NTechnology | SIEM

Руководство по установке

НЦОТ

Содержание

1. Общая информация о системе

1.1 О документе

Этот документ содержит информацию для планирования и выполнения развертывания компьютерной программы, предназначенной для сбора и анализа событий информационной безопасности (Security Information and Event Management system) «NTechnology SIEM» (далее – NT SIEM), а также о работе со службами сбора событий с машин Windows.

Комплект документации NT SIEM включает в себя следующие документы:

- Этот документ;
- Руководство по созданию запросов – содержит описание наборов запросов и результаты применения этих запросов;
- Руководство пользователя – содержит справочную информацию и инструкции по настройке и администрированию продукта. Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности;
- Руководство по написанию правил – содержит рекомендации по созданию правил нормализации, агрегации, корреляции и обогащения событий.

1.2 О NT SIEM

NT SIEM – это система, которая осуществляет сбор, хранение и анализ событий, исходящих от сетевых устройств, средств защиты информации, баз данных, ключевых корпоративных ресурсов, инфраструктуры систем и приложений.

1.3 Краткое описание возможностей системы

Система NT SIEM предоставляет следующие основные функциональные возможности:

- Сбор журналов событий с различных источников;
- Визуализация данных в виде графиков, диаграмм в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Управление инцидентами информационной безопасности;
- Хранение событий и инцидентов информационной безопасности;

- Фильтрация по различным параметрам событий и инцидентов, в том числе с использованием избранных запросов для быстрого доступа к фильтрам по событиям;
- Использование готовой базы правил, а также возможность создания собственных правил и табличных списков;
- Мониторинг состояния системы;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Формирование и выгрузка отчетов за определенный период времени;
- Осуществление интеграций, в том числе и с SOAR-системами;
- Мониторинг активов.

2. Схема взаимодействия компонентов

Для обеспечения корректного взаимодействия компонентов системы должны быть доступны для соединения указанные на рисунке 1 порты.

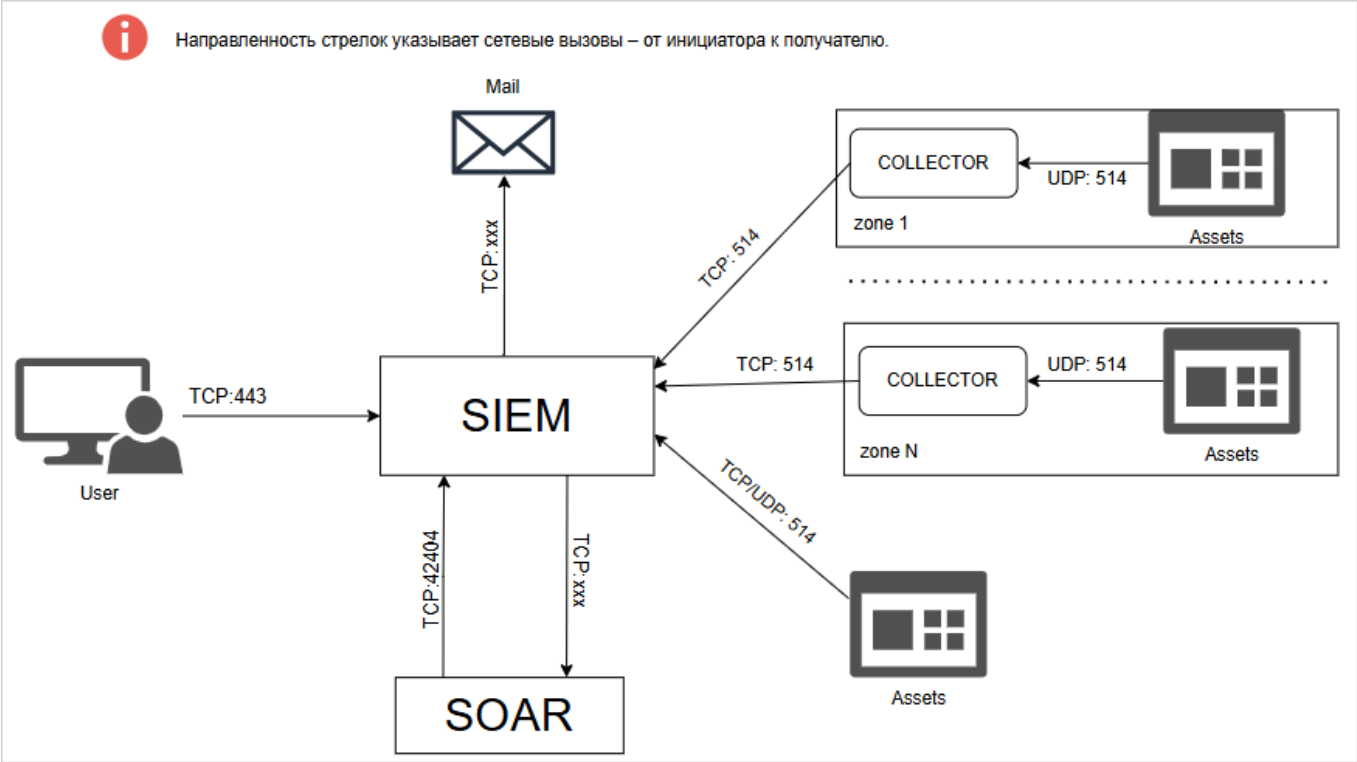


Рисунок 1 – Схема взаимодействия компонентов для версии NT SIEM

TCP:xxx – настраиваемые порты:

– для взаимодействия системы и почтового сервера для отправки электронных писем;

– для взаимодействия системы и SOAR для передачи инцидентов и/или событий.

3. Сценарий развертывания системы

3.1 Аппаратные и программные требования

3.1.1 Программные требования

Дистрибутив NT SIEM подготовлен для установки на операционную систему (далее – ОС) Ubuntu Server 22.04 (на базе ядра Linux версии 5.19 и выше). При установке Ubuntu Server 22.04 необходимо обратить внимание на следующие шаги:

– Разметка дискового пространства, в зависимости от типа хранения событий, так как база данных событий поддерживает разграничение на горячее и холодное хранение (п.3.1.2). Если нет необходимости в разграничении, то следует смонтировать все свободное пространство под корневую директорию (рис. 2).

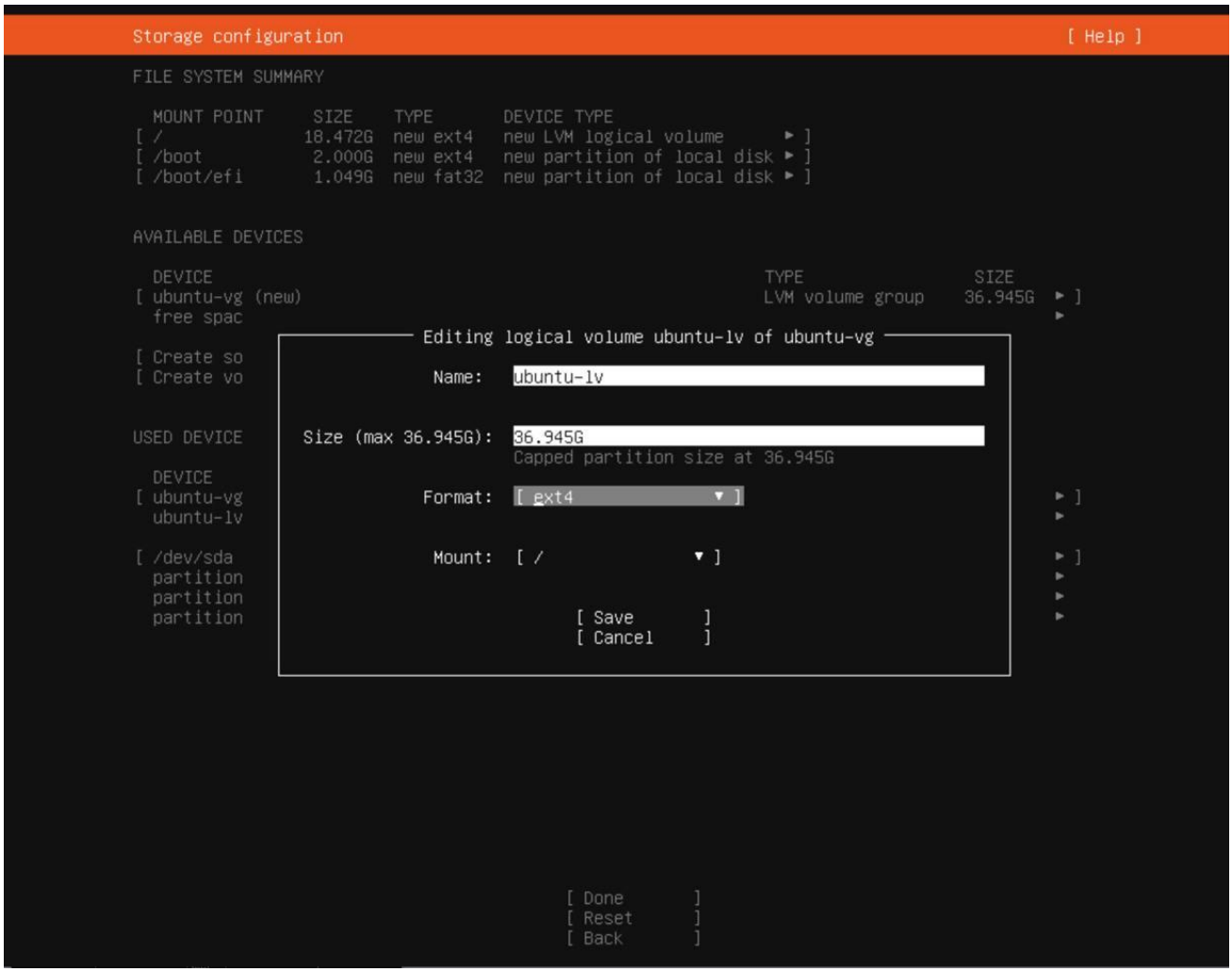


Рисунок 2 – Разметка дискового пространства

– Выбор наборов пакетов. На данном этапе не следует выбирать ни один из наборов пакетов. В противном случае дальнейшая установка может быть выполнена некорректно.

Перед развертыванием NT SIEM необходимо настроить на Firewall правила для корректной работы в пользовательском интерфейсе.

Для работы в интерфейсе NT SIEM рекомендуется использовать последние версии браузеров Google Chrome, Microsoft Chromium Edge, Mozilla Firefox.

3.1.2 Выделение дискового пространства для горячего и холодного хранения

Способ 1: выделение во время установки операционной системы и монтирования дискового пространства.

