СОГЛАСОВАНО
ООО «Энткор-Е»

_____И.О. Корявченко
«___»_____ 2025 г.

УТВЕРЖДАЮ
ООО «Энткор-Е»

_____М.Ю. Сухарь
«___»_____ 2025 г.

Программное обеспечение e-node

Руководство администратора

Чита, 2025

АННОТАЦИЯ

Настоящий документ является руководством Администратора универсального программного комплекса мониторинга и управления E-NODE (далее – Программа, Система).

В документе приведены сведения о назначении и условиях применения Программы, действиях и операциях, которые выполняет Администратор (установка Программы, взаимодействие Программы с внешними системами) для поддержки рабочих процессов.

Документ разработан в соответствии с требованиями следующих документов:

- ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;
- ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
- ГОСТ 19.503-79 «Руководство системного программиста. Требования к содержания и оформлению».

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем Руководстве администратора применяют следующие сокращения и обозначения.

Обозначение или сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
АСУ	Автоматизированная система управления
АСУ ТП	Автоматизированная система управления технологическим процессом
КИИ	Критическая информационная инфраструктура
ОС	Операционная система
ПО	Программное обеспечение
СМС-рассылка	инструмент, для отправки большого количества коротких сообщений (СМС) на мобильные устройства абонентов сотовых сетей
CMDB	Configuration Management Database
CSV	Comma-Separated Values
HTTP	HyperText Transfer Protocol
LLDP	Link-Layer Discovery Protocol
NETCONF	Network Configuration Protocol
NTP	Network Time Protocol
PDF	Portable Document Format
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SQL	Structured Query Language
WMI	Windows Management Instrumentation
ZTP	Zero-Touch Provisioning

1. Общие сведения о программе

1.1. Назначение программы

E-NODE – универсальный программный комплекс мониторинга и управления сетевой и серверной инфраструктурой, инженерным оборудованием, оборудованием АСУ, АСУ ТП, информационными системами и другими типами оборудования и программного обеспечения Заказчика, а также средство контроля, управления и обеспечения безопасности сетевой, серверной и облачной инфраструктуры.

Система может использоваться как самостоятельный, законченный продукт, так и встраиваться во внешние (существующие или разрабатываемые) информационные системы Заказчиков.

1.2. Функции и решаемые задачи программы

Система обеспечивает:

- быстрое внедрение за счёт существующего набора описанных устройств, включая российское оборудование;
- прозрачный технический учёт (инвентаризацию) физических и логических ресурсов технологических сетей связи, ИТ-инфраструктуры и инженерных систем, а также мониторинг их состояния;
- замену множества систем мониторинга оборудования на единую платформу;
- полное понимание структуры информационных потоков в сетях;
- возможность выделения сетевого взаимодействия, относящегося к определенным сервисам и приложениям, обеспечение безопасности на уровне информационных потоков;
- помощь оператору в определении критических уровней ошибок в сети и принятию оптимальных решений по устранению угроз, локализации аварийных событий и сопровождению аварийно-

восстановительных и ремонтных работ, учёт и контроль планового обслуживания;

- уведомление о событиях посредством электронного (диспетчерского) журнала, СМС-рассылки, мессенджеров и электронной почты;
- возможность управления конфигурациями и техническим учётом;
- ситуационное управление оборудованием, ресурсами технологических сетей связи, ИТ-инфраструктуры и инженерных систем;
- повышение наблюдаемости и контролируемости инфраструктуры.

Со стороны серверной части Система обеспечивает возможность:

- выбора базовой операционной системы из широкого перечня систем семейства Linux (Ubuntu, Astra Linux, ALT Linux);
- установки на виртуальные машины;
- резервирования программных узлов;
- создания сложных геораспределенных систем мониторинга и управления.

Со стороны клиентской части Система необходима для:

- технического учёта физических и логических ресурсов технологических сетей связи, ИТ-инфраструктуры и инженерных систем, а также мониторинга их состояния;
- помощи оператору в принятии оптимальных решений по устранению угроз, оперативного предоставления причин отказов, а также предиктивного анализа объектов контроля;
- ситуационного управления ресурсами технологических сетей связи, ИТ-инфраструктуры и инженерных систем;
- повышения наблюдаемости и контролируемости инфраструктуры.

Для выполнения поставленных задач программа оснащена оконным пользовательским интерфейсом, содержащим: меню выбора подсистемы,

меню вкладок, панель статусов, меню пользователя, панель навигации в левой части экрана и рабочую область экрана в виде окна.

