{KOMRAD}
Enterprise SIEM

Эшелон
комплексная безопасность

KOMRAD Enterprise SIEM

Quickstart Guide

KOMRAD Enterprise SIEM - гибкая и масштабируемая система централизованного управления событиями информационной безопасности, поддерживающая широкий спектр источников событий.

KOMRAD Enterprise SIEM позволяет осуществлять централизованный сбор событий ИБ, выявлять инциденты ИБ и оперативно на них реагировать.
Применение комплекса позволяет эффективно выполнять требования, предъявляемые регуляторами к защите персональных данных, к обеспечению безопасности государственных информационных систем и контролю критической информационной инфраструктуры предприятия.

Содержание

Подготовка к установке

Перед началом процесса установки, пожалуйста, убедитесь, что Ваша система соответствует минимальным требованиям, необходимым для комфортной работы с KOMRAD.

Характеристики	
Количество ядер процессора	2
Базовая тактовая частота процессора	2 ГГц
Оперативная память	DDR3 8 Гб
SSD/HDD	**100 Гб**

Установка с помощью инсталлятора в автоматическом режиме

Подготовка установщика

Распаковать архив, перейти в папку с дистрибутивом и запустить установку KOMRAD с помощью инсталлятора:

```
chmod +x komrad_v4.5.22-demo_astra_1.8_amd64.run
```

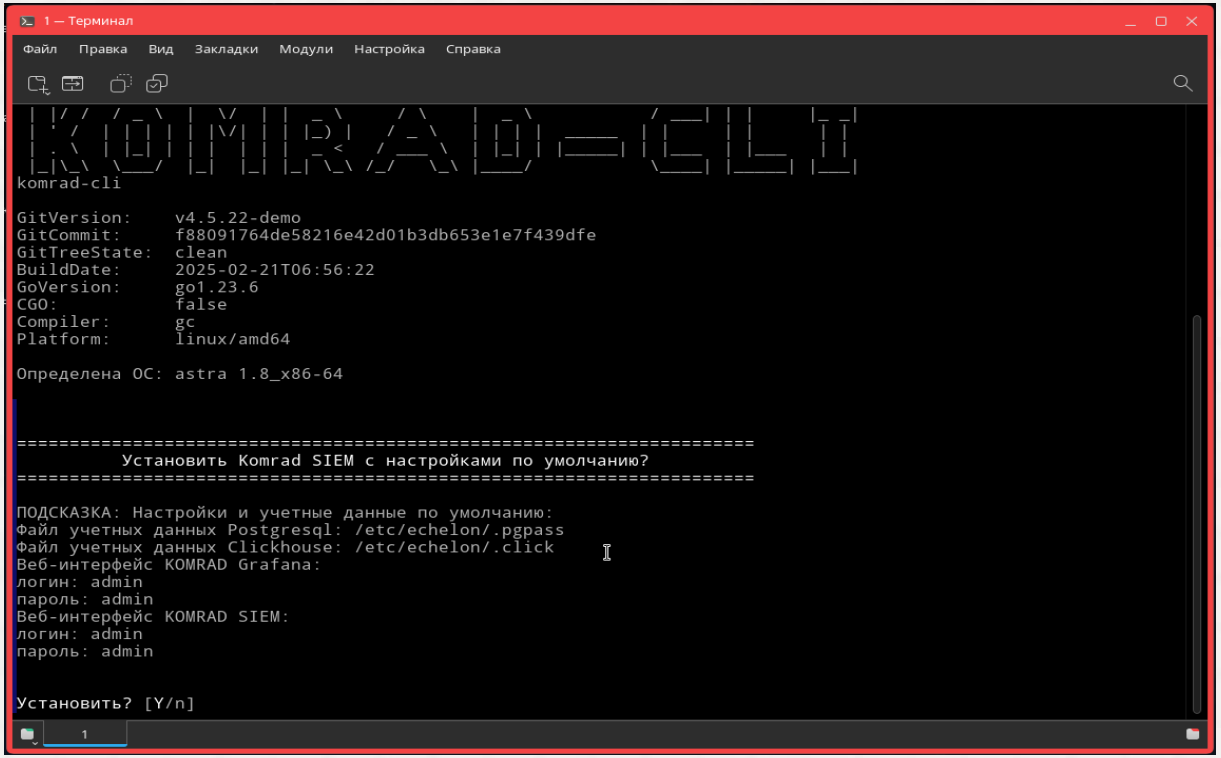
Запуск установщика

```
sudo ./komrad_v4.5.22-demo_astra_1.8_amd64.run
```

Следуйте инструкции по установке, обратите внимание на установленные по умолчанию логин и пароль для KOMRAD:

```
login: admin
password: admin
```

Нажмите Y, чтобы произвести полную установку KOMRAD со всеми пакетами.
Нажмите Enter, чтобы продолжить.



ПОДСКАЗКА

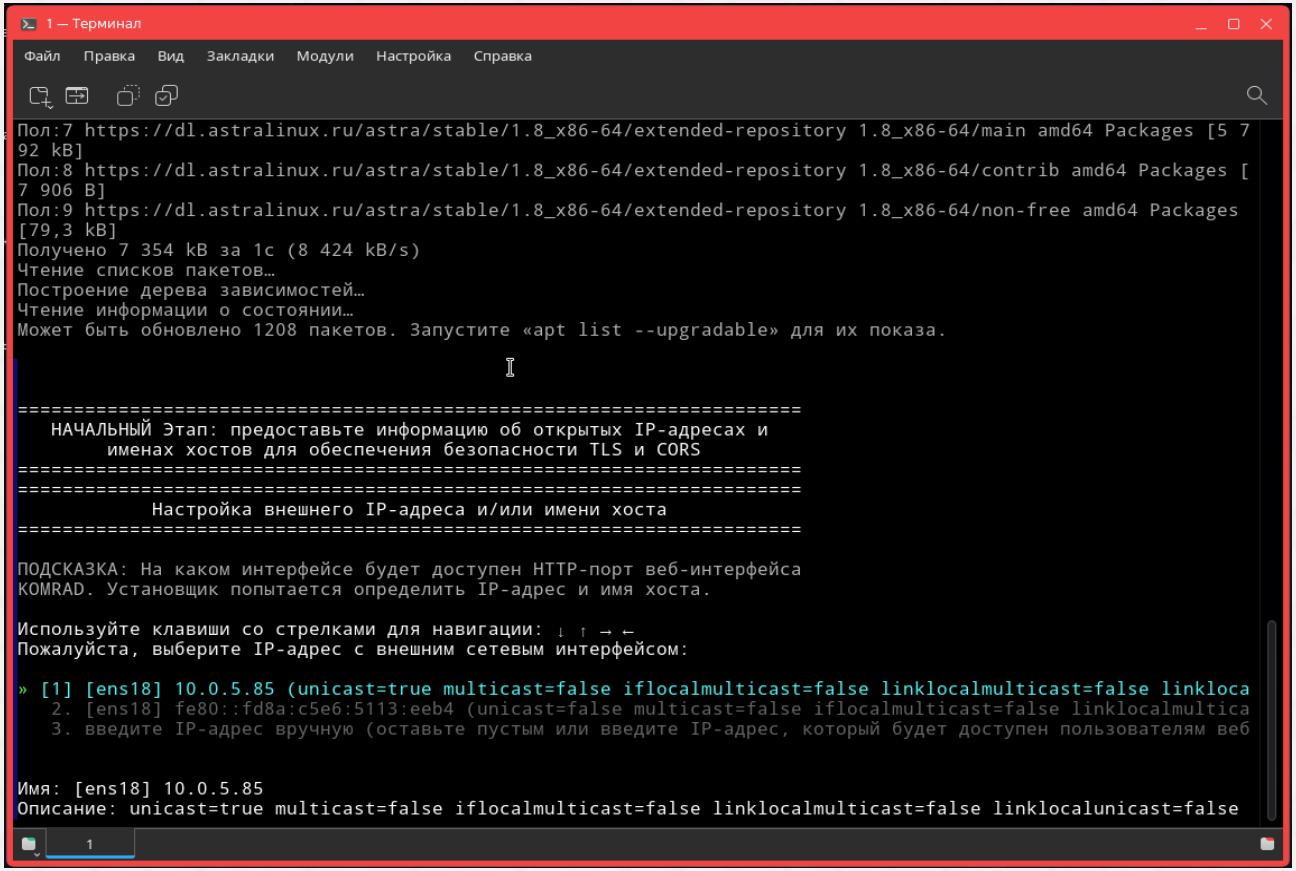
Если в процессе установки KOMRAD установщик выдаст ошибку и выйдет из диалога, то запустите его повторно для продолжения установки:

```
sudo komrad-cli install singlenode
```