Способ 2:

1. Подготовка и проверка дисков:

```
lsblk
```

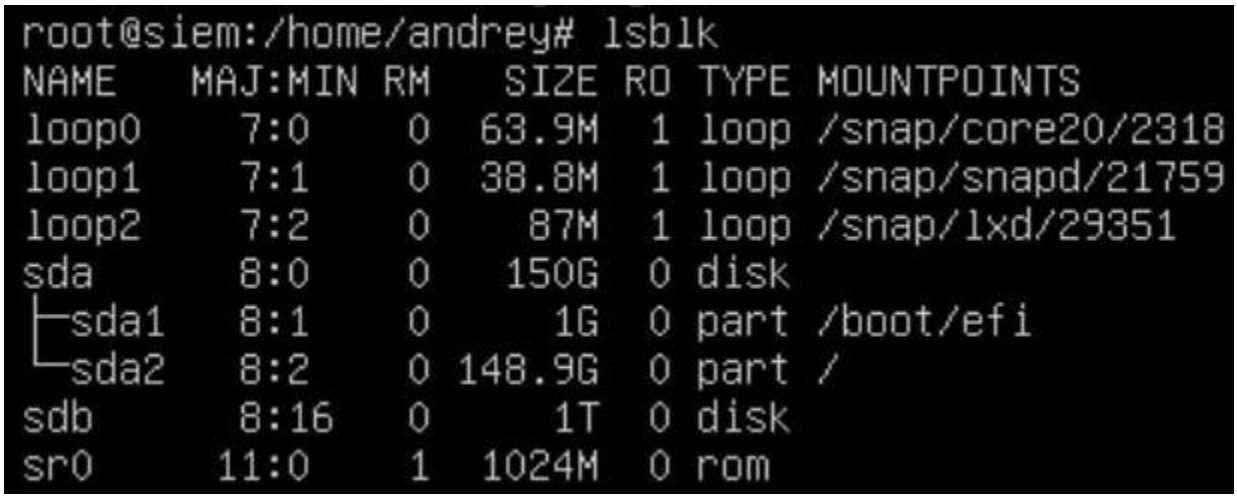


Рисунок 3 – Дисковое пространство

2. Создание папки для монтирования холодного хранения и форматирование раздел в `ext4`:

```
mkdir /mnt/cold
mkfs.ext4 /dev/sdb
```

3. Создание директории и добавление таблицы:

```
parted /dev/sdb mklabel gpt
```

4. Создание раздела `primary` от 0% до 100% диска:

```
parted -a optimal /dev/sdb mkpart primary 0% 100%
```

5. Форматирование раздела в `ext4`:

```
mkfs.ext4 /dev/sdb1
```

6. Получение UUID:

```
blkid /dev/sdb1
```

```
root@siem:/home/andrey# blkid /dev/sdb1
/dev/sdb1: UUID="2b6a4c69-7690-4975-afed-b92a9959a415" BLOCK_SIZE="4096" TYPE="ext4" PARTLABEL="primary" PARTUUID="44c84f7d-ac7a-44e6-a662
-e582fcea31da"
```

Рисунок 4 – Получение уникального идентификатора

7. Открытие файла конфигурации и указание UUID:

```
vim /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/sda2 during curtin installation
/dev/disk/by-uuid/fa142b7a-6017-46c4-91f7-ff795eddb5a8 / ext4 defaults 0 1
# /boot/efi was on /dev/sda1 during curtin installation
/dev/disk/by-uuid/CA91-BC6F /boot/efi vfat defaults 0 1
/swap.img       none    swap    sw      0       0

UUID="2b6a4c69-7690-4975-afed-b92a9959a415" /mnt/cold  ext4  defaults  0 0
```

Рисунок 5 – Указание уникального идентификатора

8. Монтирование директории:

```
mount -a
```

9. Подготовка и проверка дисков:

```
lsblk
```

```
root@siem:/mnt# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
loop0    7:0    0  63.9M  1 loop /snap/core20/2318
loop1    7:1    0  38.8M  1 loop /snap/snapd/21759
loop2    7:2    0    87M  1 loop /snap/lxd/29351
sda      8:0    0   150G  0 disk
├─sda1   8:1    0     1G  0 part /boot/efi
└─sda2   8:2    0 148.9G  0 part /
sdb      8:16   0     1T  0 disk
└─sdb1   8:17   0  1024G  0 part /mnt/cold
sr0     11:0    1  1024M  0 rom
```

Рисунок 6 – Дисковое пространство

Данная информация понадобиться в дальнейшем при установке системы.

3.1.3 Аппаратные требования

Для расчета необходимого дискового пространства следует использовать следующую формулу с учетом количества событий, генерируемых в секунды (EPS):

Объем данных (ГБ) = EPS × Размер события (байт) × Время хранения (секунды)

Далее предлагается рассмотреть пример расчета необходимого дискового пространства для 1000 EPS.

Таблица 1 – Данные для расчета

Показатель	**Значение**
EPS	1000
Средний размер события	300 байт.
Время хранения	30 дней (2 592 000 секунд).

Подставив данные в формулу, получим:

Объем данных = 1000 × 300 × 2 592 000 ≈ 0,71 ТБ.

Таким образом, для хранения данных за 30 дней потребуется около 0,71 ТБ дискового пространства.

Рекомендуемые технические требования к установке All-In-One отражены в таблице 2 с расчетом на хранение событий информационной безопасности сроком не менее 365 дней.

Таблица 2 – Рекомендуемые технические требования к установке All-In-One

	500 EPS	1 000 EPS	2 000 EPS	5 000 EPS	10 000 EPS
CPU	8 core	16 core	32 core	64 core	96 core
RAM	16 Gb	32 Gb	48 Gb	64 Gb	128 Gb
SSD/HDD	6 Tb	10 Tb	20 Tb	50 Tb	100 Tb
Link	1 Gb	1 Gb	1 Gb	10 Gb	10 Gb

Рекомендуемые технические требования для хранилища событий с разделением на горячее и холодное хранение отражены в таблице 3 с расчетом на хранение событий информационной безопасности сроком 365 дней, из которого 60 дней – горячее хранение, последующие 305 дней – холодное хранение.

Таблица 3 – Рекомендуемые технические требования для обеспечения cold/hot хранения

	500 EPS	1 000 EPS	2 000 EPS	5 000 EPS	10 000 EPS
SSD	1,5 Tb	2 Tb	4 Tb	10 Tb	20 Tb
HDD	4,5 Tb	8 Tb	16 Tb	40 Tb	80 Tb

3.2 Установка системы NT SIEM

Для того, чтобы начать процесс установки NT SIEM необходимо скачать и распаковать исходные файлы из дистрибутива, предоставляемого производителями NT SIEM.

Для того, чтобы распаковать исходные файлы следует переключиться на пользователя `root`, имеющего администраторский доступ к вашей системе, и выполнить команду для создания временной директории:

```
mkdir temp/
tar -zxvf NtechnologySiem_v2.0.0.tar.gz -C temp/
```

После распаковки архива необходимо перейти в директорию, где будут находиться два файла `2.0.0.tar.gz`, `new_install.sh` и папки с документацией, базой правил и инсталлятором служб сборки событий. Для перехода следует выполнить команду:

```
cd temp/
```

Далее необходимо поменять права доступа для файла `new_install.sh`, который уже входит в состав дистрибутива. Для этого необходимо ввести в консоли следующую команду:

```
chmod u+x new_install.sh
```

После изменения прав доступа ввести в консоли команду для запуска скрипта установки:

```
./new_install.sh
```

После произведенных команд начнется установка NT SIEM и далее необходимо в интерактивной меню ответить на следующие вопросы:

- Ввести IP-адрес хоста машины, где будет произведена установка системы;
- Необходима ли настройка точки монтирования для холодного хранения данных. Варианты ответа : `y/n`. Если есть такая необходимость, то ввести: `y`. Далее будет предложено ввести директорию для монтирования `cold storage` (рис.7). Если была выбрана опция ответа: n, то монтирование дискового пространства будет по стандартной схеме;

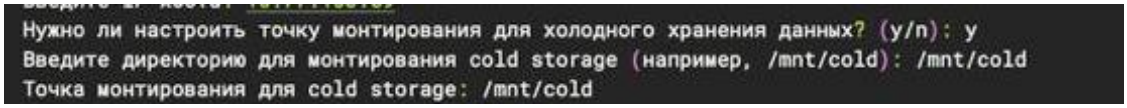


Рисунок 7 – Указание папки для монтирования `cold storage`

- Ввести основную сеть Network Syslog. В данной опции следует указать IP - адрес и маску подсети, с которой разрешен прием syslog - сообщений. Например, 10.77.163.0/24. По умолчанию разрешены все сети (0.0.0.0/ 0).

```
Ввод новых сетей...
Введите основную сеть syslog (по умолчанию 0.0.0.0/0): 10.77.163.0/24

Текущие сети:
  1. 10.77.163.0/24
```

Рисунок 8 – Ввод новых сетей

- Далее, если есть необходимость добавить еще одну сеть, то следует ввести «y», если нет, то - «n».

```
Хотите добавить еще одну сеть? (y/n): y
Введите дополнительную сеть: 10.77.163.0/24

Текущие сети:
  1. 0.0.0.0/0
  2. 10.77.163.0/24
Хотите добавить еще одну сеть? (y/n): y
Введите дополнительную сеть: 10.10.0.0/16

Текущие сети:
  1. 0.0.0.0/0
  2. 10.77.163.0/24
  3. 10.10.0.0/16
Хотите добавить еще одну сеть? (y/n): n
✅ Файл networks.property создан/обновлен.

✅ Готово!
Итоговый список сетей:
  1. 0.0.0.0/0
  2. 10.77.163.0/24
  3. 10.10.0.0/16
✅ Резервная копия сохранена в:
```

Рисунок 9 – Ввод дополнительной сети

Следует обратить внимание на то, что если понадобиться в дальнейшей работе добавить новую сеть или обновить сети, то необходимо перейди в директорию установленного проекта (по умолчанию srv/siem-docker) cd /srv/siem-docker и запустить скрипт bash networks_syslogs.sh

```
root@build-patch-siem:/home/darkneo/temp# cd /srv/siem-docker/
root@build-patch-siem:/srv/siem-docker# bash networks_syslogs.sh
Текущие сети в конфигурации:
  1. 0.0.0.0/0
  2. 10.77.163.0/24
  3. 10.10.0.0/16

Выберите действие:
  1. Использовать существующие сети
  2. Добавить новые сети к существующим
  3. Заменить все сети новыми
  4. Выйти без изменений
Ваш выбор (1-4):
```

Рисунок 10 – Обновление сети

- Указать, сколько выделить оперативной памяти, но не более 50 % от общей оперативной памяти. Обратить внимание, что необходимо выбрать цифру, под которой указана нужная вам оперативная память:

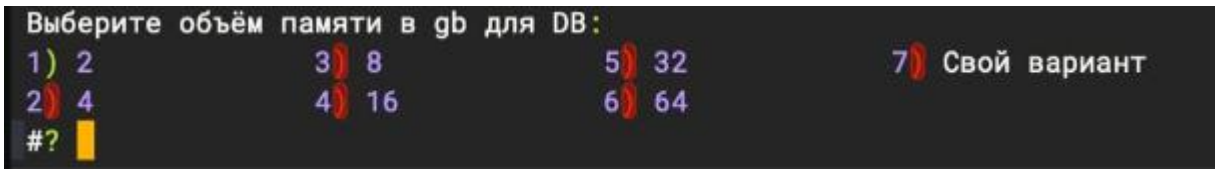
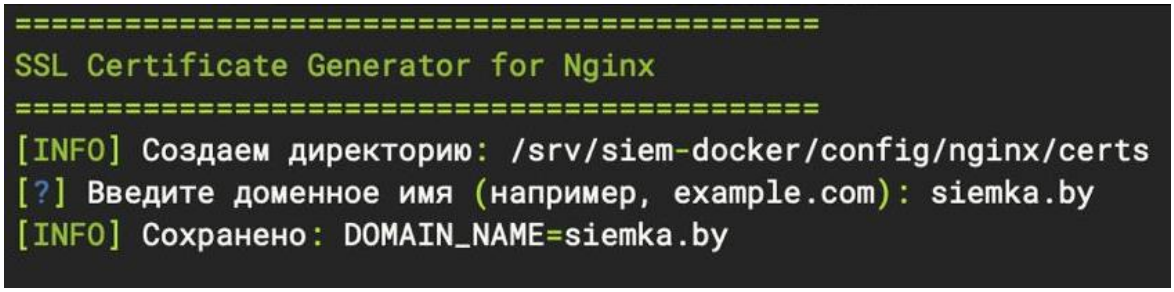


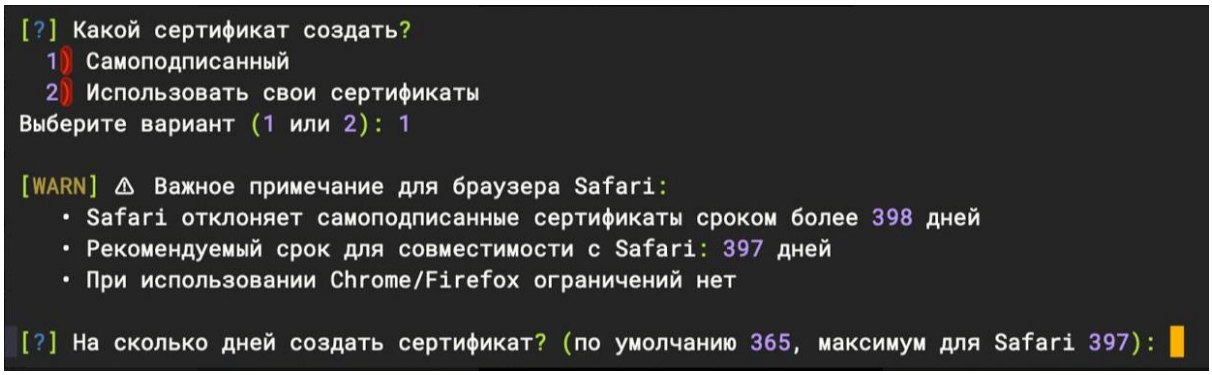
Рисунок 11 – Варианты объема оперативной памяти

Далее будет предложена установка доменного имени (по необходимости). Для этого следует выполнить следующие шаги:

- настройка доменного имени



- выбор типа сертификата



Если выбрать вариант 1, то необходимо ввести параметры самоподписанного сертификата.

