SurfSecure

Руководство по установке и настройке

Версия документа от 18 мая 2020 года

Аннотация

Настоящее Руководство по установке и настройке описывает первичный набор мероприятий и действий для установки Системы контентной фильтрации веб трафика (далее - СКФВТ).

Содержание

Перечень условных обозначений, терминов и сокращений

Обозначение	Описание
CIDR	Classless Inter-Domain Routing – метод указаения IP-адресации
DLP	Data Leak Prevention — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне
DOCX	Формат файлов, представляющий собой модернизированную версию формата DOC. Используется программами Microsoft Word 2007, 2010, 2013 и 2016 для Windows, а также Microsoft Word 2008 и 2011 для Mac OS X
IP	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
ISO	Образ оптического диска, содержащий файловую систему стандарта ISO 9660
FQDN	Fully Qualified Domain Name – уникальное доменное имя ресурса\устройства
LDAP	Lightweight Directory Access Protocol – облегченный протокол для доступа к службе каталога
NTP	Network Time Protocol — протокол сетевого времени
PDF	Универсальный файловый формат, который позволяет сохранить шрифты, изображения и сам макет исходного документа независимо от того, на какой платформе и в каком приложении такой документ создавался
SSL	Secure Sockets Layer – криптографический протокол, который обеспечивает защищенную передачу информации в Интернете
TCP	Transmission Control Protocol – протокол управления передачей данных
АРМ	Автоматизированное рабочее место
Заказчик	Конечный пользователь
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
Исполнитель	Наименование исполнителя
СКФВТ Система	Система контентной фильтрации веб трафика

1 Введение

1.1 Общие сведения

Полное наименование системы: Система контентной фильтрации веб трафика.
Условное обозначение системы: СКФВТ.

Перед эксплуатацией СКФВТ обслуживающему персоналу необходимо ознакомиться со следующими документами:

- «Пояснительная записка»;
- «Руководство администратора»;
- «Руководство по установке и настройке»;

1.2 Назначение системы

СКФВТ предназначена для контентной фильтрации и антивирусной защиты веб-трафика, а также выполнения функций по разграничению доступа пользователей к внешним веб-ресурсам сети Интернет. СКФВТ обеспечивает отказоустойчивый и контролируемый доступа в сеть Интернет корпоративных пользователей.

2 Условия применения

2.1 Требования к аппаратному обеспечению

2.1.1 Требования к аппаратному обеспечению узлов фильтрации СКФВТ

Количество серверов, их тип и параметры вычислительный характеристик указаны в документе «Пояснительная записка» в разделе требований к аппаратному обеспечению.

2.1.2 Требования к аппаратному обеспечению АРМ администратора

АРМ администратора, с которого будет выполняться подключение к узлам фильтрации СКФВТ, должно соответствовать характеристикам не ниже следующих:

- CPU: 1 процессор с тактовой частотой 1,4 ГГц;
- RAM: 4 Гб;
- HDD: 60 Гб;
- 1 сетевой Ethernet интерфейс с пропускной способностью 100 Мбит/с.

2.2 Требования к программному обеспечению

2.2.1 Требования к аппаратному обеспечению АРМ администратора

На АРМ администратора, с которого будет выполняться подключение к модулям СКФВТ, должно быть установлено следующее ПО:

- ОС Windows 7/10;
- веб-обозреватель Internet Explorer версии 10 и выше;
- Putty или аналогичный SSH-клиент.

2.3 Требования к уровню подготовки обслуживающего персонала

Администратор СКФВТ должен обладать следующими знаниями:

- понимание принципов работы протоколов стека TCP/IP;
- понимание принципов функционирования протоколов HTTP, HTTPS, FTP и SSH;
- понимание принципов функционирования средств проксирования трафика;
- навыки администрирования ОС Red Hat Enterprise Linux.

Перед началом работы с СКФВТ администратор должен ознакомиться с настоящей инструкцией и проектной документацией.

3 Варианты установки

СКФВТ может быть установлена в двух конфигурациях:

- Одиночная;
- Распределенная.

Одиночная конфигурация является базовым вариантом установки системы и подразумевает функционирование всей системы на базе единственного узла фильтрации.

Распределенная конфигурация обеспечивает возможность использования нескольких узлов фильтрации для обеспечения отказоустойчивости и централизованного управления. Для реализации данной конфигурации необходима настройка функционала кластера конфигурации и кластера балансировки – подробная информация представлена в документе «Руководство администратора» в разделе 3.10 «Отказоустойчивость и кластеризация».

4 Первоначальная установка и настройка

4.1 Установка системы из образа

Установка системы из образа допустима как на физический программно-аппаратный комплекс (далее – ПАК), так и на сервер, развернутый на базе платформы виртуализации. Установки системы осуществляется с готового ISO образа, предоставляемым производителем системы. Перед установкой системы на физический ПАК необходимо выполнить запись ISO образа на установочный диск или флэш-накопитель.

Перед выполнением процедуры установки системы необходимо обеспечить наличие как минимум одного сетевого интерфейса, подключенного к серверу, с прямым доступом в сеть интернет (допустимо размещение за межсетевым экраном, использование прокси-сервера недопустимо).

Для начала установки необходимо смонтировать установочный ISO образ к виртуальной машине или подключить флэш-накопитель\загрузить диск в ПАК и выполнить загрузку, после чего отразится окно начала установки (Рисунок 1).

