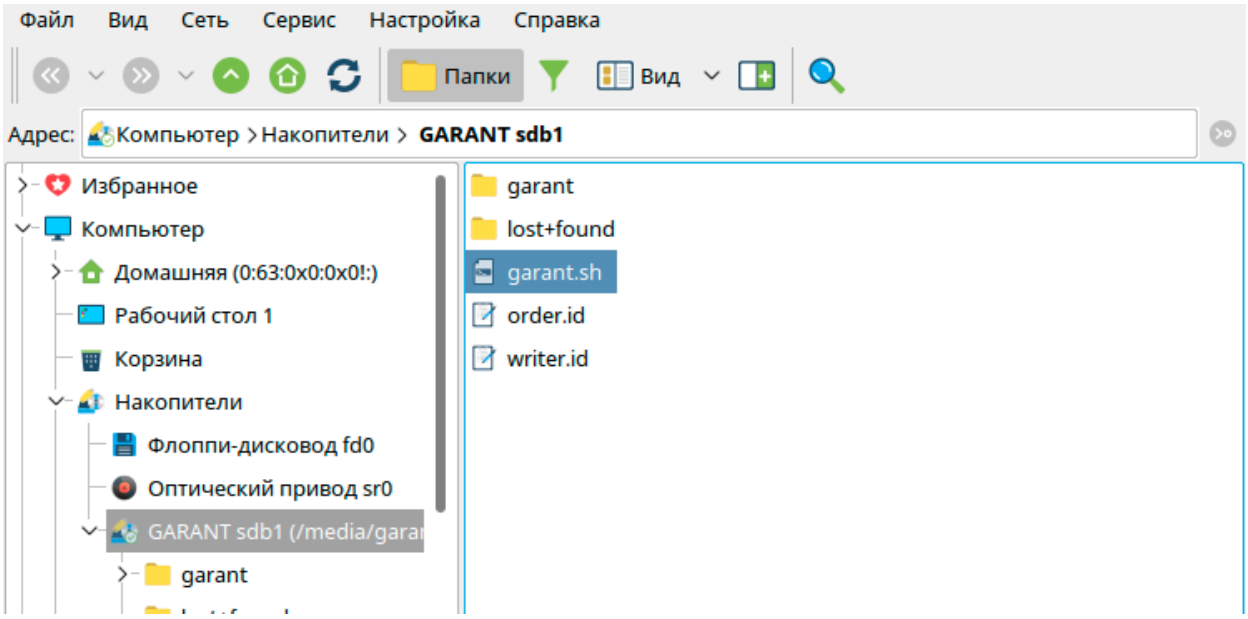
Далее необходимо сохранить файл (Ctrl+O) и выйти (Ctrl+X).

4. Отключить носитель, перезагрузить компьютер и подключить носитель снова.

5. На панели запуска отработает reflex, предложив выбрать действие с носителем. В списке нужно выбрать «Открыть в менеджере файлов».



6. Запустить скрипт **garant.sh**:

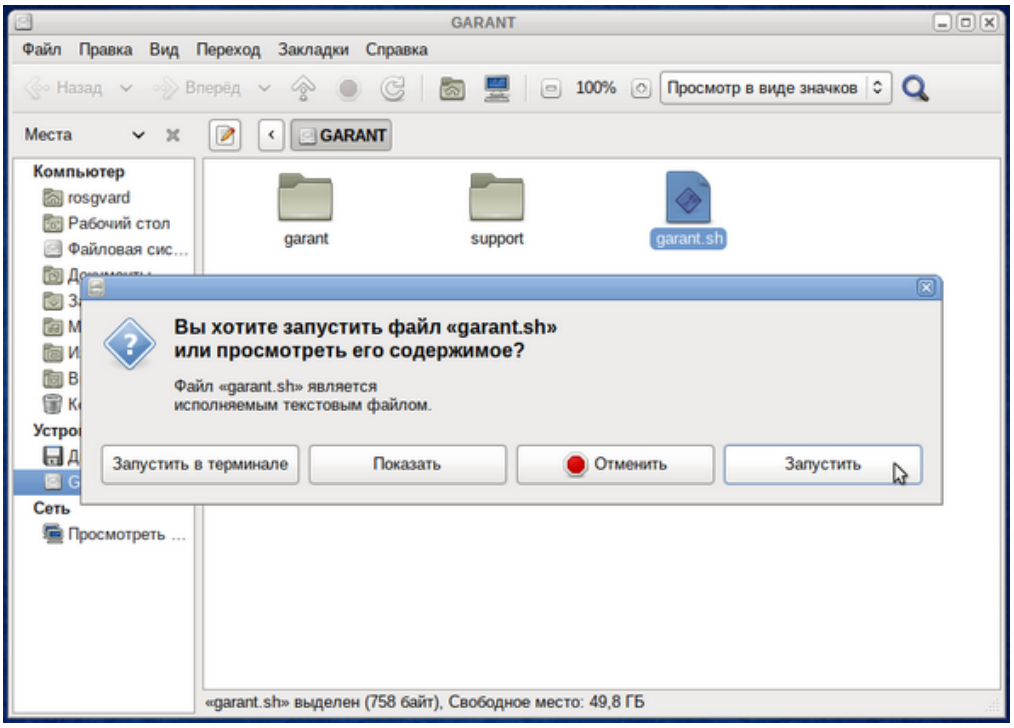


По умолчанию настройки пользователя (закладки, документы на контроле и т.д.) хранятся в домашнем каталоге пользователя на компьютере. Это означает, что на другом компьютере настройки будут другие, под другим пользователем на этом же компьютере настройки будут другие (то есть такое же поведение как и на Windows). Могут возникнуть ситуации, когда пользователь в офисе на ноутбуке работает под доменной учетной записью, а в командировке работает под локальной учетной записью. Существует возможность работать с общими настройками на одном компьютере под разными пользователями. Для этого надо один раз из под пользователя с правами суперадминистратора запустить скрипт **set_share_settings.sh** из папки **support** на флеш-носителе. Выполнение данного скрипта создаст папку для настроек в папке **/var/tmp/garant_mgo_setting** и зафиксирует этот путь для данной операционной системы. После этого на данном компьютере все пользователи будут иметь общие настройки.

