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).

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 функциональные возможности:

- Активный и пассивный сбор журналов событий с различных источников;
- Мониторинг событий и инцидентов, а также агентов и состояния системы;
- Визуализация данных в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Реагирование на инциденты 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 с возможностью дополнительно загрузить системные правила, а также создать пользовательские правила и табличные списки;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Выгрузка отчетов за настраиваемый период времени;
- Интеграция с SOAR-системами.

2. Схема взаимодействия компонентов

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

Направленность стрелок указывает сетевые вызовы – от инициатора к получателю.

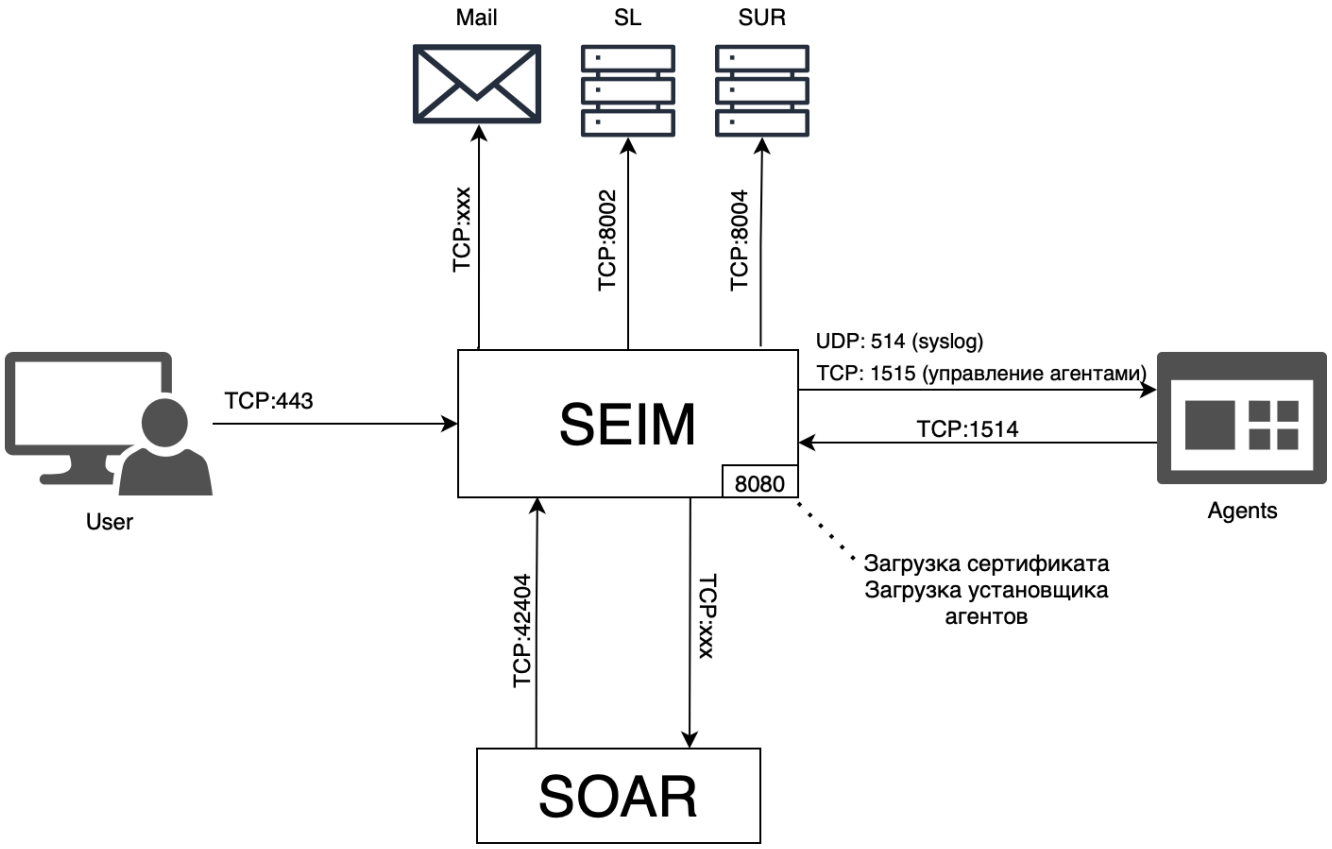

Рисунок 1 – Схема взаимодействия компонентов

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.

Обратите внимание, что с версии NT SIEM v1.0.2 для работы с пользовательским интерфейсом на межсетевом экране должен быть открыт порт 443.

3. Сценарий развертывания системы

3.1 Аппаратные и 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. Необходимо смонтировать все свободное пространство под корневую директорию (рис. 2).

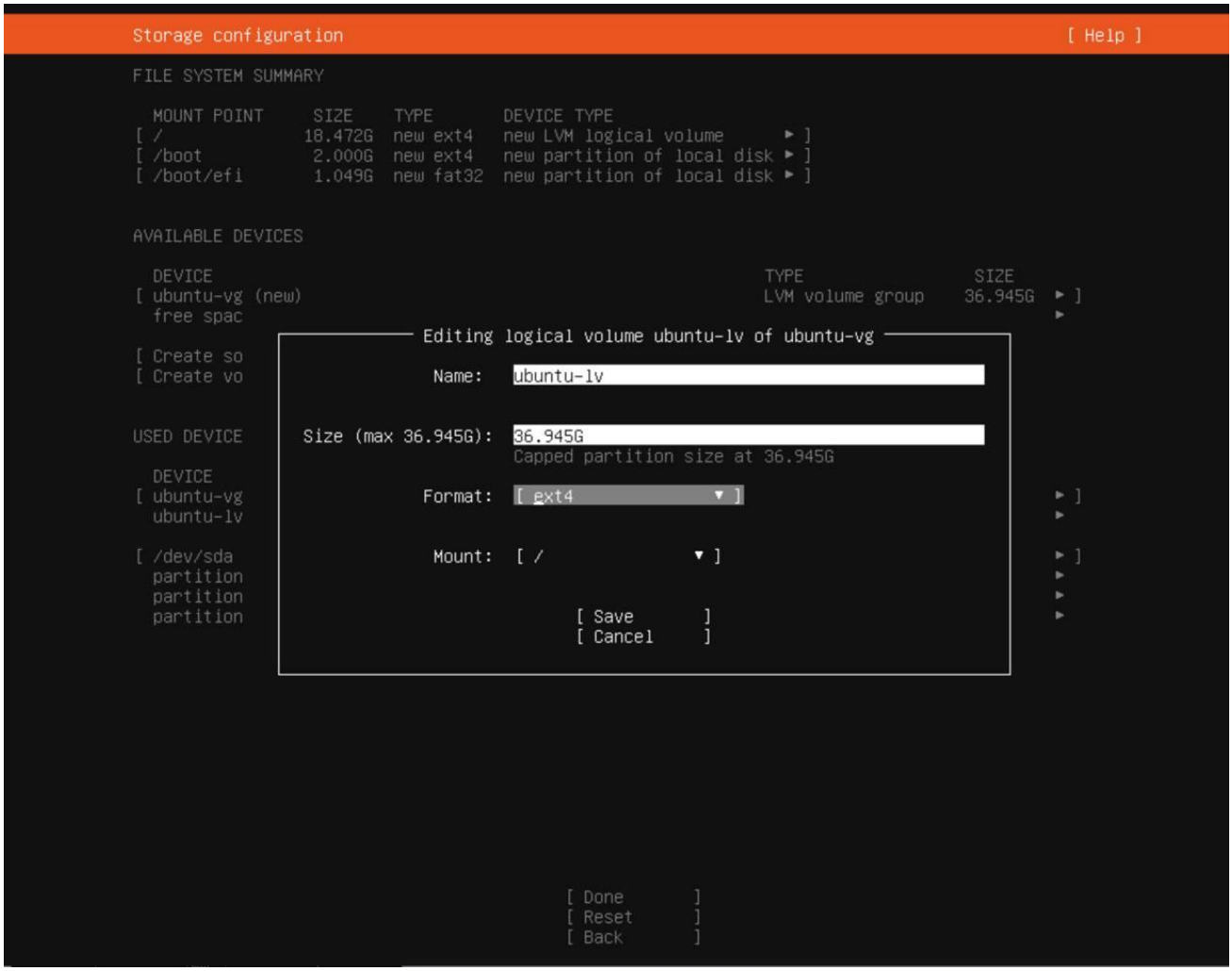

Рисунок 2 – Разметка дискового пространства

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

Кроме того, для своей работы NT SIEM использует данные, поставляемые сторонними программными продуктами – агентами, которые могут быть установлены на операционных системах семейств Linux, Windows.

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.

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	1 КБ (1024 байта).
Время хранения	30 дней (2 592 000 секунд).

Подставив данные в формулу, получим:

Объем данных = 1000 × 1024 × 2 592 000 ≈ 2.59 ТБ.

Таким образом, для хранения данных за 30 дней потребуется около 2.6 ТБ дискового пространства.

Аналогично можно посчитать, что для 1000 EPS требуется пространство в 25 ТБ с расчетом на то, что данные должны хранится год. Пример конфигурации системы для 1000 EPS отражен в таблице 2.

Таблица 2 – Примеры конфигурации для 1000 EPS

Компонент	**CPU min (ядра)**	**CPU rec (ядра)**	**RAM min (Гб)**	**RAM rec (Гб)**
Manager	4	6	8	16
Indexer	6	8	16	32
Остальные сервисы	2	4	8	16
Всего	12	18	32	64

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:

```
tar -xvf NTechnologySIEM.tar
```

Иерархическая структура каталогов до начала процесса установки должна быть как на рисунке 3.

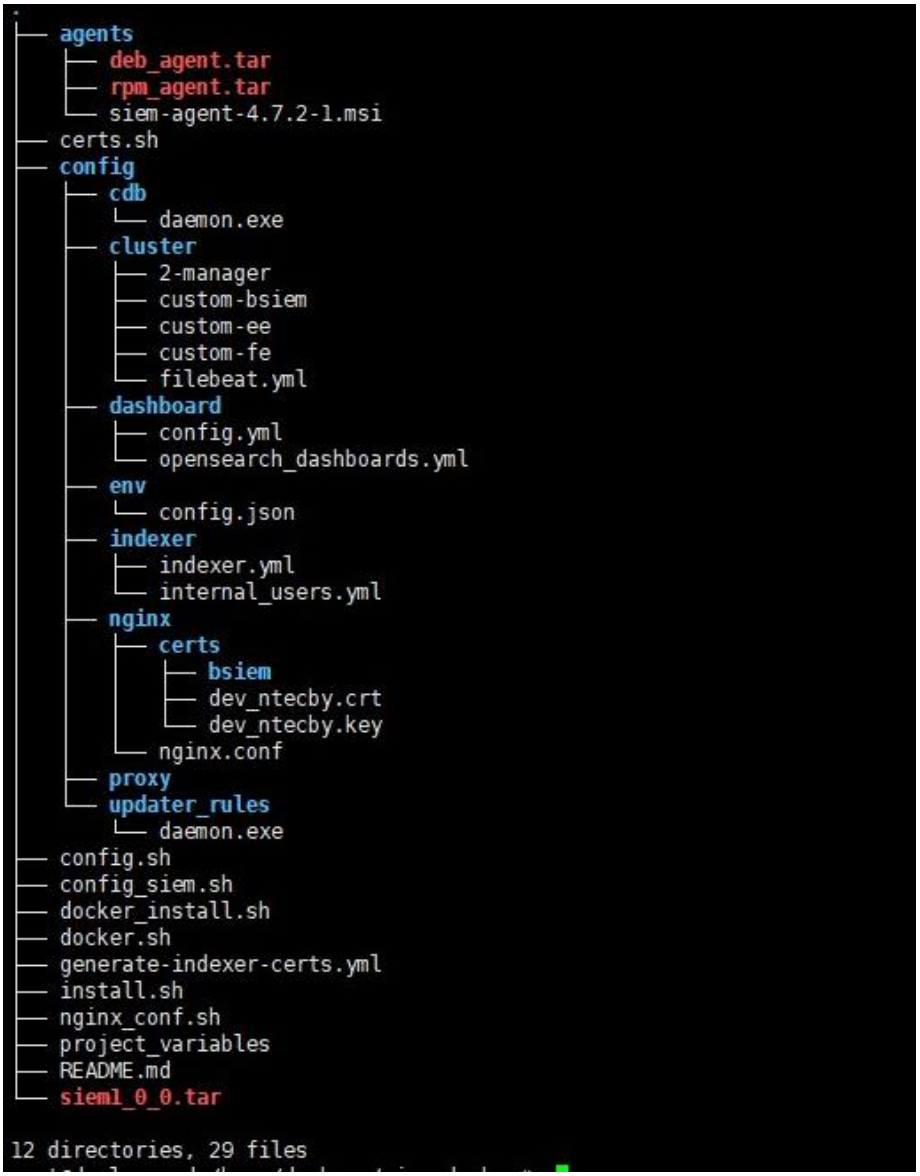

Рисунок 3 – Иерархическая структура каталогов дистрибутива до начала процесса установки