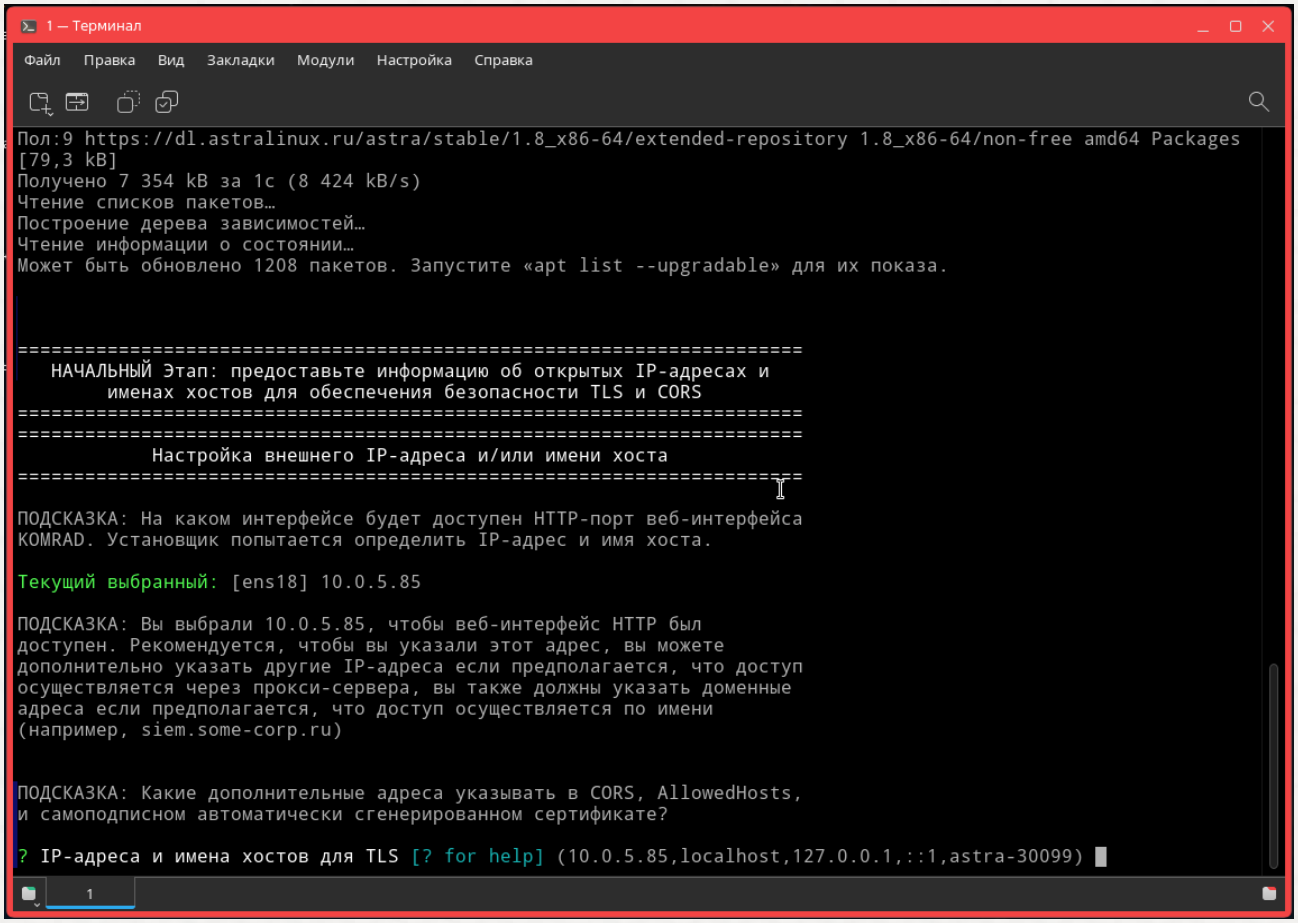
В диалоге с установщиком в консоли отклоните все пройденные ранее шаги.

Определение IP

Установщик попытается определить IP-адрес и имя хоста самостоятельно.

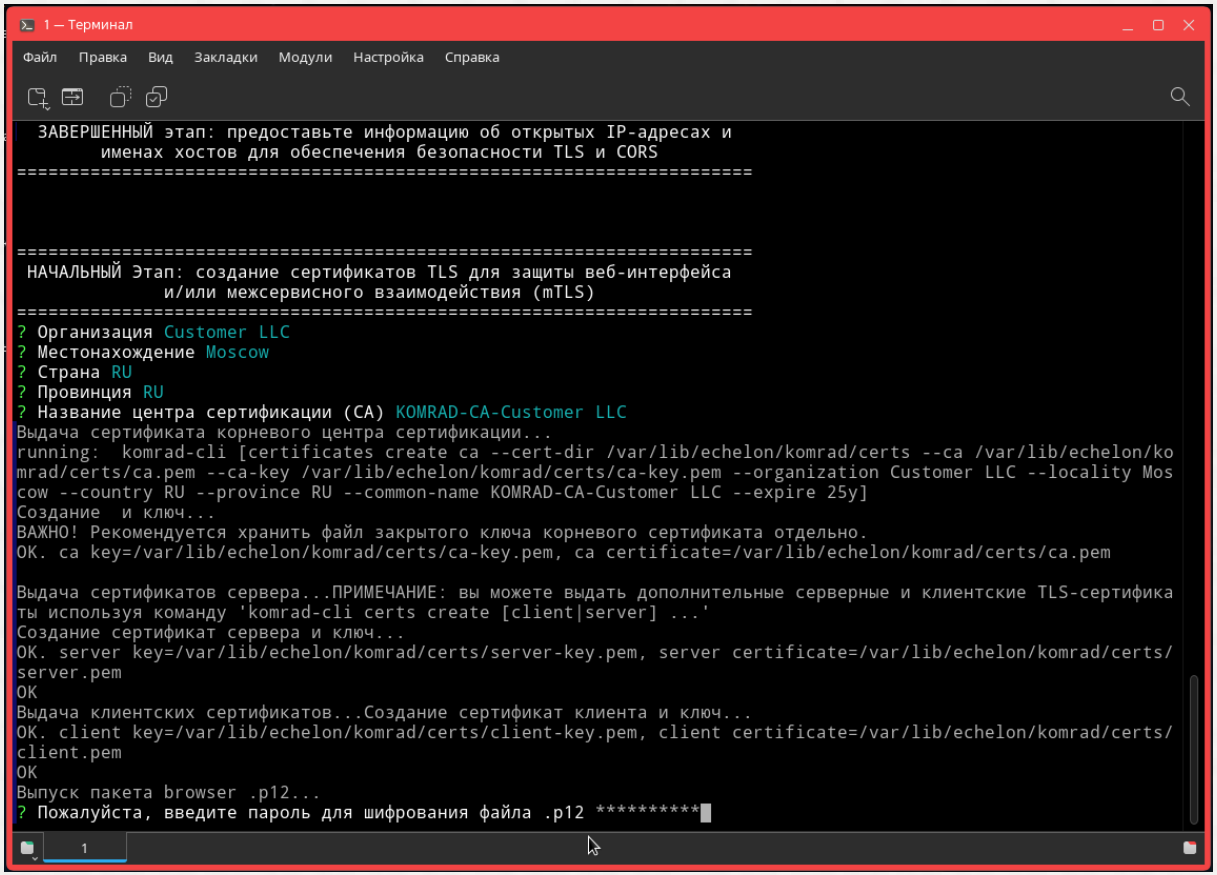


Нажмите Enter, чтобы продолжить с выбранными данными, либо введите свои.