Следует обратить внимание, для пользователей браузера Safari максимальный срок действия самоподписанных сертификатов составляет 398 дней.

```
[?] На сколько дней создать сертификат? (по умолчанию 365, максимум для Safari 397): 365

[?] Данные для сертификата (можно оставить пустыми)
Страна (2 буквы, по умолчанию BY):
Область/Штат (по умолчанию Region): Minskaya
Город (по умолчанию City): Minsk
Организация (по умолчанию Organization): NTEC
Отдел (по умолчанию Department): Devops
[INFO] Генерация SSL сертификата для домена: siemka.by
[INFO] Генерация приватного ключа...
[INFO] Генерация CSR...
[INFO] Генерация самоподписанного сертификата (действителен 365 дней)...
[INFO] Создание PEM файла...
[INFO] Создание PKCS12 архива...
```

Если выбрать вариант 2, то необходимо использовать существующие сертификаты, указав путь к ним.

```
[?] Какой сертификат создать?
  1) Самоподписанный
  2) Использовать свои сертификаты
Выберите вариант (1 или 2): 2
[?] Укажите полный путь к файлу сертификата (.crt): /srv/license.crt
[?] Укажите полный путь к файлу ключа (.key): /srv/license.key
```

- проверка валидности сертификата

```
==========================================
Проверка валидности сертификата
==========================================
[INFO] Проверка срока действия...
  📅 Действителен с: Nov 13 14:04:13 2025 GMT
  📅 Действителен до: Dec 15 14:04:12 2026 GMT
[INFO] ✅ Сертификат действителен (до Dec 15 14:04:12 2026 GMT)
[INFO] Проверка соответствия ключа и сертификата...
[INFO] ✅ Ключ соответствует сертификату
[INFO] Проверка типа сертификата...
[INFO] 🟫 Сертификат подписан CA (Issuer: C = BE, O = GlobalSign nv-sa, CN = GlobalSign GCC R6 AlphaSSL CA 2025)
[INFO] Проверка домена в сертификате...
```

После завершения процедуры установки сертификаты будут храниться в директории /srv/siem-docker/config/nginx/certs/

Если требуется сменить текущее доменное имя, то необходимо запустить скрипт bash scripts/domain.sh из корневой директории.

Процесс установки занимает несколько минут. Управление NT SIEM осуществляется через веб-интерфейс. Для этого следует открыть браузер Google Chrome и ввести в адресной строке IP-адрес (`https://IP_Address`, где IP_Address – IP-адрес сервера, где производилась инсталляция NT SIEM). Первая загрузка веб-интерфейса может занять несколько минут.

При необходимости можно изменить настройки по умолчанию сети `Docker (172.17.0.1)`, для этого необходимо:

1. Создать или отредактировать файл `/etc/docker/daemon.json`

```
sudo nano /etc/docker/daemon.json
```

2. Добавить или заменить содержимое, где `bip` — это IP-адрес и подсеть для интерфейса `docker0`:

```
{
  "bip": "100.100.1.1/16"
}
```

Следует убедиться, что выбранная сеть **не конфликтует** с локальной или VPN-сетью.

3. Перезапустить `Docker`

```
sudo systemctl restart docker
```

После загрузки веб-интерфейс будет выглядеть на как рисунке 12.

Рисунок 12 – Страница авторизации системы NT SEIM

В ходе установки системы также подгружаются системные правила, используемые для обработки и анализа данных в NT SIEM.

Учетная запись администратора по умолчанию имеет атрибуты:

- имя пользователя: admin;
- пароль: sTr0n&gg.

Рекомендуется изменить пароль сразу после входа в веб-интерфейс. В дальнейшем можно создать и другие учетные записи, например, с ролью администратора или оператора.

Для смены пароля у учетной записи администратора следует:

- Выбрать в боковом меню страницу «Настройки системы» (рис.13).
- На вкладке «Пользователи» выбрать пользователя с ролью «Супер Администратор».
- Нажать на кнопку «Редактировать».
- Ввести новый пароль.
- Нажать на кнопку «Сохранить».

Как результат, пароль учетной записи администратора изменится. Если Пользователь не подтверждает свое действие или при нажатии на кнопку «Отмена», все данные остаются неизменными.

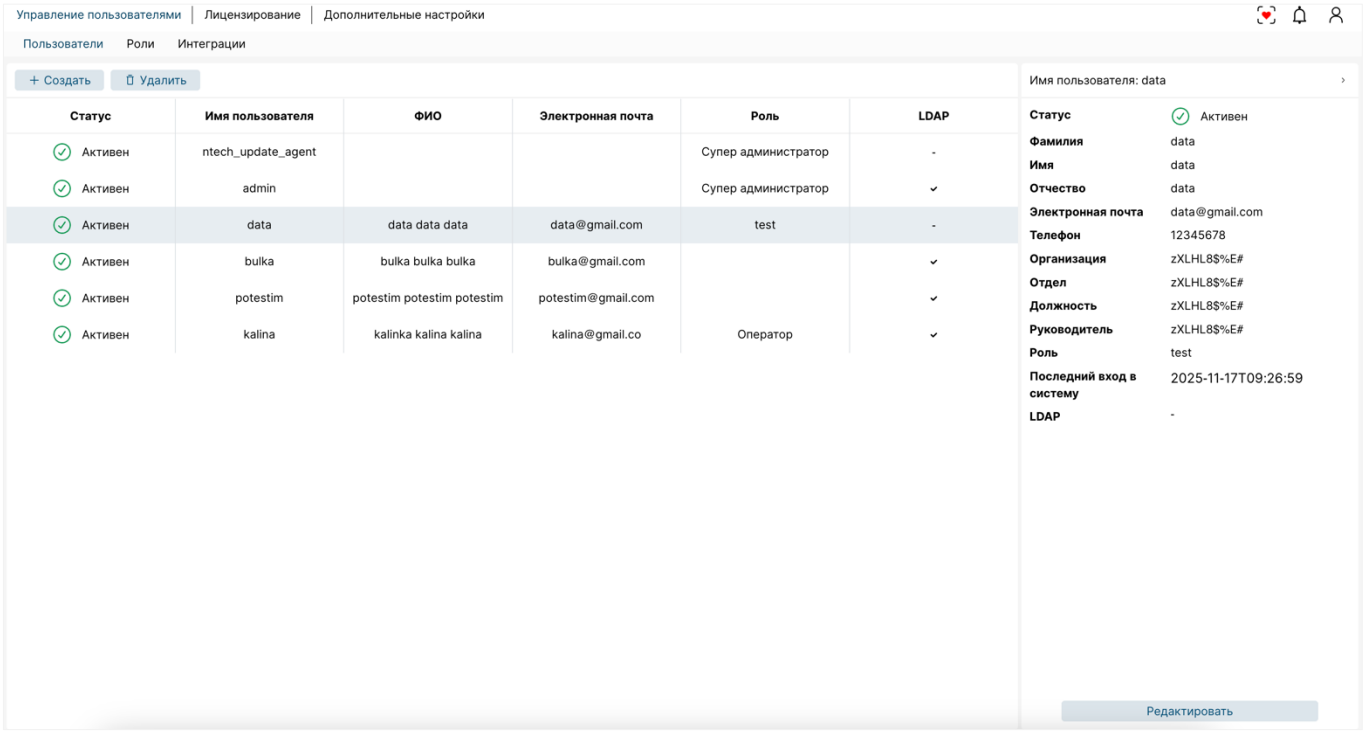


Рисунок 13 – Страница «Настройки системы»

3.3 Установка доверенного сертификата

С помощью доверенного корневого сертификата браузеры проверяют безопасность сайтов, их подлинность и шифруют данные, передаваемые между сайтом и браузером пользователя.

Большинство сторонних приложений и браузеров используют корневые сертификаты из системного хранилища операционной системы, например, Google Chrome. Некоторые программы используют собственное хранилище сертификатов, например, Mozilla Firefox.

С правами администратора можно выполнить установку корневого сертификата в хранилище сертификатов. При отсутствии таких полномочий можно добавить сертификат к браузеру.

Обратите внимание, что после работ по установке доверенного сертификата необходимо перезагрузить рабочую станцию.

3.3.1 Установка сертификата для ОС семейства Windows

Если при установке обновления необходимо подгрузить корневой сертификат, то его можно найти:

```
cat config/indexer_ssl_certs/root-ca.pem
```

Если при первичной установке необходимо подгрузить корневой сертификат, то его можно найти:

```
/srv/siem-docker/config/indexer_ssl_certs/root-ca.pem
```

Следует создать файл с расширением `.crt` и вставить содержимое сертификата из файла `root-ca.pem`.

На файле корневого сертификата нажмите правой кнопкой мыши и выберите «Установить сертификат» (рис. 14). В открывшемся окне «Мастер импорта сертификатов» помощника установки выберите необходимый пункт и нажмите «Далее».

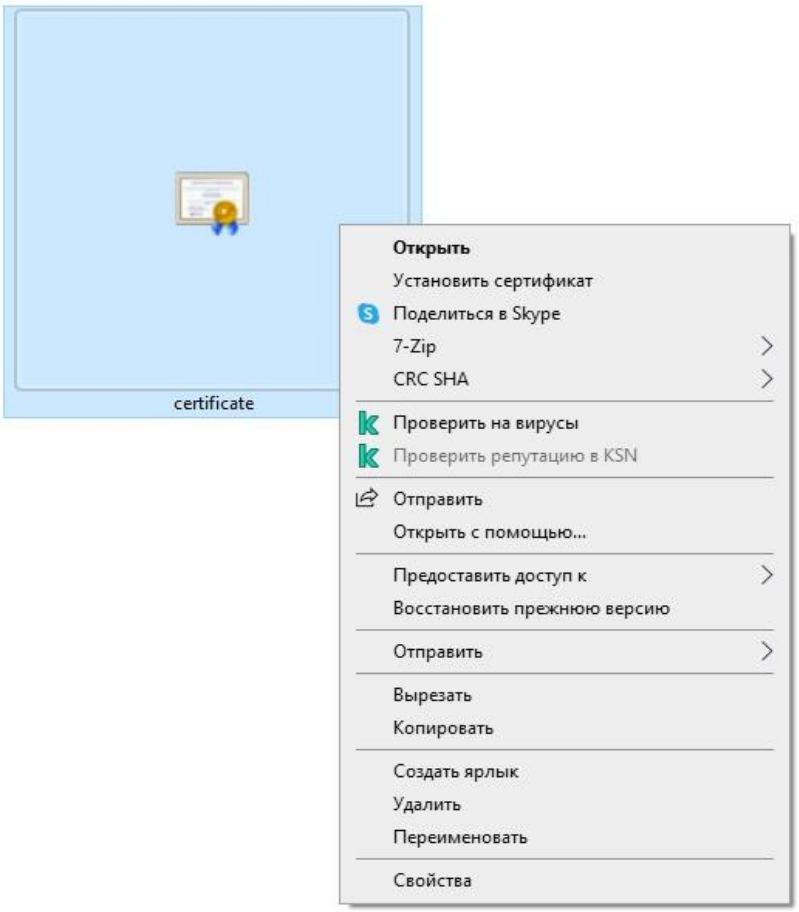


Рисунок 14 – Начало установки доверенного сертификата

На странице «Хранилище сертификатов» нужно выбрать «Поместить все сертификаты в следующее хранилище», нажать кнопку «Обзор». В открывшемся окне необходимо выбрать и подтвердить папку «Доверенные корневые центры сертификации» для сертификата. И затем нажмите кнопку «Далее» (рис 15).