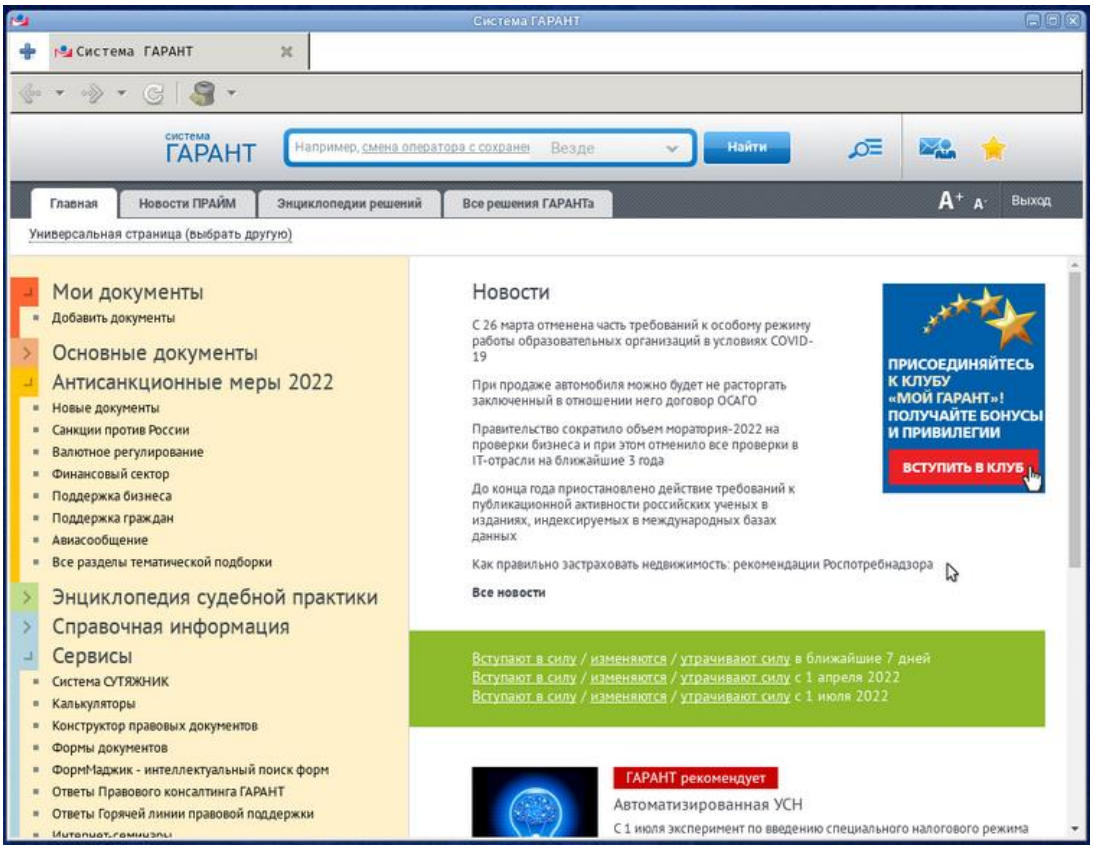
Запуск мобильной версии на ОС AltLinux

В семействе Alt достаточно много версий. Предполагается, что использование Мобильной версии будет осуществляться на дистрибутивах типа Рабочая станция. В связи с этим пример ниже приводится для дистрибутива Alt Workstation 8.

При подключении флеш-накопителя в USB-порт, на рабочем столе появляется иконка диска GARANT, так же этот диск отображается в проводнике в Устройствах. Необходимо зайти в этот диск и запустить файл **garant.sh**.



Откроется дополнительное диалоговое окно, в котором необходимо нажать кнопку «Запустить», после чего произойдет запуск системы ГАРАНТ ПРОКСИМА.



ПРИЛОЖЕНИЯ

Приложение 1. КРАТКАЯ СПРАВКА ПО РАБОТЕ С ОС LINUX

В справке приведены основные команды для работы в терминале Линукса.

Основные операционные системы, поддерживаемые системой ГАРАНТ ПРОКСИМА, - это AstraLinux и AltLinux. По нашим наблюдениям у данных операционных систем отличается способ выполнения команд от суперпользователя (суперадминистратора или root-пользователя, имеющего наивысшие права).

В AstraLinux для выполнения команды с правами суперпользователя надо перед командой добавить команду sudo, при этом сам пользователь должен входить в группу sudo. Обращаем внимание, что в AstraLinux большинство команд надо выполнять именно с sudo, иначе система будет писать, что команда не найдена. Например, для запуска установки оболочки ГАРАНТ ПРОКСИМА на AstraLinux с правами суперпользователя надо выполнить команду:

sudo dpkg -i garant-intranet-xx.x-x-astra.deb

В то же время в AltLinux этот способ не работает. Для работы с командами из под суперпользователя нужно сначала перейти в режим суперпользователя, а потом выполнять команды обычным способом. Для того, чтобы перейти в режим суперпользователя необходимо выполнить команду **su-** (с минусом на конце) и ввести пароль учетной записи root. То есть для установки оболочки ГАРАНТ ПРОКСИМА на AltLinux нужно выполнить две команды:

su- (и ввести пароль root)

и уже затем

apt-get install /srv/share/garant-intranet-xx.x-x-alt.rpm

Еще одно отличие данных операционных систем, - это использование разных установщиков пакетов: в случае с AstrLinux используется deb пакет, а в случае с AltLinux используется rpm пакет.

Установщик ГАРАНТ ПРОКСИМА выполнен в командной строке (терминале) в связи с тем, что есть вероятность установки на сервере ОС Linux без графического интерфейса.

В терминале существуют команды, предназначенные для работы с файлами и каталогами. Далее будут приведены наиболее важные из них. При этом сразу сделаем замечание: в Linux-системах нет дисков C, D или чего-то подобного, как в Windows. Вместо этого, адреса всех файлов начинаются с корня, а дополнительные разделы, флешки или оптические диски подключаются в папки корневого каталога. Корень обозначается слешом «/» - это главный каталог в системе Linux. По сути, это и есть файловая система Linux.

Для получения справки по любой команде необходимо запустить ее с ключом **--help**.