Система предназначена для решения следующих задач:

- Мониторинг состояния объектов мониторинга:
  - опрос объектов с использованием различных протоколов;
  - формирование статуса объектов на основе пороговых значений;
  - построение зависимости объектов на основе иерархии с автоматическим наследованием статуса.
- Безопасность и контроль сетевых взаимодействий и глубокий анализ сетевого трафика:
  - визуализация сетевых потоков в гибридных средах (традиционные ЦОД, облака, Kubernetes, Docker);
  - диагностирование аномалий сетевого трафика, анализ поведения информационных систем;
  - блокировка несанкционированных связей на основе политик «белых списков».
- Распределенный программный межсетевой экран:
  - пакетная фильтрация;
  - блокировка/разрешение трафика по IP-адресам, портам и протоколам (TCP/UDP/ICMP);
  - Stateful Inspection;
  - контроль состояния соединений (отслеживание сессий);
  - защита от подмены пакетов и атак типа «подделка соединений»;
  - централизованное управление политиками;
  - автоматизированное реагирование (блокировка атакующих IP на основе данных от подсистемы мониторинга, подсистемы инвентаризации сетевых пакетов);
  - единая система протоколирования событий безопасности.

- Визуализация состояния объектов мониторинга:
  - настраиваемые сводные панели (dashboard) с консолидированной информацией;
  - топология сети с географической привязкой;
  - иерархическое отображение объектов с наследованием состояния;
  - автоматическое и ручное добавление объектов;
  - отображение объектов с детальным состоянием их компонентов;
  - встроенные фильтры для отображения объектов по различным признакам.
- Инвентаризация объектов:
  - хранение различной инвентарной информации объектов, включая данные об обслуживании, с возможностью поиска;
  - загрузка и привязка документов к объектам.
- Контроль производительности:
  - формирование графического представления метрик, собираемых с объектов.
- Управление оборудованием:
  - встроенные средства создания сценариев конфигурирования объектов с помощью различных протоколов (SSH, NETCONF, SNMP);
  - наличие готовых коннекторов для управления объектов;
  - возможность заказа разработки специализированных коннекторов для объектов.
- Управление конфигурациями:
  - импорт, экспорт и хранение конфигураций оборудования с контролем версий;
  - отслеживание изменений конфигурации;
  - встроенные средства редактирования конфигурации.

- События и оповещение:
  - регистрация событий с формированием журнала по всем объектам;
  - встроенный сервер SYSLOG;
  - экспорт событий по протоколу SYSLOG;
  - отправка оповещений по электронной почте, интеграция с мессенджерами;
- Отчетность:
  - шаблоны отчетов с возможностью редактирования;
  - шаблоны представления для экспорта вывода данных из консоли управления.
- Контроль доступа:
  - ролевая модель доступа;
  - разделение доступа на уровне отдельных объектов и групп иерархии.

1.3. Требования к техническому обеспечению

1.3.1. Требования к аппаратному обеспечения серверной части

Минимальные требования к конфигурации аппаратного обеспечения серверной части представлены в таблице 1.1. Конфигурация продуктивных и тестовых серверов должна иметь или превосходить по параметрам характеристики, изложенные в ней.

Таблица 1.1– Минимальные требования к конфигурации аппаратного обеспечения серверной части

Компонент	**Минимальная конфигурация**
Процессор	*2.4 ГГц с 12 ядрами*
Оперативная память	*32 ГБ DDR3*
Жесткий диск	*100 ГБ HDD SATA Enterprise*
Сетевая плата	*Соединение 1 Гбит/с*
Веб браузер	*Яндекс.Браузер 22 и выше* *Google Chrome (актуальные версии)* *Mozilla Firefox (актуальные версии)* *Microsoft Edge (Chromium) 112 и выше* *Opera (актуальные версии)* *Safari (актуальные версии)*

1.3.2. Требования к программному обеспечению

Для запуска E-NODE к программному обеспечению предъявляются минимальные требования, перечисленные в таблице 1.2.

Таблица 1.2 – Требования к конфигурации программного обеспечения клиентской части

Компонент	**Конфигурация**
Операционная система	*Linux*
Общесистемное ПО	*Система виртуализации Docker*

Для сборки исходного кода E-NODE к программному обеспечению предъявляются минимальные требования, перечисленные в таблице 1.3.