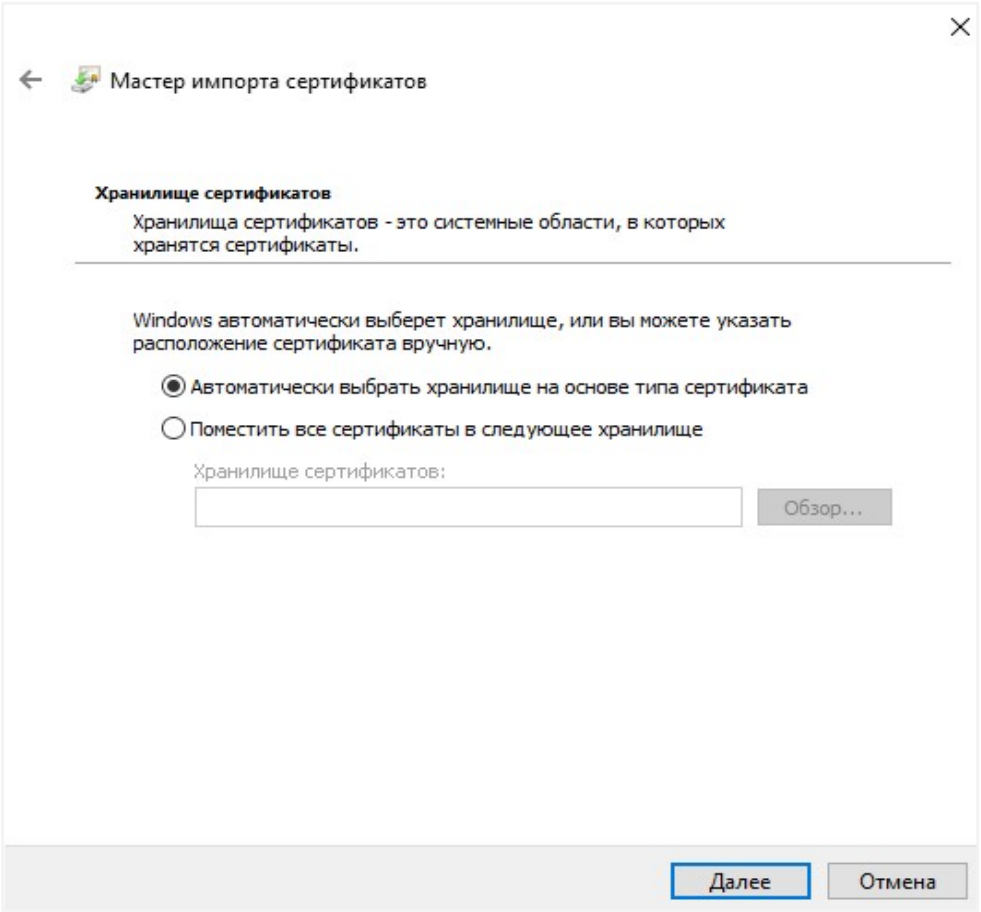


Рисунок 15 – Хранилище сертификатов

Затем следует продолжать выполнять предлагаемые шаги помощника. Нажать кнопку «Готово», а затем кнопку «ОК», чтобы подтвердить успешное выполнение импорта сертификата.

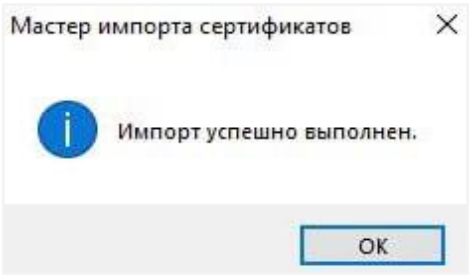


Рисунок 16 – Успешное выполнение импорта сертификата

Перед работой с системой NT SIEM следует перезагрузить рабочую станцию.

3.3.2 Установка сертификата для ОС семейства MacOS

Если при установке обновления необходимо подгрузить корневой сертификат, то его можно найти:

```
cat config/indexer_ssl_certs/root-ca.pem
```

Если при первичной установке необходимо подгрузить корневой сертификат, то его можно найти:

```
/srv/siem-docker/config/indexer_ssl_certs/root-ca.pem
```

Следует создать файл с расширением `.crt` и вставить содержимое сертификата из файла `root-ca.pem`.

В папке скачивания, открыть сертификат и введите пароль от системы MacOS, если необходимо.

Затем в настройках системы открыть приложение «Связка ключей». Во вкладке «Сертификаты», выбрать нужный файл с сертификатом и открыть его (например, двойным нажатием). Перейти во вложенный список «Доверие» и выбрать вариант «Всегда доверять» (рисунок 17), ввести пароль, при необходимости и закрыть приложение «Связка ключей» (см. подробную информацию в справочном центре Apple).

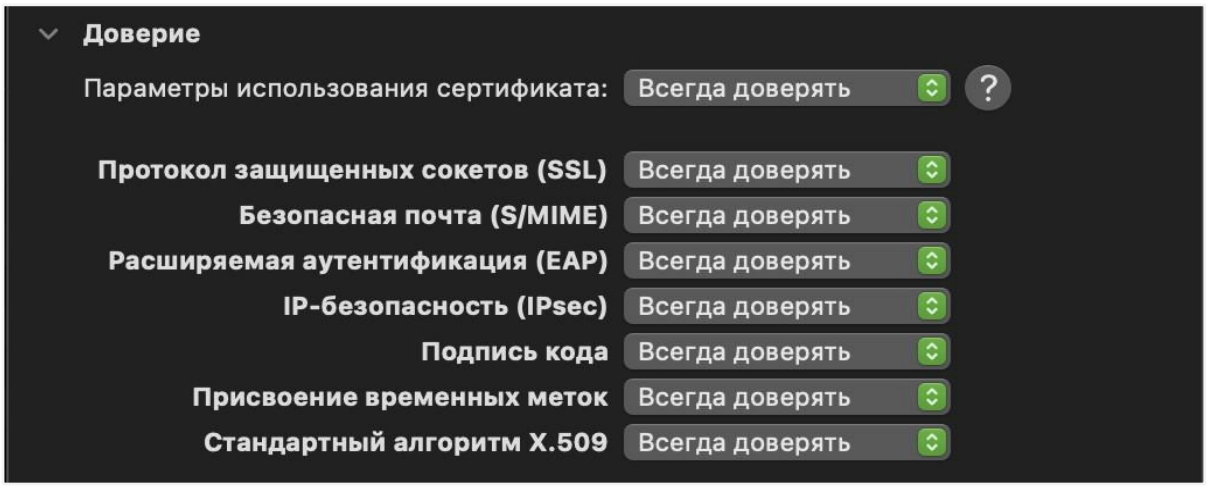


Рисунок 17 – Вкладка «Доверие» приложения «Связка ключей»

Перед работой с системой NT SIEM следует перезагрузить рабочую станцию.

3.3.3 Установка сертификата для браузера Google Chrome

Если при установке обновления необходимо подгрузить корневой сертификат, то его можно найти:

```
cat config/indexer_ssl_certs/root-ca.pem
```

Если при первичной установке необходимо подгрузить корневой сертификат, то его можно найти:

```
/srv/siem-docker/config/indexer_ssl_certs/root-ca.pem
```

Следует создать файл с расширением `.crt` и вставить содержимое сертификата из файла `root-ca.pem`.

Открыть браузер Google Chrome. Для начала необходимо перейти в окно «Настройки», в левой части страницы нажмите «Конфиденциальность и безопасность», и затем в раздел «Безопасность». Прокрутить страницу вниз до раздела «Дополнительно» и нажать «Настроить сертификаты» (рис. 18).

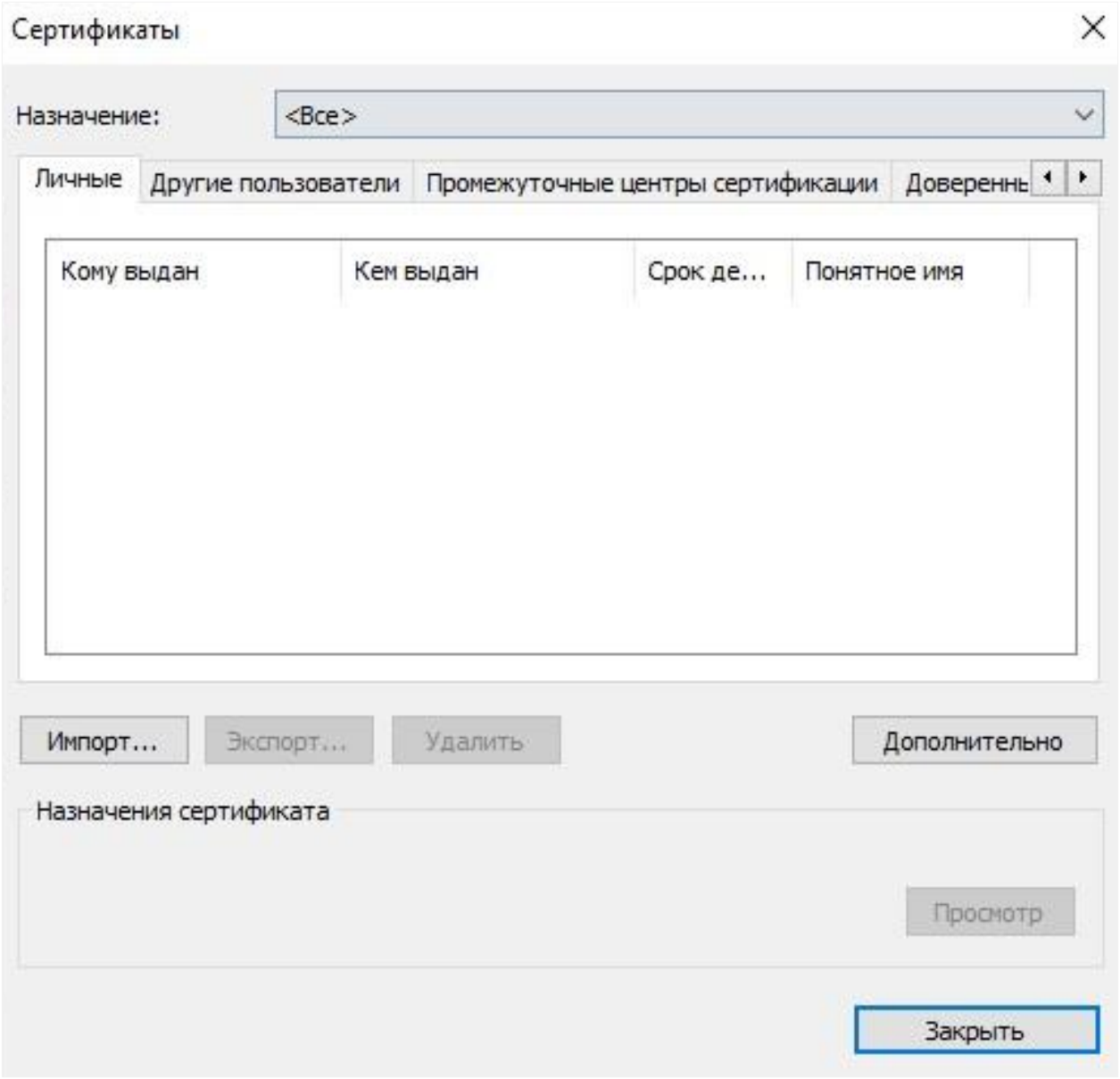


Рисунок 18 – Страница «Сертификаты»

Для установки сертификата следует перейти на вкладку «Доверенные корневые центры сертификации» и нажмите кнопку «Импорт...». Откроется окно «Мастер импорта сертификатов» (рис. 19).

