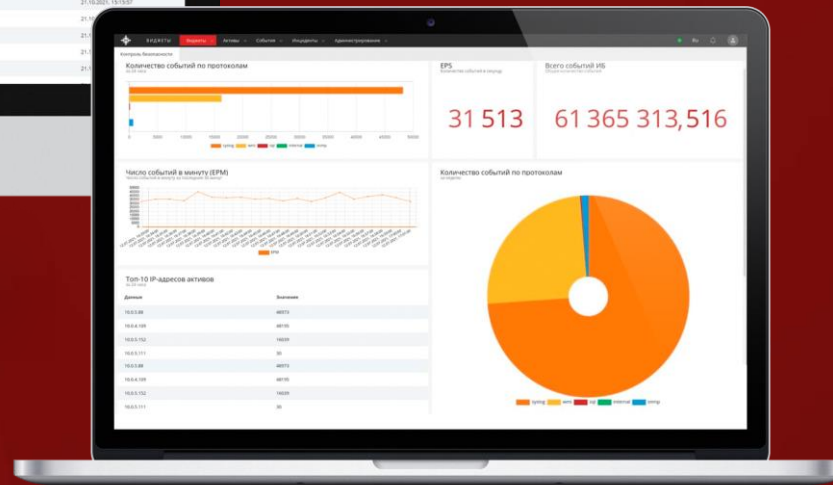
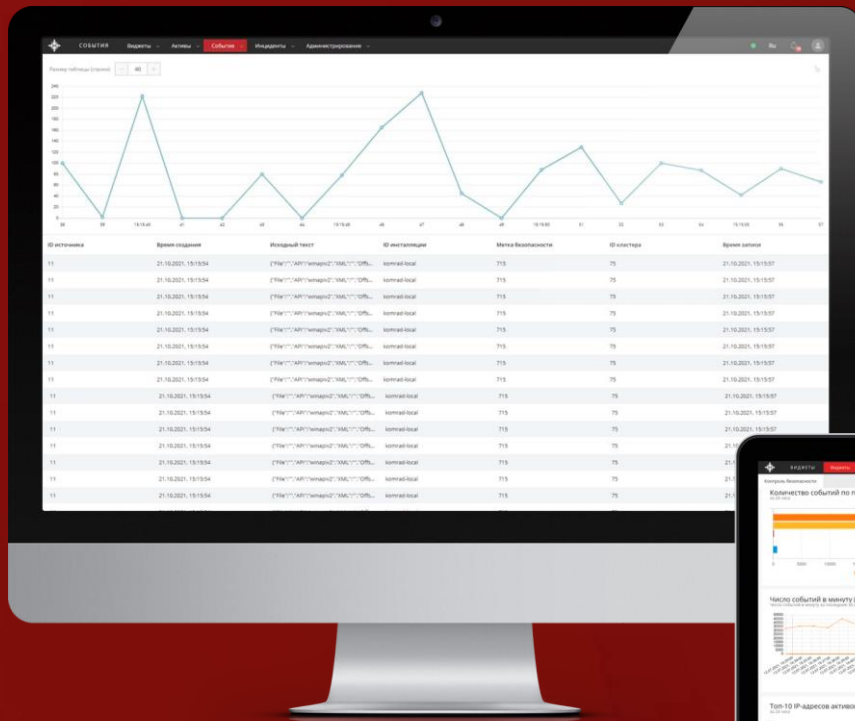


KOMRAD Enterprise SIEM

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	4
Установка с помощью инсталлятора в автоматическом режиме.....	5
Подготовка установщика	5
Запуск установщика	5
Определение IP.....	7
Создание сертификатов	8
Установка корневого сертификата в браузере (Firefox).....	10
Проверка работоспособности	13
Установка WMI-агента.....	15

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

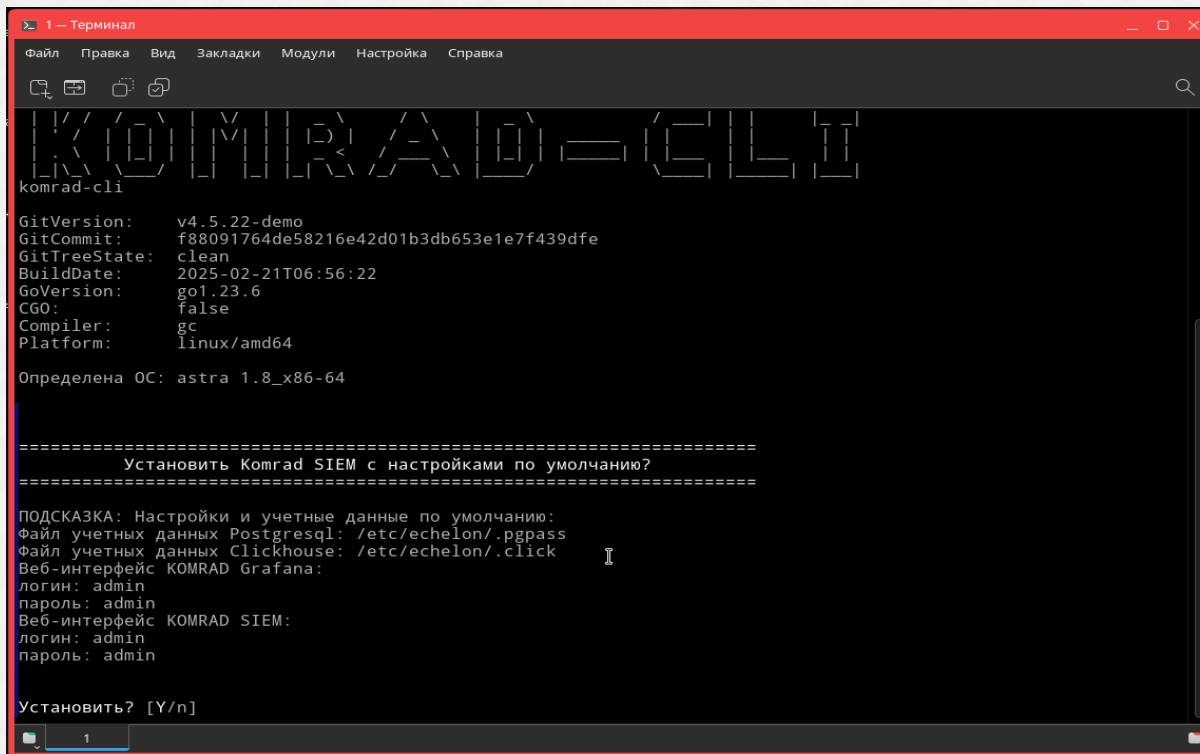
```
sudo ./komrad_v4.5.22-demo_astra_1.8_amd64.run
```

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.



```
1 — Терминал
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка

KOMRAD@-CLI
komrad-cli
GitVersion:      v4.5.22-demo
GitCommit:       f88091764de58216e42d01b3db653e1e7f439dfe
GitTreeState:    clean
BuildDate:       2025-02-21T06:56:22
GoVersion:       go1.23.6
CGO:             false
Compiler:        gc
Platform:        linux/amd64

Определена ОС: astra 1.8_x86-64

=====
      Установить Komrad SIEM с настройками по умолчанию?
=====

ПОДСКАЗКА: Настройки и учетные данные по умолчанию:
Файл учетных данных Postgresql: /etc/echelon/.pgpass
Файл учетных данных Clickhouse: /etc/echelon/.click
Веб-интерфейс KOMRAD Grafana:
логин: admin
пароль: admin
Веб-интерфейс KOMRAD SIEM:
логин: admin
пароль: admin

Установить? [Y/n]
```