Таблица 1.3 – Требования к конфигурации программного обеспечения клиентской части для сборки E-NODE

Компонент	**Конфигурация**
Операционная система	*Linux*
Общесистемное ПО	*Система виртуализации Docker*

1.3.3. Требования к аппаратному обеспечению клиентской части

Для работы с E-NODE АРМ пользователя должен удовлетворять минимальным требованиям к аппаратному обеспечению, перечисленным в таблице Таблица 1.4.

Таблица 1.4 – Требования к конфигурации аппаратного обеспечения клиентской части

Компонент	**Минимальная конфигурация**
Процессор	*2.4 ГГц с 4 ядра*
Оперативная память	*8 ГБ DDR3*
Жесткий диск	*50 ГБ HDD SATA Enterprise*
Сетевая плата	*Соединение 100 Гбит/с*

1.4. Требования администратору

1.4.1. Требования к квалификации администратора:

- наличие навыков установки и настройки ПО;
- наличие знаний основ мониторинга и настройки производительности ПО и баз данных;
- наличие опыта работы по настройке вычислительной техники и ПО в локальных сетях;
- наличие навыков настройки системной политики прав пользователей в операционных системах семейства Linux;
- наличие навыков по организации сред виртуализации и контейнеризации.

1.4.2. Обязанности администратора:

- ведение учетных записей пользователей Системы;
- управление правами доступа пользователей Системы к её функциям;
- управление разделами АРМ Администратора Системы.

2. Структура Системы

Структура Системы и схема взаимодействия компонентов представлены на рисунке 2.1.