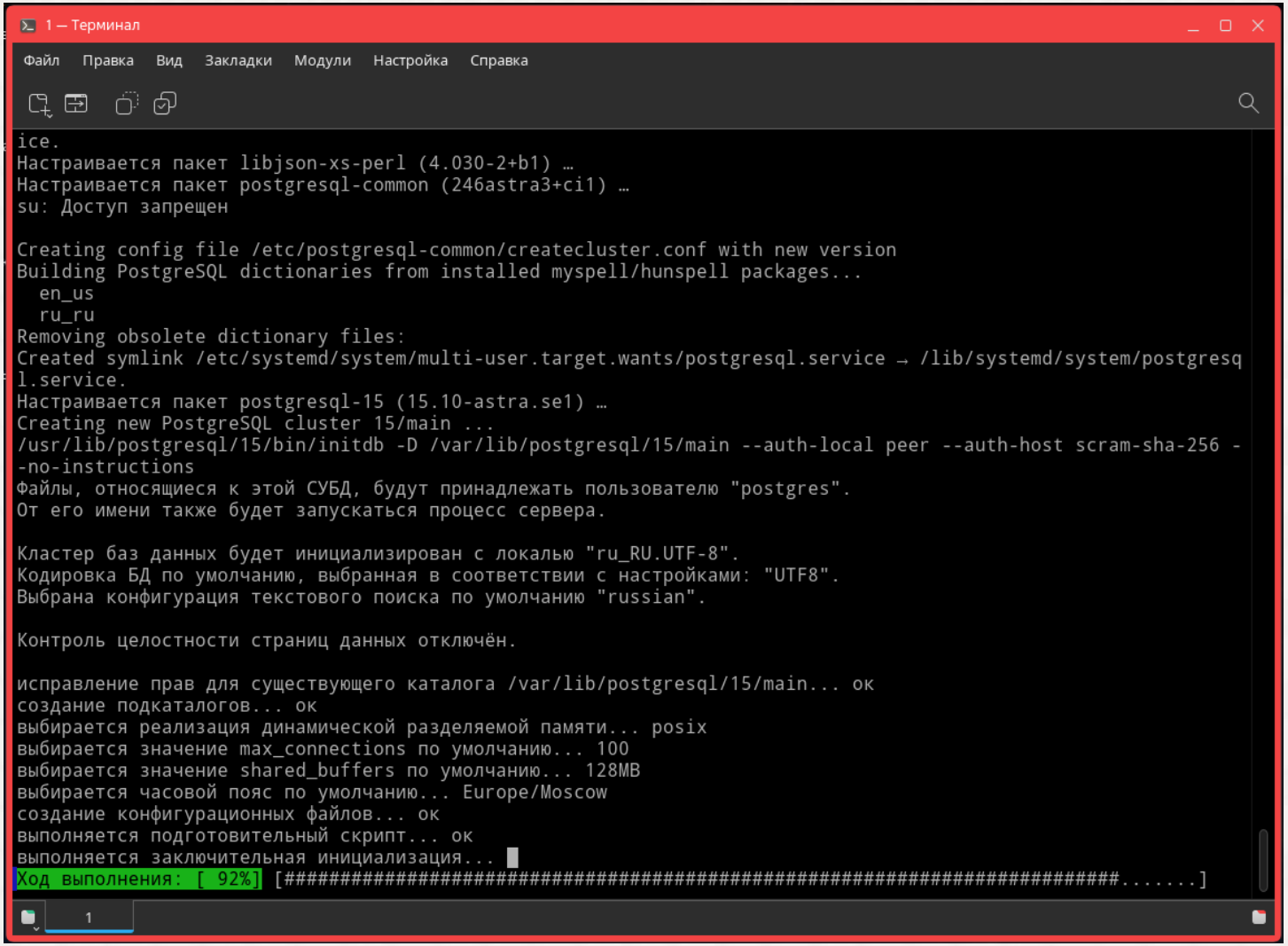


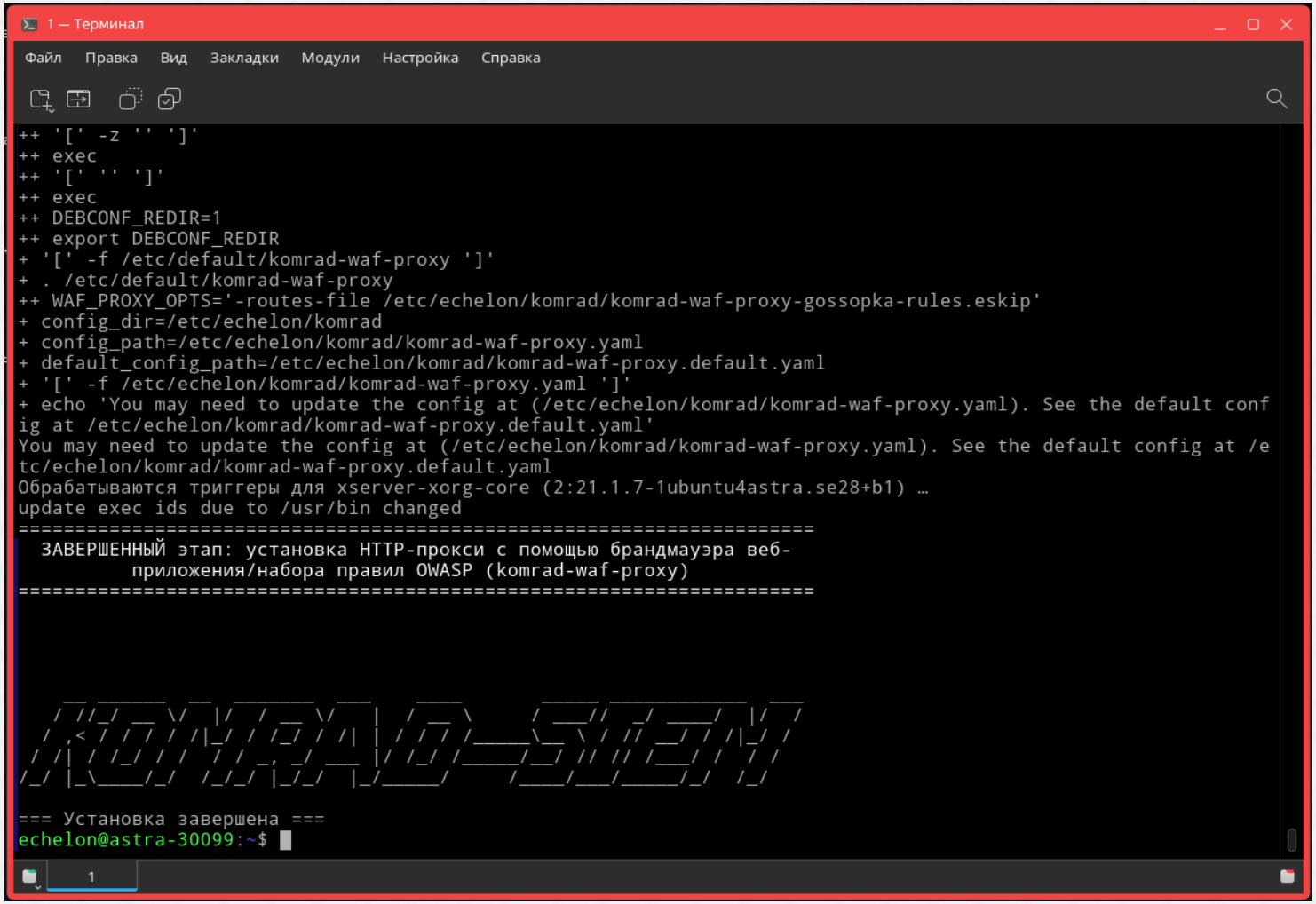
Создание сертификатов

Далее укажите имя организации, местонахождение (по умолчанию – Moscow), страну (по умолчанию – RU), провинцию (по умолчанию – RU) и название центра сертификации.
Укажите пароль для сертификатов, которые в дальнейшем будут использоваться в браузере.
Запомните или запишите этот пароль, он потребуется при импорте сертификатов в браузер.



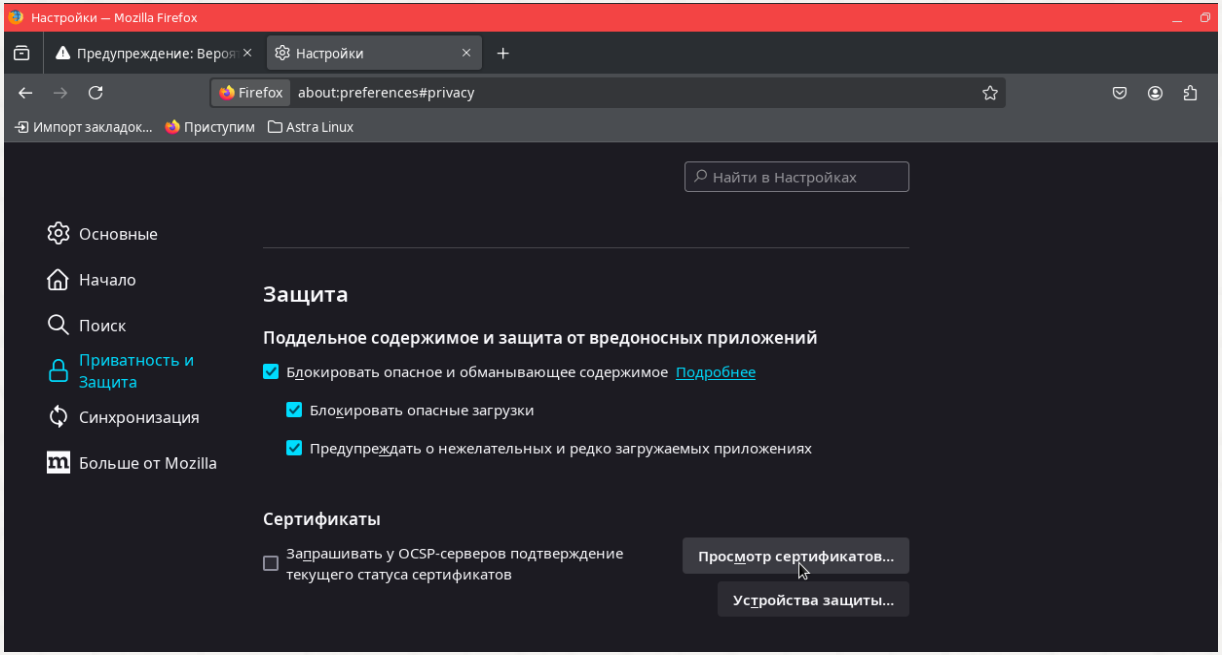
После ввода пароля, нажмите Enter и дождитесь окончания установки.