Список основных команд для каталогов

Команда	Описание
pwd	вывод полного пути текущего каталога
cd	переход в домашний каталог пользователя
cd /	переход в корень диска
cd dirname	перейти в папку «dirname», находящуюся в текущем каталоге
cd /usr/local/garant/intranet	переход в папку по указанному пути

Команда	Описание
ls	просмотреть список файлов в текущем каталоге
ls -d */	просмотреть список папок в текущем каталоге
ls -la	вывести содержимое текущего каталога с указанием подробной информации о файлах и папках (права доступа, кто владелец, размер, дата)
mkdir dirname	создать папку с наименованием «dirname»
rmdir dirname	удалить папку «dirname»
rm -rf dirname	удалить папку «dirname» с её содержимым (опция -r) и без предупреждения пользователя (опция -f). Надо быть осторожным с данной командой, если ее выполнить находясь в корне файловой системы, можно «убить» Линкус
du -h dirname	размер папки «dirname» (если не указать имя папки, то покажет размер всех папок в текущем каталоге). Будет отображать размер каждой папки и файла внутри папки
du -s dirname	покажет только итоговый размер папки (не будет отображать размеры каждого элемента)

Помимо этого, существуют полезные сокращения. Например, текущая директория обозначается с помощью «.». Знак «..» позволяет задействовать родительский каталог. Для представления домашней директории используется «~».

Например, для перехода в родительский (на уровень выше) каталог можно использовать команду **cd ..** , а для перехода в каталог находящийся в домашнем каталоге команду **cd ~/dirname** .

Список основных команд для работы с файлами

Команда	Описание
touch file	создать файл с именем file
stat file	получение информации о «file» (размер файла, дата создания файла и т. д.) и проверка существования файла
cat file	вывод содержимого файла (пример использования: cat version.txt)
find -name file	поиск файла по имени в каталогах, относительно текущего каталога
nano file	редактирование файла в редакторе Nano, также можно использовать редактор vi, например **vi file**
sh filename	запустить файл со сценарием Bash
./filename	запустить исполняемый файл из текущего каталога
cp file1 file2	копировать файл «file1» с переименованием на «file2». Произойдёт замена файлов, если элемент с таким же названием существует. При этом можно указывать полные пути файлов относительно корня

Команда	Описание
mv file1 file2	переименовать файл «file1» в «file2» (переместить, если указать новый путь)
mv filename dirname	переместить файл «filename» в каталог «dirname»
grep text filename	поиск и вывод строк из файла «filename», содержащих «text»
rm filename	удалить файл

Также удобным инструментом для работы с файлами и каталогами в терминале является файловый менеджер Midnight Commander (похож на Far или старый NortonComander в MS-DOS). Для его запуска выполните команду в терминале: **mc**

Чтобы иметь максимальные права, в случае с AstraLinux нужно выполнить **sudo mc**, а в AltLinux сначала перейти в режим суперпользователя командой **su-** и только потом команду **mc**

Еще несколько важных команд — это диспечер задач и определение свободного места на диске:

top — отображение списка всех выполняемых процессов

top -u ru-garant — отображение списка выполняемых процессов пользователя ru-garant

df -h — отображает список разделов на диске и место на них

Монтирование носителя в Linux

Разделы дисков в Linux подключаются к системе совсем не так, как в Windows. Здесь есть корневая файловая система, куда подключаются все другие разделы и устройства. Системные разделы монтируются автоматически при старте системы. Если нужно подключить дополнительные носители, в некоторых случаях, может понадобиться сделать это вручную. Для монтирования в Linux используется команда **mount**. Синтаксис команды следующий:

mount файл_устройства папка_назначения

Или расширенный вариант:

mount опции -t файловая_система -o опции_монтирования файл_устройства папка_назначения

Фактически в большинстве случаев будет достаточно упрощенной версии команды:

sudo mount /dev/sdb6 /mnt/

где /dev/sdb6 - имя монтируемого устройства; /mnt/ - место, где монтируемое устройство будет доступно.

Имя устройств в системе можно определить командой: **sudo blkid**

При монтировании внешних носителей для установки системы ГАРАНТ ПРОКСИМА может потребоваться сменить владельца точки монтирования и дать необходимые права.