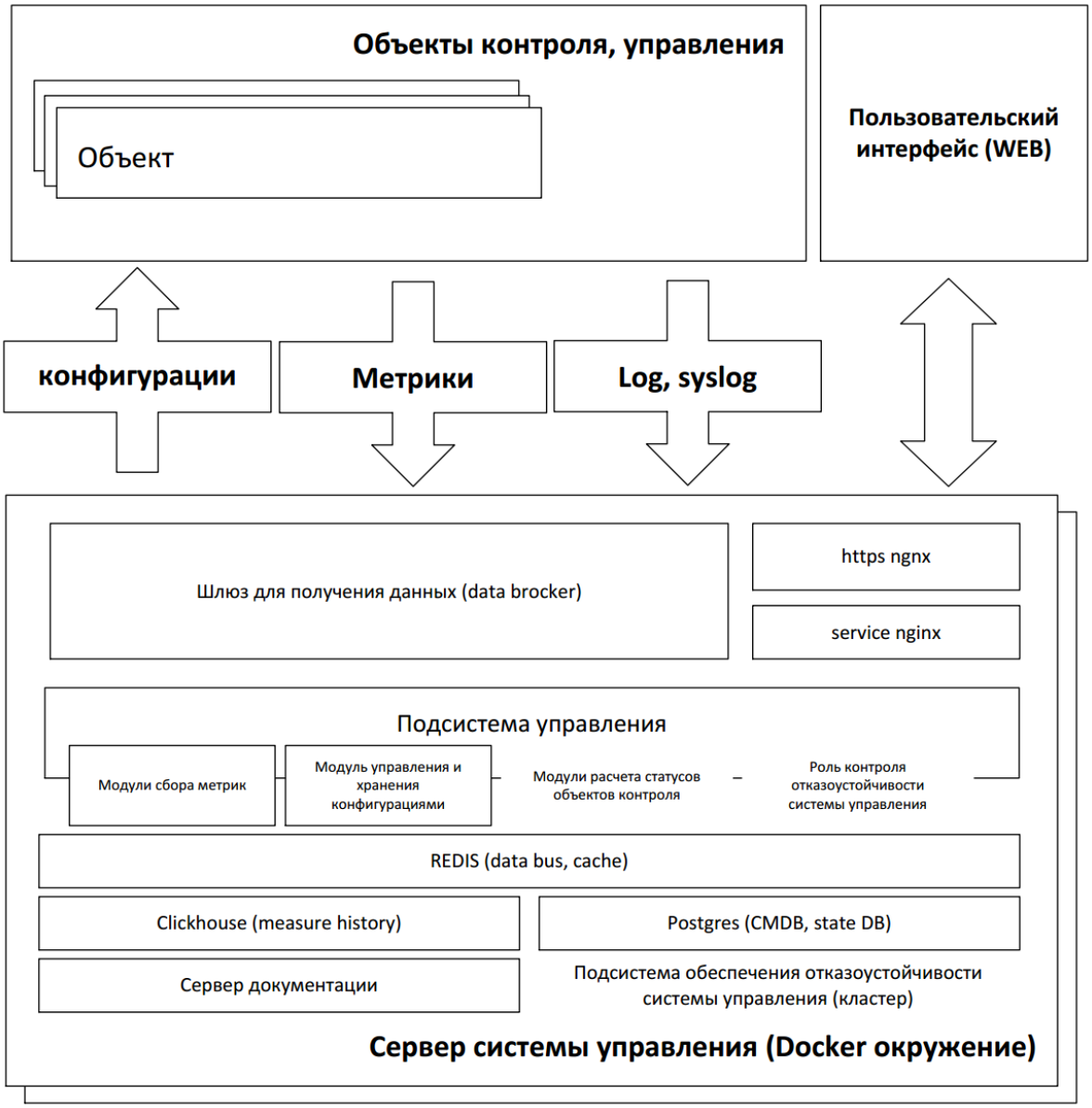

Рисунок 2.1 – Структура Системы

Архитектура Системы включает в себя следующие модули:

- Модуль мониторинга состояния объектов (Fault Management);
- Модуль визуализации состояния объектов;
- Модуль инвентаризации объектов (NRI);
- Модуль управления объектами;

- Модуль управления конфигурациями объектов (Configuration Management);
- Модуль контроля параметров устойчивого функционирования;
- Модуль отображения событий и оповещения и управления заявками (Notification and order management);
- Программный агент сбора информации с узлов контроля;
- Модуль инвентаризации сетевых потоков;
- Модуль межсетевого экрана;
- Модуль формирования отчетов.

Система построена на базе микросервисной архитектуры и может функционировать в среде Docker, Kubernetes.

2.1.1. Модуль мониторинга состояния объектов (Fault Management)

Данный модуль позволяет пользователю создать иерархию объектов, которая соответствует реальной топологии инфраструктуры предприятия, например – «здание по адресу – этаж – комната – стойка – объект – компонент объекта».

Также данный модуль позволяет:

- проводить мониторинг объектов с использованием протоколов SNMP, HTTP, ModBus, МЭК 60870-5-104, WMI, SQL, MQTT;
- формировать статус объектов на основе пороговых значений;
- строить зависимости объектов на основе иерархии с автоматическим наследованием статус;
- настраивать индивидуальные параметры опроса для каждого устройства;
- фильтровать и выгружать основные события Системы в формате PDF или CSV.

2.1.2. Модуль визуализации состояния объектов

Данный модуль позволяет:

- настраивать сводные панели (dashboard) с консолидированной информацией;
- отображать топологию сети с географической привязкой (а также в виде графа с отображением статусов связи между объектами);
- отображать объекты согласно иерархии с возможностью наследования состояния;
- автоматически и вручную добавлять объекты;
- автоматически строить сети на основе протокола LLDP;
- отображать объекты с детальным состоянием их компонентов;
- использовать встроенные фильтры для отображения объектов по различным признакам.

2.1.3. Модуль инвентаризации объектов (CMDB)

Данный модуль позволяет:

- автоматически собирать и хранить инвентарную информацию об объекте, включая данные об обслуживании, с возможностью поиска;
- формировать события на основе указания даты проведения обслуживаний;
- загружать и привязывать документы к объектам;
- указывать у объектов владельца, обслуживающую организацию и тип системы;
- визуализировать телекоммуникационные стойки;
- сканировать объекты мониторинга по расписанию на предмет изменения встраиваемых модулей (в разработке);
- произвести интеграцию с внешними CMDB и системами управления заявок.

2.1.4. Модуль управления объектами

Данный модуль позволяет:

- использовать встроенные средства создания сценариев конфигурации объектов с помощью различных протоколов (SSH, SNMP);
- осуществлять обновления программного обеспечения устройств;
- использовать готовые коннекторы для управления объектами;
- заказывать разработку специализированных коннекторов для управления объектами;
- использовать модуль ZTP (Zero-Touch Provisioning) для первоначальной настройки оборудования в автоматическом режиме;
- использовать встроенную консоль SSH для управления объектами.

2.1.5. Модуль управления конфигурациями объектов (Configuration Management)

Данный модуль позволяет:

- производить импорт, экспорт и хранение конфигураций оборудования с контролем версий;
- отслеживать изменений конфигураций;
- использовать встроенные средства сравнения и редактирования конфигураций.