ПОДСКАЗКА

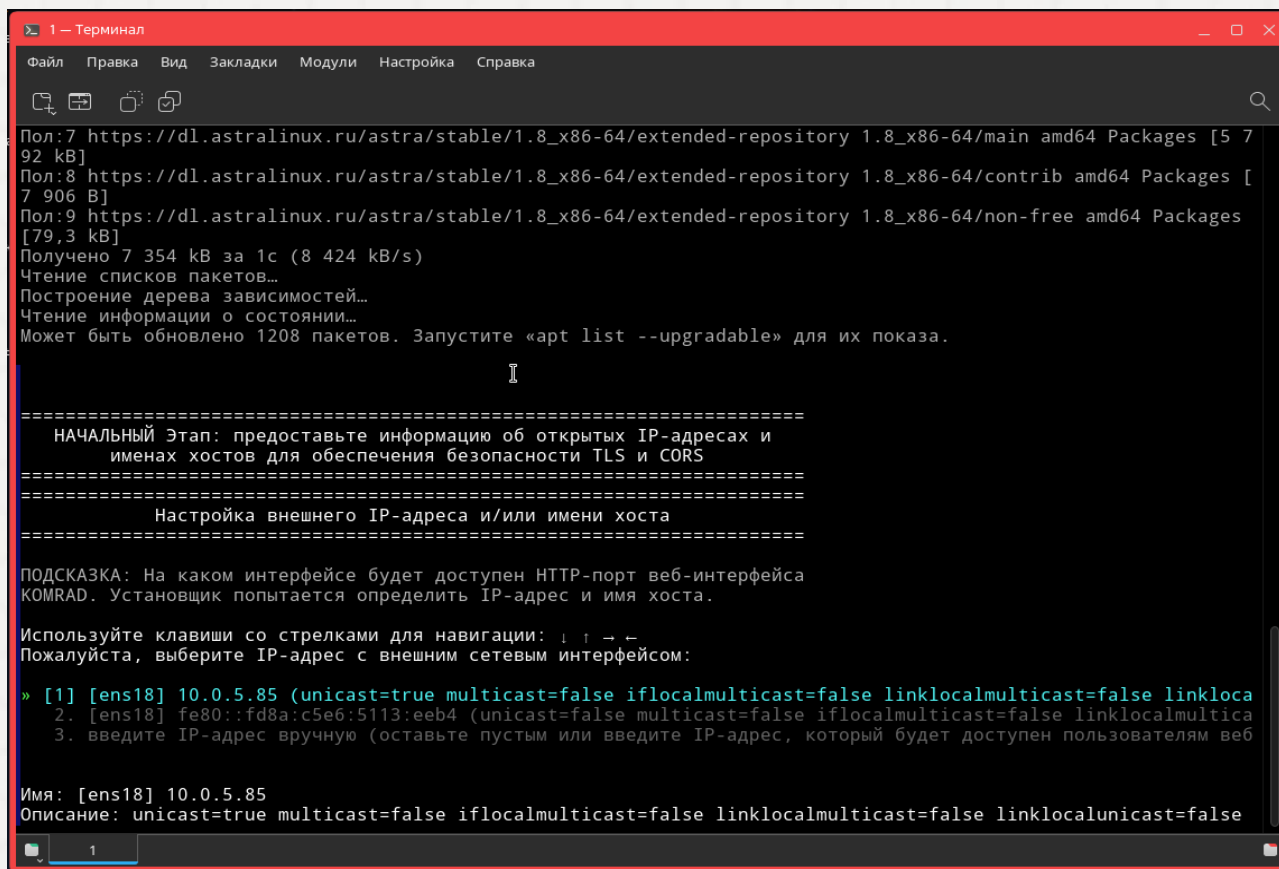
Если в процессе установки KOMRAD установщик выдаст ошибку и выйдет из диалога, то запустите его повторно для продолжения установки:

```
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.



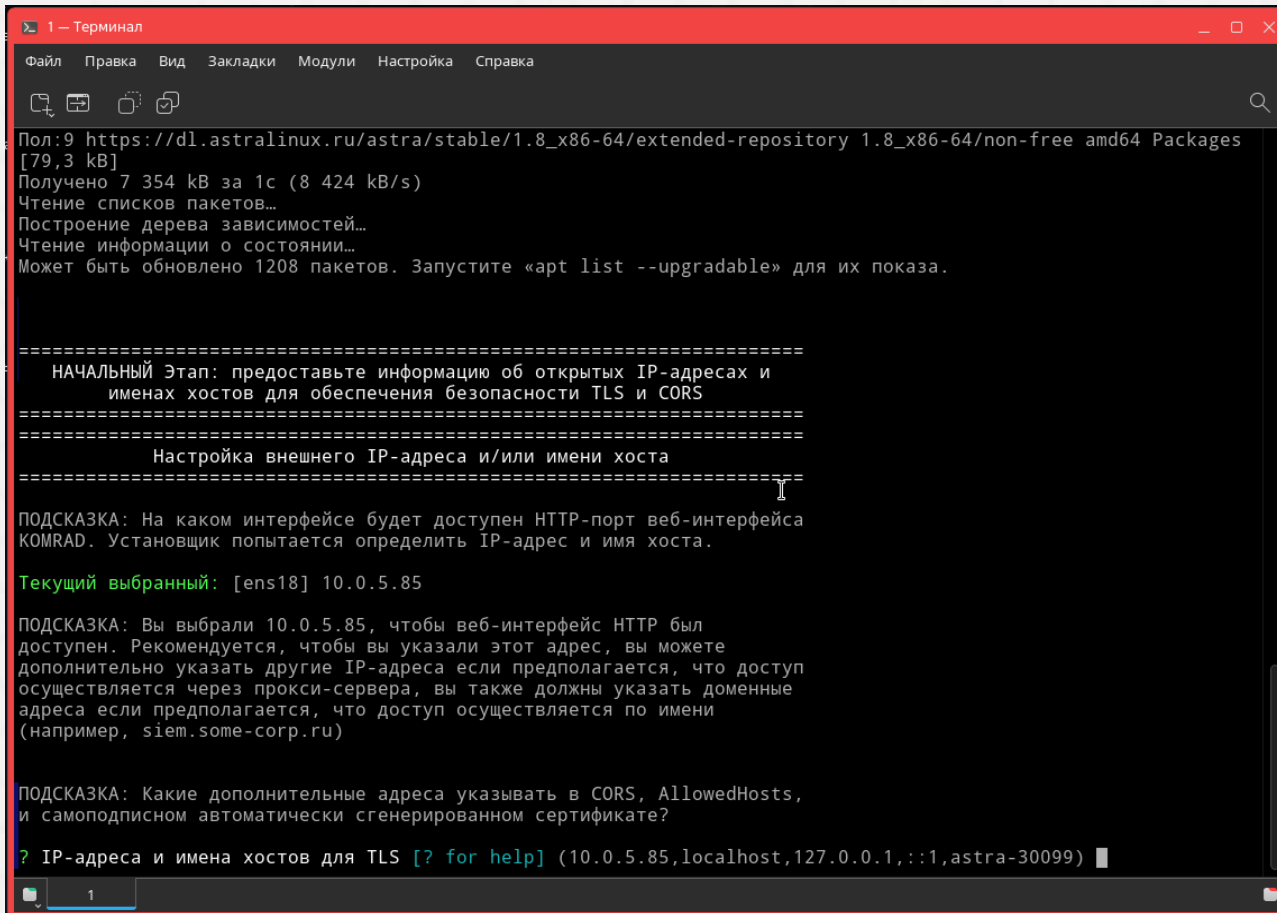
```
1 — Терминал
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка
Пол:7 https://dl.astralinux.ru/astra/stable/1.8_x86-64/extended-repository 1.8_x86-64/main amd64 Packages [5 7
92 kB]
Пол:8 https://dl.astralinux.ru/astra/stable/1.8_x86-64/extended-repository 1.8_x86-64/contrib amd64 Packages [
7 906 B]
Пол:9 https://dl.astralinux.ru/astra/stable/1.8_x86-64/extended-repository 1.8_x86-64/non-free amd64 Packages
[79,3 kB]
Получено 7 354 kB за 1с (8 424 kB/s)
Чтение списков пакетов...
Построение дерева зависимостей...
Чтение информации о состоянии...
Может быть обновлено 1208 пакетов. Запустите «apt list --upgradable» для их показа.

=====
НАЧАЛЬНЫЙ Этап: предоставьте информацию об открытых IP-адресах и
именах хостов для обеспечения безопасности TLS и CORS
=====
Настройка внешнего IP-адреса и/или имени хоста
=====
ПОДСКАЗКА: На каком интерфейсе будет доступен HTTP-порт веб-интерфейса
KOMRAD. Установщик попытается определить IP-адрес и имя хоста.
Используйте клавиши со стрелками для навигации: ↑ ↓ ← →
Пожалуйста, выберите IP-адрес с внешним сетевым интерфейсом:

» [1] [ens18] 10.0.5.85 (unicast=true multicast=false iflocalmulticast=false linklocalmulticast=false linkloca
2. [ens18] fe80::fd8a:c5e6:5113:eeb4 (unicast=false multicast=false iflocalmulticast=false linklocalmultica
3. введите IP-адрес вручную (оставьте пустым или введите IP-адрес, который будет доступен пользователям веб

Имя: [ens18] 10.0.5.85
Описание: unicast=true multicast=false iflocalmulticast=false linklocalmulticast=false linklocalunicast=false
```

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



```
1 — Терминал
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка
Пол:9 https://dl.astralinux.ru/astra/stable/1.8_x86-64/extended-repository 1.8_x86-64/non-free amd64 Packages
[79,3 kB]
Получено 7 354 kB за 1с (8 424 kB/s)
Чтение списков пакетов...
Построение дерева зависимостей...
Чтение информации о состоянии...
Может быть обновлено 1208 пакетов. Запустите «apt list --upgradable» для их показа.