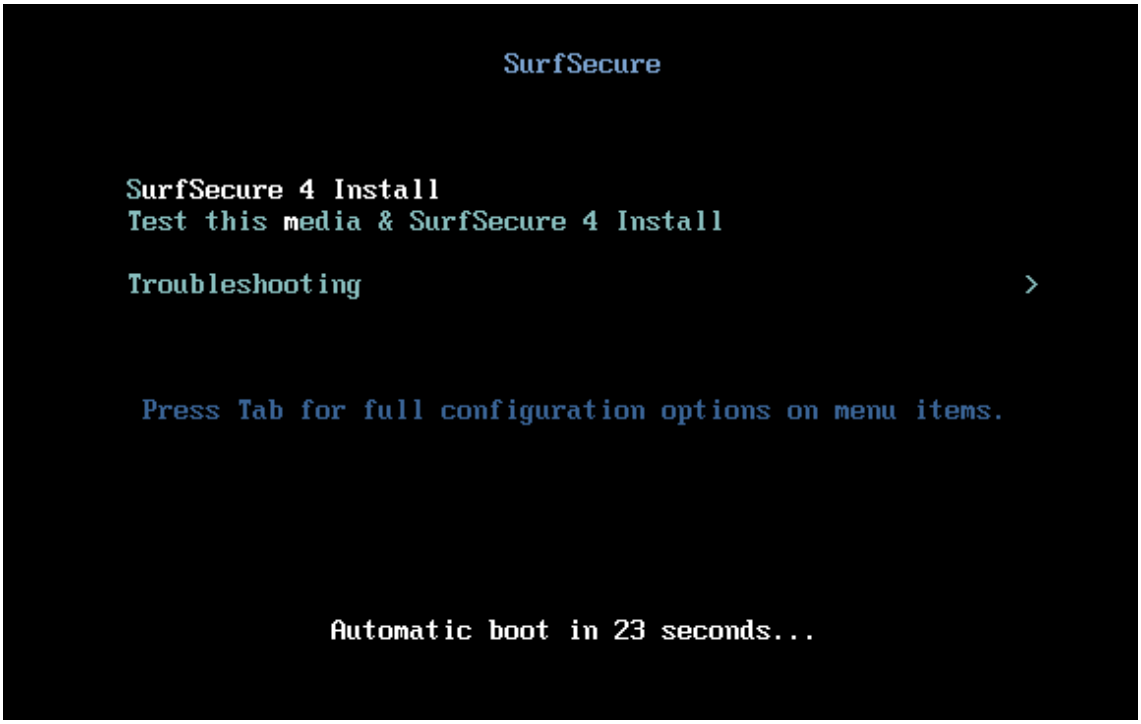


Рисунок 1 – Окно первоначальной установки системы

По истечению 30 секунд установщик автоматически перейдет к процессу загрузки необходимых компонент. Допустимо нажать кнопку «Enter» для пропуска времени ожидания и перехода к процессу загрузки.

После выполнения необходимых процедур по загрузки установщика будет отображен окно конфигурации параметров сетевого интерфейса (Рисунок 2).

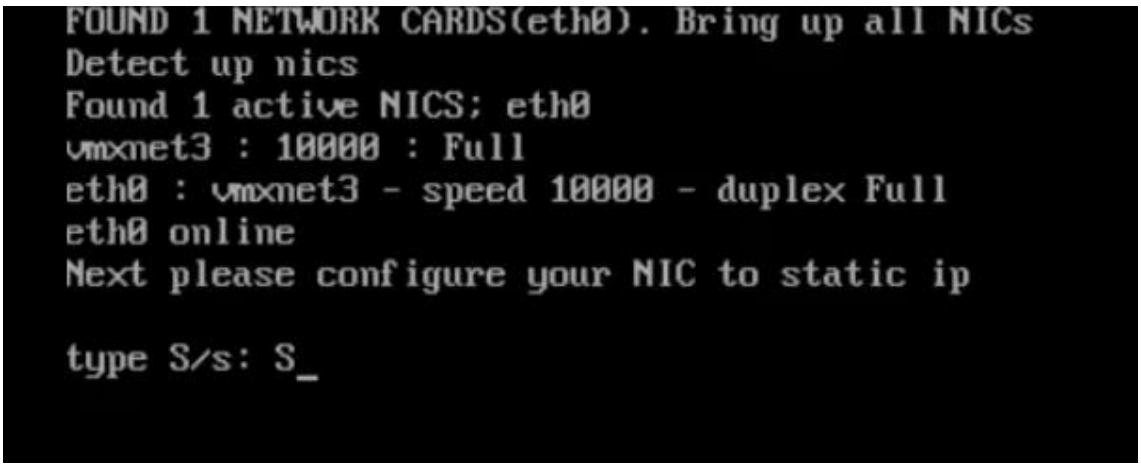


Рисунок 2 – Окно конфигурации сетевого интерфейса

Для начала ввода параметров сетевого интерфейса необходимо нажать кнопку «S».

Примечание: в случае некорректного ввода параметров сетевого интерфейса необходимо повторить процедуру установки системы. FQDN имя сервера является неотъемлемым параметром для формирования лицензионного ключа, последующее изменение данного параметра после установки системы потребует обращения к производителю для изменения параметров лицензионного ключа.

Далее необходимо указать следующие настройки сетевого интерфейса:

- Type IP – IP адрес сетевой карты;
- Type NetMask – маска сети;
- Type Gateway – адрес шлюза по умолчанию;
- Type DNS Server – адрес сервера DNS;
- Type FQDN hostname – имя сервера.

Пример корректной конфигурации интерфейса отражен на Рисунке 3.