1 — Терминал
Файл Правка Вид Закладки Модули Настройка Справка
ice.
Настраивается пакет libjson-xs-perl (4.030-2+b1) …
Настраивается пакет postgresql-common (246astra3+ci1) …
su: Доступ запрещен
Creating config file /etc/postgresql-common/createcluster.conf with new version
Building PostgreSQL dictionaries from installed myspell/hunspell packages...
en_us
ru_ru
Removing obsolete dictionary files:
Created symlink /etc/systemd/system/multi-user.target.wants/postgresql.service → /lib/systemd/system/postgresql.service.
Настраивается пакет postgresql-15 (15.10-astra.se1) …
Creating new PostgreSQL cluster 15/main ...
/usr/lib/postgresql/15/bin/initdb -D /var/lib/postgresql/15/main --auth-local peer --auth-host scram-sha-256 --no-instructions
Файлы, относящиеся к этой СУБД, будут принадлежать пользователю "postgres".
От его имени также будет запускаться процесс сервера.
Кластер баз данных будет инициализирован с локалью "ru_RU.UTF-8".
Кодировка БД по умолчанию, выбранная в соответствии с настройками: "UTF8".
Выбрана конфигурация текстового поиска по умолчанию "russian".
Контроль целостности страниц данных отключён.
исправление прав для существующего каталога /var/lib/postgresql/15/main... ок
создание подкаталогов... ок
выбирается реализация динамической разделяемой памяти... posix
выбирается значение max_connections по умолчанию... 100
выбирается значение shared_buffers по умолчанию... 128MB
выбирается часовой пояс по умолчанию... Europe/Moscow
создание конфигурационных файлов... ок
выполняется подготовительный скрипт... ок
выполняется заключительная инициализация...
Ход выполнения: [92%] [.....]
1


1 — Терминал
Файл Правка Вид Закладки Модули Настройка Справка
++ '[' -z '' ']'
++ exec
++ '[' '' ']'
++ exec
++ DEBCONF_REDIR=1
++ export DEBCONF_REDIR
+ '[' -f /etc/default/komrad-waf-proxy ']'
+ . /etc/default/komrad-waf-proxy
++ WAF_PROXY_OPTS='-routes-file /etc/echelon/komrad/komrad-waf-proxy-gossopka-rules.eskip'
+ config_dir=/etc/echelon/komrad
+ config_path=/etc/echelon/komrad/komrad-waf-proxy.yaml
+ default_config_path=/etc/echelon/komrad/komrad-waf-proxy.default.yaml
+ '[' -f /etc/echelon/komrad/komrad-waf-proxy.yaml ']'
+ echo 'You may need to update the config at (/etc/echelon/komrad/komrad-waf-proxy.yaml). See the default conf
ig at /etc/echelon/komrad/komrad-waf-proxy.default.yaml'
You may need to update the config at (/etc/echelon/komrad/komrad-waf-proxy.yaml). See the default config at /e
tc/echelon/komrad/komrad-waf-proxy.default.yaml
Обрабатываются триггеры для xserver-xorg-core (2:21.1.7-1ubuntu4astra.se28+b1) …
update exec ids due to /usr/bin changed
==========
ЗАВЕРШЕННЫЙ этап: установка HTTP-прокси с помощью брандмауэра веб-
приложения/набора правил OWASP (komrad-waf-proxy)
==========
=== Установка завершена ===
echelon@astra-30099:~$
1

Установка корневого сертификата в браузере (Firefox)

Для поддержки шифрования в целях повышения безопасности необходимо импортировать сгенерированные в процессе установки сертификаты в ваш браузер.