После распаковки архива необходимо перейти в директорию *siem-docker*, выполнив команду:

```
cd siem-docker/
```

После скачивания файлов из дистрибутива необходимо подготовить файл с переменными для установки путем редактирования файла-шаблона `project_variables`, который уже входит в состав дистрибутива. В файле необходимо указать переменные, актуальные для инфраструктуры.

```
#!/bin/bash
#Ввести IP-адрес хоста машины, где будет произведена установка системы (заменить данные после знака «=»)

IP=IP_Address

 # IP-адрес сервера лицензирования

IP2=IP_ADDRESS_SERVER_LICENSE

# Ввести Network Syslog. В данной опции следует указывать из каких ip-сетей осуществлять сбор событий от агентов (заменить данные после знака «=»). Например, NETWORK=0.0.0.0 означает, что сбор событий от агентов происходит из всех подсетей.

NETWORK=0.0.0.0

MASK=0

#DB RAM (2048, 4096, 8192,16384). Следует указать, сколько выделить оперативной памяти, но не более 50 % от общей оперативной памяти. Обратить внимание, что необходимо изменять цифры в выражении (2048, 4096, 8192, 16384).

DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms4096m -Xmx4096m"'

ИЛИ

DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms2048m -Xmx2048m"'
```

После подготовки файла с переменными необходимо ввести по порядку следующие команды:

```
chmod u+x docker_install.sh
./docker_install.sh
docker load -i siem1_0_0.tar
docker tag harbor.dev.ntecby/siem/main-backend-develop:1.0.0 harbor.dev.ntecby/siem/main-backend:1.0.0
docker tag harbor.dev.ntecby/siem/notifier-develop:1.0.0 harbor.dev.ntecby/siem/notifier:1.0.0
docker tag harbor.dev.ntecby/siem/frontend-new-develop:1.0.0 harbor.dev.ntecby/siem/frontend-new:1.0.0
docker tag harbor.dev.ntecby/siem/report-engine-develop:1.0.0 harbor.dev.ntecby/siem/report-engine:1.0.0
docker tag harbor.dev.ntecby/siem/query-engine-develop:1.0.0 harbor.dev.ntecby/siem/query-engine:1.0.0
docker tag harbor.dev.ntecby/siem/incident-engine-develop:1.0.0 harbor.dev.ntecby/siem/incident-engine:1.0.0
docker tag harbor.dev.ntecby/siem/dashboard-engine-develop:1.0.0 harbor.dev.ntecby/siem/dashboard-engine:1.0.0
```

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

```
chmod u+x install.sh
```

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

```
./install.sh
```

При успешном завершении установки NT SIEM будет показан результат как на рисунке 4:

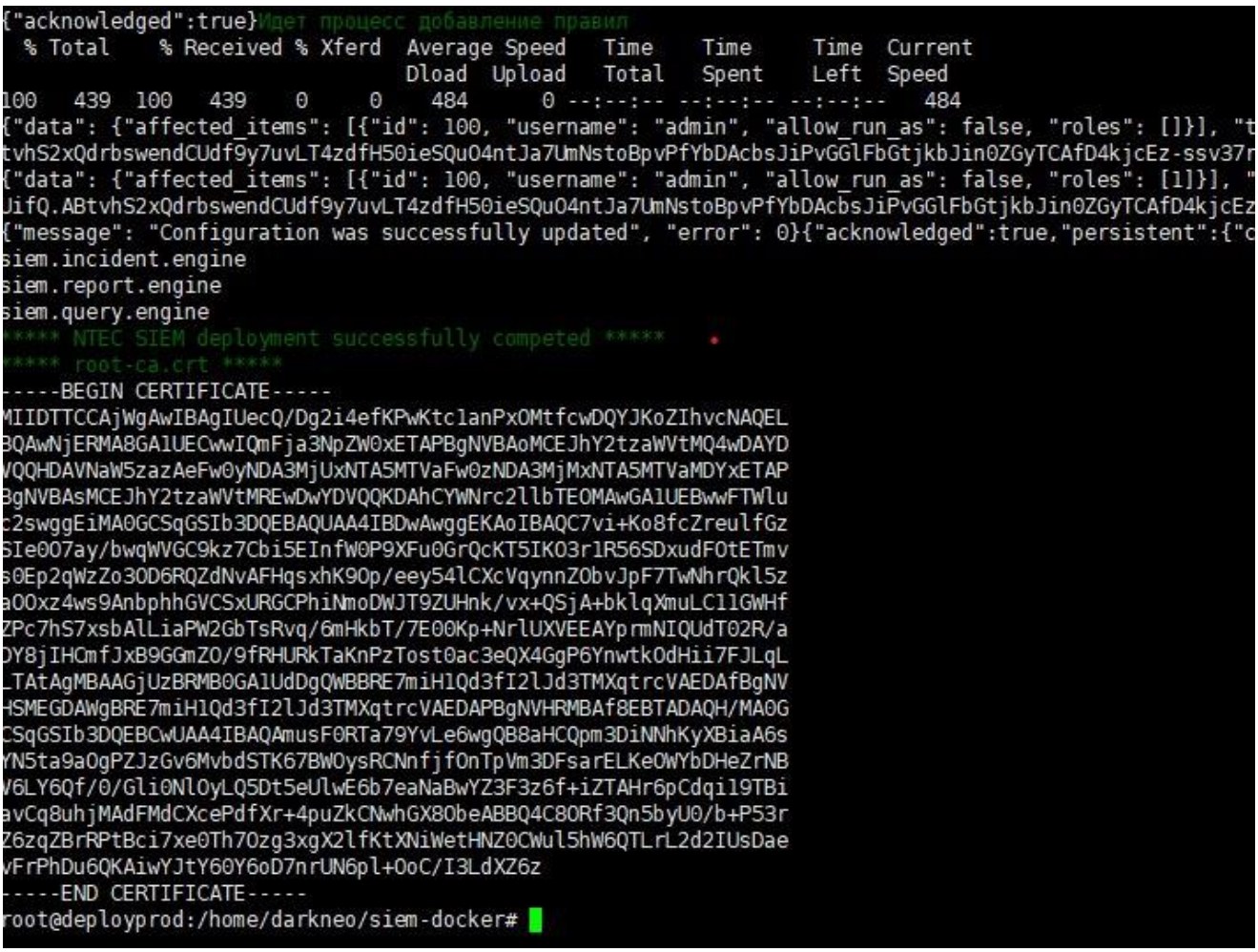

Рисунок 4 – Положительный результат выполнения процесса установки NT SIEM

Иерархическая структура каталогов после процесса установки должна быть как на рисунке 5.

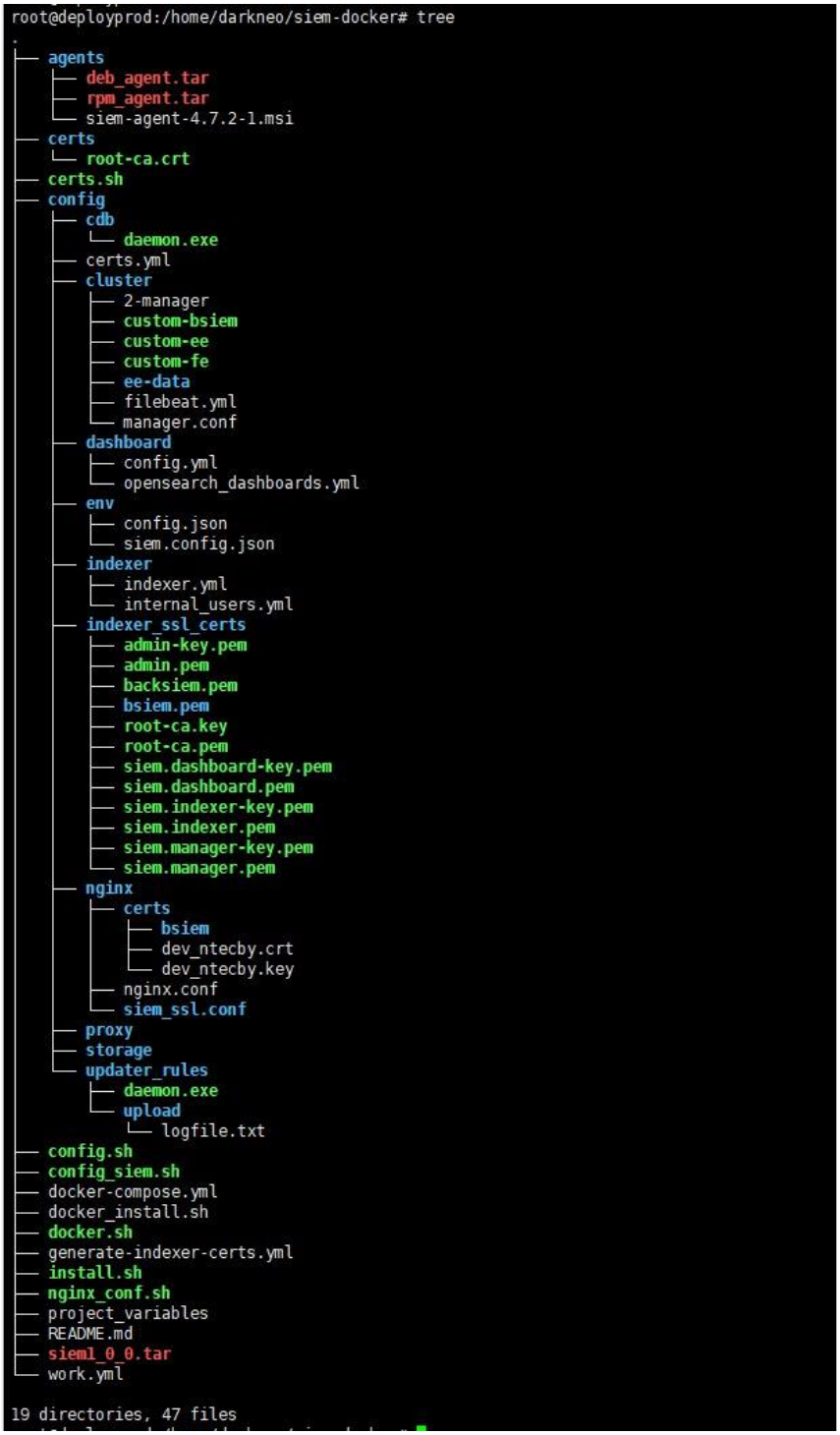

Рисунок 5 – Иерархическая структура каталогов дистрибутива

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.