=====
НАЧАЛЬНЫЙ Этап: предоставьте информацию об открытых IP-адресах и
именах хостов для обеспечения безопасности TLS и CORS
=====
Настройка внешнего IP-адреса и/или имени хоста
=====
ПОДСКАЗКА: На каком интерфейсе будет доступен HTTP-порт веб-интерфейса
KOMRAD. Установщик попытается определить IP-адрес и имя хоста.

Текущий выбранный: [ens18] 10.0.5.85

ПОДСКАЗКА: Вы выбрали 10.0.5.85, чтобы веб-интерфейс HTTP был
доступен. Рекомендуется, чтобы вы указали этот адрес, вы можете
дополнительно указать другие IP-адреса если предполагается, что доступ
осуществляется через прокси-сервера, вы также должны указать доменные
адреса если предполагается, что доступ осуществляется по имени
(например, siem.some-corp.ru)

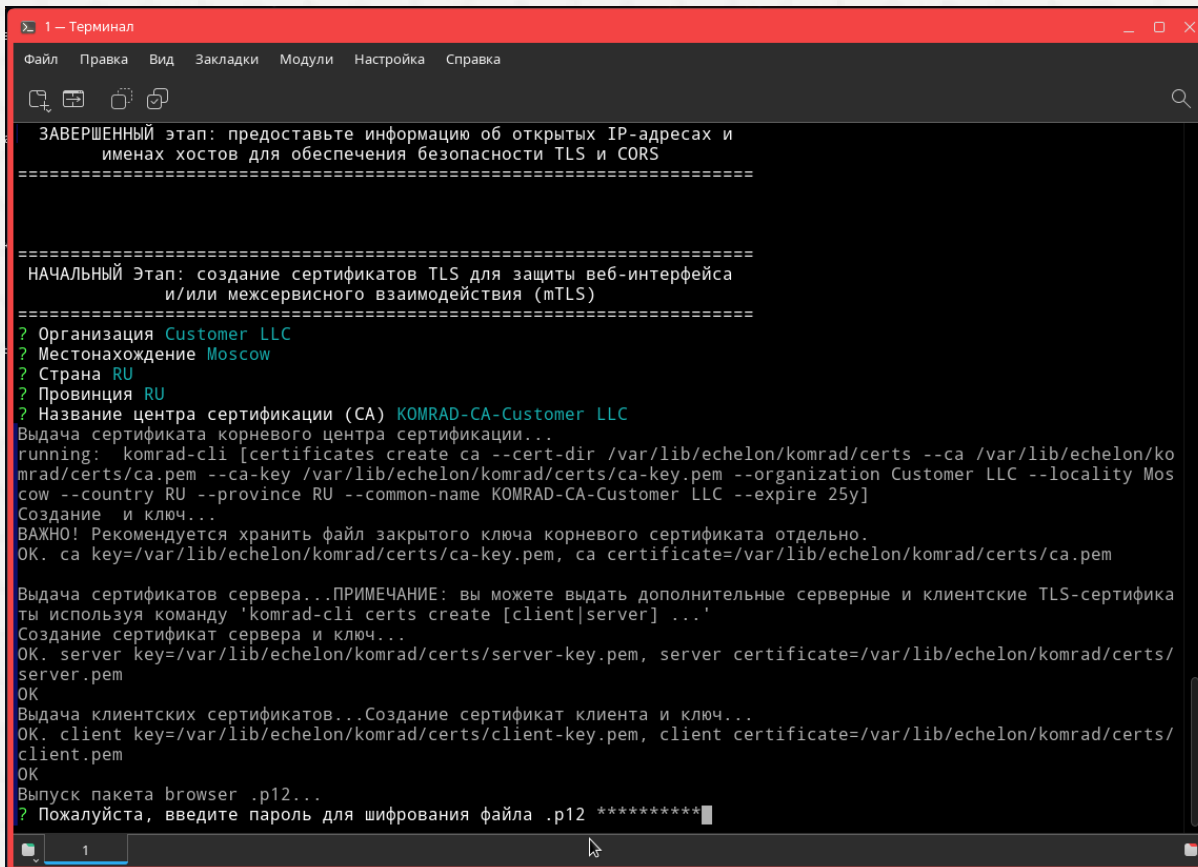
ПОДСКАЗКА: Какие дополнительные адреса указывать в CORS, AllowedHosts,
и самоподписном автоматически сгенерированном сертификате?

? IP-адреса и имена хостов для TLS [? for help] (10.0.5.85,localhost,127.0.0.1,::1,astra-30099) █
```


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.



```
1 — Терминал
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка

ЗАВЕРШЕННЫЙ этап: предоставьте информацию об открытых IP-адресах и
именах хостов для обеспечения безопасности TLS и CORS
=====

НАЧАЛЬНЫЙ Этап: создание сертификатов TLS для защиты веб-интерфейса
и/или межсервисного взаимодействия (mTLS)
=====
? Организация Customer LLC
? Местонахождение Moscow
? Страна RU
? Провинция RU
? Название центра сертификации (CA) KOMRAD-CA-Customer LLC
Выдача сертификата корневого центра сертификации...
running: komrad-cli [certificates create ca --cert-dir /var/lib/echelon/komrad/certs --ca /var/lib/echelon/ko
mrad/certs/ca.pem --ca-key /var/lib/echelon/komrad/certs/ca-key.pem --organization Customer LLC --locality Mos
cow --country RU --province RU --common-name KOMRAD-CA-Customer LLC --expire 25y]
Создание и ключ...
ВАЖНО! Рекомендуется хранить файл закрытого ключа корневого сертификата отдельно.
OK. ca key=/var/lib/echelon/komrad/certs/ca-key.pem, ca certificate=/var/lib/echelon/komrad/certs/ca.pem

Выдача сертификатов сервера...ПРИМЕЧАНИЕ: вы можете выдать дополнительные серверные и клиентские TLS-сертифика
ты используя команду 'komrad-cli certs create [client|server] ...'
Создание сертификат сервера и ключ...
OK. server key=/var/lib/echelon/komrad/certs/server-key.pem, server certificate=/var/lib/echelon/komrad/certs/
server.pem
OK
Выдача клиентских сертификатов...Создание сертификат клиента и ключ...
OK. client key=/var/lib/echelon/komrad/certs/client-key.pem, client certificate=/var/lib/echelon/komrad/certs/
client.pem
OK
Выпуск пакета browser .p12...
? Пожалуйста, введите пароль для шифрования файла .p12 *****
```

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.sel) ...
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".

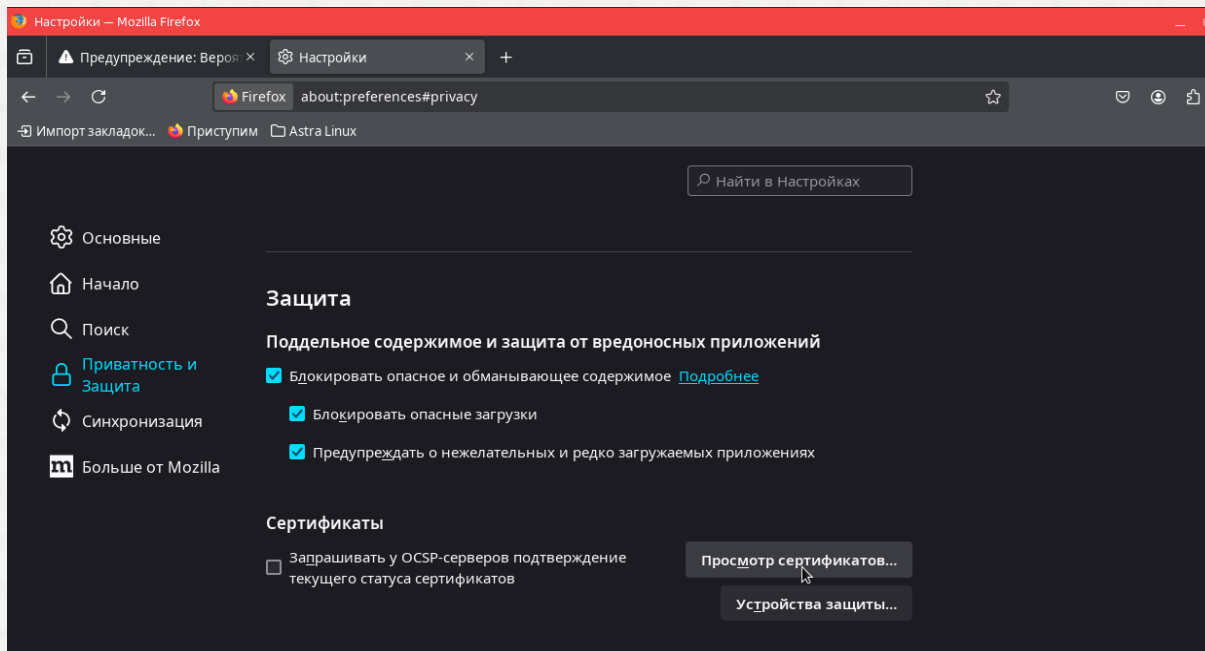
Контроль целостности страниц данных отключён.

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 – Терминал
Файл  Правка  Вид  Закладки  Модули  Настройка  Справка
[Icons] [Search]
++ '[' -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 config 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 /etc/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)
=====
[Stylized ASCII art logo]
=== Установка завершена ===
echelon@astra-30099:~$
```