Как посмотреть открытые порты Linux

Открытые порты в Linux можно посмотреть различными способами. Приведем несколько из них:

1. Утилита netstat позволяет увидеть открытые в системе порты, а также открытые на данный момент сетевые соединения. Для отображения максимально подробной информации надо использовать опции:

-l или --listening - посмотреть только прослушиваемые порты;

-p или --program - показать имя программы и ее PID;

-t или --tcp - показать tcp порты;

-u или --udp показать udp порты;

-n или --numeric показывать ip адреса в числовом виде.

Пример использования: **sudo netstat -tulpn**

2. Утилита ss - это современная альтернатива для команды netstat. В отличие от netstat, которая берет информацию из каталога /proc, утилита ss напрямую связывается со специальной подсистемой ядра Linux, поэтому работает быстрее и её данные более точные. Если вы хотите выполнить просмотр открытых портов, - это не имеет большого значения. Опции у неё такие же.

Пример использования: **sudo ss -tulpn**

Можно вывести только процессы, работающие на указанном порту (8082):

sudo ss -tulpn | grep :8082

3. Утилита lsof позволяет посмотреть все открытые в системе соединения, в том числе и сетевые, для этого нужно использовать опцию –i. Чтобы отображались именно порты, а не названия сетевых служб следует использовать опцию -P:

Пример использования: **sudo lsof -i -P**

Можно посмотреть какие процессы работают с указанным портом (8082):

sudo lsof -i -P | grep :8082

Список команд для работы с пользователями в Linux

Команда	Описание
su user	работа в терминале под другим пользователем (user)
id или groups	вывод групп, куда входит текущий пользователь
getent group	вывод всех групп в ОС
adduser test	добавить нового пользователя test в систему (необходимы права админа)
usermod -a -G group_name user_name	добавление существующей учетной записи пользователя user_name в группу group_name (необходимы права админа)

Планировщик заданий Cron

В Windows-системах есть утилита «Планировщик зданий», которая позволяет запланировать запуск программ или скриптов в определенные моменты времени с определенным интервалом. В Linux-системах тоже есть подобная утилита, называется она Cron.

Cron работает как служба и выполняет действия, которые описаны в конфигурационных файлах, в определенное время. При этом эта служба может быть выключена по умолчанию, например, в AltLinux. Для того чтобы она работала, ее надо включить в автозагрузку и запустить, для этого выполните команды из под пользователя с правами суперпользователя:

systemctl enable crond

systemctl start crond

Признаком того, что cron выключен, будет сообщение после правки конфигурационных файлов cron:

crontab: warning, cron does not appear to be running

Для создания и редактирования cron-заданий (правки конфигурационных файлов cron) используется утилита crontab. Для ее запуска в терминале надо выполнить команду:

crontab -e

Для настройки выполнения задания от другого пользователя, например, от ru-garant, необходимо выполнить команду:

crontab -u ru-garant - e

После ее выполнения откроется редактор заданий для данного пользователя, скорее всего откроется в редакторе vi. Правила задания задаются особым синтаксисом. Фактически строка записи задания состоит из двух частей: таймера расписания и выполняемого файла. Вот так записывается задание:

*** * * * * /usr/local/garant/intranet/bin/download,**

по сути здесь прописывается следующее:

минута час день месяц день_недели /путь/к/исполняемому/файлу

Важно! *Обязательно нужно писать полный путь к исполняемому файлу, потому что для команд, запускаемых от имени cron, переменная среды PATH будет отличаться, и сервис просто не сможет найти ваш исполняемый файл.*

Дата и время указываются с помощью цифр или символа '*' - этот символ означает, что файл нужно выполнять каждый (-ую) минуту/час/день/день недели. Вместо звездочки могут быть следующие значения:

минута - от 0 до 59

час - от 0 до 23

день - от 1 до 31

месяц - от 1 до 12

день недели - от 1 до 7

Например,

0 2 * * * /usr/local/garant/intranet/bin/download – означает «будет выполнять файл каждый день в 2:00»

0 2 * * 5 /usr/local/garant/intranet/bin/download – означает «будет выполнять файл каждую пятницу в 2:00»

Важно! *Обычно cron требует перевод каретки после всех заданий, то есть должна быть еще пустая строка в конце файла.*

Текстовый редактор vi

Данный текстовый редактор предназначен для редактирования (составления и изменения) файлов, содержащих только текст, например: программа на языке C, bash или системный конфигурационный файл. При том, что имеется много различных редакторов для системы Linux, единственный, чьё присутствие будет гарантировано в любой Linux-системе — это vi (visual editor). Редактор vi не является самым простым в использовании, его интерфейс не очень понятен сам по себе. Однако, ввиду своей распространённости, а отчасти и потому, что владение им в некоторых ситуациях необходимо, опишем здесь основы работы с ним.