2.1.6. Модуль контроля параметров устойчивого функционирования

Модуль является средством (инструментом), предоставляющим возможность комплексной оценки объектов в КИИ, с целью определения рисков, возникновение которых может привести к снижению устойчивости функционирования объекта.

Модуль обеспечивает возможность расчета фактических свойств объекта, включающий в себя функциональность, надежность как для комплекса в целом, так и для отдельных его компонентов.

2.1.7. Модуль отображения событий и оповещения

Данный модуль позволяет:

- регистрировать события и формировать журнал по всем объектам;
- использовать встроенный сервер SYSLOG для приёма событий от объектов;
- экспортировать события по протоколу SYSLOG;
- отправлять оповещения по электронной почте и производить интеграцию с мессенджерами.

2.1.8. Программный агент сбора информации с узлов контроля;

Данный модуль позволяет представляет собой микросервис, устанавливаемый на целевые узлы для выполнения задач мониторинга. Передача конфигураций модулю производится через систему распределенных конфигураций. Все метрики и события передаются в централизованную систему управления.

Также данный модуль позволяет:

- выполнять сбор метрик о работе операционной системы (процессы, загрузка, использование ресурсов);
- выполнять сбор метрик о работе каналов связи: точка – точка, качество, количество сбоев, задержки, пропускная способность;
- выполнять сбор информации о всех сетевых пакетах на всех интерфейсах;
- применять правила межсетевого экрана;
- выполнять сбор информации о системах виртуализации;
- реализовывать функции Policy Based Routing на уровне eBPF;
- осуществлять мониторинг состояния сетевых интерфейсов.

2.1.9. Модуль инвентаризации сетевых потоков

Данный модуль позволяет:

- выполнять визуализацию сетевых потоков в гибридных средах (традиционные ЦОД, облака, Kubernetes, Docker);
- диагностировать аномалии сетевого трафика, осуществлять анализ поведения информационных систем;
- выполнять блокировку несанкционированных связей на основе политик «белых списков».

2.1.10. Модуль межсетевого экрана

Данный модуль позволяет:

- выполнять пакетную фильтрацию трафика посредством статических правил межсетевого экрана на основе IP-адресов и портов источника и назначения, а также используемых интерфейсов;
- выполнять пакетную фильтрацию трафика посредством динамических правил, формируемых во время работы Системы на основе анализа сетевых потоков;
- осуществлять контроль состояния соединений (отслеживание сессий);
- осуществлять защиту от подмены пакетов и атак типа «подделка соединений»;
- выполнять автоматизированное реагирование на инциденты сетевой безопасности (блокировка атакующих IP на основе данных от подсистемы мониторинга, подсистемы инвентаризации сетевых пакетов);
- осуществлять централизованное управление правилами межсетевого экрана, выполнять их редактирование, активацию/деактивацию, в т.ч. по определенным условиям;
- обеспечивать комплексное протоколирование событий безопасности.

2.1.11. Модуль формирования отчетов

Данный модуль позволяет формировать необходимые отчеты, в частности:

- статистику по типам узлов;
- отчет по созданию новых потоков;
- топ узлов источников (по количеству трафика);
- топ узлов назначения (по количеству трафика);
- топ потоков (по количеству трафика);
- топ узлов назначения (по количеству трафика по потокам).

3. Подготовка к работе, установка и проверка работоспособности

Установка программного комплекса E-NODE осуществляется согласно изложенным ниже инструкциям.

3.1. Подготовка к установке

Перед началом работ по установке программного комплекса E-NODE предварительно необходимо выполнить подключение аппаратной платформы комплекса к сети согласно схеме подключения интерфейсов, а также выбрать статические IP-адреса для дальнейшей настройки. Кроме того, необходимо подготовить переносной Flash-накопитель, содержащий ISO-образ базовой операционной системы для ее дальнейшей установки.

3.2. Процедура установки Системы

3.2.1. Установка базовой ОС

В процессе базовой настройки программного комплекса E-NODE прежде всего необходимо выполнить установку ОС Linux (рекомендуются серверные редакции систем Ubuntu/Debian или Astra Linux/ALT Linux).