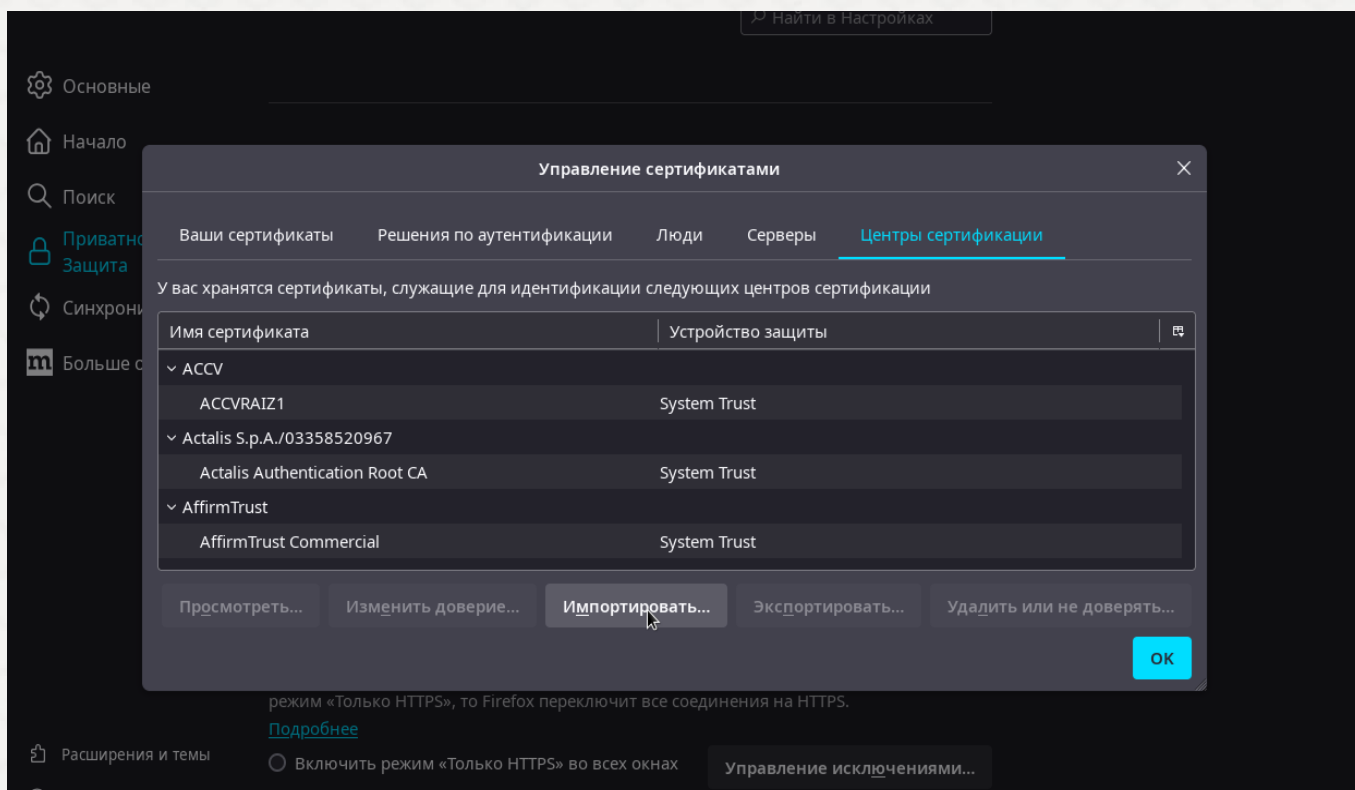
Установка корневого сертификата в браузере (Firefox)

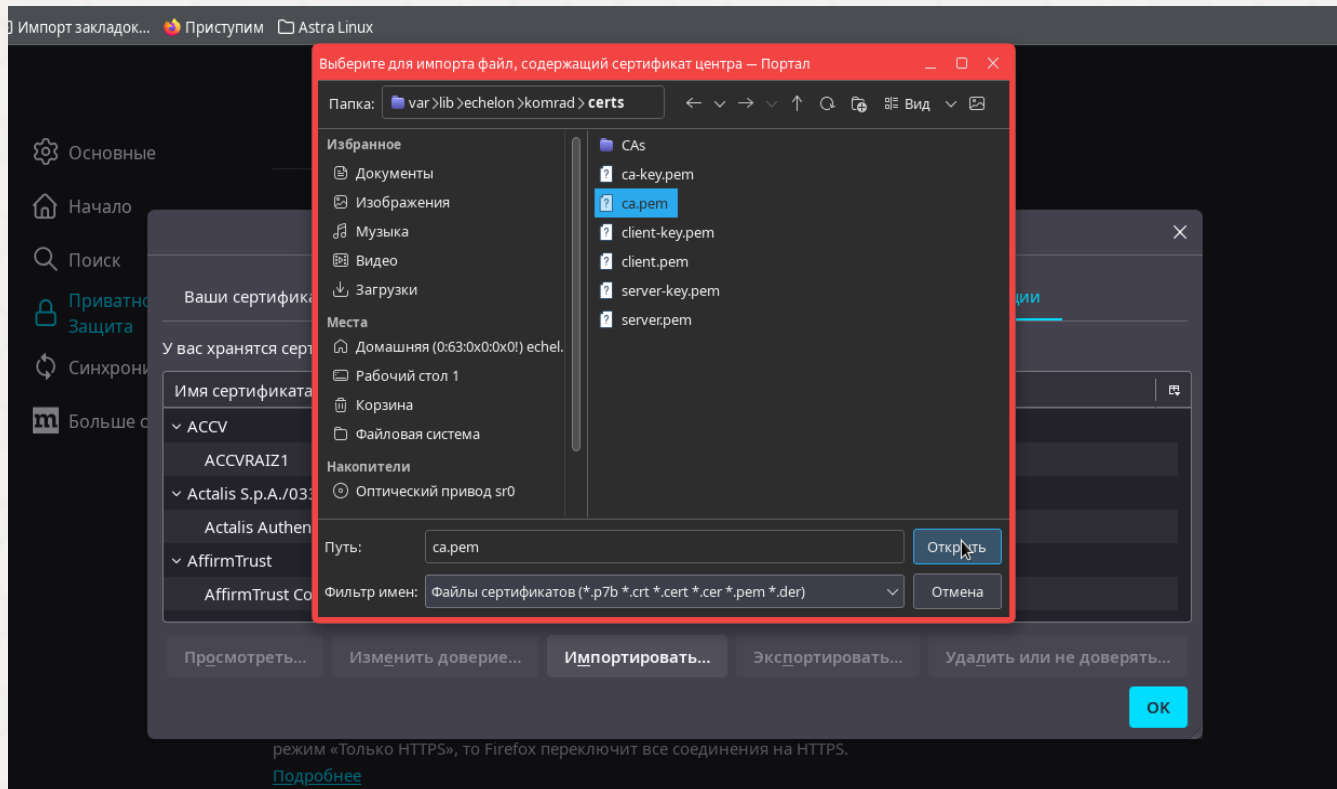
Для поддержки шифрования в целях повышения безопасности необходимо импортировать сгенерированные в процессе установки сертификаты в ваш браузер.