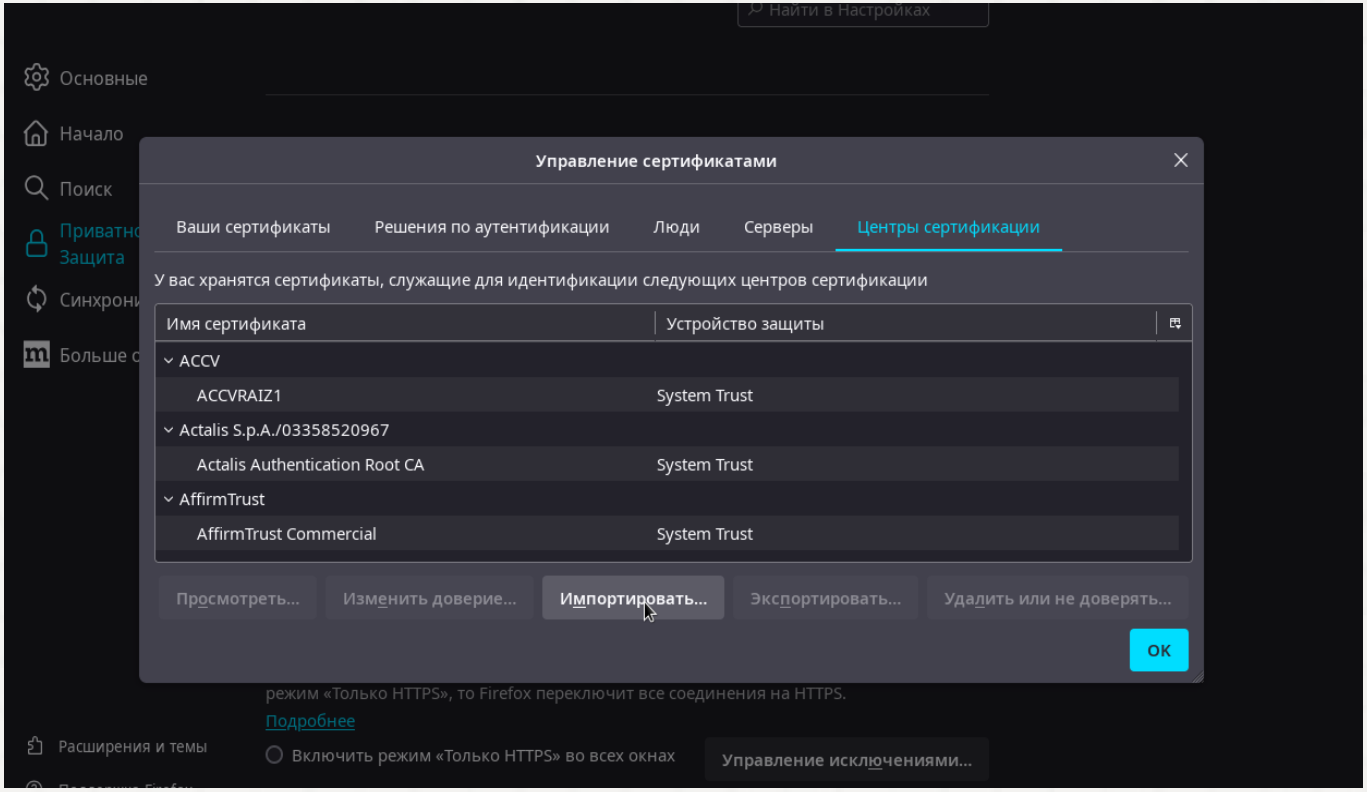


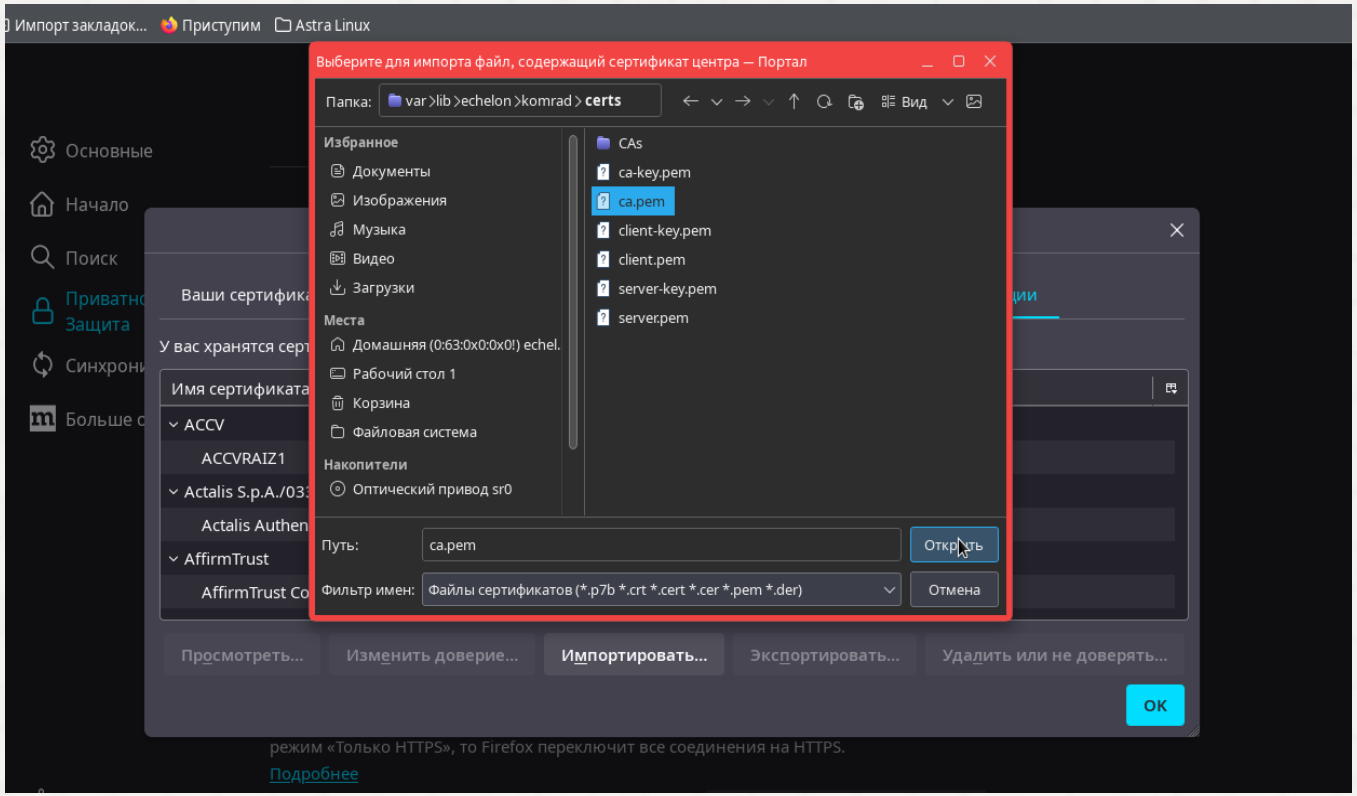
Перечень необходимых для этого действий:

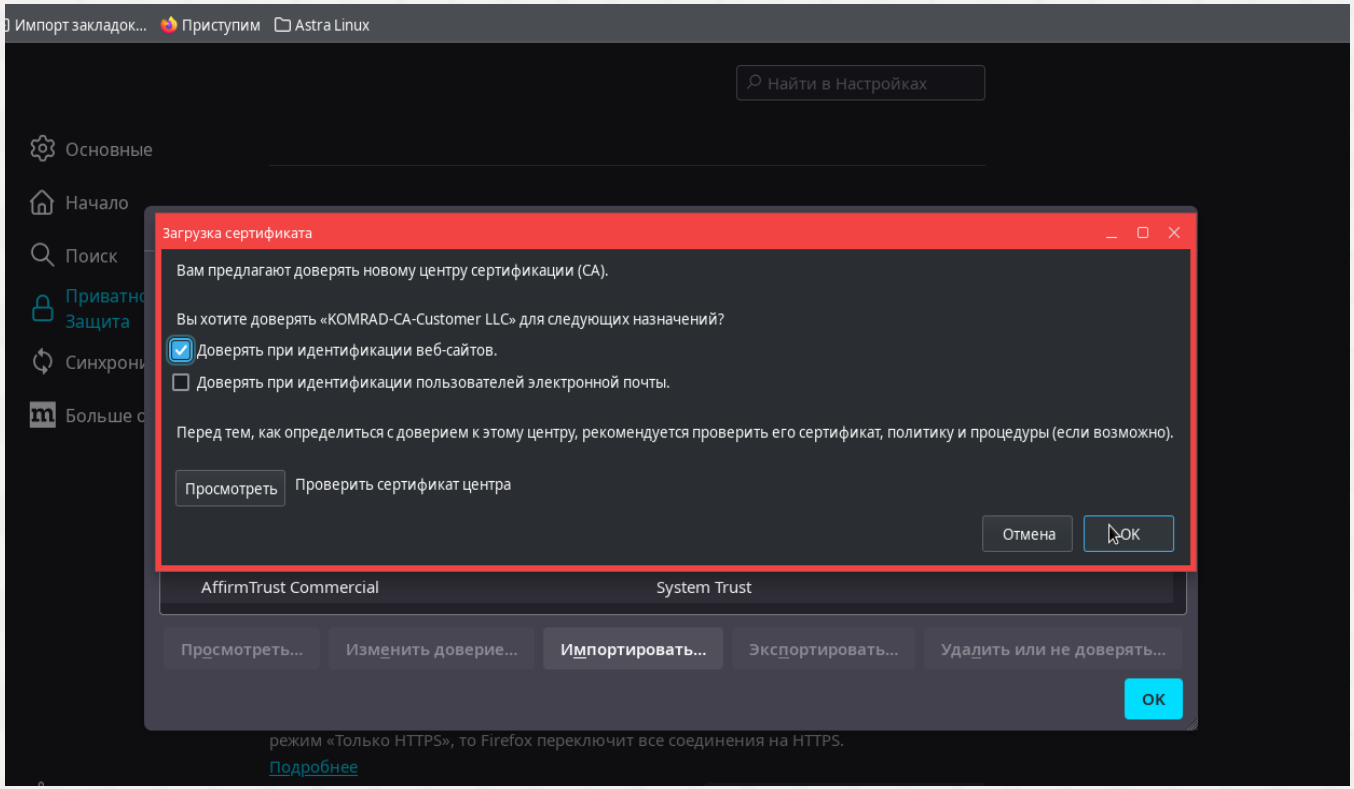
1. Скопировать сертификат ca.pem из папки и перенесите на целевую машину командой

```
sudo cp /var/lib/echelon/komrad/certs/ca.pem ./
```

2. Импортировать **ca.pem** в «Центры сертификации» вашего браузера




Импорт закладок...
Приступим
Astra Linux
Выберите для импорта файл, содержащий сертификат центра — Портал
Папка:
var > lib > echelon > komrad > certs
Вид
Избранное
Документы
Изображения
Музыка
Видео
Загрузки
Места
Домашняя (0:63:0x0:0x0!) echel.
Рабочий стол 1
Корзина
Файловая система
Накопители
Оптический привод sr0
CAs
ca-key.pem
ca.pem
client-key.pem
client.pem
server-key.pem
server.pem
Путь:
ca.pem
Открыть
Фильтр имен:
Файлы сертификатов (*.p7b *.crt *.cert *.cer *.pem *.der)
Отмена
Основные
Начало
Поиск
Защита
Синхрони
Больше
Имя сертификата
ACCV
ACCVRAIZ1
Actalis S.p.A./03
Actalis Authen
AffirmTrust
AffirmTrust Co
Просмотреть...
Изменить доверие...
Импортировать...
Экспортировать...
Удалить или не доверять...
OK
режим «Только HTTPS», то Firefox переключит все соединения на HTTPS.
Подробнее