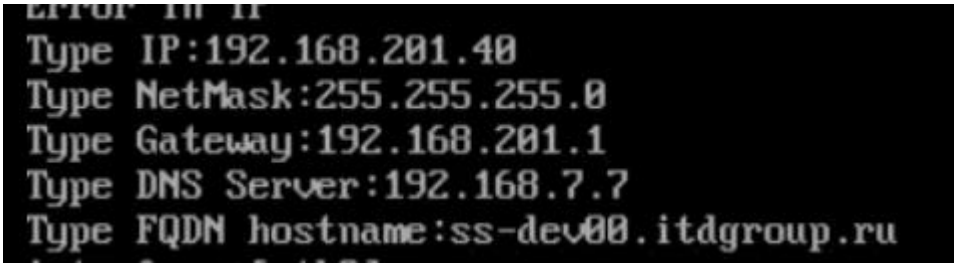


Рисунок 3 – Параметры конфигурации сетевого интерфейса

Система подтвердит корректность введенных данных сообщением «Configure ok» и перейдет к процессу установки операционной системы (Рисунок 4).

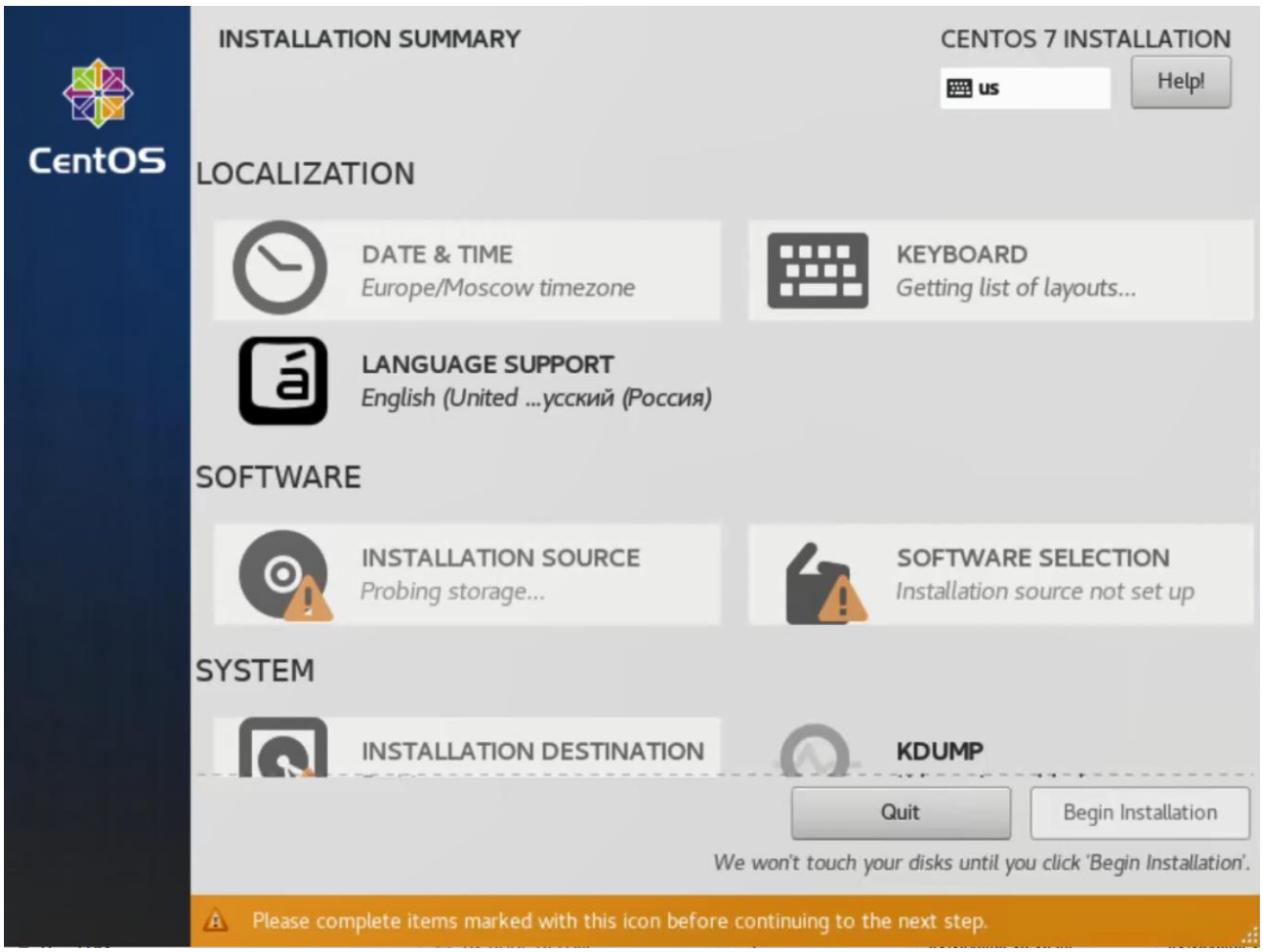


Рисунок 4 – Процесс установки операционной системы

Система автоматически начнёт проверку доступности репозиториев для загрузки необходимых компонент. По окончанию проверки (если инсталляция не продолжилась автоматически) станет доступным кнопка «Begin installation», которую необходимо нажать для старта установки компонент. Процесс установки занимает около 30 минут, после чего установщик выполнит перезагрузку сервера и первичный запуск системы. После перезагрузки, системе требуется некоторое время (около 20 минут в среднем) на выполнение первоначальной настройки. После этого веб-интерфейс станет доступен.

Для дальнейшей настройки системы необходимо использовать веб-интерфейс системы, для чего необходимо воспользоваться веб браузером и осуществить подключение к системе по ссылке http://<ip>, где <ip> это назначенный ip адрес сетевой карты сервера.