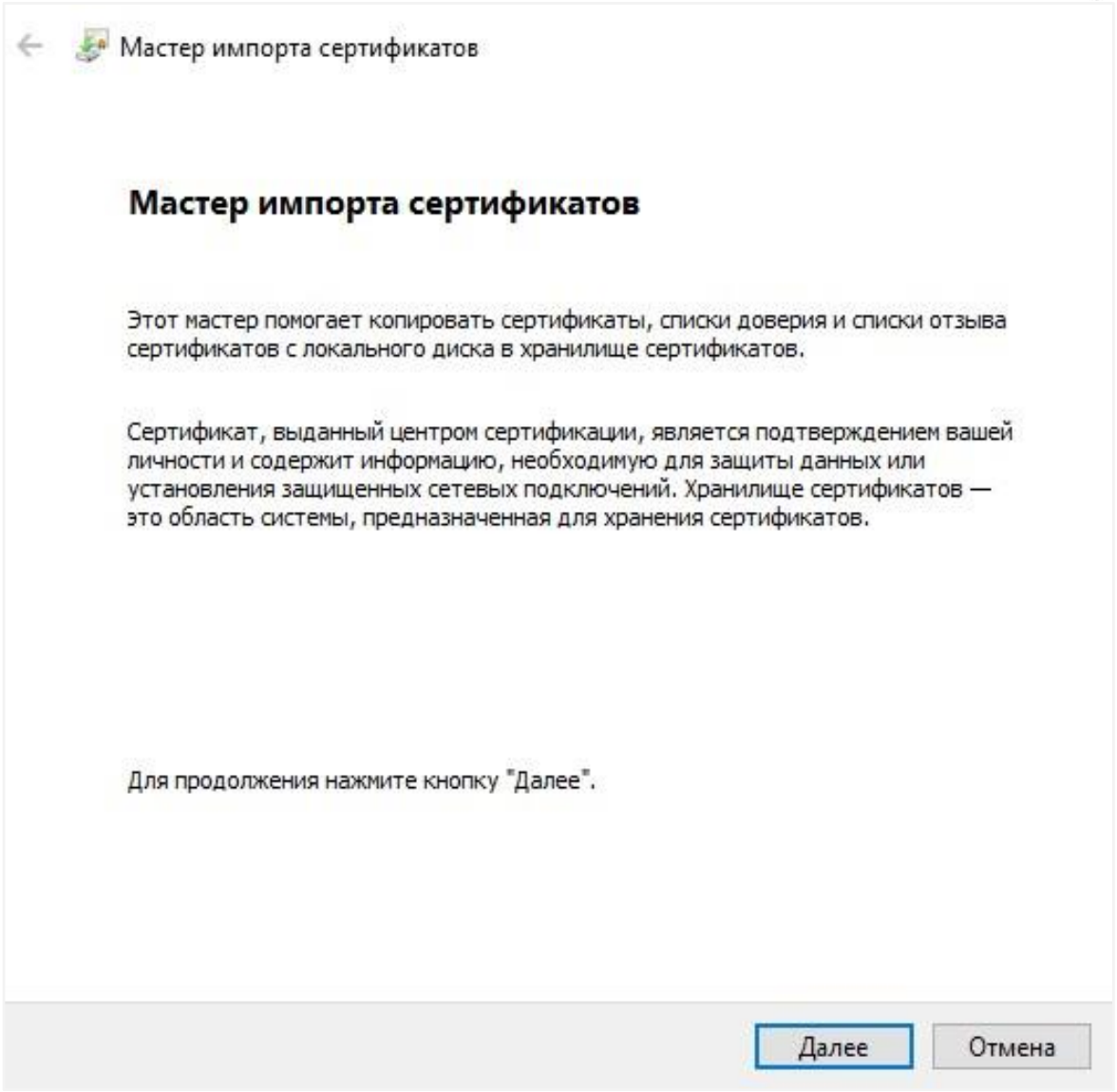


Рисунок 19 – Окно «Мастер импорта сертификатов»

В открывшемся окне «Мастер импорта сертификатов» помощника нажать «Далее», откроется окно «Импортируемый файл» (рис. 20). Далее необходимо нажать кнопку «Обзор», выбрать ранее скачанный сертификат. Результат представлен на рисунке 21.

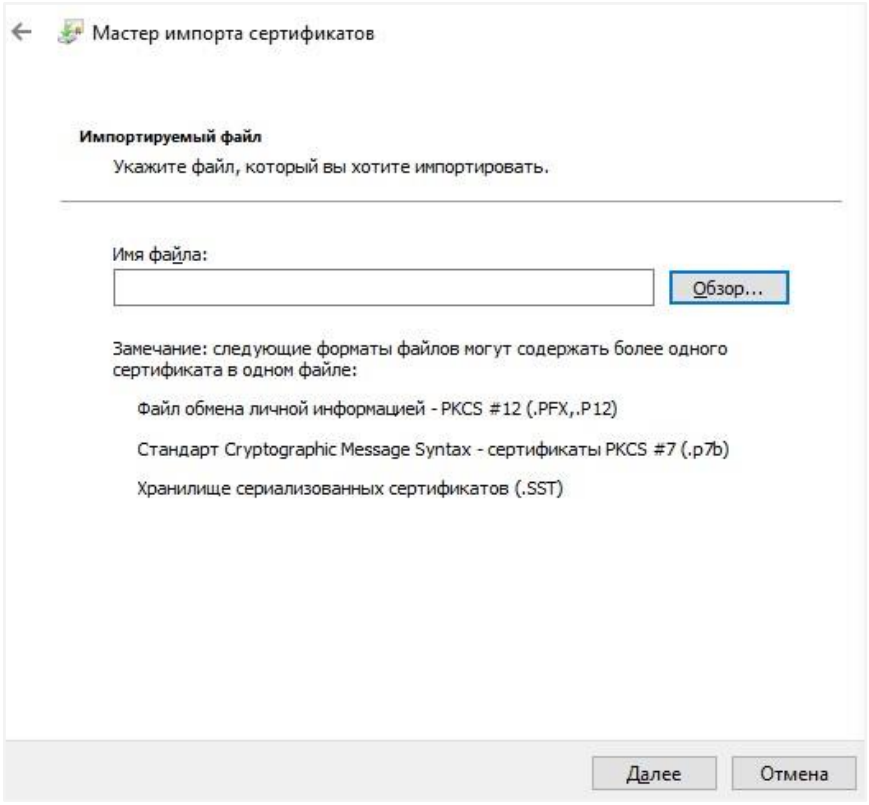


Рисунок 20 – Окно «Импортируемый файл»

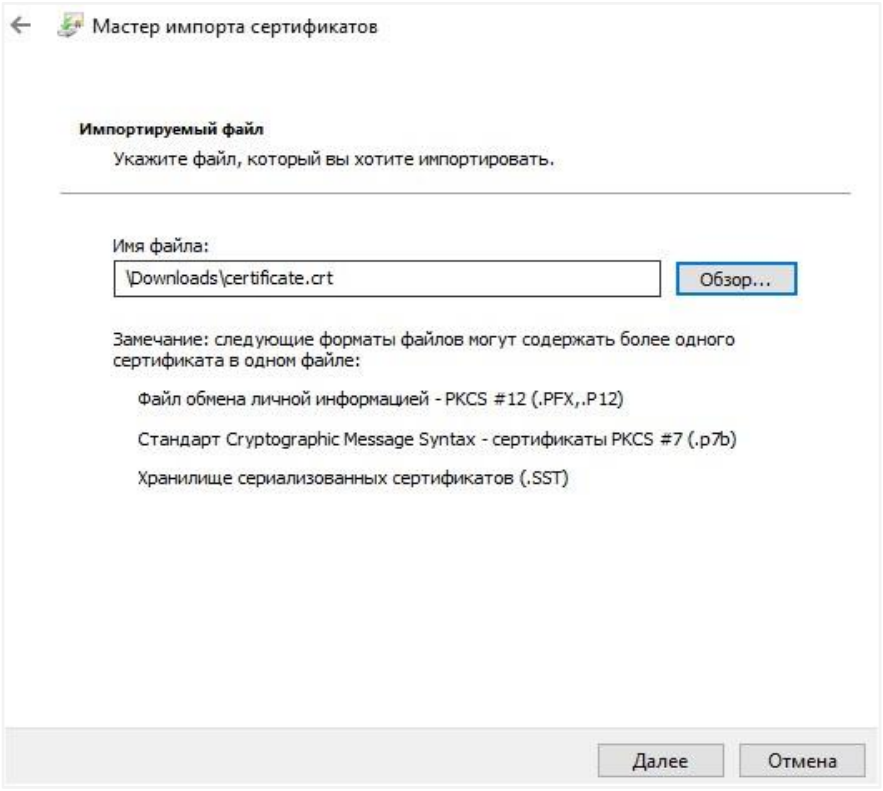


Рисунок 8 – Результат выбора сертификата для установки

Затем следует продолжать выполнять предлагаемые шаги помощника. Нажать кнопку «Готово», а потом кнопку «ОК», чтобы подтвердить успешное выполнение импорта сертификата (см. подробную информацию в справочном центре Google).

Перед работой с системой NT SIEM перезагрузите рабочую станцию.

3.3.4 Установка сертификата для браузера Mozilla Firefox

Если при установке обновления необходимо подгрузить корневой сертификат, то его можно найти:

```
cat config/indexer_ssl_certs/root-ca.pem
```

Если при первичной установке необходимо подгрузить корневой сертификат, то его можно найти:

```
/srv/siem-docker/config/indexer_ssl_certs/root-ca.pem
```

Следует создать файл с расширением `.crt` и вставить содержимое сертификата из файла `root-ca.pem`.

Далее следует открыть браузер Mozilla Firefox и перейти в окно «Настройки» (рис. 22).

Рисунок 22 – Переход в настройки браузера Mozilla Firefox

В левой части страницы перейти в раздел «Приватность и защита», найдите раздел «Защита» и нажать «Просмотр сертификатов» (рис. 23).

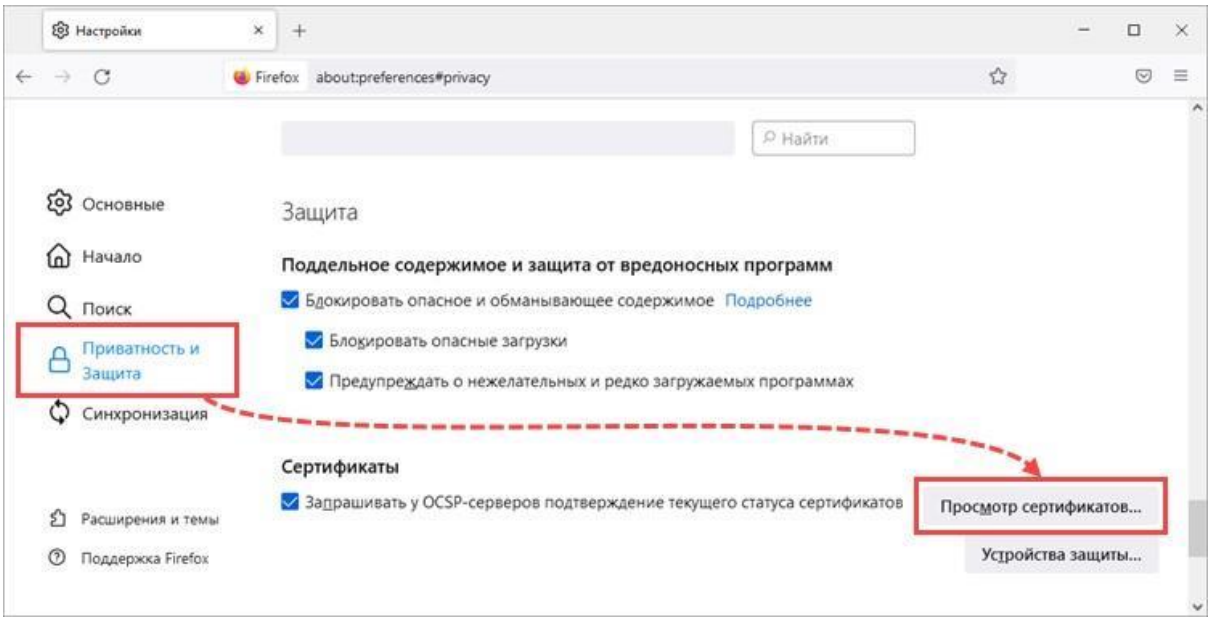


Рисунок 9 – Настройки браузера Mozilla Firefox раздел «Приватность и защита»

Перейти на вкладку «Центры сертификации» и нажать «Импортировать» (рис.24). Выбрать ранее скачанный сертификат.