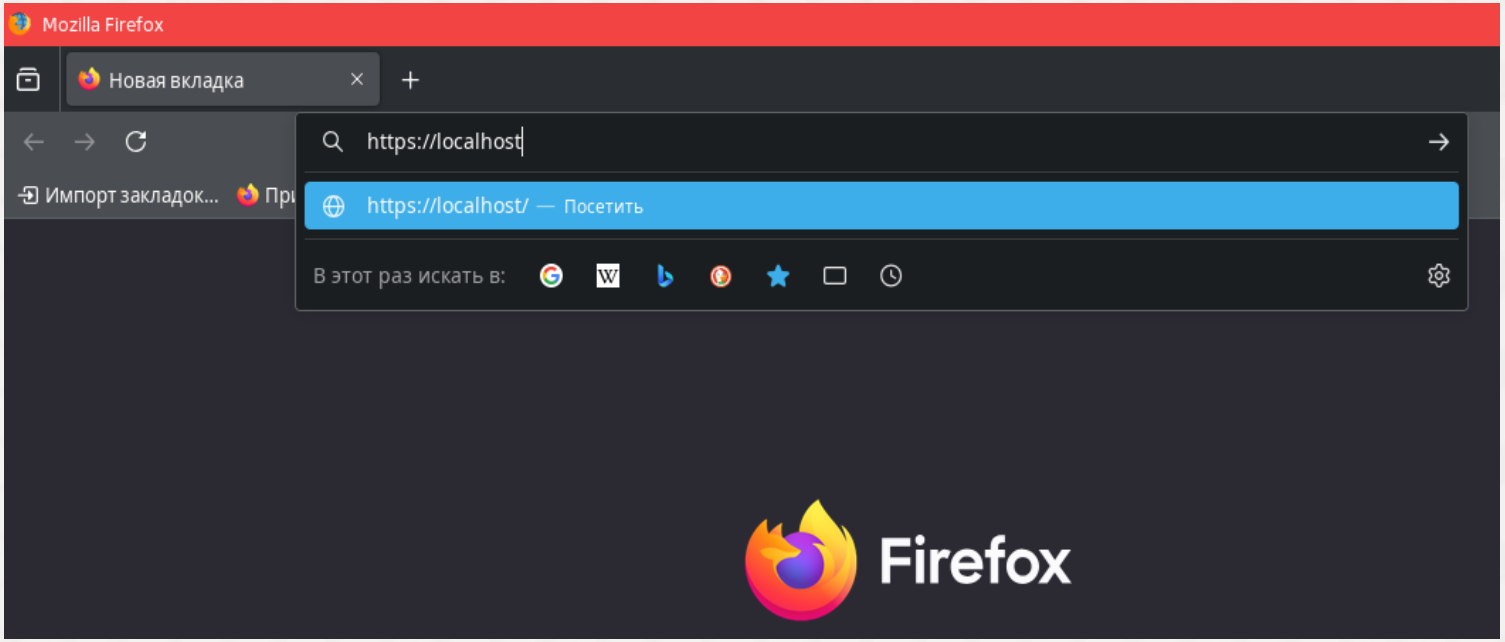
3. Перезапустить браузер

ПОДСКАЗКА

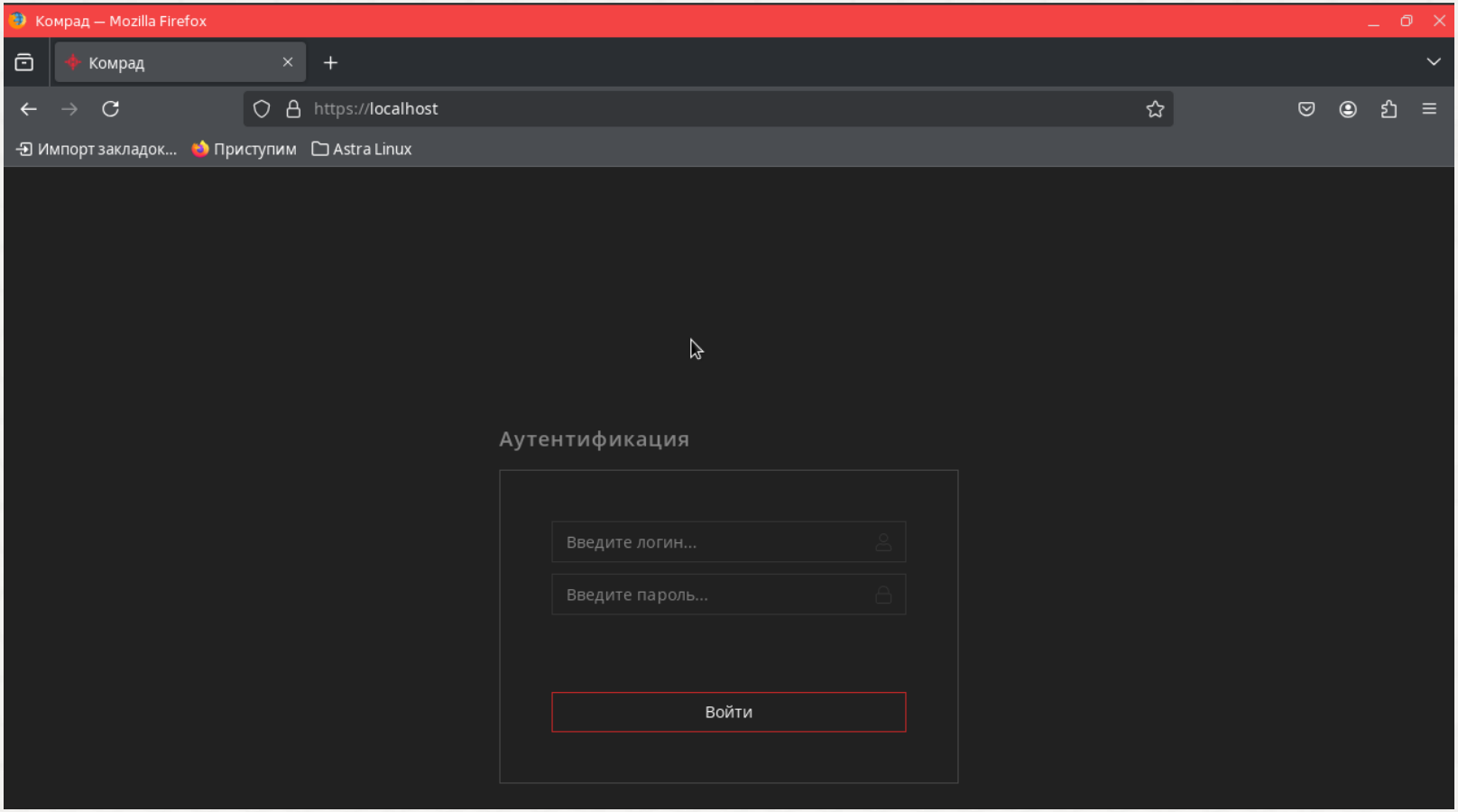
Вы можете выполнить вход без импорта сертификатов, но это будет менее безопасно.

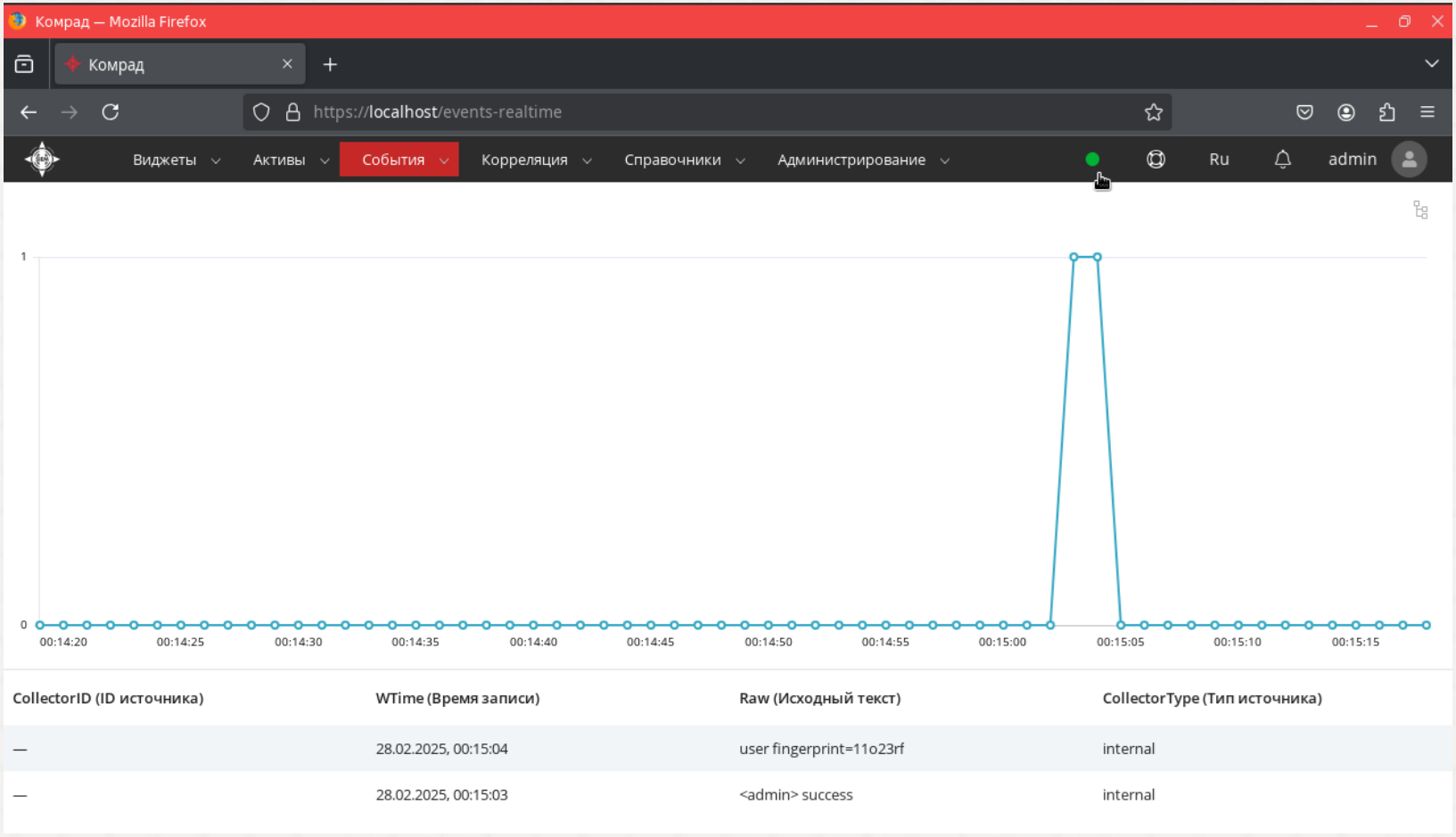
Проверка работоспособности

KOMRAD установлен и доступен по адресу **https://localhost**



Проверьте работоспособность системы.