После загрузки веб-интерфейс будет выглядеть на как рисунке 5. Далее необходимо скачать и установить доверенный корневой сертификат (см. пункт 3.2). Чтобы установить доверенный сертификат, необходимо сначала открыть систему NT SIEM в браузере и скачать сертификат, нажав на кнопку «Скачать сертификат» на странице авторизации в правом нижнем углу.

Просим обратить внимание, что в случае использования браузера Mozilla Firefox (см. пункт 3.2.4) добавление доверенного сертификата обязательно. В этом случае, нужно предварительно скачать сертификат в другом браузере.

Рисунок 6 – Страница авторизации системы NT SEIM

В ходе установки системы также подгружаются системные правила, используемые для обработки и анализа данных в NT SIEM. Стоит обратить внимание, что описание ручной загрузки системных правил можно найти в «Руководство Пользователя».

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:

1. Выбрать в боковом меню страницу «Настройки системы» (рис. 5).
2. На вкладке «Пользователи» выбрать пользователя с ролью «Супер Администратор».
3. Нажать на кнопку «Редактировать».
4. Ввести новый пароль.
5. 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.

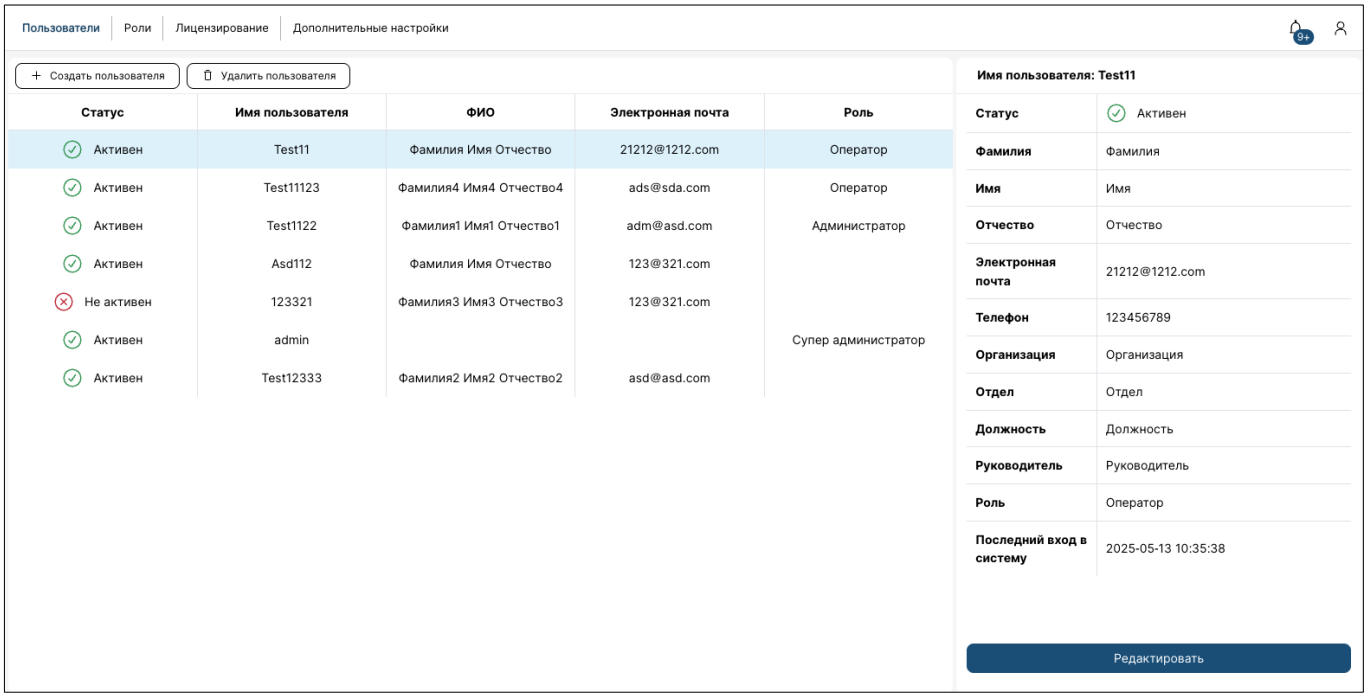

Рисунок 7 – Страница «Настройки системы»

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

Скачайте сертификат из веб-интерфейса системы NT SIEM (рис 6, 8).

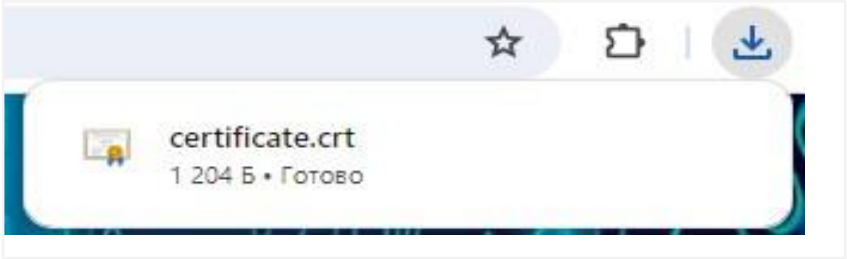

Рисунок 8 – Результат скачивания

На скачанном файле корневого сертификата нажмите правой кнопкой мыши и выберите «Установить сертификат» (рис. 9). В открывшемся окне «Мастер импорта сертификатов» помощника установки выберите необходимый пункт и нажмите «Далее».

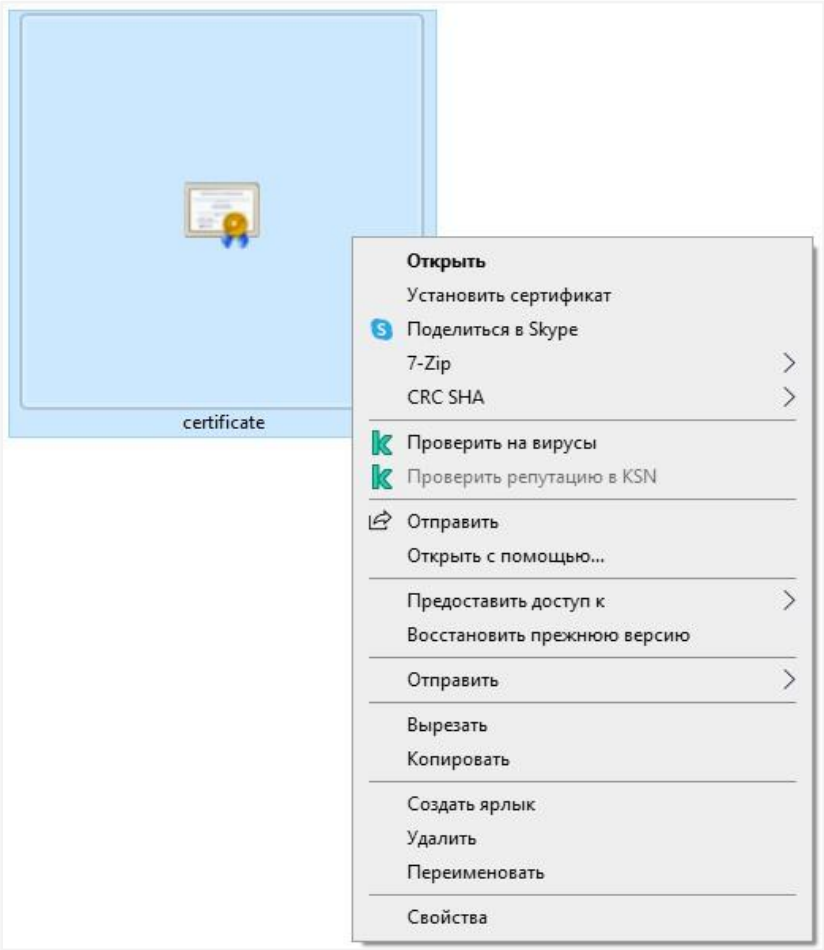

Рисунок 9 – Начало установки доверенного сертификата

На странице «Хранилище сертификатов» нужно выбрать «Поместить все сертификаты в следующее хранилище», выберите «Обзор», найдите необходимую папку для сертификата и затем нажмите кнопку «Далее» (рис 10).

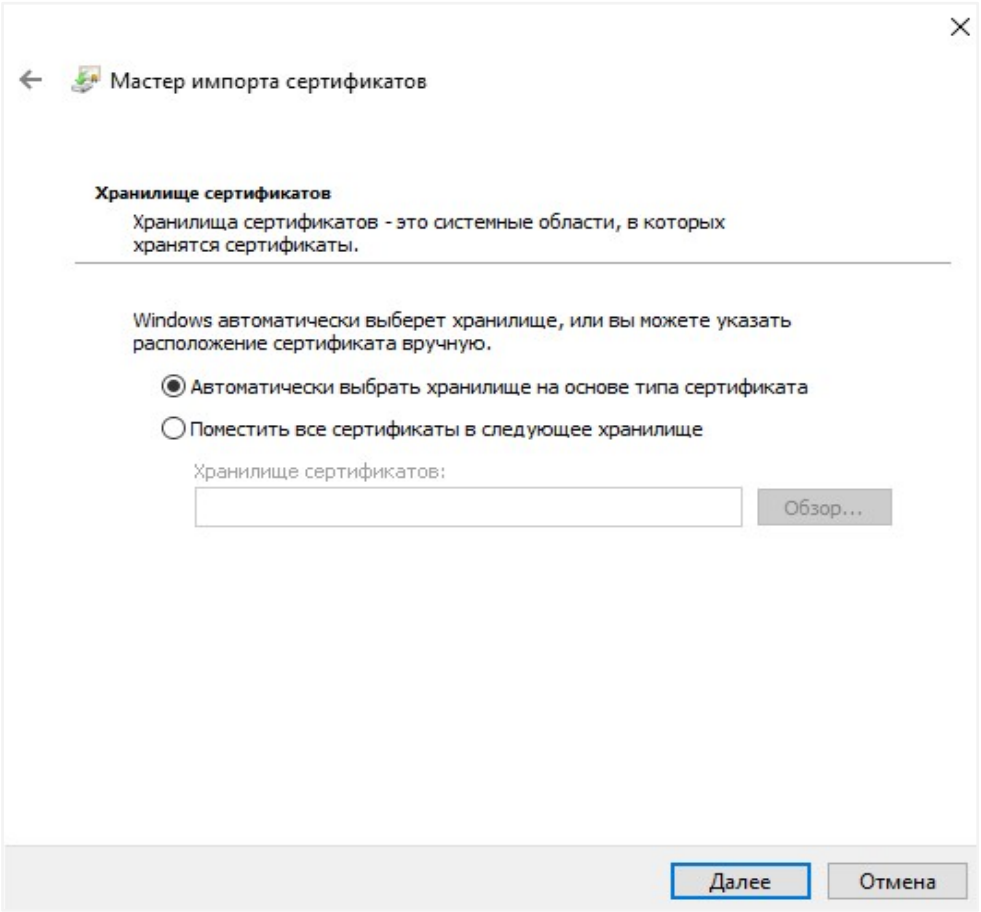

Рисунок 10 – Хранилище сертификатов

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

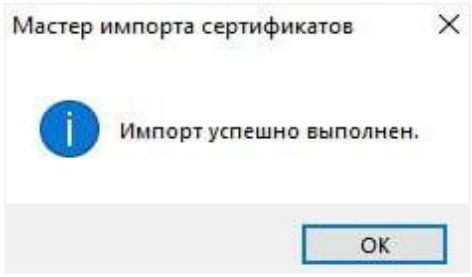

Рисунок 11 – Успешное выполнение импорта сертификата

Перед работой с системой NT SIEM следует перезагрузить рабочую станцию.