Запуск данного редактора осуществляется следующим образом:

vi filename

где filename — имя файла, который надо редактировать (можно указать путь к файлу, если не находитесь в той же директории), а если такого файла нет, то редактор может его создать.

В любой момент при работе в редакторе vi вы находитесь в одном из трёх режимов редактора: *командный режим* (command mode), *режим ввода* (insert mode) и *режим последней строки* (last line mode).

При запуске редактора vi вы оказываетесь в *командном режиме*. В этом режиме можно давать команды для редактирования файлов или перейти в другой режим. Например, вводя x в командном режиме, мы удаляем символ, на который указывает курсор. Клавиши-стрелки перемещают курсор по редактируемому файлу. Как правило, команды, используемые в командном режиме, состоят из одного или двух символов.

Основной ввод и редактирование текста осуществляется в *режиме ввода*. Переход в режим ввода из командного режима осуществляется командой **i** (от слова insert). Находясь в режиме ввода, можно вводить текст в то место, куда указывает курсор. Выход из режима ввода в командный режим осуществляется клавишей **Esc**.

Режим последней строки — это специальный режим, в котором редактору даются сложные команды. При вводе этих команд они отображаются в последней строке экрана (отсюда пошло название режима). Например, если ввести в командном режиме команду **:** (двоеточие), то осуществится переход в режим последней строки, и можно будет вводить такие команды, как **wq** (записать файл и покинуть редактор vi) или **q!** (выйти из редактора vi без сохранения изменений). В режиме последней строки обычно вводятся команды, название которых состоит из нескольких символов. В этом режиме в последнюю строку вводится команда, после чего нажимается клавиша **Enter**, и команда исполняется.

Резюмируя описанное выше, хочется сказать, что в командном режиме удобно перемещать курсор по тексту стрелками и удалять ненужные символы кнопкой X, в режиме ввода необходимо вводить текст, а в режиме командной строки можно сохранить файл (**wq**) или выйти без сохранения (**q!**) (при этом можно многократно переходить из режима в режим).

Работа со службами в Linux

В Linux есть специальный инструмент для управления службами - systemctl. Эта утилита позволяет делать очень много вещей, - от перезапуска службы Linux и проверки ее состояния до анализа эффективности загрузки службы. Синтаксис у утилиты такой:

systemctl опции команда служба служба...

Опции сильно зависят от команд, поэтому здесь рассматривать их не будем.

Приведем список некоторых команд:

Команда	Описание
start	запустить службу linux
stop	остановить службу linux
restart	перезапустить службу
status	посмотреть состояние и вывод службы
enable	добавить службу в автозагрузку
disable	удалить службу из автозагрузки

Для запуска службы во время загрузки используйте команду enable:

sudo systemctl enable crond

Для запуска службы в текущем сеансе используйте команду start:

sudo systemctl start crond

Передача дистрибутива на сервер

При наличии Интернета на сервере можно скачивать дистрибутив из Интернета непосредственно на сервер.

Если доставка дистрибутива осуществляется на носителе и сервер физический, то можно вставить переносной носитель в USB-порт сервера или DVD-ROM, смонтировать в определенную папку, после чего устанавливать ГАРАНТ ПРОКСИМА непосредственно с USB носителя. Однако, есть вероятность отсутствия доступа к файлам дистрибутива на USB- или DVD-носителе из-за разных владельцев. Для решения данной проблемы можно изменить права доступа и владельца точки монтирования носителя.

В большинстве случаев сервер является виртуальным, и тогда работа с дистрибутивом несколько усложняется. Есть несколько вариантов, например, если на сервере ограничено место и скопировать дополнительно дистрибутив невозможно, то рекомендуется средствами виртуализации «прокинуть» USB- или DVD-носитель на виртуальную машину и опять же ставить сразу с USB- или DVD-носителя. Если есть вариант, когда можно скопировать дистрибутив на сервер по сети, тогда можно ставить ГАРАНТ ПРОКСИМА непосредственно с сервера. В данном случае тоже могут быть различные варианты:

1. Сервер на Linux, рабочая станция на Windows.
2. Сервер на Linux, рабочая станция тоже на Linux.
3. Сервер на Windows, рабочая станция на Linux.