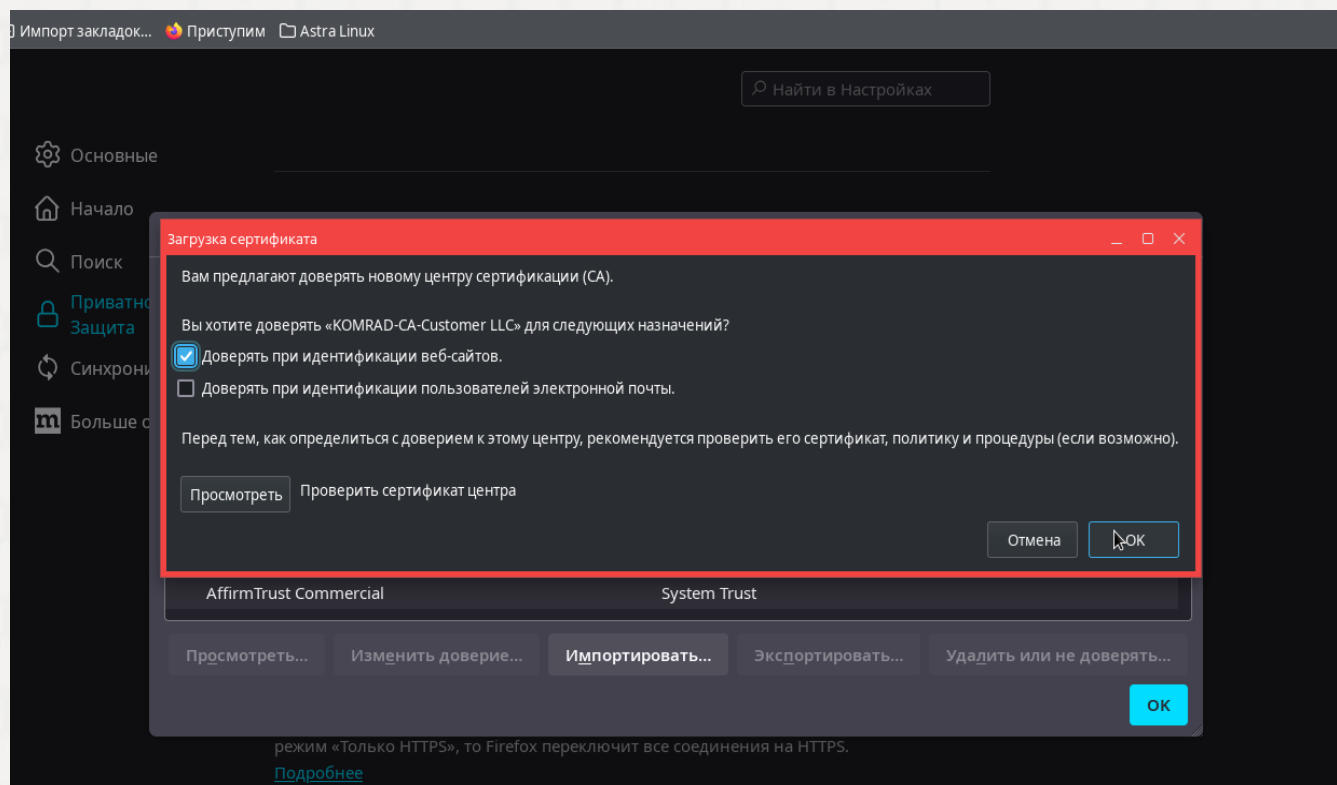


Перечень необходимых для этого действий:

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







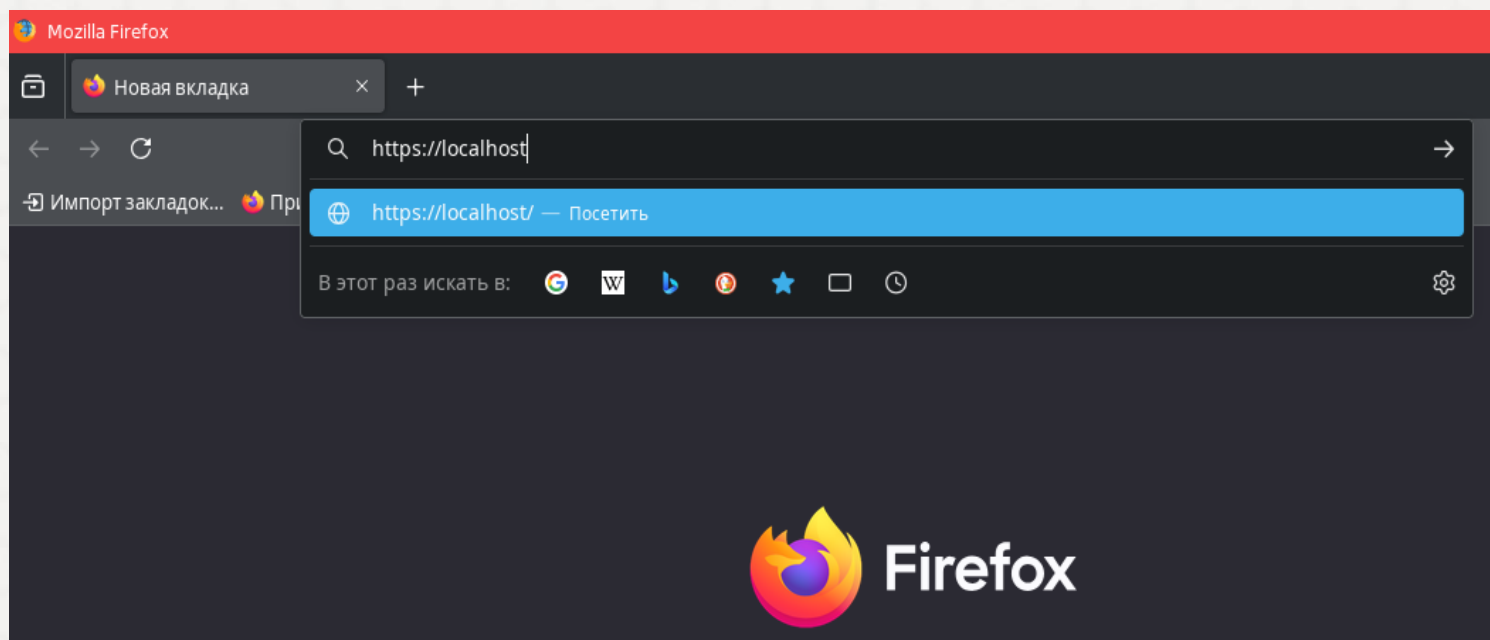
3. Перезапустить браузер

ПОДСКАЗКА

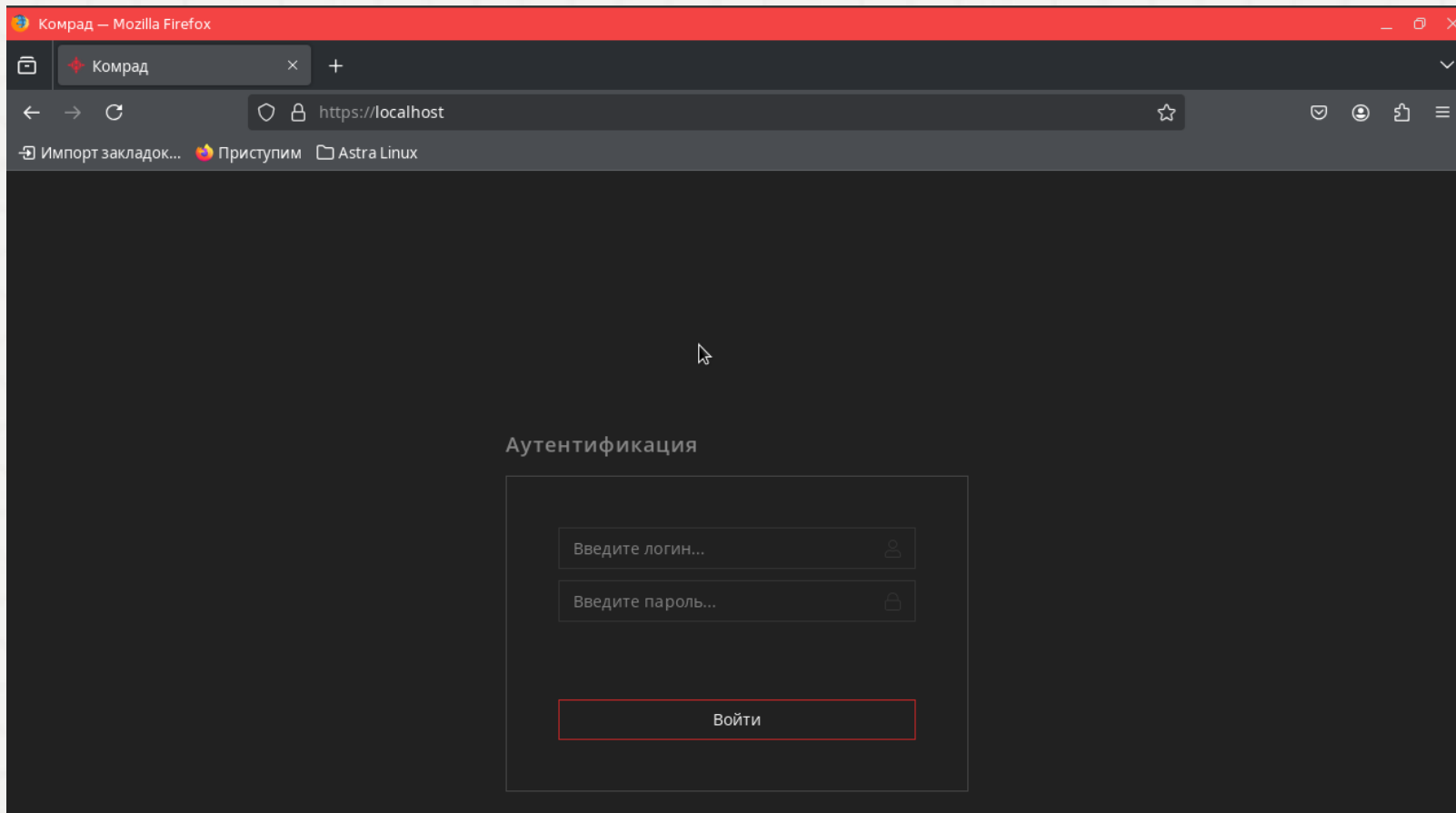
Вы можете выполнить вход без импорта сертификатов, но это будет менее безопасно.

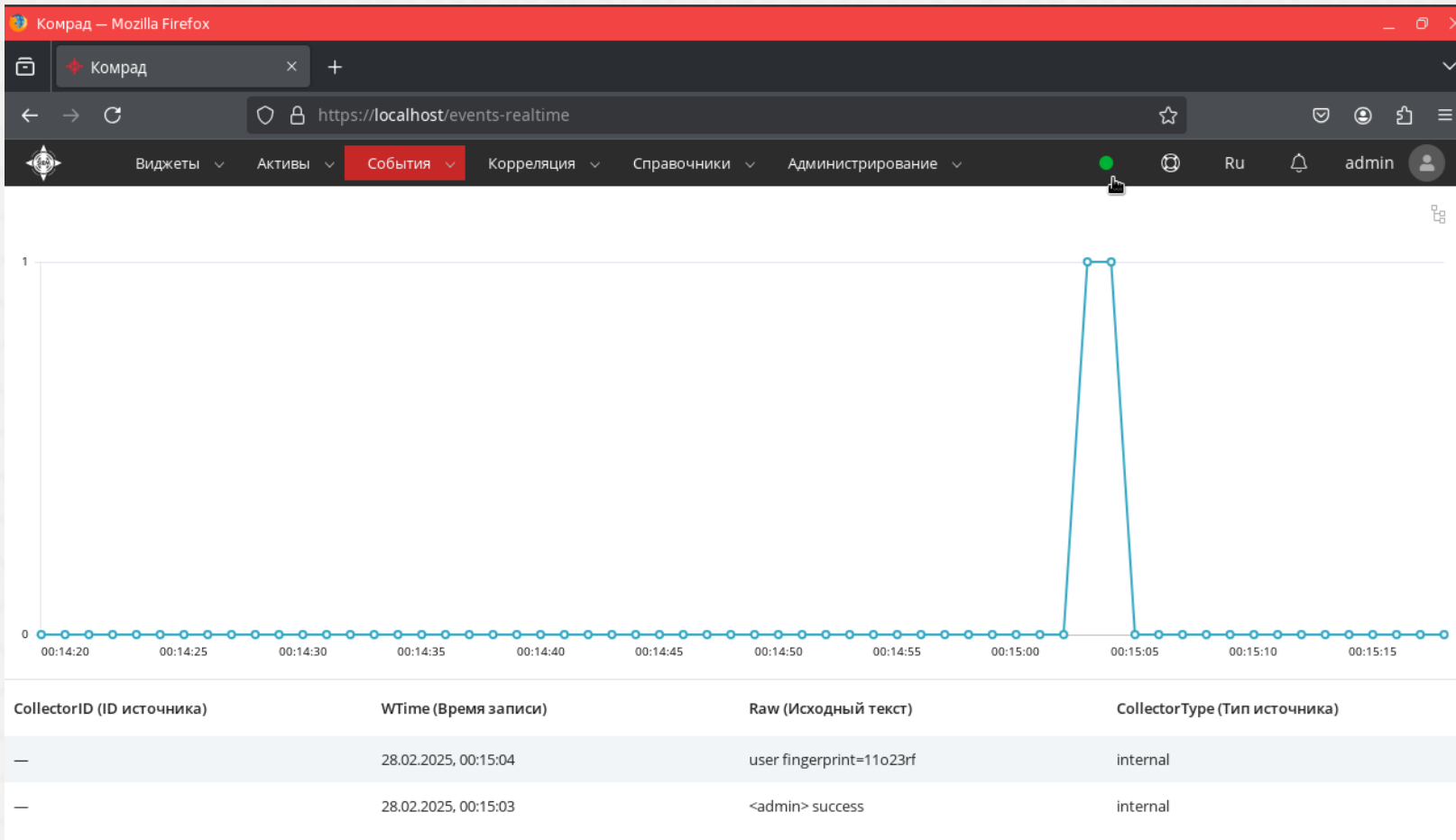
Проверка работоспособности

KOMRAD установлен и доступен по адресу <https://localhost>



Проверьте работоспособность системы.