3.3.2 Установка сертификата для ОС семейства MacOS

Скачать сертификат из веб-интерфейса системы NT SIEM (рис 6, 8). 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 12), ввести пароль, при необходимости и закрыть приложение «Связка ключей» (см. подробную информацию в справочном центре Apple).

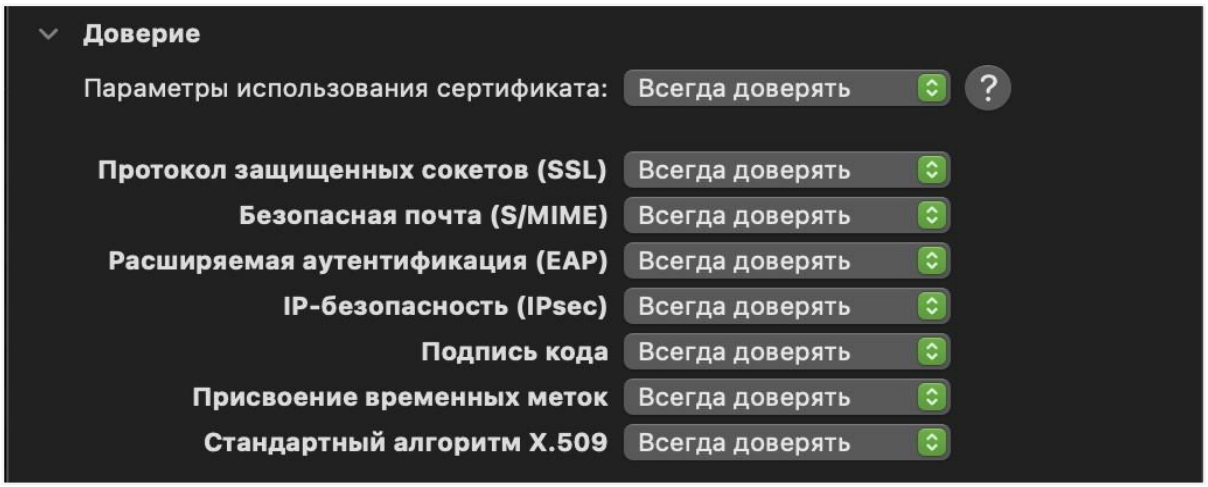

Рисунок 12 – Вкладка «Доверие» приложения «Связка ключей»

Перед работой с системой NT SIEM следует перезагрузить рабочую станцию.

3.3.3 Установка сертификата для браузера Google Chrome

Открыть браузер Google Chrome. Скачать сертификат из веб-интерфейса системы NT SIEM (рис 6, 8).

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. 13).

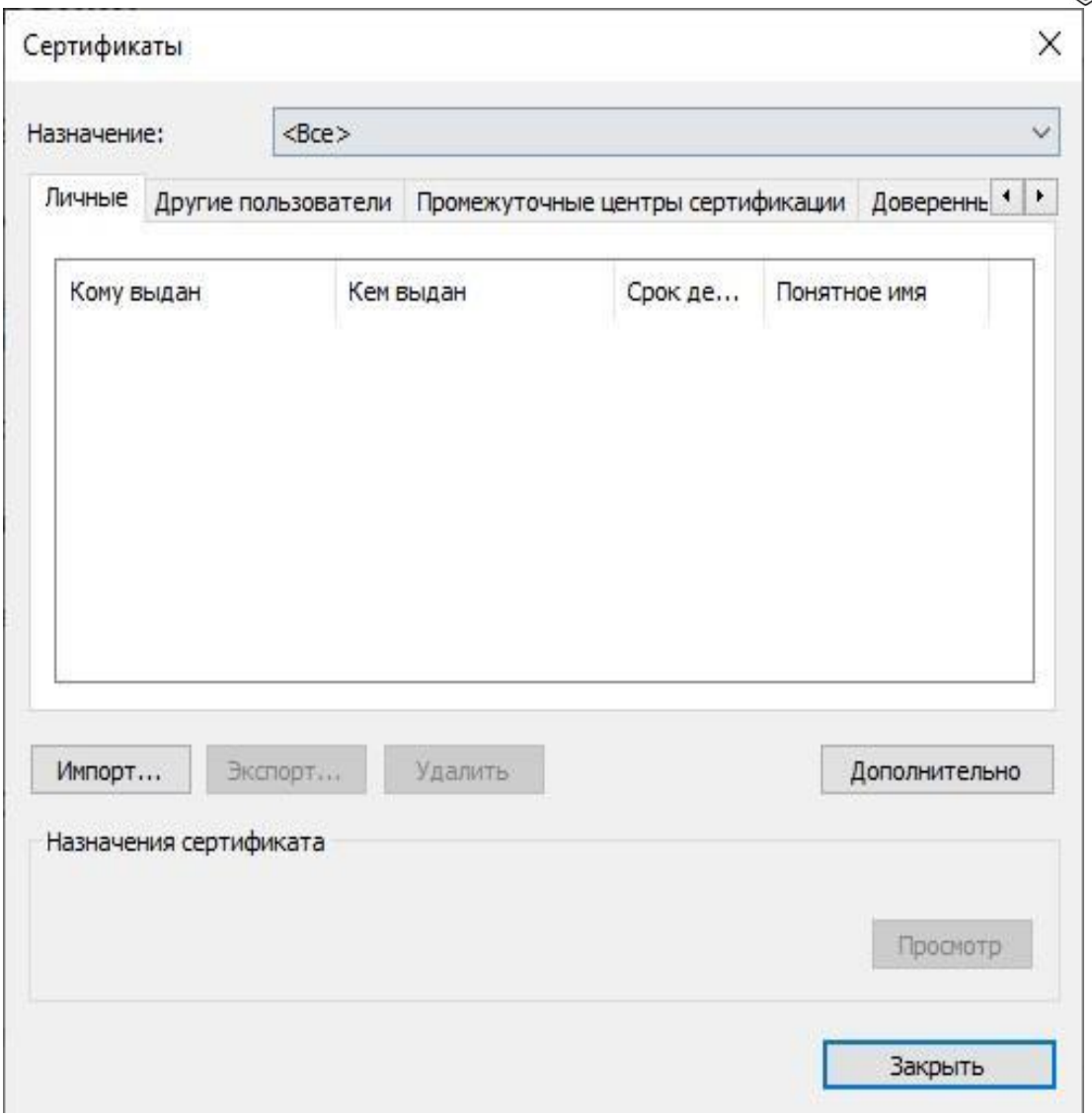

Рисунок 13 – Страница «Сертификаты»

Для установки сертификата следует перейти на вкладку «Доверенные корневые центры сертификации» и нажмите кнопку «Импорт...». Откроется окно «Мастер импорта сертификатов» (рис. 14).

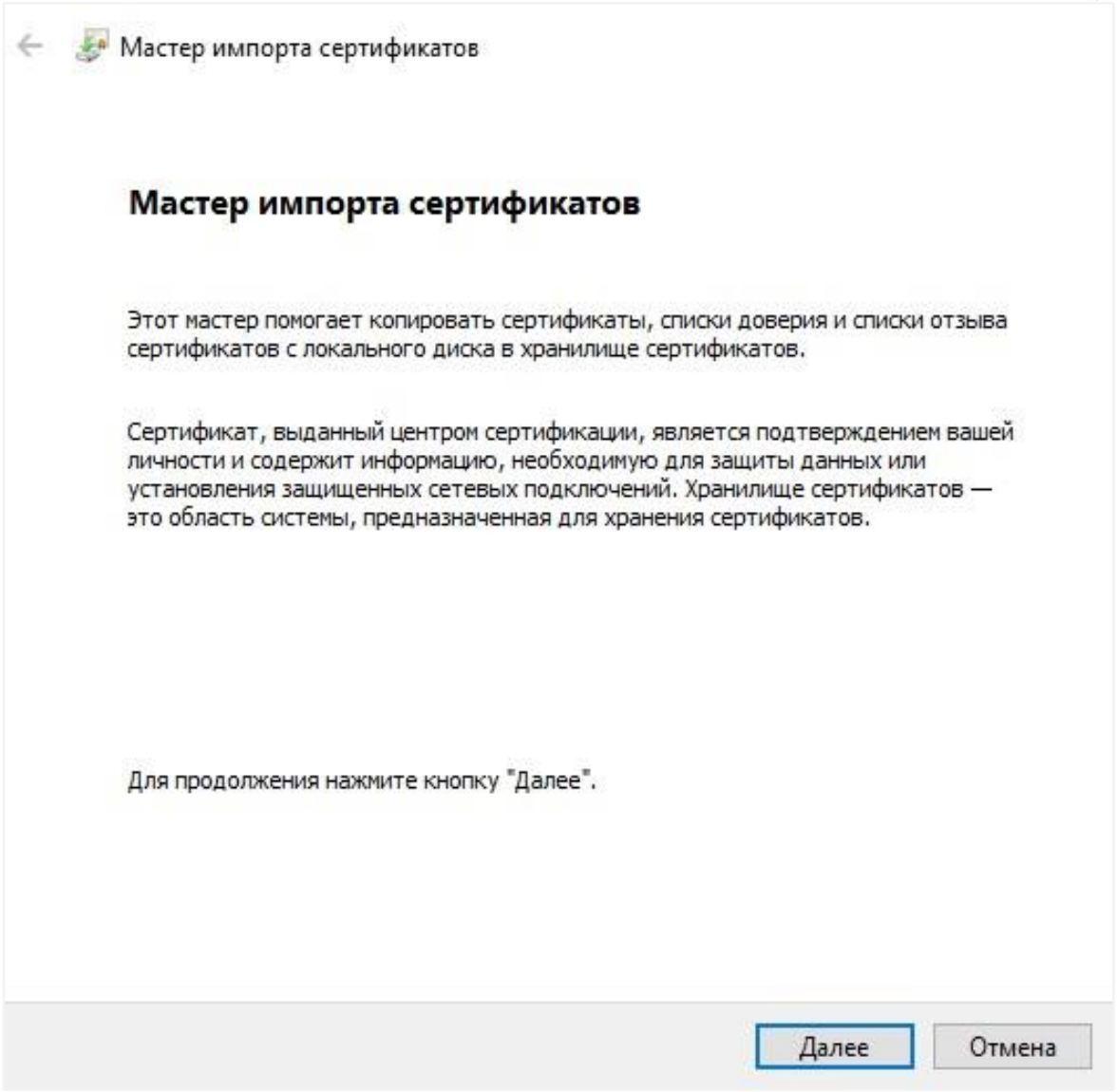

Рисунок 14 – Окно «Мастер импорта сертификатов»

В открывшемся окне «Мастер импорта сертификатов» помощника нажать «Далее», откроется окно «Импортируемый файл» (рис. 15). Далее необходимо нажать кнопку «Обзор», выбрать ранее скачанный сертификат. Результат представлен на рисунке 16.