Доступ к веб интерфейсу системы должен осуществляться без использования прокси сервера.

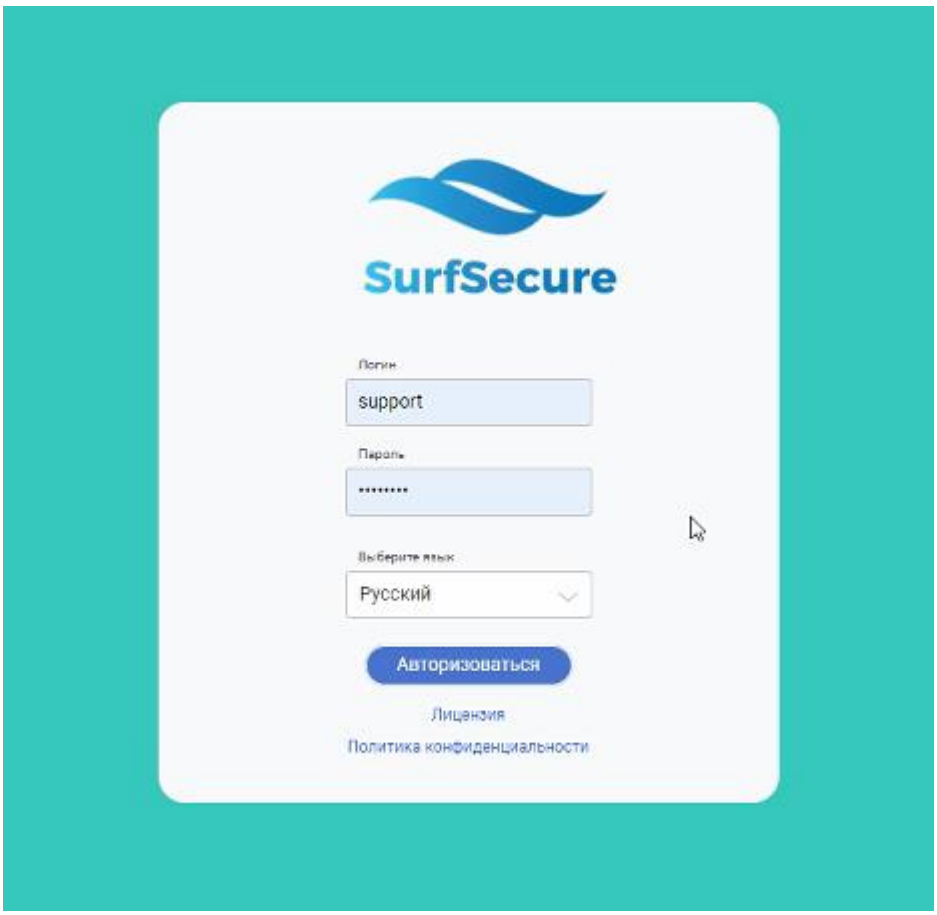


Рисунок 5 – Окно авторизации веб интерфейса системы

Для первичного входа в интерфейс необходимо воспользоваться встроенной учетной записью:

- Логин – support;
- Пароль – password.

Следующим шагом необходимо выбрать язык интерфейса системы и нажать кнопку «Старт».

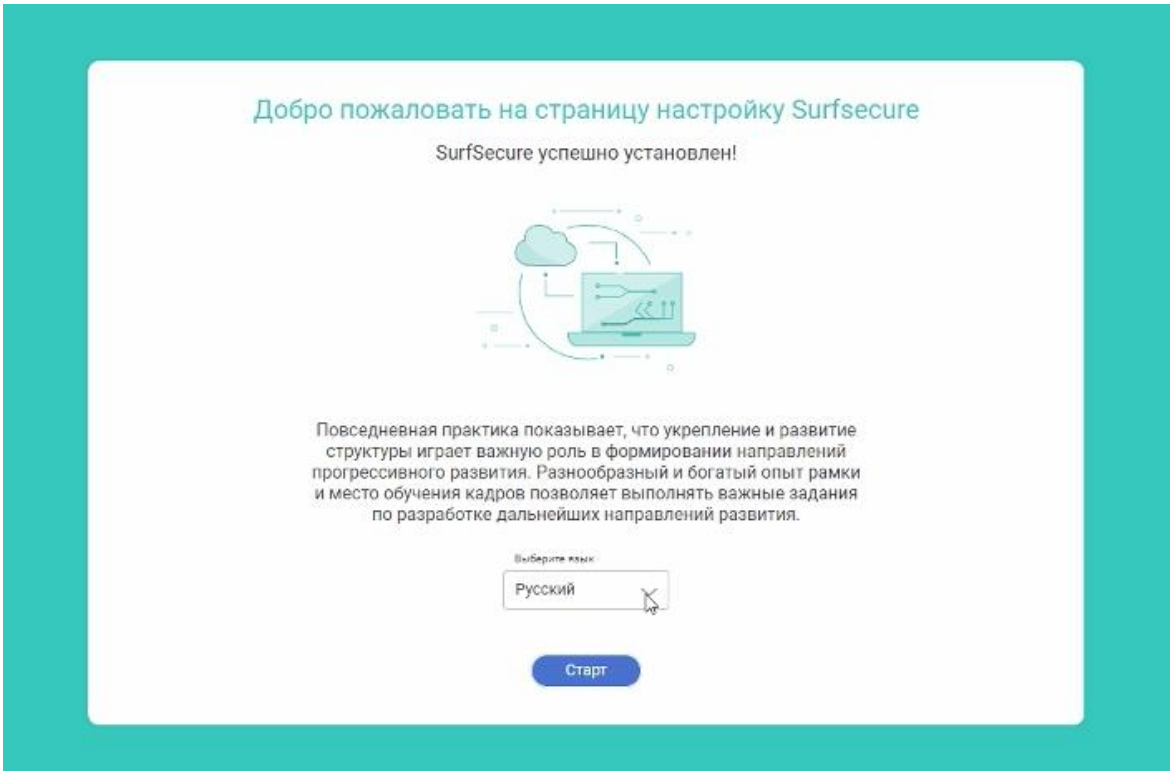


Рисунок 6 – Выбор языка интерфейса

Начальная конфигурация системы предполагает следующие этапы настроек:

- Интерфейс – настройка сетевых интерфейсов системы;
- Параметры сети – настройка серверов DNS;
- Время – настройка NTP серверов и часового пояса;
- Лицензия – указание ключевой информации для активации системы.

Веб интерфейс содержит ряд визуальных пиктограмм для работы:

- - Добавление нового параметра;
- - Корректировка заданного значения параметра;
- - Удаление значения\параметра

В окне настройке сетевых интерфейсов будет отражена информация, которая была указана на предыдущих этапах установки системы (Рисунок 7).

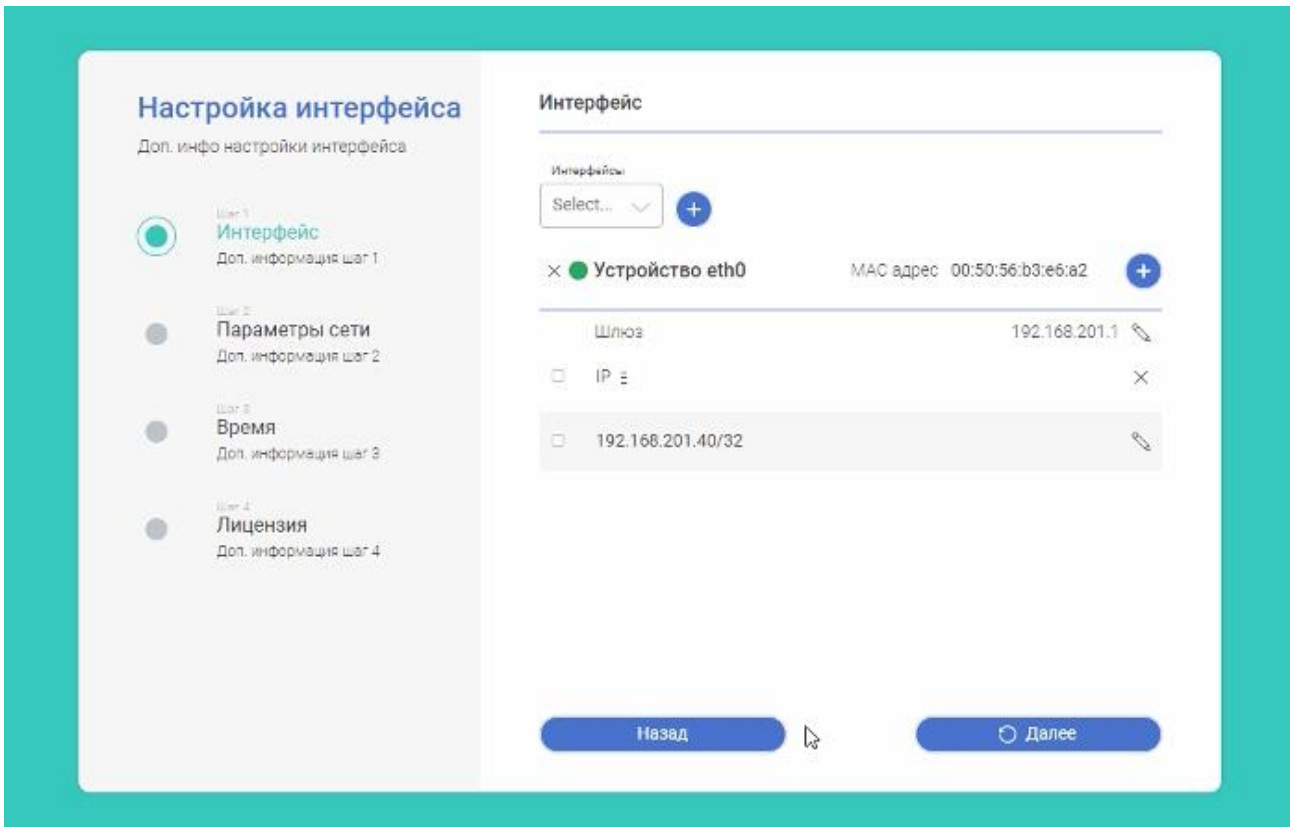
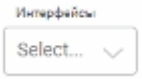


Рисунок 7 – Интерфейс конфигурации сетевых настроек

Необходимо проверить корректность ввода настроек сетевого интерфейса и шлюза по умолчанию.

При необходимости, на данном этапе возможно добавить настройки других сетевых интерфейсов системы путем выбора интерфейса и из выпадающего меню 

, добавлением кнопкой  и указания соответствующих параметров. На данном этапе маска подсети указывается в формате CIDR (например – 192.168.1.1/24). По окончанию настройки параметров сетевых интерфейсов необходимо нажать кнопку «Далее» для перехода к этапу конфигурации настроек DNS (Рисунок 8).