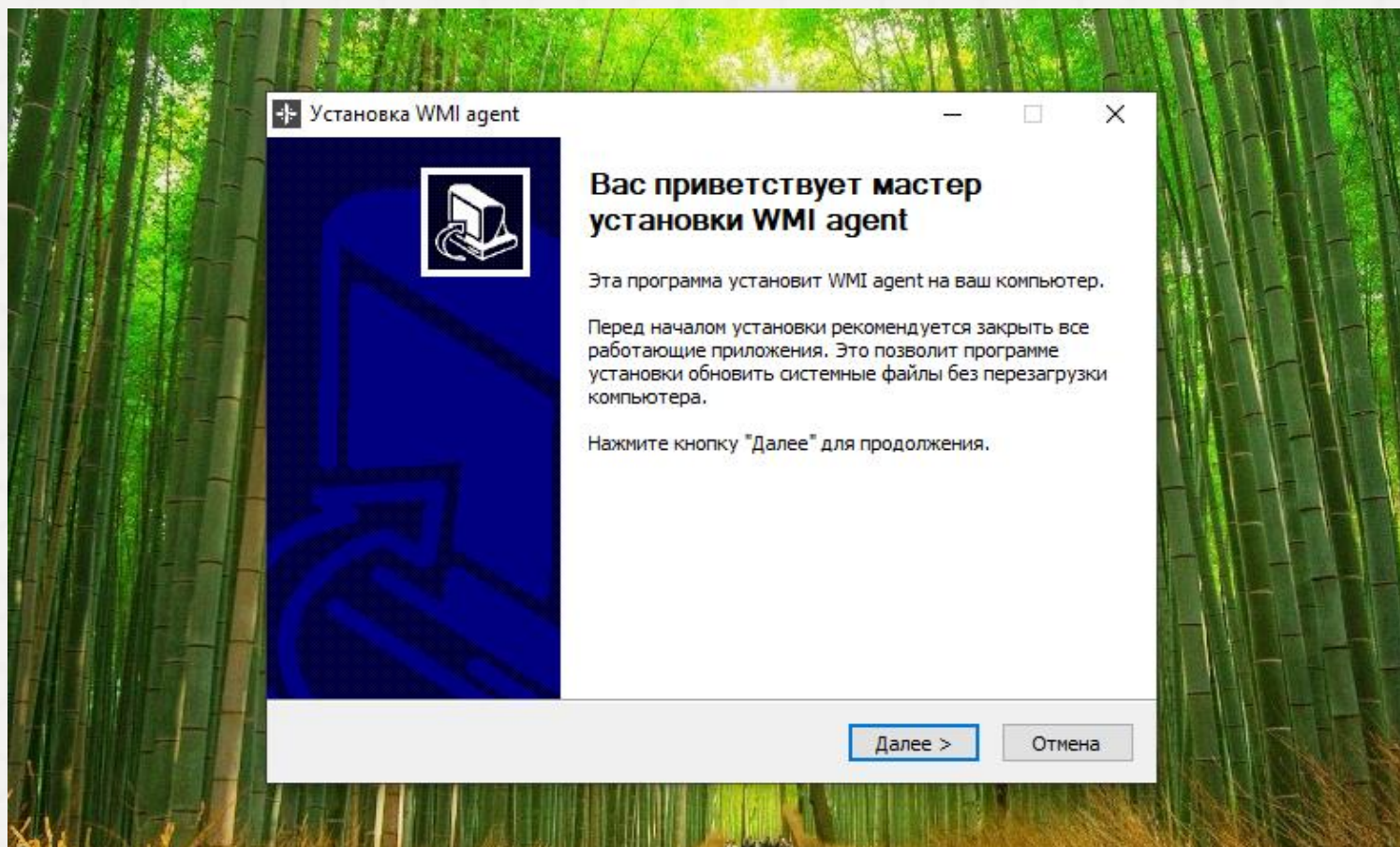
Установка WMI-агента

Для установки wmi-агента на windows – необходимо:

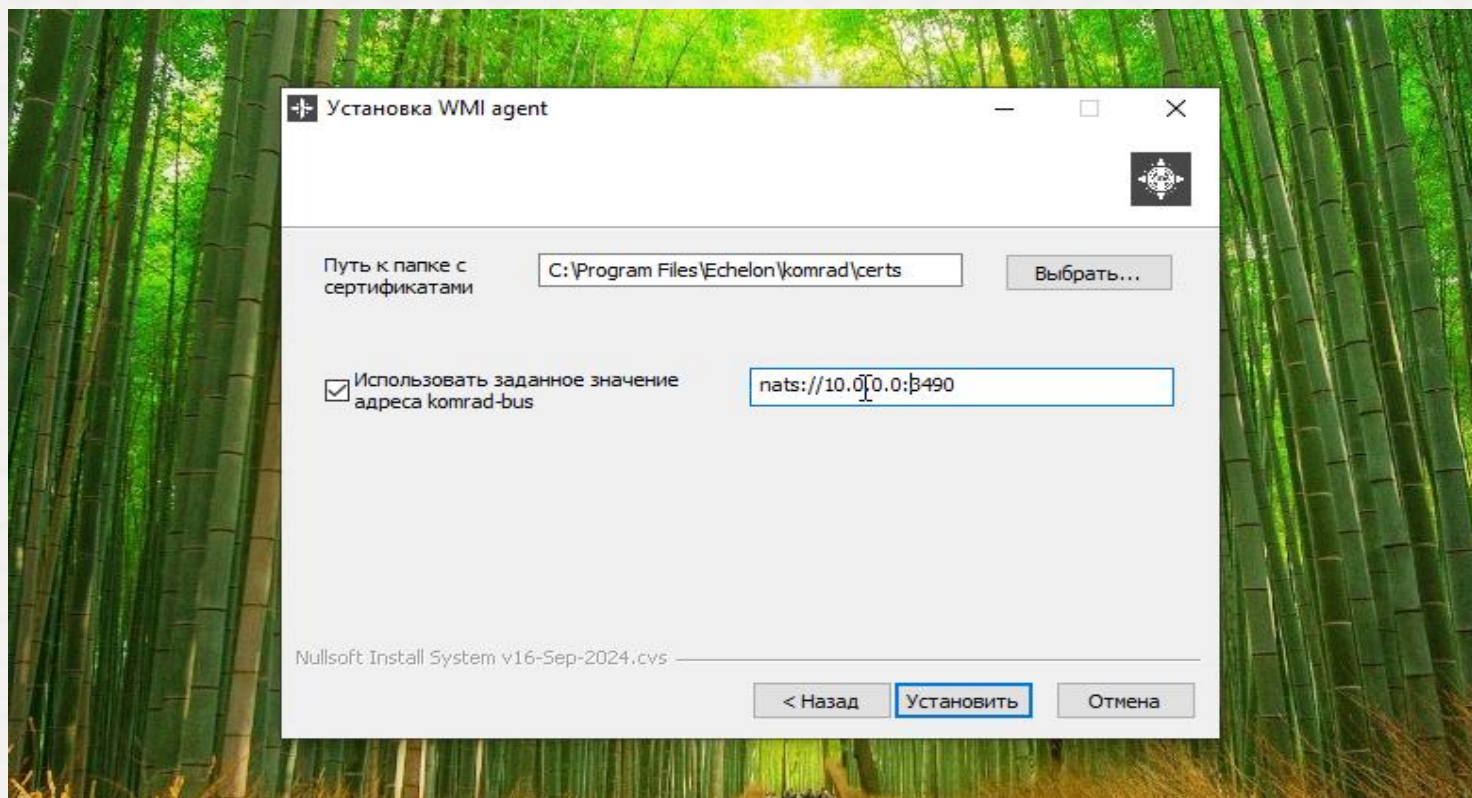
1. Скопировать сертификаты на целевую машину
Копируем сертификаты с машины где установили KOMRAD на целевую машину (где устанавливаем WMI-агент) при помощи ssh или другими средствами.

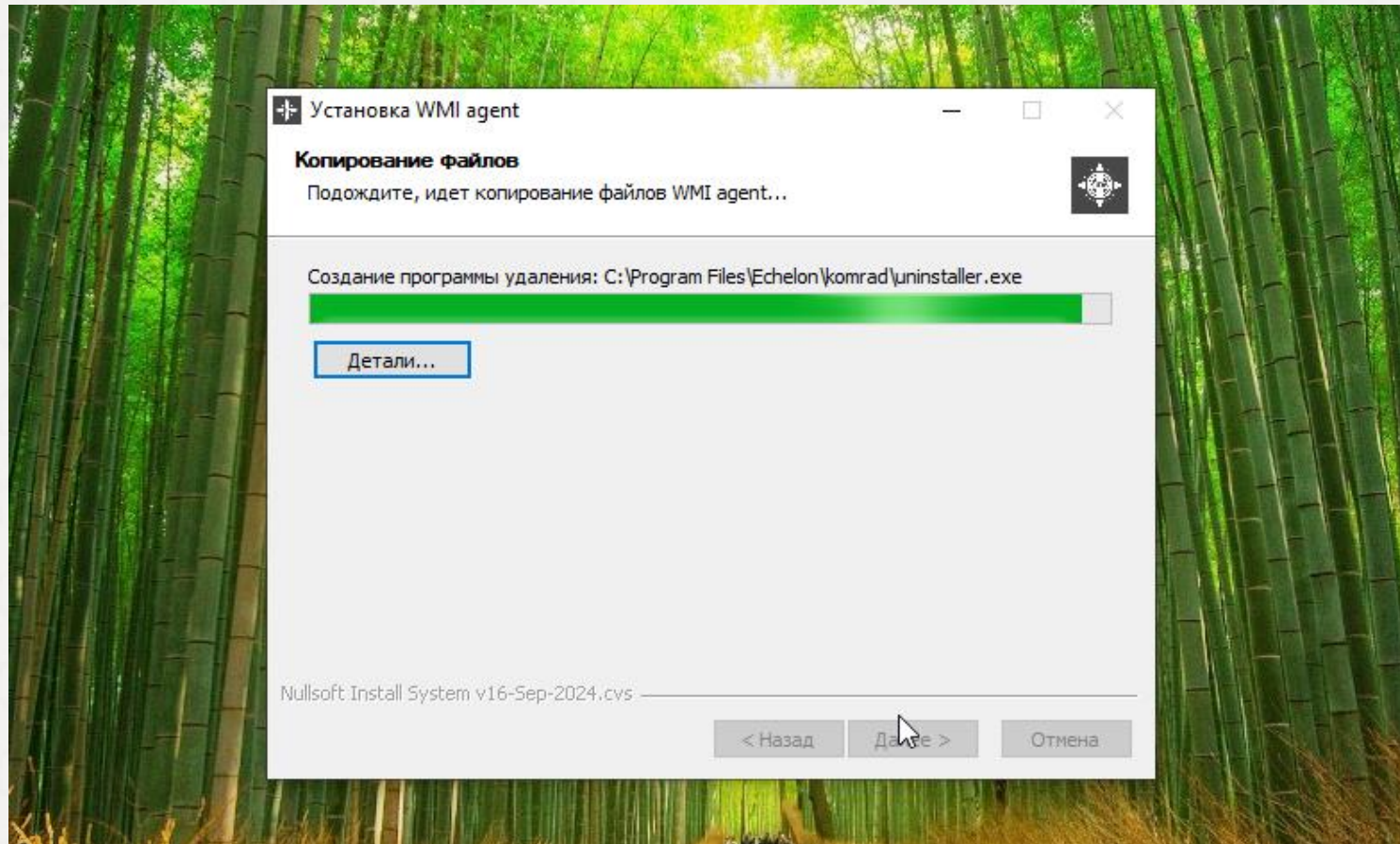
```
scp -r /var/lib/echelon/komrad/certs/ user@127.0.0.1:~/
```