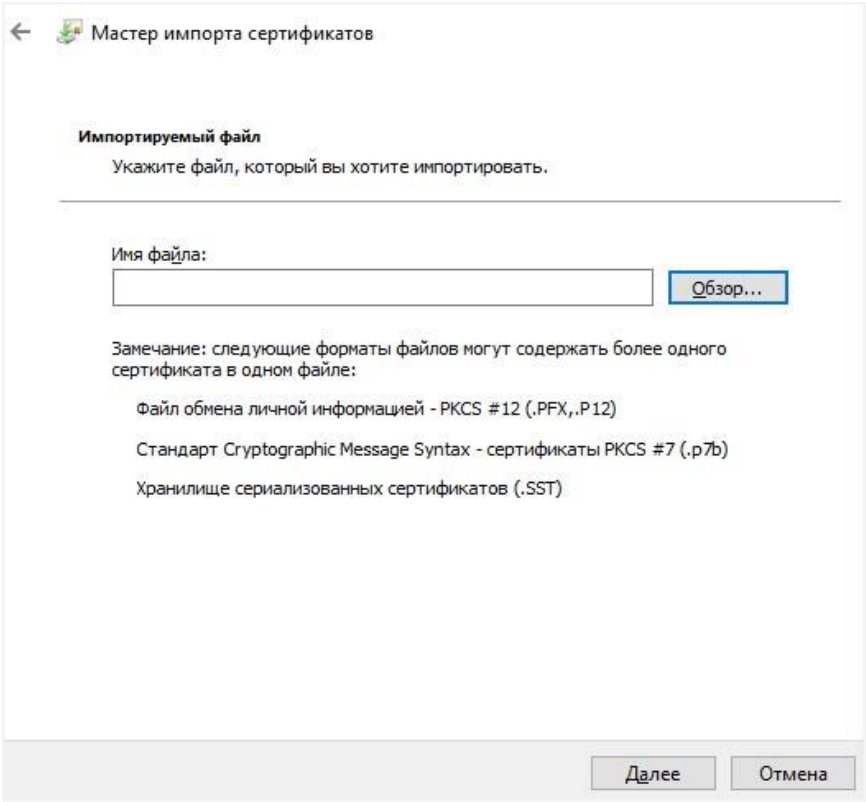

Рисунок 15 – Окно «Импортируемый файл»

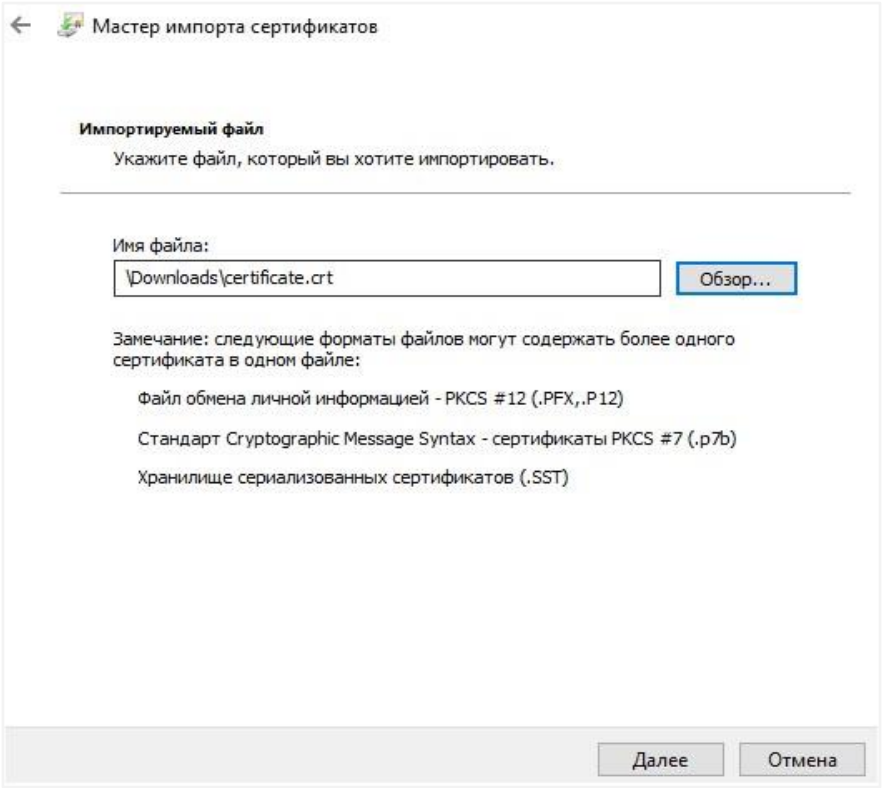

Рисунок 16 – Результат выбора сертификата для установки

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 нужно перезагрузить рабочую станцию.

3.3.4 Установка сертификата для браузера Mozilla Firefox

Скачать сертификат из веб-интерфейса системы NT SIEM (рис 6, 8), но не через браузер Mozilla Firefox. Затем открыть браузер Mozilla Firefox и перейти в окно «Настройки» (рис. 17).

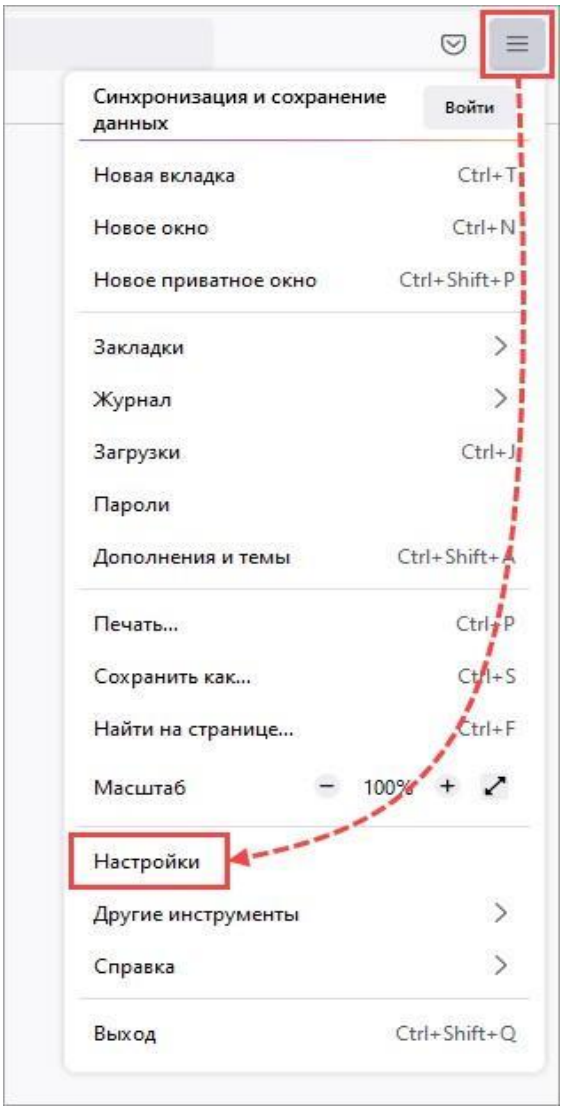

Рисунок 17 – Переход в настройки браузера Mozilla Firefox

В левой части страницы перейти в раздел «Приватность и защита», найдите раздел «Защита» и нажать «Просмотр сертификатов» (рис. 18).

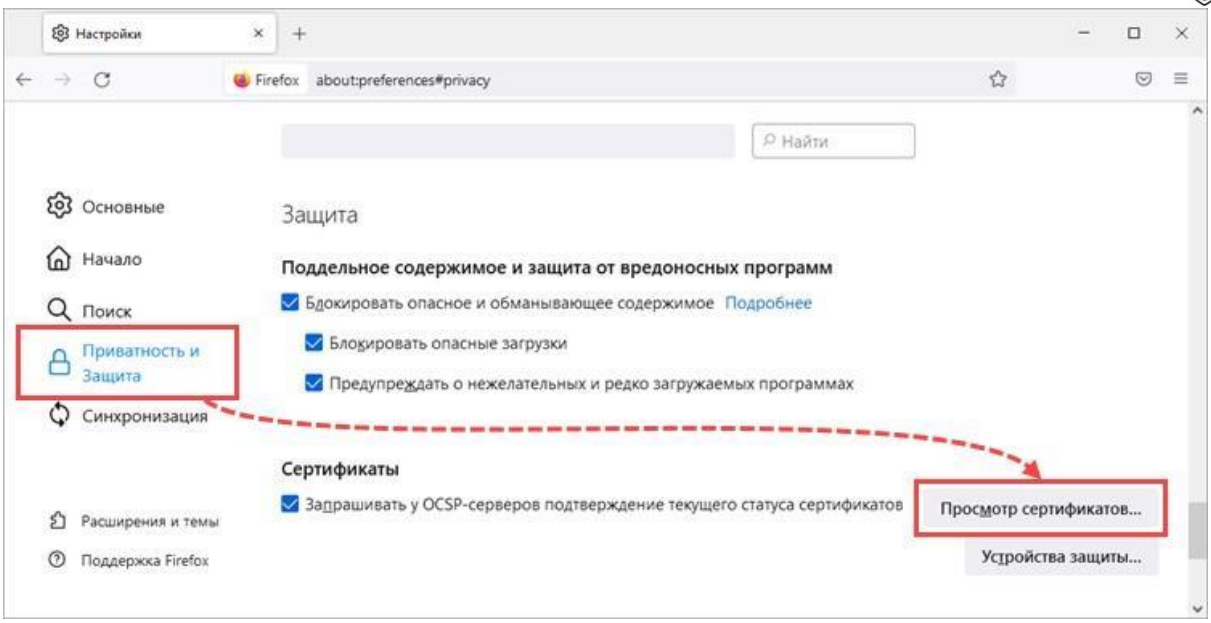

Рисунок 18 – Настройки браузера Mozilla Firefox раздел «Приватность и защита»

Перейти на вкладку «Центры сертификации» и нажать «Импортировать» (рис.19). Выбрать ранее скачанный сертификат.