Сервер на Linux, рабочая станция на Windows:

Самым правильным будет запустить и настроить Samba-сервер на Linux и тогда можно подключаться к расшаренной папке на сервере как и к Windows-серверу, это позволит всегда работать в обычном проводнике. \\servername\share.

Второй вариант это использовать SSH-подключение, для чего на сервере надо установить и запустить SSH сервер (по умолчанию SSH сервер может быть не установлен). В ОС Windows 10 уже присутствует утилита scp, для Windows 7 необходимо проинсталлировать SSH клиент, например, Putty (необходима честная инсталляция, тогда добавится аналогичная утилита pscp, работающая так же, как и scp). Далее запускаем командную строку (cmd) в Windows. Команда будет выглядеть следующим образом:

scp -R d:\temp\garantDistr user@host:/var/tmp

Если используется Putty, то команда будет выглядеть следующим образом:

pscp -R d:\temp\garantDistr user@host:/var/tmp,

где user - это логин пользователя на сервере Linux, host - это IP-адрес или имя сервера.

Далее система запросит пароль от пользователя user, и начнется копирование дистрибутива. В Windows 10 первый раз утилита попросит подтвердить доверие серверу, - надо написать yes (при этом на экране символы отображаться не будут).

Сервер на Linux, рабочая станция тоже на Linux

В этом случае так же есть два варианта. Первый вариант - на сервере поднять Samba-сервер и расшарить папку, а на рабочей станции по протоколу smb создать соединение и копировать обычным способом (на рабочей станции должен быть графический интерфейс). Для этого в левой части проводника на значке Сеть нажать правой кнопкой мышки и выбрать пункт Новое место, где в поле адрес ввести smb://name_server/name_share, в результате появится папка на сервере, куда можно копировать дистрибутив.

Второй вариант - использовать SSH-соединение. Для этого на сервере так же надо установить и запустить SSH-сервер (по умолчанию SSH-сервер может быть не установлен) и использовать копирование по SSH-протоколу (рабочая станция может быть без графического интерфейса).

Пакет SSH входит в дистрибутивы AstraLinux, но по умолчанию устанавливается только клиент.

Установку сервера можно выполнить:

1. при инсталляции системы, отметив соответствующий пункт в диалоге выбора программного обеспечения,
2. после установки системы с помощью графического менеджера пакетов или из командной строки: **apt install ssh.**

После установки сервис SSH может не быть запущен автоматически, поэтому желательно его включить и запустить отдельно командами:

systemctl enable ssh

systemctl start ssh

Затем на рабочей станции в терминале можно организовать копирование следующей командой:

scp -r /source user@host:/destinationdir/

где /source - путь к папке, которую хотим скопировать,

/destinationdir - путь на удаленном сервере, куда будем копировать (на конце должен быть слэш),

user - пользователь на сервере,

host - IP адрес или имя сервера.

После выполнения команды система запросит пароль пользователя user и начнет копирование.

Сервер на Windows, рабочая станция на Linux

В данном случае можно использовать SMB-протокол для копирования дистрибутива на расшаренную папку. На сервере стандартными средствами Windows расшаривается папка, а на Linux, как и в предыдущем случае, в проводнике — Сеть, создается новое место (link) на эту папку, и обычным способом через проводник копируется дистрибутив в данную папку.

Права доступа в Linux

Каждый файл или папка в Linux имеет три категории пользователей, для которых можно устанавливать различные сочетания прав доступа:

Владелец - набор прав для владельца файла, пользователя, который его создал или сейчас установлен его владельцем. Обычно владелец имеет все права: чтение, запись и выполнение.

Группа - любая группа пользователей, существующая в системе и привязанная к файлу. Но это может быть только одна группа и, обычно, это группа владельца, хотя для файла можно назначить и другую группу.

Остальные - все пользователи, кроме владельца и пользователей, входящих в группу файла.