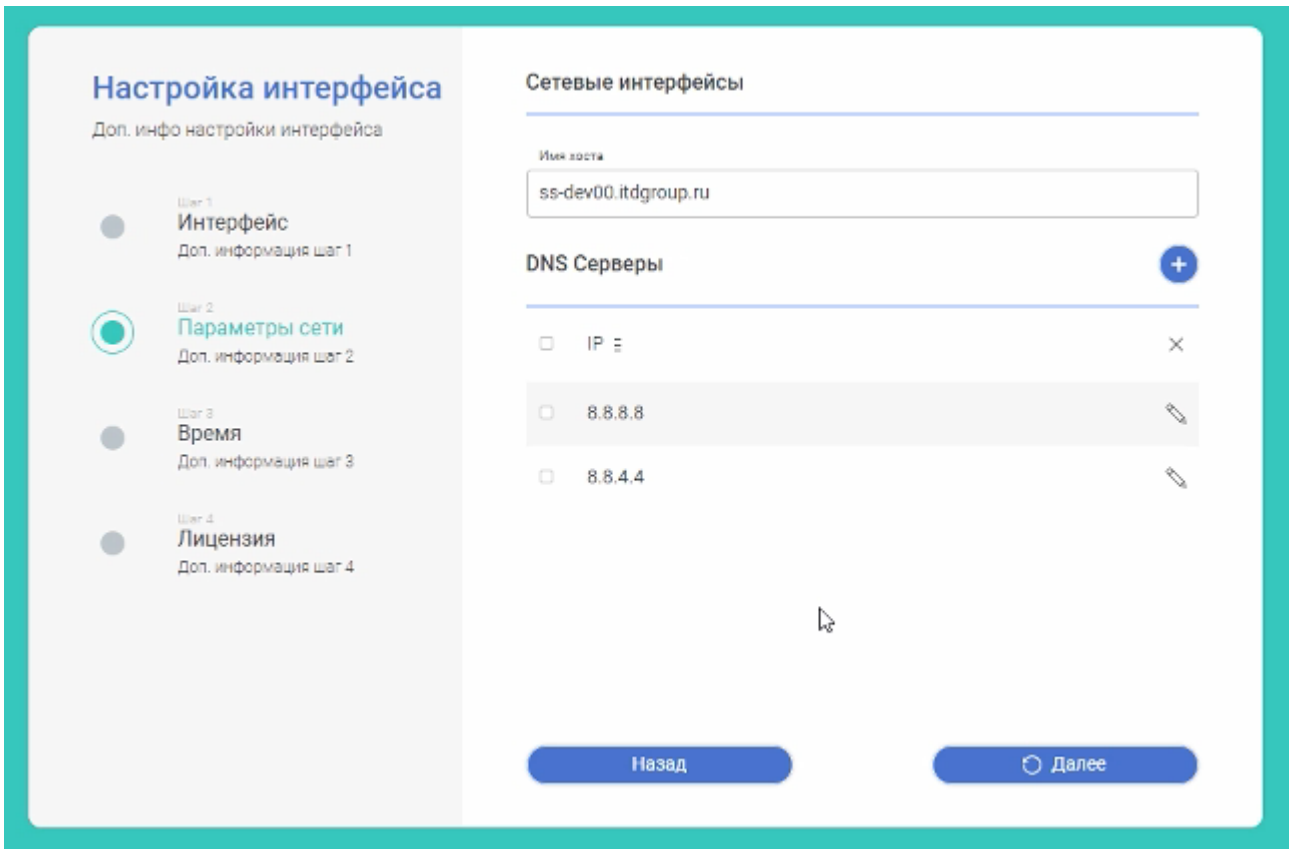


Рисунок 8 – Интерфейс конфигурации настроек DNS

В поле «Имя хоста» будет отражено ранее заданное имя сервера, его изменение не требуется.

В разделе «DNS серверы» необходимо указать IP адреса DNS серверов, которые будет использовать узел фильтрации для разрешения имен. Если в организации существует свой DNS сервер, который может разрешать A-записи доменов сети интернет (внешних по отношению к локальному домену), то необходимо IP адреса локальных DNS. В противном случае, необходимо указать ip адреса DNS серверов провайдера или публичные.

Следующим шагом необходимо перейти в раздел конфигурации параметров времени сервера (Рисунок 9), для этого необходимо нажать кнопку «Далее».