Комрад — Mozilla Firefox
Комрад
https://localhost
Импорт закладок...
Приступим
Astra Linux
Аутентификация
Введите логин...
Введите пароль...
Войти



CollectorID (ID источника)	WTime (Время записи)	Raw (Исходный текст)	CollectorType (Тип источника)
—	28.02.2025, 00:15:04	user fingerprint=11o23rf	internal
—	28.02.2025, 00:15:03	<admin> success	internal

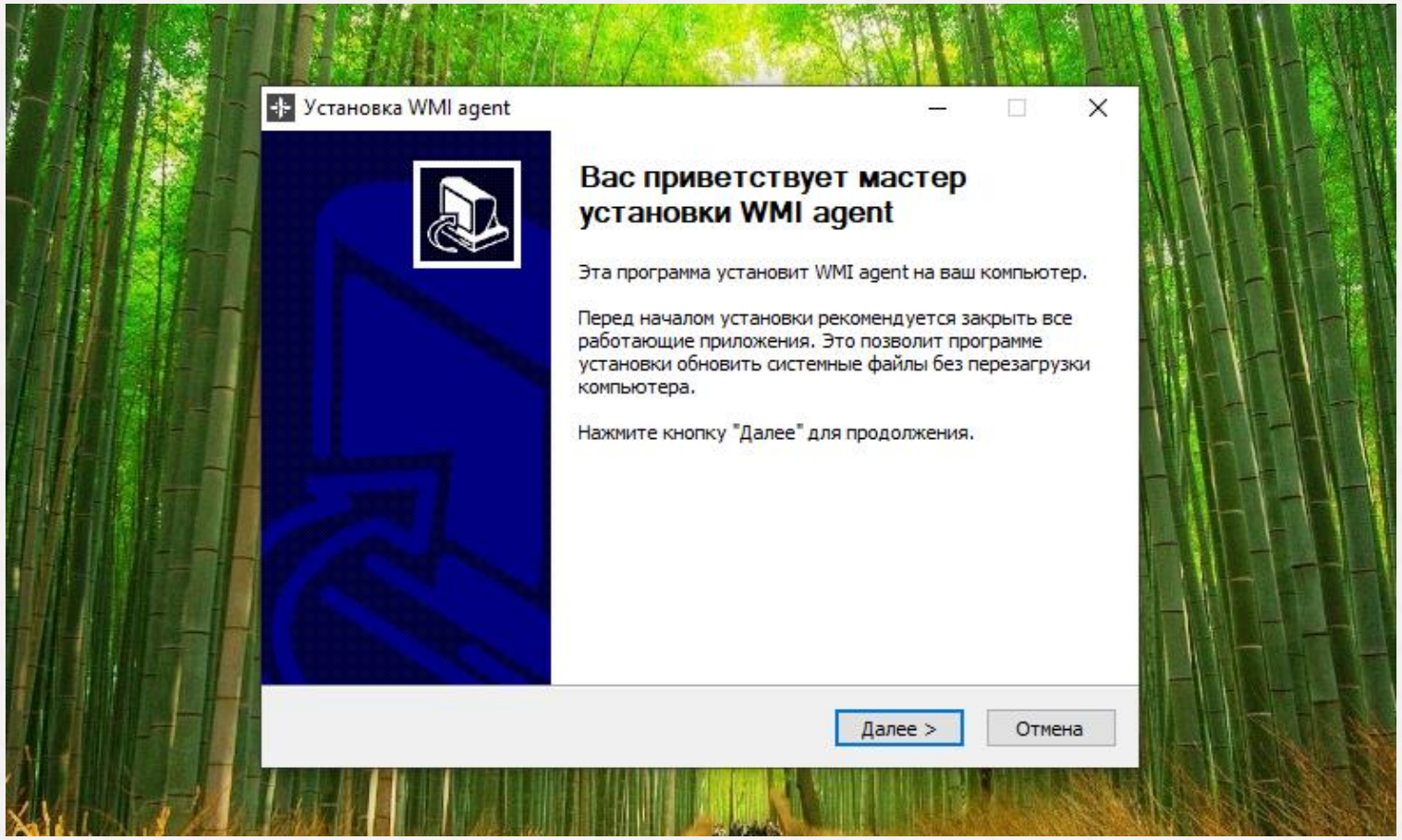
Установка WMI-агента

Для установки wmi-агента на windows – необходимо:

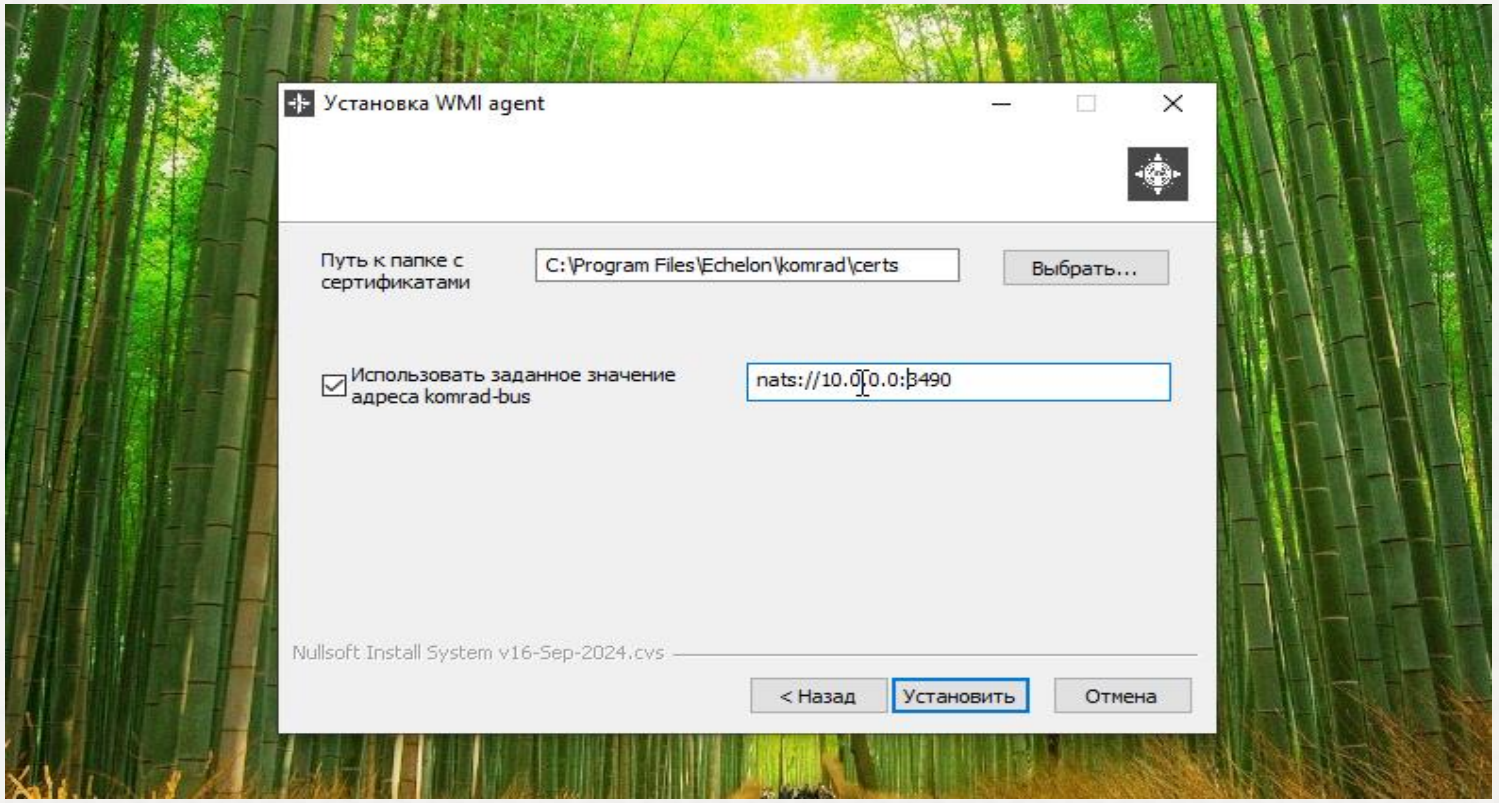
1. Скопировать сертификаты на целевую машину
   Копируем сертификаты с машины где установили KOMRAD
   на целевую машину (где устанавливаем WMI-агент)
   при помощи ssh или другими средствами.