Именно с помощью этих наборов полномочий устанавливаются права файлов в Linux. Каждый пользователь может получить полный доступ только к файлам, владельцем которых он является, или к тем, доступ к которым ему разрешен. Только пользователь Root (суперпользователь) может работать со всеми файлами независимо от их набора разрешений.

Чтобы узнать права на файл Linux, выполните такую команду в папке, где находится этот файл:

ls –l

Будет получен ответ в следующем виде:

```
[root@alt-server administrator]# ls -l
итого 16
-rw-r--r-- 1 administrator administrator   81 апр 13 18:51  test
-rw-rw-rw- 1 ru-garant     ru-garant        0 апр 15 18:34  test2
-rwxrwxrw- 1 root          root             0 апр 15 18:36  test3
drwxr-xr-x 6 administrator administrator 4096 апр  4 23:41  Документы
drwxr-xr-x 2 administrator administrator 4096 апр  4 23:41  Загрузки
drwxr-xr-x 2 administrator administrator 4096 апр  4 23:41 'Рабочий стол'
[root@alt-server administrator]#
```

В первом столбце отображаются права на файлы и папки, которые состоят из 10 символов. Первый символ указывает на тип файла или каталога. Далее идут три группы по три символа, которые относятся к трем вышеописанным категориям пользователей, и которые означают следующее:

- — нет прав совсем,

r — права только на чтение файла или каталога,

w — права на запись (изменение) файла или каталога,

x — права на выполнение (запуск) файла или файлов внутри каталога.

Также существуют другие значения в третьем разряде каждой группы (значения s и t), но здесь мы их рассматривать не будем.

Комбинация этих трех регистров задает права для каждой из категорий пользователей (владельца, привязанной к файлу группы и всех остальных пользователей). Для каждой из этих трех групп можно запретить доступ совсем (-), дать доступ читать файл (r), дать возможность изменять файл (w) или запускать (x). Значения r, w, x всегда стоят в соответствующем регистре. Если стоит прочерк в каком-то регистре, значит это действие для данной группы запрещено. В третьем столбце на скриншоте видим как раз владельца файла, а в четвертом группу, связанную с этим файлом.

Для изменения прав доступа к файлам в Linux используется команда chmod. Ее синтаксис:

chmod опции категория действие флаг файл

Опции сейчас нас интересовать не будут, разве что только одна. С помощью опции -R вы можете заставить программу применять изменения ко всем файлам и каталогам рекурсивно, то есть поменять права на все файлы внутри папок.

Категория указывает, для какой группы пользователей нужно применять права:

u - владелец файла;

g - группа файла;

o - другие пользователи.

Действие может быть одно из двух: либо добавить права - знак "+", либо убрать права - знак "-". Что касается самих прав доступа, то они аналогичны выводу утилиты ls: r - чтение, w - запись, x - выполнение. Например, всем пользователям даем полный доступ к файлу file:

chmod ugo+rwx file

Или заберем все права у группы и остальных пользователей:

chmod go-rwx file

Дадим группе право на чтение и выполнение:

chmod g+rx file

Остальным пользователям только чтение:

chmod o+r file

Для каталога dirname и всем файлам внутри установим права на чтение (находимся в каталоге, где лежит dirname):

chmod -R ug+r dirname

Также существует восьмеричный формат записи. В этом случае права записываются цифрами для каждой категории пользователей:

0 - никаких прав;

1 - только выполнение;

2 - только запись;

3 - выполнение и запись;

4 - только чтение;

5 - чтение и выполнение;

6 - чтение и запись;

7 - чтение запись и выполнение.

Права на папку в Linux такие же, как и для файла. Во время установки прав сначала укажите цифру прав для владельца, затем для группы, а потом для остальных. Например:

744 - разрешить все для владельца, а остальным только чтение;

755 - все для владельца, остальным только чтение и выполнение;

764 - все для владельца, чтение и запись для группы, и только чтение для остальных;

777 - всем разрешено все.

Например, разрешим все для владельца файла, а остальным только чтение:

chmod 744 file

Дадим полный доступ всем на папку:

chmod -R 777 dirname

Для смены владельца папки или файла используется команда chown:

sudo chown -R ru-garant:ru-garant /var/tmp/garant/garant

где /var/tmp/garant/garant — каталог, где хранится дистрибутив с базой данных (это может быть точка монтирования внешнего USB-носителя).