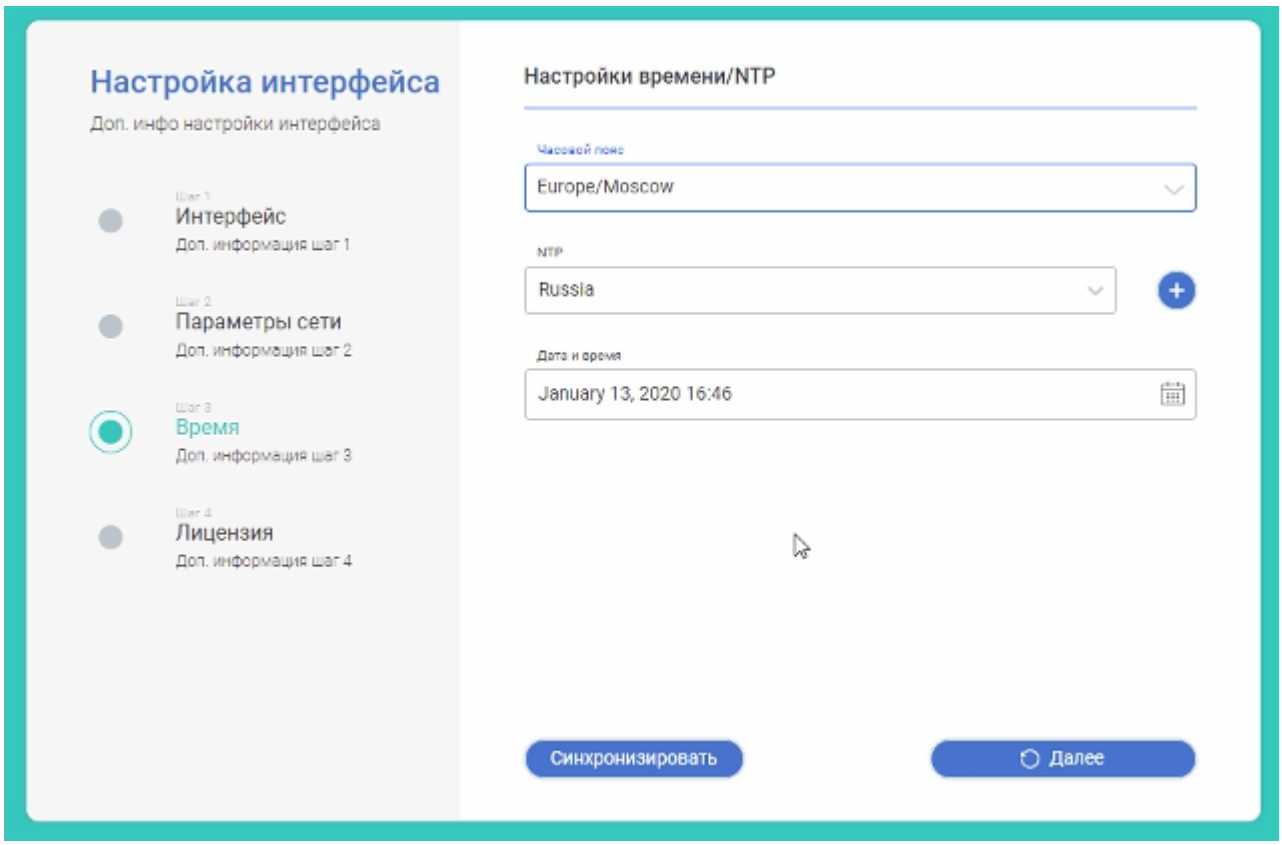


Рисунок 9 – Интерфейс конфигурации параметров времени

В графе «Часовой пояс» из выпадающего списка необходимо выбрать часовой пояс, в котором находится сервер.

В графе «NTP» необходимо выбрать из выпадающего списка предпочтительный сервер времени, который предусмотрен производителем. Для указания собственного NTP сервера необходимо его добавить при помощи кнопки , указать его IP адрес и имя, после чего выбрать из выпадающего списка.

При необходимости нужно скорректировать текущую дату и время и нажать кнопку «Далее» для перехода к этапу конфигурации лицензии (Рисунок 10).

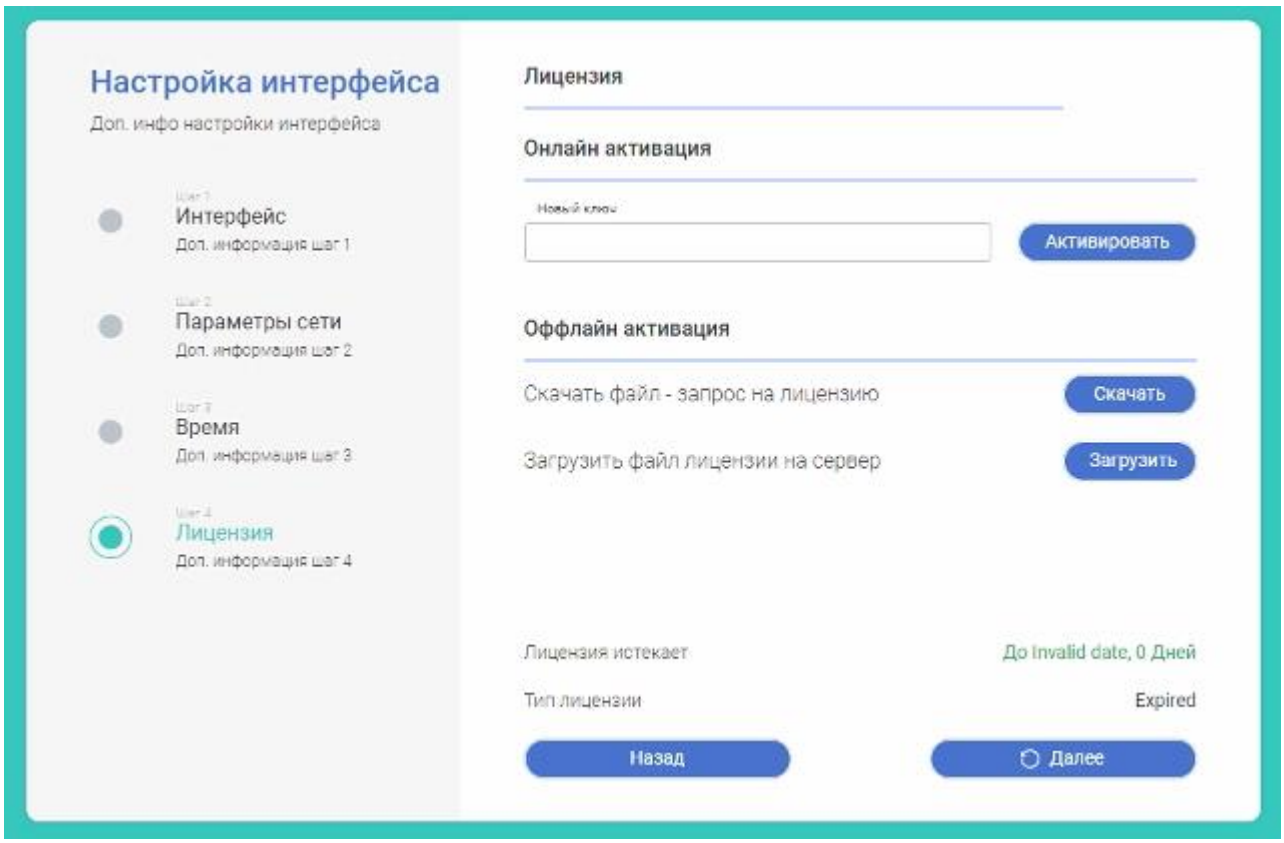


Рисунок 10 – Интерфейс конфигурации параметров лицензии

Ввод лицензионной информации может быть осуществлен любым из двух сценариев:

- Онлайн активация;
- Оффлайн активация.

Для онлайн активации в поле «Новый ключ» необходимо ввести лицензионный ключ в формате XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX, который был ранее получен от производителя системы. После чего, необходимо нажать кнопку «Активировать».

Для оффлайн активации необходимо нажать кнопку «Скачать», после чего будет осуществлена загрузка файла-запроса лицензии. Данный файл необходимо передать производителю системы, в ответ на который будет получен файл-ответ, который необходимо установить при помощи кнопки «Загрузить».

После активации системы необходимо нажать кнопку «Далее» и перейти к интерфейсу выбора режима конфигурации системы (Рисунок 11).

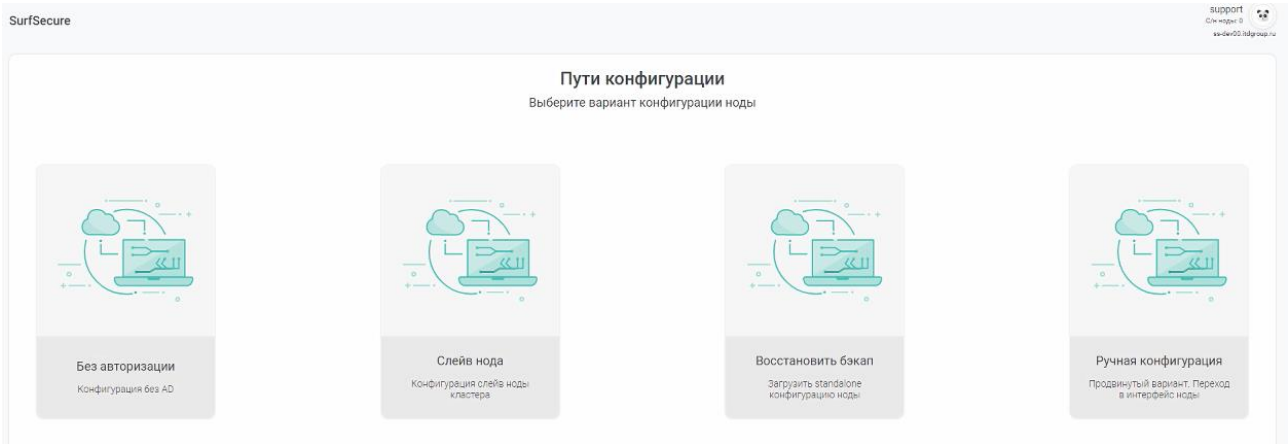


Рисунок 11 – Интерфейс выбора типа конфигурации

Интерфейс выбора типа конфигурации системы предлагает следующие возможности первичной настройки системы:

- Без авторизации;
- Слейв нода;
- Восстановить бэкап;
- Ручная конфигурация.

Режим «Без авторизации» обеспечивает перевод в режим запуска системы без дополнительных настроек соединения с каталогом Active Directory.

Режим «Слейв нода» обеспечивает конфигурирование узла фильтрации как дополнительного узла к существующему кластеру конфигурации (Рисунок 12).

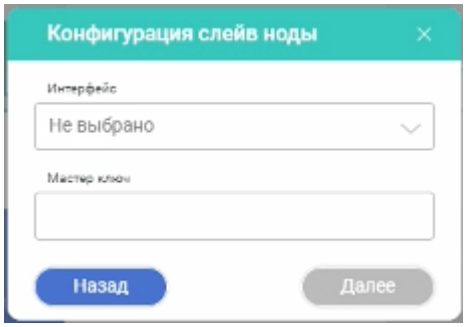


Рисунок 12 – Конфигурация параметров для подключения к кластеру конфигурации

На данном этапе необходимо выбрать сетевой интерфейс узла фильтрации, с которого будет осуществляться взаимодействие с основным узлом (мастер нодой) кластера конфигурации и в поле «Мастер ключ» указать ключ для взаимодействия. Данный ключ можно запросить на мастер ноде кластера конфигурации.

Режим «Восстановить бэкап» позволяет восстановить набор конфигурационных настроек с существующего узла фильтрации, который был предварительно сохранен с действующего узла фильтрации.

Режим «Ручная конфигурация» позволяет перейти в режим расширенной конфигурации настроек. Выбор данного режима должен осуществляться только опытными пользователями системы.

После выбора режима конфигурации и указания необходимых параметров необходимо нажать кнопку «Далее» завершения первичной конфигурации узла фильтрации и переходу в интерфейс администрирования системы.

5 Источники разработки

Настоящее Техническое задание разработано на основе следующих информационных материалов и документов:

– ГОСТ 34.003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;

– ГОСТ 34.601-90 Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

– ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

– ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

– ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем;

– РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов;

– РД 50-680-88 Методические указания. Автоматизированные системы. Основные положения.