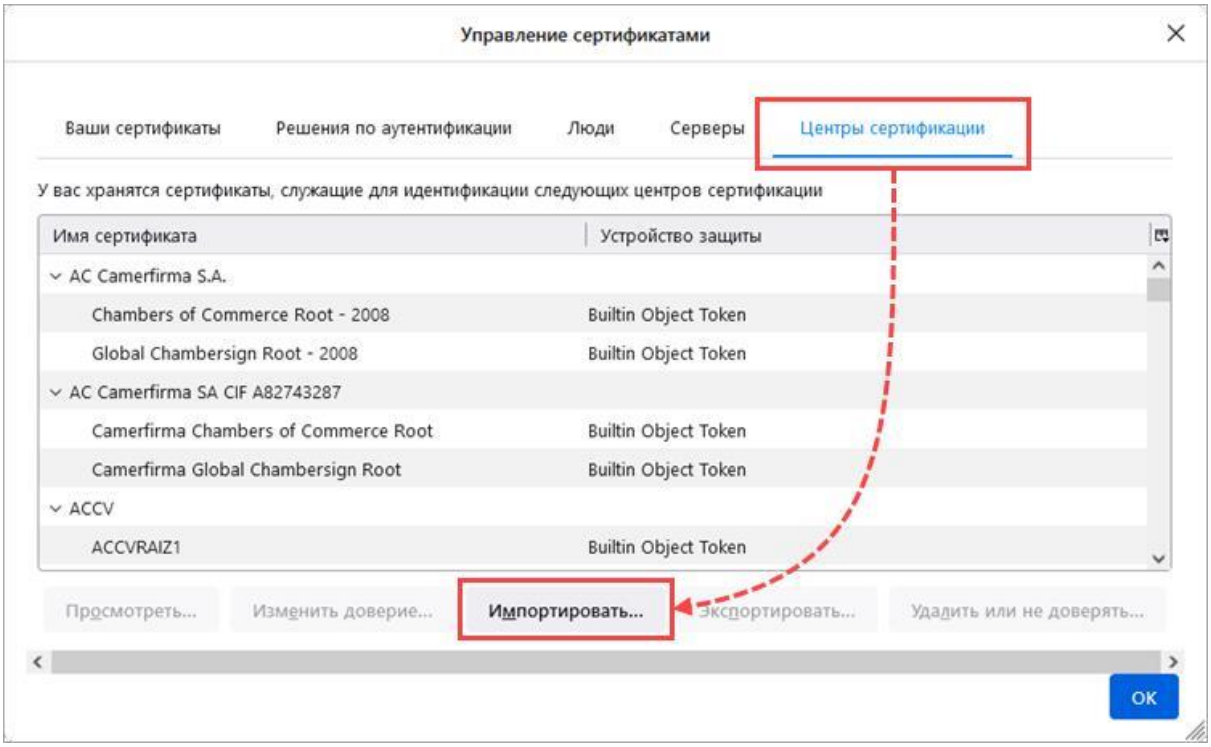


Рисунок 24 – Окно «Управление сертификатами»

Установить флажки «Доверять при идентификации веб-сайтов» и «Доверять при идентификации пользователей электронной почты». Нажать «ОК» (рис.25).

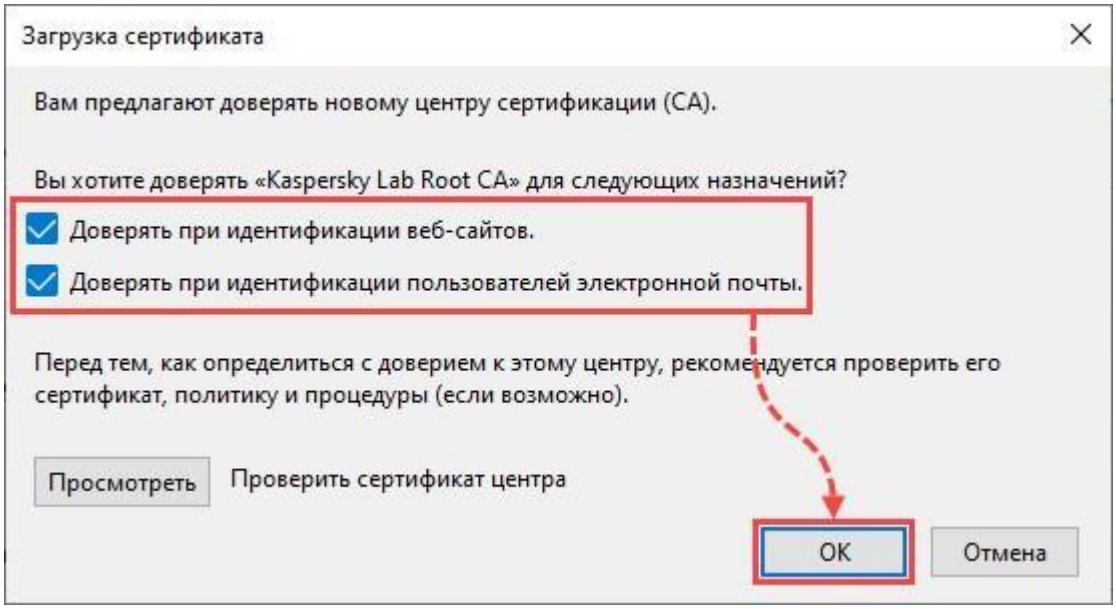


Рисунок 25 – Окно «Загрузка сертификата»

Корневой сертификат будет установлен в хранилище Mozilla Firefox. Перед работой с системой NT SIEM следует перезагрузить рабочую станцию.

3.4 Синхронизация времени на серверах

Для корректной работы системы необходимо настроить синхронизацию времени.

Первым шагом, необходимо установить «chrony» с помощью следующей команды:

```
sudo apt install chrony
```

Далее, необходимо убедиться, что виртуальная машина имеет доступ в интернет. Если доступ в Интернет отсутствует, то необходимо отредактировать файл `/etc/chrony/chrony.conf`, заменив значение NTP-сервера на имя или IP-адрес внутреннего NTP-сервера вашей организации.

Затем необходимо запустить сервис синхронизации системного времени, выполнив команду:

```
sudo systemctl enable --now chrony
```

Через несколько секунд выполнить команду:

```
sudo timedatectl | grep 'System clock synchronized'
```

При успешной синхронизации системного времени, вывод будет содержать строку:

```
System clock synchronized: yes.
```

3.5 Добавление лицензии

После установки системы, для получения полного функционала системы, необходимо загрузить ключ лицензии: с/без подключения к серверу лицензирования.

Для этого сначала необходимо перейти на группу страниц «Настройки системы», а затем на страницу «Лицензирование» (рис.26), скопировать данные из поля «Хэш» с помощью и передать его поставщику системы.

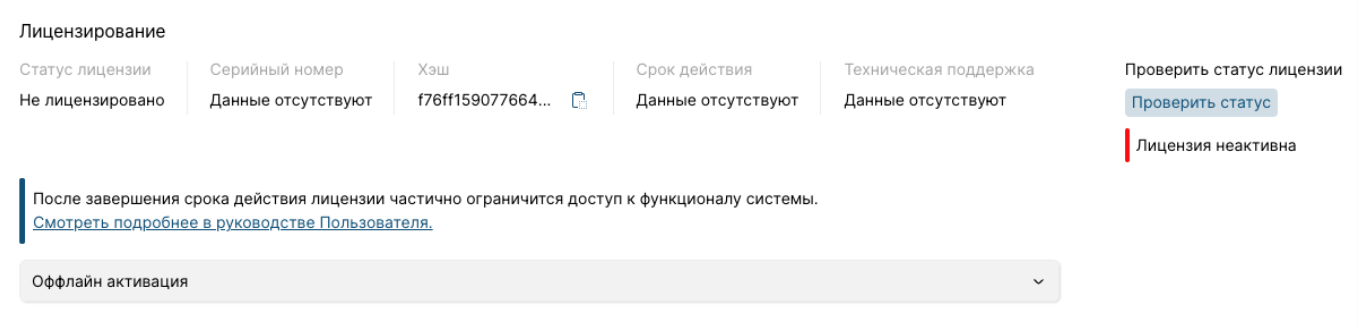


Рисунок 26 – Страница «Лицензирование» без активной лицензии»

После чего поставщиком системы будет выдан файл с расширением. json, который необходимо будет загрузить вручную. Для этого необходимо перетащить файл в поле (рис.27) для загрузки или нажатием на данное поле, открыть проводник и выбрать файл. В случае продления лицензии, весь процесс необходимо будет повторить.

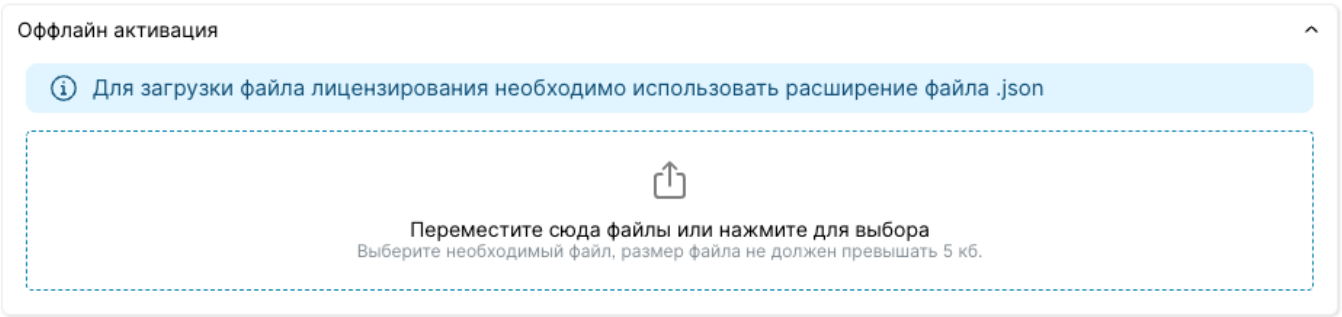


Рисунок 2710 – Блок «Оффлайн активация»

При успешной установке лицензии поля «Серийный номер», «Срок действия», «Техническая поддержка» и «Срок действия технической поддержки» будут заполнены данными о текущей лицензии, и статус лицензии изменится на «Активна» (рис.28).

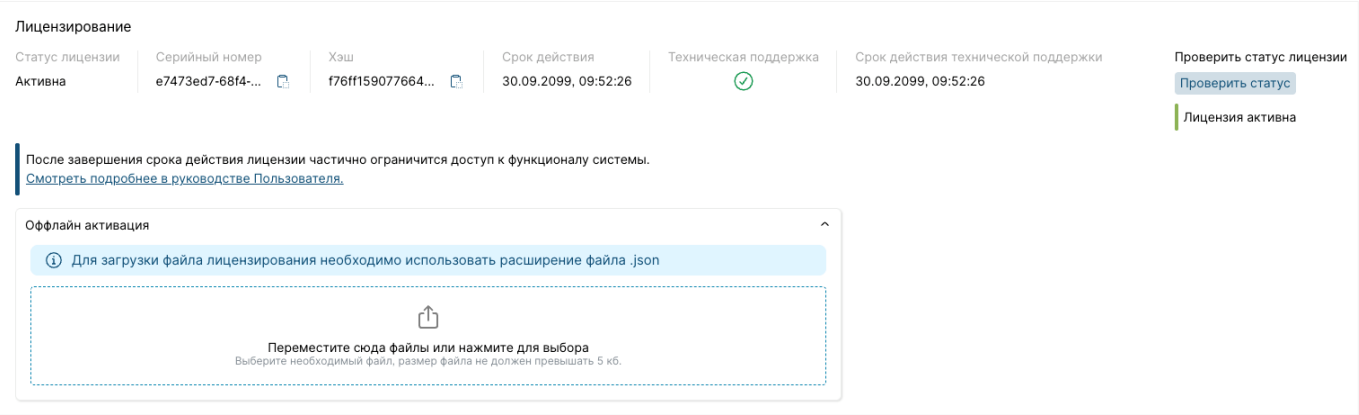


Рисунок 28– Страница «Лицензирование» с активной лицензией

Следует обратить внимание, что при изменении конфигурации, необходимо обновление лицензии, для этого следует обратиться к поставщику программного обеспечения.