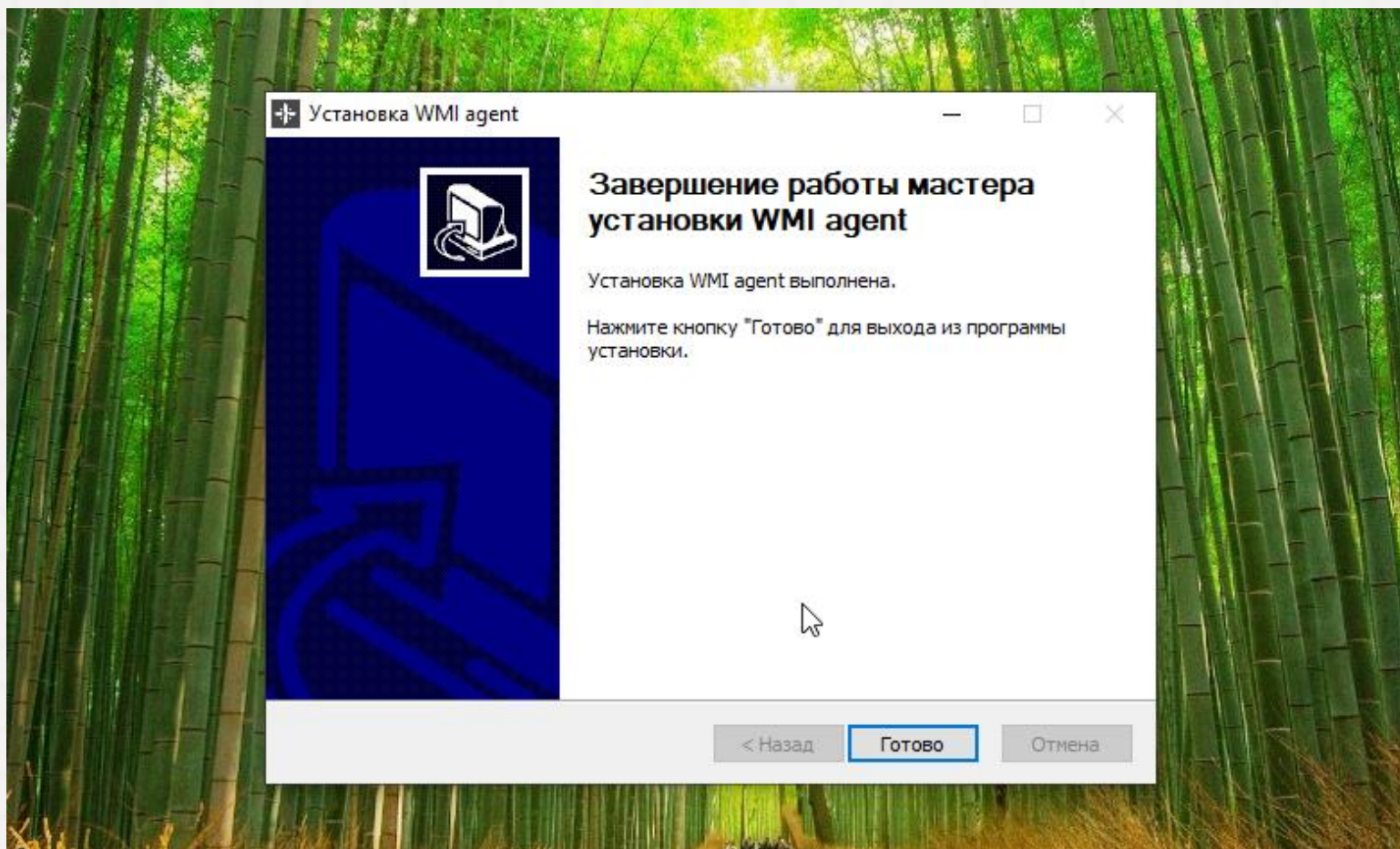
2. Запустить от имени администратора файл инсталлятора
komrad_v4.5.22-demo_windows_amd64_wmi-installer.exe



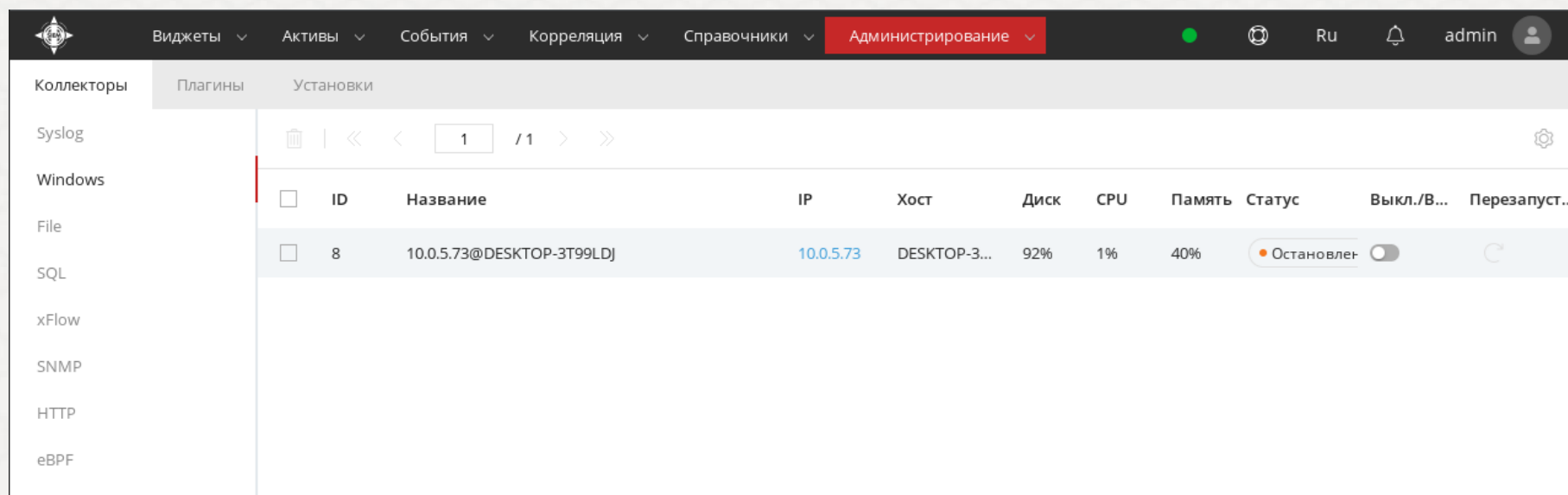
3. Указать путь до сертификатов и адрес komrad-bus
Указать путь до сертификатов, которые скопированы по п.1
Адрес komrad-bus – ip адрес машины на которой установлен KOMRAD







Проверка успешной установки и соединения с KOMRAD Enterprise SIEM



Администрирование

Коллекторы

Плагины

Установки

Syslog

Windows

File

SQL

xFlow

SNMP

HTTP

eBPF

1 / 1

ID	Название	IP	Хост	Диск	CPU	Память	Статус	Выкл./В...	Перезапуст...
8	10.0.5.73@DESKTOP-3T99LDJ	10.0.5.73	DESKTOP-3...	92%	1%	40%	Остановлен		