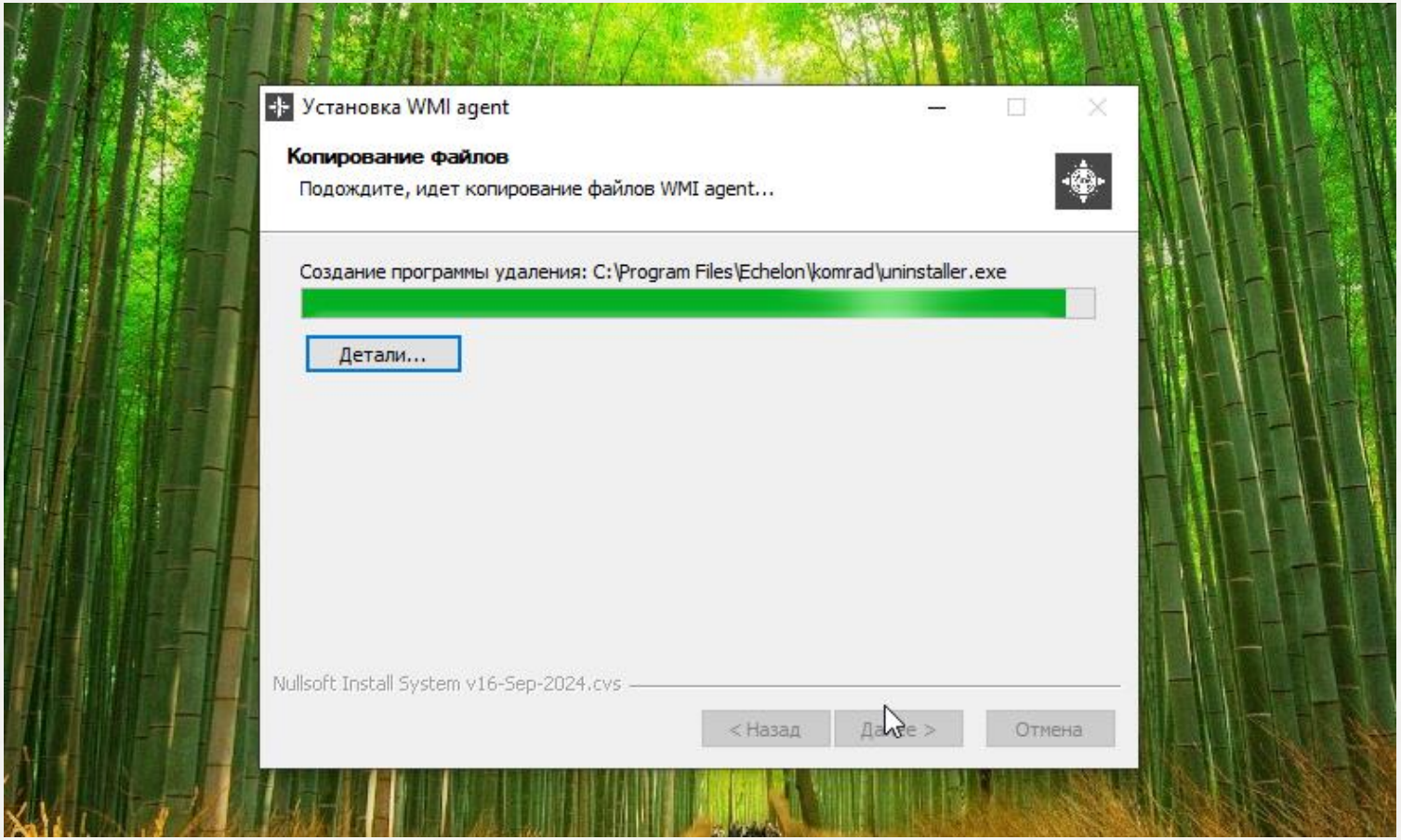
```
scp -r /var/lib/echelon/komrad/certs/ user@127.0.0.1:~/
```

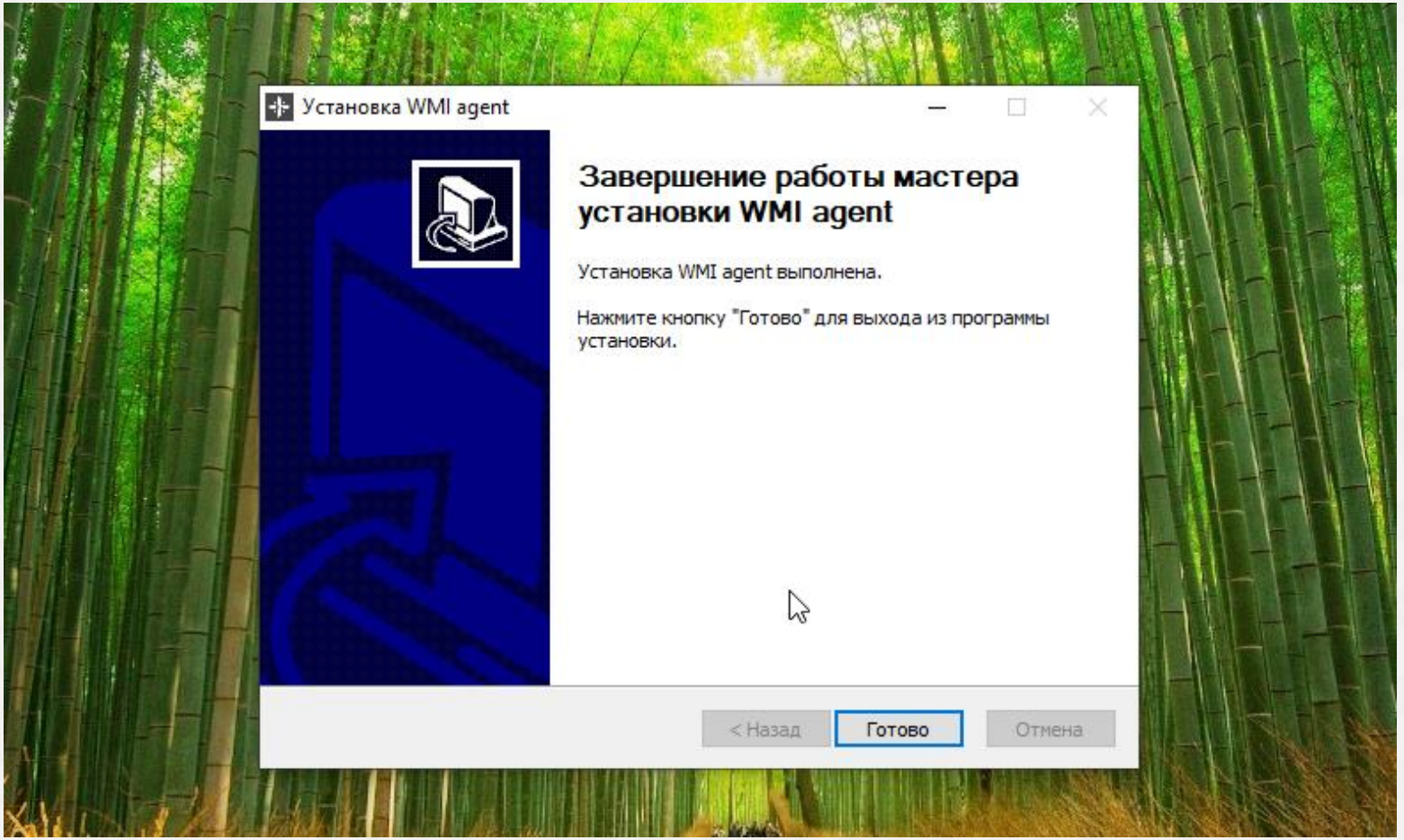
2. Запустить от имени администратора файл инсталлятора
   komrad_v4.5.22-demo_windows_amd64_wmi-installer.exe


Установка WMI agent
Вас приветствует мастер установки WMI agent
Эта программа установит WMI agent на ваш компьютер.
Перед началом установки рекомендуется закрыть все работающие приложения. Это позволит программе установки обновить системные файлы без перезагрузки компьютера.
Нажмите кнопку "Далее" для продолжения.
Далее >
Отмена

3. Указать путь до сертификатов и адрес komrad-bus
   Указать путь до сертификатов, которые скопированы по п.1
   Адрес komrad-bus – ip адрес машины на которой установлен KOMRAD




Установка WMI agent
Копирование файлов
Подождите, идет копирование файлов WMI agent...
Создание программы удаления: C:\Program Files\Echelon\komrad\uninstaller.exe
Детали...
Nullsoft Install System v16-Sep-2024.cvs
< Назад
Далее >
Отмена


Установка WMI agent
Завершение работы мастера установки WMI agent
Установка WMI agent выполнена.
Нажмите кнопку "Готово" для выхода из программы установки.
< Назад
Готово
Отмена

Проверка успешной установки и соединения с KOMRAD Enterprise SIEM