3.6 Загрузка и активация базы правил

После успешной установки NT SIEM и активации лицензии база правил нормализации и корреляции остается пустой. Для обеспечения корректной обработки событий необходимо выполнить импорт предустановленного набора правил и последующую их загрузку в систему.

3.6.1 Импорт правил

Для загрузки предустановленного набора правил необходимо выполнить следующий порядок действий:

- следует перейти в раздел «База правил»,
- нажать кнопку Импорт ,
- в модальном окне выбрать опцию «Архив с папками и файлами»,
- нажать кнопку Продолжить,
- в открывшемся проводнике указать путь к архиву с правилами (например, KB_2_1_1.zip) и подтвердить выбор.

В результате папки с файлами правил отобразятся на странице «Драфт зона».

3.6.2 Активация правил

Импортированные правила находятся в статусе «черновик» и не участвуют в обработке событий. Для ввода их в эксплуатацию необходимо выполнить загрузку в систему.

Для корректной работы механизма обработки событий необходимо соблюдать последовательность загрузки: сначала все папки с правилами нормализации, затем — с правилами корреляции.

Для этого следует выполнить следующий порядок действий:

- на странице «Драфт зона» необходимо открыть первую папку с правилами нормализации. Выделить все правила внутри папки, удерживая клавишу Shift для множественного выбора,
- нажать кнопку Загрузить в систему,
- далее повторить перечисленные действия выше для каждой последующей папки с правилами нормализации,
- после завершения загрузки всех папок с правилами нормализации необходимо открыть первую папку с правилами корреляции. Выделить все правила внутри папки, удерживая клавишу Shift для множественного выбора,
- нажать кнопку Загрузить в систему,
- аналогичным образом последовательно загрузить все оставшиеся папки с правилами корреляции,
- после загрузки всех папок с правилами нормализации и корреляции необходимо нажать кнопку Перезапустить менеджер для применения изменений.

4. Сценарий развертывания коллектора

4.1. Аппаратные и программные требования

Минимальные требования для операционной системы перед установкой коллектора следующие: Ubuntu 22.04.

Аппаратные требования:

- CPU: 4 core (рекомендуется 8)
- RAM: минимум 8 ГБ (рекомендуется 16+ ГБ)
- SSD: минимум 100 ГБ свободного места (рекомендуется SSD)

Следует обратить внимание, 2 Gb RAM сверху идет на контейнер (т.е. если выбрать 8 Gb RAM - то контейнер заберет на себя 10 Gb, 8 Gb на Logstash и 2 Gb на сам контейнер).

4.2. Установка коллектора

Перед началом установки необходимо скопировать файл установщика collector.sh на удаленную машину, где будет развернут коллектор. Следующим шагом требуется повысить права до суперпользователя (root) командой sudo su.

Далее следует запустить установщик командой ./collector.sh и пройти процесс интерактивной установки (ввести следующие параметры):

Параметр	Описание	Пример
IP-адрес SIEM	Адрес центрального сервера SIEM	10.10.10.10
Размер Persistent Queue	Дисковый кэш на случай недоступности SIEM (Примерный расчет 3000eps/сутки = 260 Gb	300 (Gb)
Директория установки	Куда установить Collector	/opt/collector
JVM Heap	Память для Java (рекомендуется 50% от RAM целевой машины)	8 (Gb RAM)
Port SIEM	Порт для отправки событий (по умолчанию - 514)	514

Необходимо учитывать, что значение Persistent Queue должно быть больше суточного объема событий. При 3000 eps суточный объем ~260 Gb, поэтому 300 Gb запас на день.

После ввода данных установщик покажет выбранные параметры установки:

```
┌──────────────────────────────────────────┐
| SIEM:       10.10.10.10:514              |
| JVM Heap:   -Xms8g -Xmx8g                |
| Docker mem: limit 10g / reserve 8g       |
| PQ size:    500gb                        |
| Директория: /opt/collector
└──────────────────────────────────────────┘
```

Для продолжения установки необходимо ввести «y» или просто нажать кнопку Enter, так как «y» выбран по умолчанию:

```
Начать установку? (Y/n): y
```

Далее установщик выполнит автоматически следующие шаги:

- Шаг 1-3: Проверка наличия Docker, Docker Compose и их версий (если его нет, установщик попытается его загрузить, либо используется локальный офлайн-образ).
- Шаг 4: Проверка наличия образа Logstash (если его нет, установщик попытается его загрузить, либо используется локальный офлайн-образ).
- Шаг 5: Создание конфигурационных файлов на основе введенных параметров.
- Шаг 6: Проверка и настройка системных параметров.
- Шаг 7: Запуск контейнера Collector.

В результате будет создан Docker-контейнер, запущенный с помощью Docker Compose.

Установщик будет ожидать до 90 секунд, пока Logstash полностью запустится.

Успешный запуск Logstash будет подтвержден сообщением «[INFO] Logstash запущен».

Далее последует следующий вывод, который свидетельствует об успешной установке коллектора:

```
============================================================
  Установка завершена!
============================================================
  Docker:       Docker version 29.2.1, build a5c7197
  Heap:         8g
  PQ size:      500gb
  SIEM:         10.10.10.10:514
  Директория:   /opt/collector
  Управление:   /opt/collector/manage.sh
============================================================
```

4.3. Управление коллектором

Для управления установленным коллектором необходимо использовать скрипт manage.sh, расположенный в директории установки.

```
root@server:/opt/collector# /opt/collector/manage.sh

Usage: ./manage.sh {start|stop|restart|status|logs [N]|test|siem <host> <port>|uninstall}
```

Доступные команды для коллектора приведены в таблице ниже:

Команда	Описание	Пример
start	Запустить коллектор	/opt/collector/manage.sh start
stop	Остановить коллектор	/opt/collector/manage.sh stop
restart	Перезапустить коллектор	/opt/collector/manage.sh restart
status	Показать статус и статистику	/opt/collector/manage.sh status
logs N	Показать логи (аргумент N - количество последних строк)	/opt/collector/manage.sh logs 50
test	Отправить тестовое сообщение	/opt/collector/manage.sh test
siem host port	Показать/изменить адрес SIEM (без аргументов покажет адрес SIEM)	/opt/collector/manage.sh siem 10.10.10.11 514
uninstall	Удалить коллектор	/opt/collector/manage.sh uninstall

4.3.1 Просмотр статуса и статистики коллектора

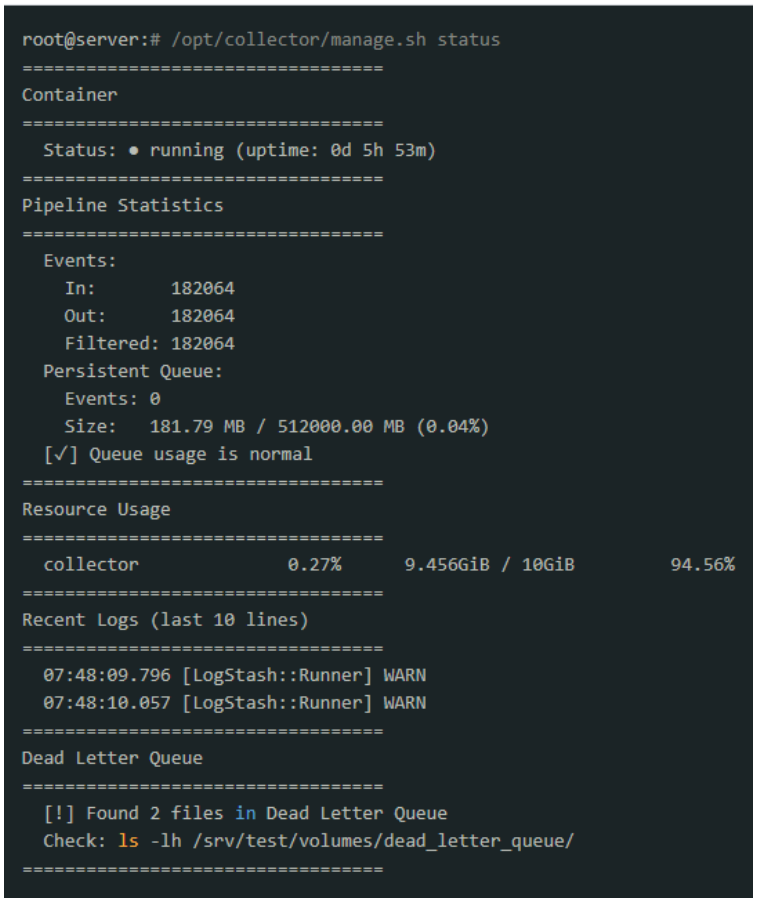
Для мониторинга работы коллектора используется команда status. Она выводит подробную информацию о работе сервиса, статистику обработки событий и использовании ресурсов.

Чтобы проверить состояние коллектора необходимо запустить скрипт **root@server:# /opt/collector/manage.sh status**, который отобразить следующие параметры:

Раздел	Параметр	Описание	Нормальное состояние
Container	Status	Состояние Docker-контейнера	Running (работает)
Pipeline Statistics	In / Out / Filtered	Количество принятых, отправленных и обработанных событий.	Значения должны совпадать (In = Out = Filtered)
Persistent Queue	Events	Количество событий в очереди	0 – очереди событий нет – коллектор работает в штатном режиме

Раздел	Параметр	Описание	Нормальное состояние
	Size	Текущий размер очереди / максимальный размер	Должен быть значительно меньше максимума, например 0,4%
	Queue usage	Статус использования очереди	[✓] normal — очередь в норме
Resource Usage	Collector	Состояние загрузки ресурсов контейнера	CPU < 95% , RAM < 95%
Recent Logs	Последние 10 строк лога	Логи состояния контейнера	Чистые логи (без ERROR)
Dead Letter Queue	Наличие файлов	События, которые не удалось обработать (если есть)	[!] — требует внимания

Пример вывода статуса коллектора с диагностической информацией:



4.3.2 Изменение адреса SIEM (без переустановки коллектора)

Для изменения IP – адреса или порта сервера SIEM необходимо использовать встроенную команду siem:

1. Просмотр текущего IP- адреса Siem:

   /opt/collector/manage.sh siem

2. Установка нового адреса и порта:
   /opt/collector/manage.sh siem <новый_IP> <новый_порт>
   Например:
   /opt/collector/manage.sh siem 10.10.10.11 514
3. Перезапуск коллектора для применения изменений:
   /opt/collector/manage.sh restart

Пример изменения адреса SIEM (без переустановки коллектора):

```
root@server:# /opt/collector/manage.sh siem
SIEM_HOST=10.10.10.10
SIEM_PORT=514
# Проверяем изменения
root@server:# /opt/collector/manage.sh siem 10.10.10.11 514
10.10.10.11:514
# Перезапустить для применения новых настроек
root@server:# /opt/collector/manage.sh restart
```

4.3.3 Обновление коллектора

Для обновления коллектора необходимо выполнить следующий алгоритм действий:

1. Скачать файл установщика новой версии
2. Остановить работающий коллектор с помощью команды **cd /opt/collector**
   ./manage.sh stop
3. Сделать файл установки исполняемым следующей командой **chmod +x collector_********.sh**
4. Запустить установщик новой версии с помощью команды **sudo bash collector-9.2.5-XXXXXXXX.sh**
5. Указать ту же директорию (/opt/collector)

Пример обновления коллектора:

```
# 1. Скачать новую версию установщика
# 2. Остановить старую версию
cd /opt/collector
./manage.sh stop

# 3. Запустить новый установщик
sudo bash collector-9.2.5-XXXXXXXX.sh

# 4. Указать ТУ ЖЕ директорию (/opt/collector)
# Установщик сохранит существующую очередь и конфиги
```

4.3.4 Полное удаление коллектора

Для полного удаления коллектора с сервера предусмотрено два способа:
- автоматическое (с помощью встроенной команды),
- ручное.