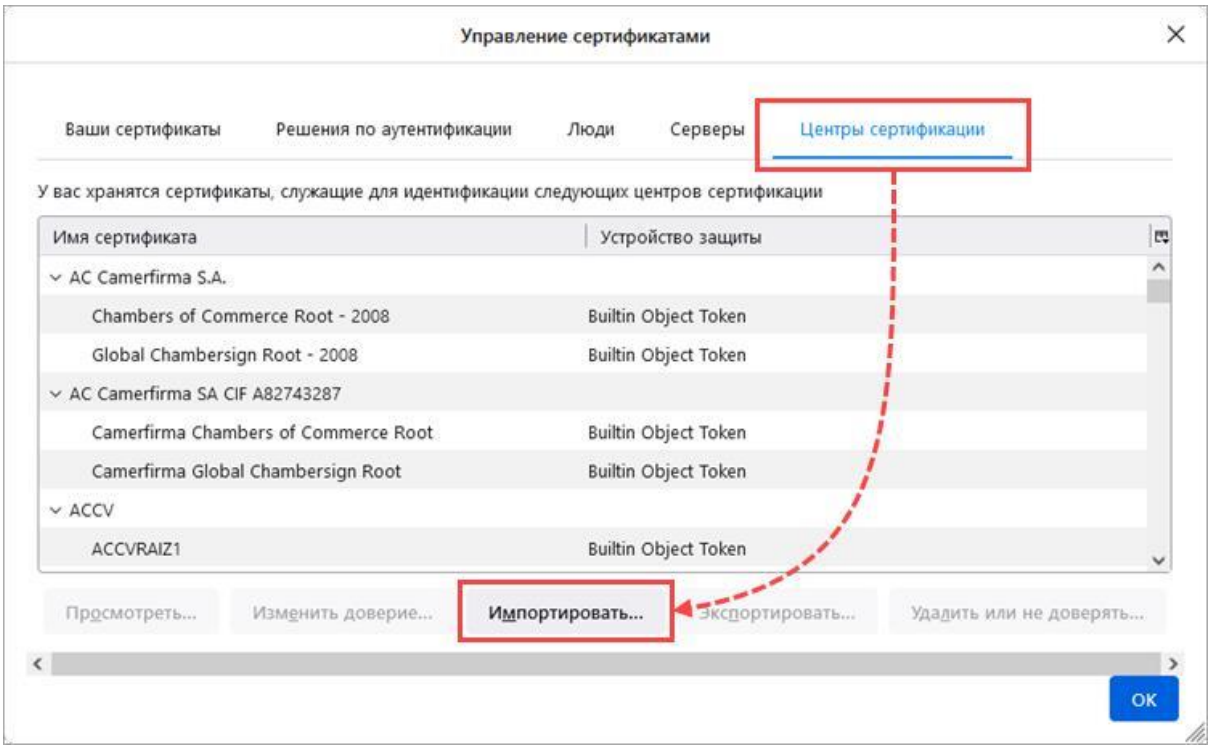

Рисунок 19 – Окно «Управление сертификатами»

Установить флажки «Доверять при идентификации веб-сайтов» и «Доверять при идентификации пользователей электронной почты». Нажать «OK» (рис.20).

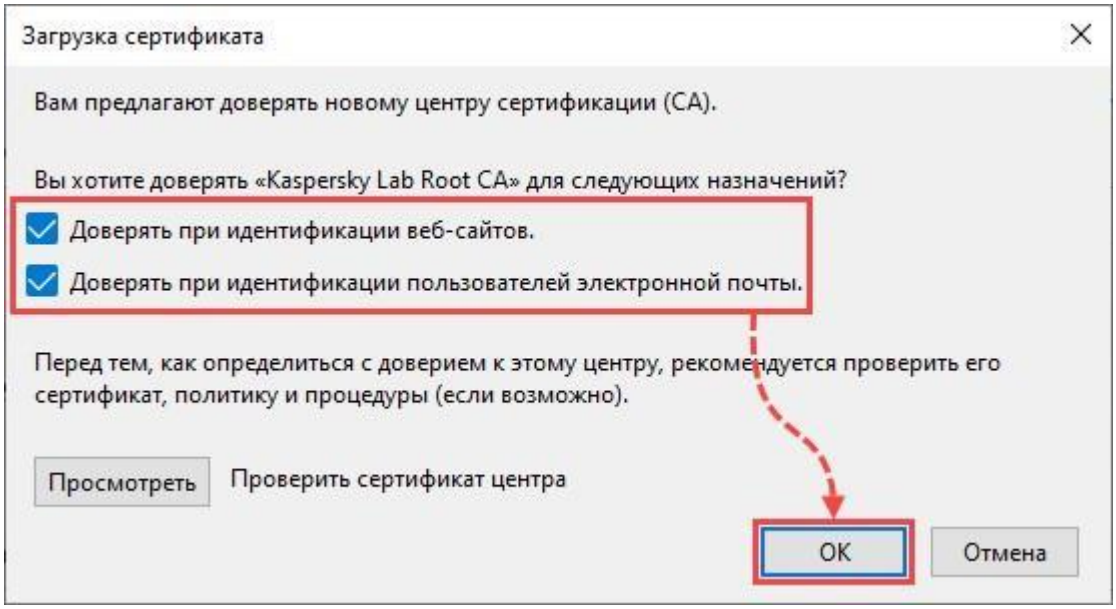

Рисунок 20 – Окно «Загрузка сертификата»

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

3.4 Работа с агентами

3.4.1 Установка и развертывание агентов

Для полноценной работы системы NT SIEM необходимо организовать передачу данных в систему путем установки агента на конечное устройство. Для того, чтобы развернуть новый агент, необходимо перейти на группу страниц «Агенты», затем на страницу «Новый агент» и следовать пошаговой инструкции в пользовательском интерфейсе NT SIEM.

Первый шаг «Выбор пакетов установки». На данном шаге вы можете выбрать на какую систему будете устанавливать агента (рис.21).

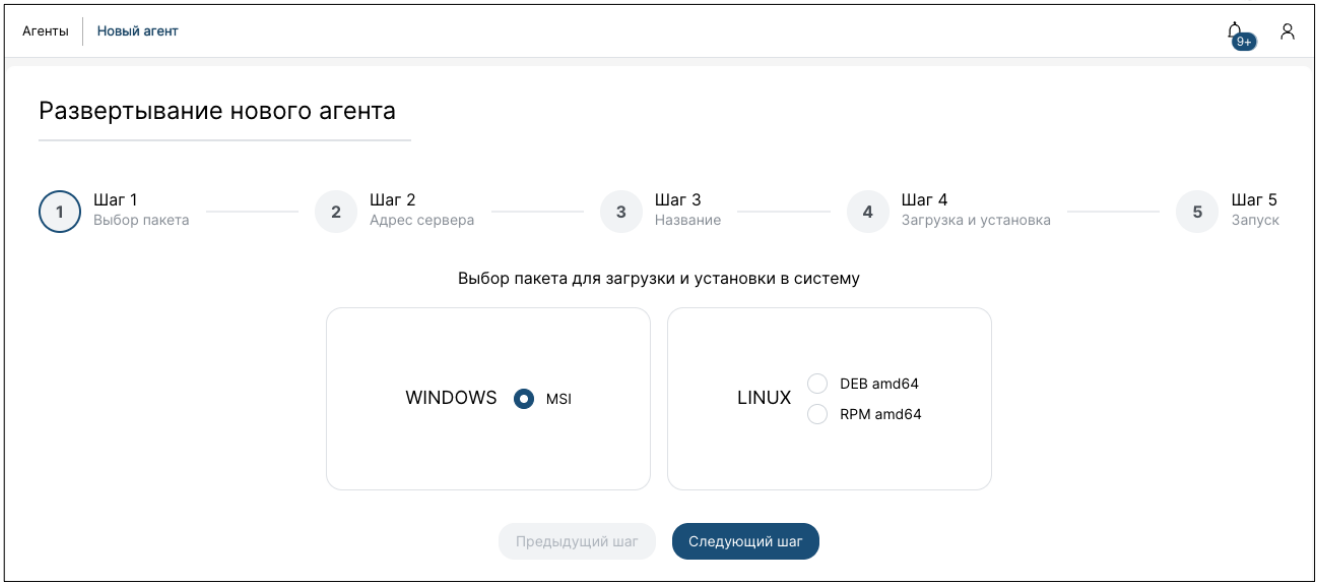

Рисунок 21 – Категория «Новый агент», шаг №1

На втором шаге следует задать IP-адрес сервера в виде IPv4, это тот адрес, который агент будет использовать для связи с сервером (рис.22). Данное поле не может быть пустым.

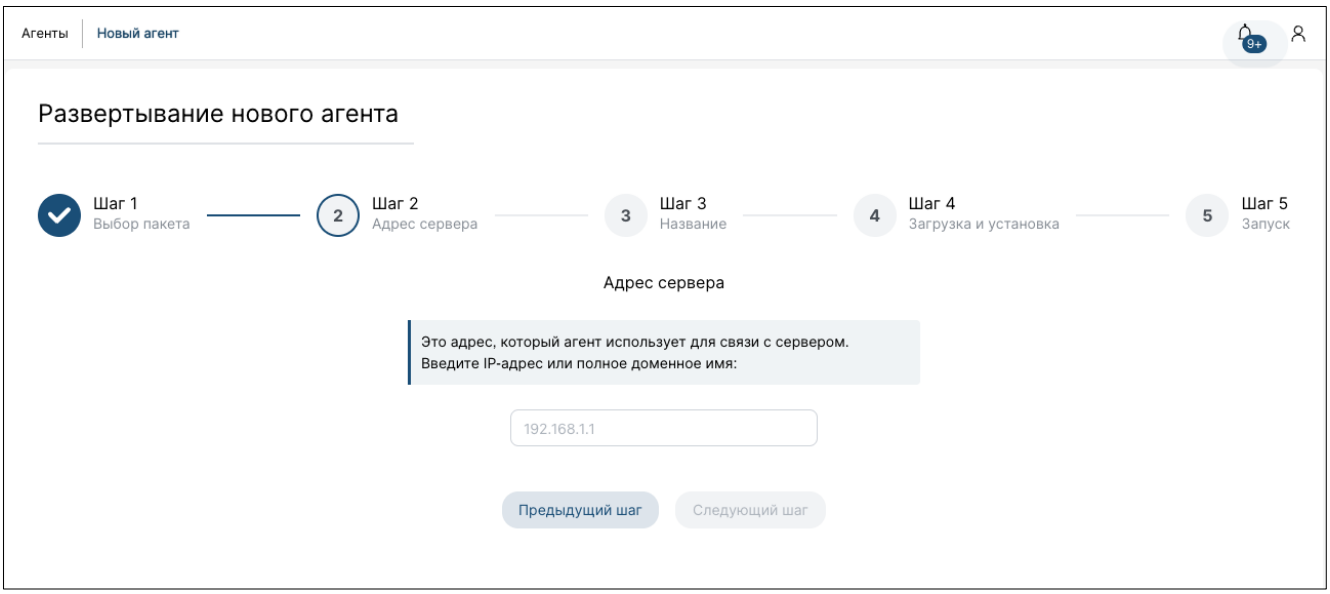

Рисунок 22 – Категория «Новый агент», шаг №2

На третьем шаге следует задать имя агента. Имя должно быть уникальным, и оно не может быть изменено после регистрации агента (рис.23). Поле можно оставить пустым, в следствии чего агент присвоит себе имя машины, на которой он будет установлен (`hostname`).

Рисунок 23 – Категория «Новый агент», шаг №3

На шаге четвертом будет сгенерирована команда для загрузки и установки агента. Необходимо скопировать и выполнить команду: для ОС семейства Lunix следует использовать командную строку Lunix, для ОС семейства Windows слеудет использовать Windows Powershell. Все действия следует выполнять от имени учетной записи **`root`** (рис.24).