При автоматическом удалении необходимо выполнить следующие команды последовательно:

1. Необходимо перейти в директорию установки:
   cd /opt/collector
2. Запустить процесс удаления:
   ./manage.sh uninstall
3. Подтвердить удаление, введя «y»

При ручном удалении необходимо выполнить следующие команды последовательно:

1. Зайти в директорию /opt/collector командой **cd /opt/collector**
2. Остановить и удалить данные из docker compsoe командой **docker compose down -v**
3. Удалить образ контейнера коллектора командой **docker rmi docker.elastic.co/logstash/logstash:9.2.4**
4. Удалить полностью директорию, где был установлен коллектор командой **rm -rf /opt/collector**

Пример полного удаления коллектора:

```
cd /opt/collector
./manage.sh uninstall
# Подтвердить удаление (y)

# Или вручную:
docker compose down -v
docker rmi docker.elastic.co/logstash/logstash:9.2.4
rm -rf /opt/collector
```

5.Установка обновлений

Для определения версий NTechnology SIEM применяется подход семантического версионирования, в котором существуют следующие категории:

– мажорное обновление (MAJOR) – внесение изменений, нарушающих обратную совместимость;

– минорное обновление (MINOR) – добавление новой функциональности при сохранении обратной совместимости;

– обновление посредством патча (PATCH) – исправление ошибок или внесение мелких функциональных изменений.

Версия представляется в виде трех чисел, разделенных точками: MAJOR.MINOR.PATCH. Каждое из этих чисел отражает определенный аспект изменений. Так, например:

– переход от версии 1.1.1 к версии 2.0.0 свидетельствует о значительных необратимых изменениях, например, в методе обработки информации;

– переход от версии 1.1.1 к версии 1.2.0 свидетельствует о таких дополнениях, как изменение интерфейса с добавлением новой функциональности;

– переход от версии 1.1.1 к версии 1.1.2 свидетельствует об исправлениях или небольших улучшениях, которые не влияют на основную функциональность.

Установка новых версий NTechnology SIEM должна производиться строго в соответствии с приведенной ниже таблицей совместимости.

Версия для установки	**С каких версий можно выполнить обновление**
v1.0.1	v1.0.0
v1.0.2	v1.0.1
v1.1.0	v1.0.2
v1.1.1	v1.1.0
v1.1.2	v1.1.1
v1.2.0	v1.1.2
v1.2.1	v1.2.0, v1.1.2
v1.2.2	v1.2.1, v1.2.0, v1.1.2
v1.2.3	v1.2.2, v1.2.1, v1.2.0, v1.1.2
v2.0.0	v1.2.3
v2.0.1	v2.0.0
v2.1.0	v2.0.1
v2.1.1	v2.1.0

Следует обратить внимание, что в период установки новой версии могут происходить потери событий, следовательно, для их минимизации, рекомендуется проводить обновления в периоды низкой нагрузки.

5.1 Установка обновлений NT SIEM v1.0.1, v1.0.2, v1.1.0, v1.1.1, v1.1.2

В период установки новой версии могут происходить потери событий, следовательно, для их минимизации, рекомендуется проводить обновления в периоды низкой нагрузки.

Для установки версий NT SIEM v1.0.1, v1.0.2, v1.1.0, v1.1.1, v1.1.2 необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf MAJOR.MINOR.PATCH.tar.gz -C siem-docker/
```

где **MAJOR.MINOR.PATCH.** – номер версии NTechnology SIEM.

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x a.b.c.sh
./ MAJOR.MINOR.PATCH.sh
```

где **MAJOR.MINOR.PATCH.** – номер версии NTechnology SIEM.

5.2 Установка обновлений NT SIEM v1.2.0, v1.2.1, v1.2.2, v1.2.3, v2.0.0, v2.0.1, v2.1.0, v2.1.1

Для того, чтобы распаковать исходные файлы следует переключиться на пользователя `root`, имеющего администраторский доступ к вашей системе, и выполнить команду для создания временной директории:

```
mkdir temp/
tar -zxvf NtechnologySiem_vMAJOR.MINOR.PATCH.tar.gz -C temp/
```

где **MAJOR.MINOR.PATCH.** – номер версии NTechnology SIEM

После распаковки архива необходимо перейти в директорию, выполнив команду, где будут находиться два файла **MAJOR.MINOR.PATCH**`.tar.gz, new_install.sh`:

```
cd temp/
```

где **MAJOR.MINOR.PATCH.** – номер версии NTechnology SIEM.

Далее необходимо поменять права доступа для файла `new_install.sh`, который уже входит в состав дистрибутива. Для этого необходимо ввести в консоли следующую команду:

```
chmod u+x new_install.sh
```

После изменения прав доступа ввести в консоли команду для запуска скрипта установки:

```
./ new_install.sh
```

Для корректной работы просмотра действий пользователей рекомендуется произвести замену токена в ранее настроенных интеграциях.

6. Работа с сервисами для сбора событий с Windows

6.1 Установка, удаление, остановка работы сервиса

Перед установкой сервиса необходимо заполнить файл конфигурации (п.6.2). Установка может происходить с использованием интерпретатора командной строки или с добавлением сервиса в программы и компоненты.

Установка с использованием интерпретатора командной строки. Для того чтобы установить сервис, необходимо запустить файл инсталлятор `ntechnology-events-collector-x32.exe` или `ntechnology-events-collector-x64.exe` с параметром `install`, которые находятся в директории `NtechnologyEventsCollector` в распакованном при установке архиве.

После запуска инсталлятор запускает службу сбора событий и создает файл конфигурации в папке `C:\Program Files \NEC`. Там же будут хранить логи по работе сервиса. Можно запустить с параметром `start`, удалить с параметром `uninstall` или остановить работу сервиса с параметром `stop`.

Установка с добавлением сервиса в программы и компоненты. Необходимо запустить двойным кликом файл инсталлятор `ntechnology-events-collector-x32.msi` или `ntechnology-events-collector-x64.msi`, которые находятся в директории `NtechnologyEventsCollector` в распакованном при установке архиве.

После запуска инсталлятор запускает службу сбора событий и создает файл конфигурации в папке `C:\Program Files \NEC`. Там же будут хранить логи по работе сервиса. Удаление сервиса происходит через раздел «Программы и компоненты» в «Панели управления» Windows.

6.2 Заполнение файла конфигурации

Для корректной работы необходимо заполнить файл конфигурации. Файл конфигурации должен быть в формате `.toml`. Шаблон представлен ниже:

```
# # Service is enabled, can be started manually (Required).
# service_start_type = "OnDemand"
```

```
# # Disabled service (Required).
# service_start_type = "Disabled"
# # Autostart on system startup (Required).
service_start_type = "AutoStart"
# # Start delay in secs (Required).
start_delay = 10

[nec_config]
# Log level. One of ["info", "debug","error", "warn", "trace"].
# Default = "info"
log_level = "info"

# Win Event Wmi section.
# Can connect to local machines.
# Describes by set (must be uniq) of [[nec_config.win_event_wmi]] sections.

# Local 1
[[nec_config.win_event_wmi]]

[nec_config.win_event_wmi.local]
# Namespace path (Optional, default = "ROOT\\\\CIMV2").
# namespace_path = "local1"

[nec_config.win_event_wmi.local.poll_config]
# Polling interval in secs (Required).
interval = 5
# List of log files (Required).
log_files = ["Application"]



# # Local 2
# [[nec_config.win_event_wmi]]

# [nec_config.win_event_wmi.local]
# # Namespace path (Optional, default = "ROOT\\\\CIMV2").
# namespace_path = "local2"
```

```
# [nec_config.win_event_wmi.local.poll_config]
# # Polling interval in secs (Required).
# interval = 5
# # List of log files (Required).
# log_files = ["Application", "Windows Powershell"]



# # Win Event Subscriber section (enable only for Windows.Client >= Vista &
Windows.Server >= 2008).
# [nec_config.win_event_subscriber]
# # A query that specifies the types of events that you want the
subscription service to return.
# x_query = '''
# <QueryList>
#   <Query Id="0">
#     <Select Path="Windows PowerShell">*</Select>
#     <Select Path="Application">*</Select>
#   </Query>
# </QueryList>
# '''



# File Watcher section.
[nec_config.file_watcher]
# Paths for watch (Required).
paths = ['D:\path.txt']
# # Retrys to send event to inner channel (Optional, default = 3).
# send_to_channel_retrys = 3

# Poll watcher kind.
[nec_config.file_watcher.watcher_kind.poll]
# Polling interval in secs (Required).
interval = 5

# # Recommended watcher (get notification from system, maybe not work in
some cases).
# [nec_config.file_watcher.watcher_kind.recommended]
```

```
# Event Sender section.

# Udp section.
[nec_config.event_sender_config.udp]
local_addr = "0.0.0.0"
local_port = 8081
remote_addr = "127.0.0.1"
remote_port = 514
# # Bound of inner channel for events (Optional, default = 10000).
# channel_bound = 10000

# # Tcp section.
# [nec_config.event_sender_config.tcp]
# remote_addr = "127.0.0.1"
# remote_port = 8888
```

Описание файла конфигурации и его составляющий представлена в таблице 4:

Таблица 4– Параметры файла конфигурации

Параметр	**Описание**
Конфигурация сервиса	
`service_start_type`	Допустимые значения: `OnDemand` – сервис включен, но необходим ручной запуск; `Disabled` – сервис выключен; `AutoStart` – сервис включен и запускается автоматически.
`start_delay`	Время ожидания запуска после поднятия системы в секундах, используется при `service_start_type = "AutoStart"`.
Конфигурация коллектора `[nec_config]`	
`log_level`	По умолчанию, `log_level = "info"` Допустимые значения:

Параметр	Описание
	info – минимально необходимая информация; debug – подробная информация необходимая для отладки приложения; error – ситуация которая не должна была случиться в приложении (ошибка); warn – предупреждение; trace – полное логирование всех входящих и исходящих сообщений.
Блок [nec_config.win_event_wmi]	
namespace_path	Путь до возможного пространства имен. По умолчанию, default = "ROOT\\\\CIMV2"
[nec_config.win_event_wmi.local.poll_config]	
log_files	Массив названий каналов, откуда будут собираться события.
interval	Частота сбора событий, в секундах.
Блок [nec_config.win_event_subscriber]	
x_query	Обязательно поле для указания каналов сбора событий.
<Select Path="Windows PowerShell">*</Select>	* – используется для задания фильтра поиска событий.
Блок [nec_config.file_watcher]	
paths	Массив путей до файлов, с которых необходимо совершать сбор событий.
send_to_channel_retrys	Количество попыток для отправки данных по каналу channel_bound.
[nec_config.file_watcher.watcher_kind.poll]	
interval	Частота сбора событий, в секундах.
Блок [nec_config.event_sender_config.udp]	

Параметр	Описание
local_addr	По умолчанию, local_addr = "0.0.0.0" IP-адрес, откуда будет совершаться сбор данных.
local_port	Порт, откуда будет совершаться сбор данных.
remote_addr	IP-адрес, где стоит SIEM-система для передачи собранных событий.
remote_port	Порт, где стоит SIEM-система для передачи собранных событий.
channel_bound	По умолчанию, channel_bound = 10000. Размер очереди событий.
Блок [nec_config.event_sender_config.tcp]	
remote_addr	IP-адрес, где стоит SIEM-система для передачи собранных событий.
remote_port	Порт, где стоит SIEM-система для передачи собранных событий.

Блоки Win Event Wmi и Win Event Subscriber собирают события из Windows Event Log.

Блок Win Event Subscriber рекомендуется для использования, так как данные Windows машина передает сама, и нет необходимости в постоянном опросе. Однако есть ограничения. Блок Win Event Subscriber доступен для Windows.Client >= Vista & Windows.Server >= 2008.

Блок File Watcher используется для подключения к файлам с целью мониторинга и сбора событий.

Блок Poll watcher kind используется для указания интервала опроса.

Блок Event Sender используется для указания параметров, определяющих, куда направлять собранные данные.