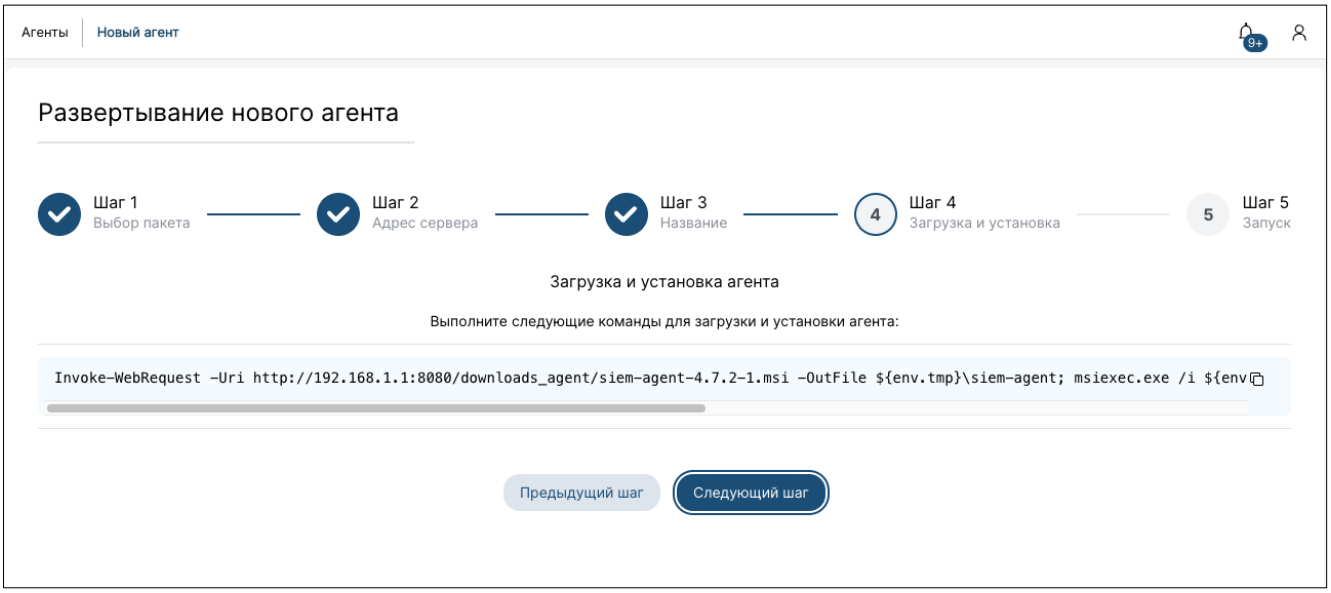

Рисунок 24 – Категория «Новый агент», шаг №4

Команда для выполнения, представленная на рисунке 24:

```
Invoke-WebRequest -Uri http://10.72.144.12:8080/downloads_agent/siem-
agent4.7.2-1.msi -OutFile ${env.tmp}\siem-agent; msiexec.exe /i
${env.tmp}\siem-agent
/q          SIEM_MANAGER="1.1.1.1"            SIEM_AGENT_GROUP="default"
SIEM_AGENT_NAME="test_agent"
SIEM_REGISTRATION_SERVER="1.1.1.1"
```

`SIEM_AGENT_NAME="test_agent"` не является обязательным параметром.

На пятом шаге будет представлена команда для запуска агента, ее необходимо скопировать и выполнить: для ОС семейства Lunix следует использовать командную строку Lunix, для ОС семейства Windows слеудет использовать Windows Powershell. Все действия следует выполнять от имени учетной записи `root` (рис.25).

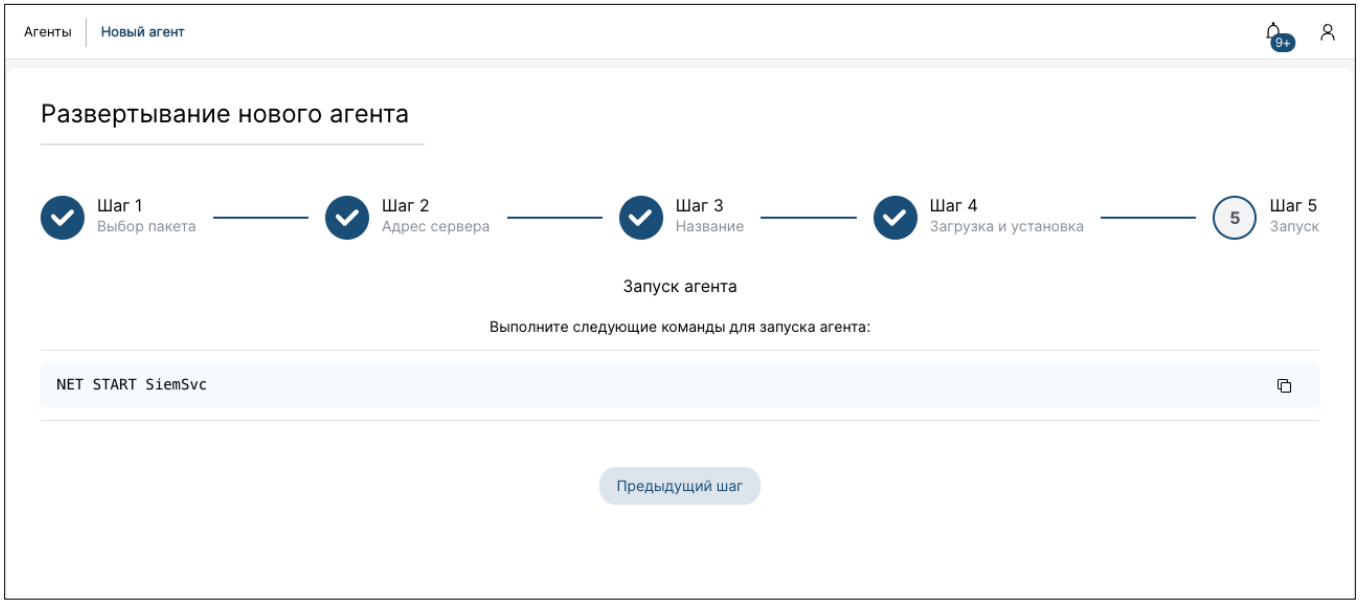

Рисунок 25 – Категория «Новый агент», шаг №5

Команда для запуска, представленная на рисунке 25:

```
NET START SiemSvc
```

3.4.2 Удаление агентов с конечных устройств

При необходимости можно удалить ранее установленный агент с конечного устройства.

Удаление на ОС семейства Windows.

Способ 1. Удаление на странице «Параметры»:

1. Нажать кнопку «Пуск», выбрать «Параметры» и перейти на вкладку «Приложения и возможности»;
2. Выбрать агента, который необходимо удалить;
3. Нажать кнопку «Удалить».

Способ 2. Удаление на панели управления:

1. Ввести в поле поиска на панели задач «Панель управления», а затем в списке результатов выбрать «Панель управления»;
2. Выбрать «Программы», а затем «Программы и компоненты»;

3. Нажать и удерживать (или щелкните правой кнопкой мыши) агента, который необходимо удалить;
4. Выбрать «Удалить» или «Удалить, или изменить»;
5. Затем следует выполнить предлагаемые инструкции на экране.

Удаление на ОС семейства Linux.

Для удаления агентов на Linux Debian и Red Hat необходимо ввести команду:

```
uninstall-siem
```

Результат представлен на рисунке 26.

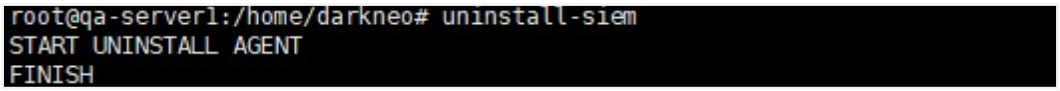

Рисунок 26 – Выполнение удаления агента на ОС Linux

3.4.3 Изменение стандартных настроек агентов

Для того, чтобы изменить стандартные настройки агентов необходимо внести изменения в конфигурационный файл.

Для Unix подобных системах.

Перед началом каких-либо работ с файлом конфигурации рекомендуется создать его резервную копию. Далее следует найти и открыть файл конфигурации в режиме редактирования:

```
nano /var/ossec/etc/ossec.conf
```

Затем следует отредактировать интересующие конфигурационные параметры, сохранить все внесенные изменения и перезапустить агента после проведенных работ:

```
systemctl stop siem-agent && sudo systemctl start siem-agent
```

Для ОС семейства Windows.

Перед началом каких-либо работ с файлом конфигурации рекомендуется создать его резервную копию. Далее следует найти и открыть файл в режиме редактирования (например, в блокноте). Путь, по которому можно найти файл для 64-разрядной версии Windows:

```
C:\Program Files (x86)\ossec-agent\ossec.conf
```

Путь, по которому можно найти файл для 32-разрядной версии Windows:

```
C:\Program Files\ossec-agent\ossec.conf
```

Затем следует отредактировать интересующие конфигурационные параметры. После сохранить все внесенные изменения и перезапустить агента. после проведенных работ

Список конфигурационных параметров.

Файл `ossec.conf` представлен в формате `XML`, и следовательно все параметры конфигурации должны быть заключены в теги. Тег `<ossec_config>` является корневым элементом.

Пример файла с конфигурационным параметром `<alerts>`.

```
<ossec_config>
    <alerts>
        ...
    </alerts>
</ossec_config>
```

Список с возможными конфигурационными параметрами можно найти в таблице 3. Все конфигурационные параметры должны находится внутри тега `<ossec_config>`.

Таблица 3 – Конфигурационные параметры

Конфигурационный параметр	Поддерживаемые варианты для установки
`active-response`	Агент
`agent-upgrade`	Агент
`anti_tampering`	Агент
`client`	Агент
`client_buffer`	Агент
`fluent-forward`	Агент
`github`	Агент
`labels`	Агент
`localfile`	Агент
`logging`	Агент
`ms-graph`	Агент
`office365`	Агент
`rootcheck`	Агент

sca	Агент
socket	Агент
syscheck	Агент
wodle name="aws-s3"	Агент
wodle name="azure-logs"	Агент
wodle name="command"	Агент
wodle name="docker-listener"	Агент
wodle name="osquery"	Агент
wodle name="syscollector"	Агент
gcp-pubsub	Агент
gcp-bucket	Агент

3.5 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.
```

3.6 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.27), скопировать данные из поля «Хэш» с помощью и передать его поставщику системы.

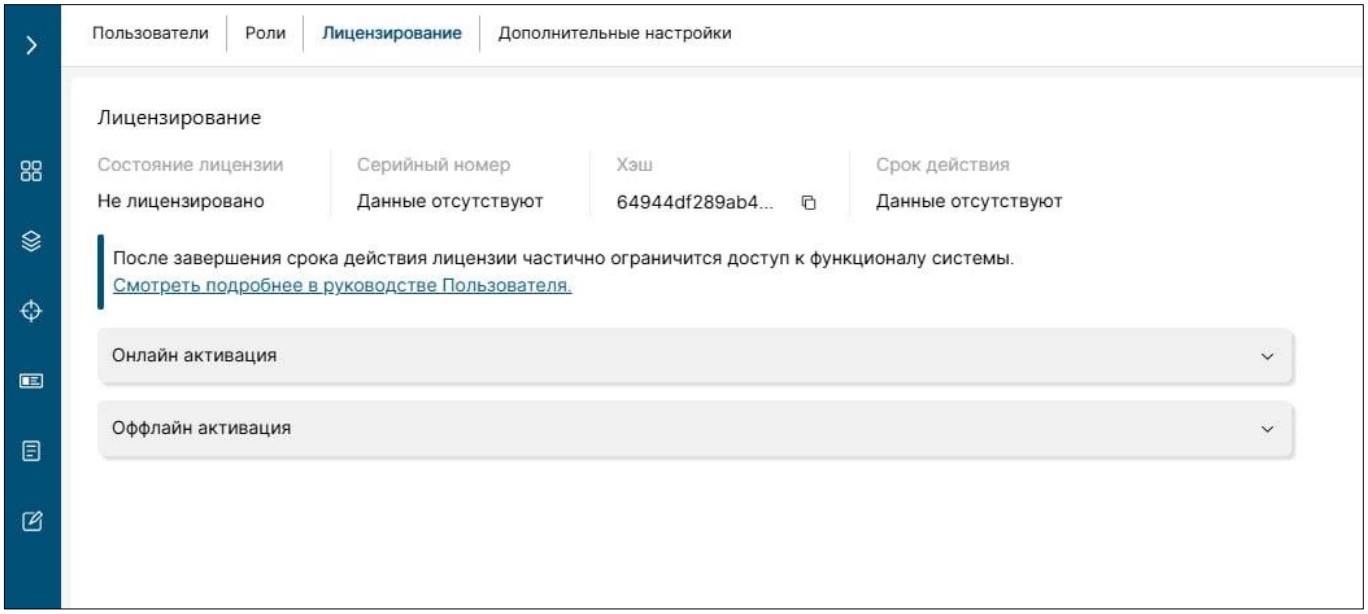

Рисунок 27 – Страница «Лицензирование» без активной лицензии

После того, поставщиком системы будет выдан ключ лицензии или файл с расширением `.dat` (рис. 28):

Если есть подключение к серверу лицензирования, то необходимо ввести, полученный от поставщика ПО, ключ лицензирования в блок «Онлайн лицензия» (рис.27) и нажать на кнопку «Активировать». В случае продления лицензии, вводить повторно ключ лицензирования не нужно.

Если нет подключения к серверу лицензирования, то полученный файл необходимо будет загрузить вручную. Для этого можно перетащить файл в поле для загрузки или нажатием на данное поле, открыть проводник и выбрать файл. В случае продления лицензии, весь процесс необходимо будет повторить.

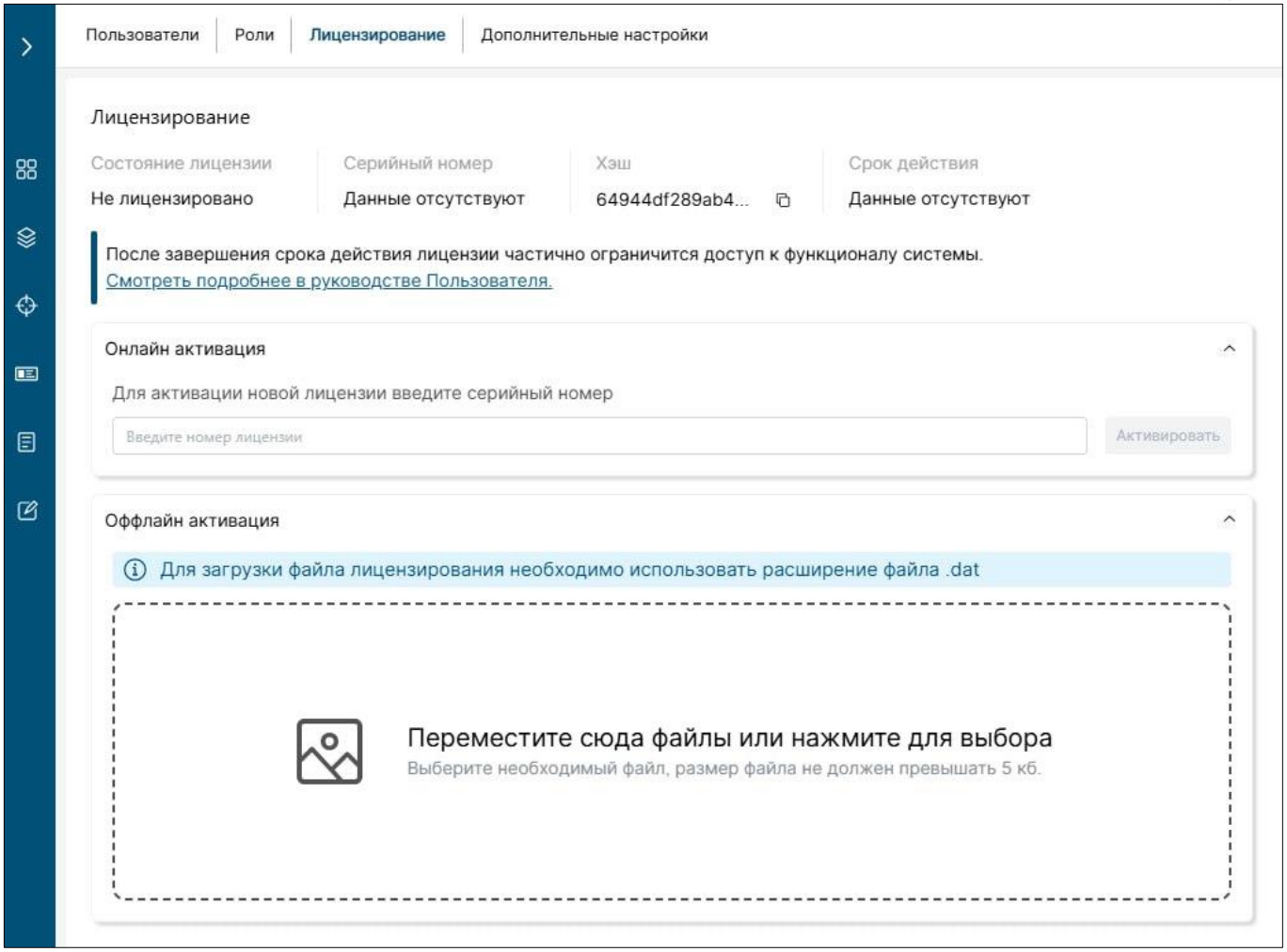

Рисунок 28 – Страница «Лицензирование» без активной лицензии

При успешной установке лицензии поля «Серийный номер лицензии» и «Срок действия» будут заполнены данными о текущей лицензии, и состояние лицензии изменится на «Активна» (рис.29).

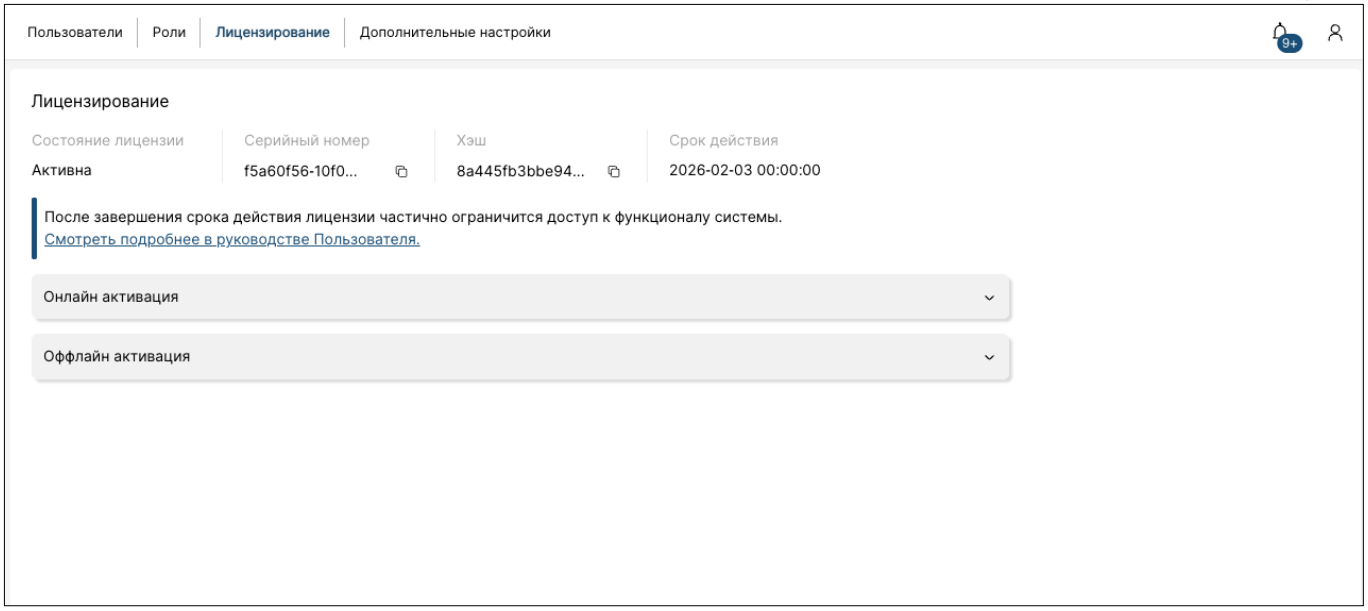

Рисунок 29 – Страница «Лицензирование» с активной лицензией

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

4. Установка обновлений

Обратите внимание, что установка версий выполняется последовательно. Например, перед установкой версии NT SIEM v1.0.2 сначала необходимо установить NT SIEM v1.0.1 и только потом начинать процесс установки NT SIEM v1.0.2, иначе процесс установки будет завершен неудачно.

4.1 Установка обновления NT SIEM v1.0.1

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

Для установки версии NT SIEM v1.0.1 необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.0.1.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.0.1.sh
./1.0.1.sh
```

4.2 Установка обновления NT SIEM v1.0.2

Перед установкой версии NT SIEM v1.0.2 необходимо удостовериться, что версия NT SIEM v1.0.1 уже установлена. Иначе, процесс установки NT SIEM v1.0.2 будет завершен неудачно.

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

Рекомендуется проверить параметры, внесенные в файл `project_variables` (стр. 9), в частности показатель оперативной памяти:

```
DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms4096m -Xmx4096m"'
```

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.0.2.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.0.2.sh
./1.0.2.sh
```

4.3 Установка обновления NT SIEM v1.1.0

Перед установкой версии NT SIEM v1.1.0 необходимо удостовериться, что версия NT SIEM v1.0.2 уже установлена. Иначе, процесс установки NT SIEM v1.1.0 будет завершен неудачно.

Рекомендуется проверить параметры, внесенные в файл `project_variables` (стр. 9), в частности показатель оперативной памяти:

```
DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms4096m -Xmx4096m"'
```

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.1.0.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.0.sh
./1.1.0.sh
```

4.4 Установка обновления NT SIEM v1.1.1

Перед установкой версии NT SIEM v1.1.1 необходимо удостовериться, что версия NT SIEM v1.1.0 уже установлена. Иначе, процесс установки NT SIEM v1.1.1 будет завершен неудачно.

Рекомендуется проверить параметры, внесенные в файл `project_variables` (стр. 9), в частности показатель оперативной памяти:

```
DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms4096m -Xmx4096m"'
```

Далее необходимо распаковать архив с расширением .tar в директорию, в которой установлен NT SIEM:

```
tar -xzvf 1.1.1.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.1.sh
./1.1.1.sh
```

4.5 Установка обновления NT SIEM v1.1.2

Перед установкой версии NT SIEM v1.1.2 необходимо удостовериться, что версия NT SIEM v1.1.1 уже установлена. Иначе, процесс установки NT SIEM v1.1.2 будет завершен неудачно.

Рекомендуется проверить параметры, внесенные в файл `project_variables` (стр. 9), в частности показатель оперативной памяти:

```
DB_RAM='"OPENSEARCH_JAVA_OPTS=-Xms4096m -Xmx4096m"'
```

Далее необходимо распаковать архив с расширением `.tar` в директорию, в которой установлен NT SIEM.

```
tar -xzvf 1.1.2.tar.gz -C siem-docker/
```

Далее необходимо перейти в директорию `siem-docker`:

```
cd siem-docker/
```

После перехода в директорию следует выполнить команды:

```
chmod u+x 1.1.2.sh
./1.1.2.sh
```