Установка любого из выпусков операционной системы Linux производится обычным образом в варианте Minimal Installation. После установки системы необходимо установить последние обновления, а также настроить удаленный доступ к ней по SSH, после чего управление сервером программного комплекса E-NODE и все дальнейшие манипуляции можно будет осуществлять удаленно с консоли управления:

```
ssh -l <имя пользователя> <имя или IP-адрес устройства МКИ>
```

3.2.2. Сетевые настройки

Для корректной работы сетевых интерфейсов и сохранения их параметров после перезагрузки сервера необходимо в каталоге /etc/netplan

создать файл с расширением .yaml (например, 01-network.yaml) со следующим содержимым:

```
network:
    version: 2
    ethernets:
        enp5s0:
            dhcp4: false
            addresses:
                - 192.168.1.15/24
            routes:
              - to: default
                via: 192.168.1.1
            nameservers:
                addresses: [8.8.8.8]
        enp6s0:
            dhcp4: false
        enp7s0:
            dhcp4: false
        enp8s0:
            dhcp4: false
            addresses:
                - 192.168.199.1/24
    bridges:
        docker0:
            interfaces: [enp6s0, enp7s0]
```

Примечания:

- Для выбранного интерфейса администрирования (в примере выше выбран **enp5s0**) следует указать нужный статический адрес сервера, также при необходимости следует указать фактически используемые адреса шлюза и DNS (в via и nameservers соответственно, для DNS рекомендуется в общем случае указывать 8.8.8.8).
- В файле конфигурации заранее определяется мост docker0, который будет использоваться Docker'ом после его установки. Таким образом, выбранные для этого интерфейсы заранее подключаются к мосту docker0, и, соответственно, в будущем будут доступны из Docker.

- Для удобства работы рекомендуется скопировать готовый файл 01-network.yaml с компьютера администратора и положить его в /etc/netplan, при этом для файла следует установить права по маске 0100600.
- Существующий в /etc/netplan файл конфигурации по умолчанию 50-cloud-init.yaml необходимо переименовать, иначе у интерфейса будет образовываться 2 адреса - статический из настроек в 01-network.yaml и динамический, который будет дополнительно выдаваться по DHCP и создавать путаницу. Во избежание конфликтов рекомендуется держать в /etc/netplan только один файл 01-network.yaml с настройками интерфейсов.
- Для применения настроек интерфейсов и сохранения настроек после перезагрузки сервера рекомендуется выполнение **netplan generate** . Это позволит проверить конфигурацию перед применением и выявить возможные ошибки. Саму конфигурацию следует применять через **netplan try --timeout 10** чтобы обеспечить автоотмену в случае ошибок конфигурации. Также рекомендуется в обязательном порядке выполнить контрольную перезагрузку сервера, чтобы убедиться, что настройки после нее восстанавливаются правильно.
- Один из интерфейсов на сервере рекомендуется сконфигурировать отдельно вне моста docker0 с техническим IP вида 192.168.199.1/24, чтобы при необходимости можно было напрямую подключиться к нему с ноутбука.

3.2.3. Установка сертификата Entcor

С компьютера администратора следует скопировать файл сертификата entcor.crt на сервер программного комплекса E-NODE по следующему пути:

```
scp entcor.crt <имя или IP-адрес устройства МКИ>:/home/<имя пользователя>
```

Затем на сервере программного комплекса E-NODE следует перенести сертификат в необходимый каталог и выполнить его обновление:

```
sudo mv entcor.crt /usr/local/share/ca-certificates
sudo update-ca-certificates
```

Примечание: после обновления сертификатов необходимо выполнить перезагрузку программного комплекса E-NODE.

3.2.4. Установка системы контейнерной виртуализации Docker

Установка на сервер программного комплекса E-NODE системы контейнерной виртуализации Docker выполняется стандартно с использованием репозитория Docker согласно рекомендациям по установке, изложенным в документации Docker:

https://docs.docker.com/engine/install/ubuntu/#install-using-the-repository

```
sudo apt-get update
sudo apt-get install ca-certificates curl
sudo install -m 0755 -d /etc/apt/keyrings
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o \
/etc/apt/keyrings/docker.asc
sudo chmod a+r /etc/apt/keyrings/docker.asc

echo \
«deb   [arch=$(dpkg   --print-architecture)   signed-by   =   \
/etc/apt/keyrings/docker.asc]\
$(. /etc/os-release && echo «$VERSION_CODENAME») stable» | \
sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
sudo apt-get update
sudo apt-get install docker-ce docker-ce-cli containerd.io \
docker-buildx-plugin docker-compose-plugin
```

3.2.5. Установка компонентов Системы

Для установки компонентов системы E-NODE необходимо:

1. Скопировать следующие файлы:

- **installPacket.sh** – скрипт по установке окружения для E-NODE
- **pre_install.tar** – архив с пакетами окружения
- **installenms.sh** – скрипт по установке E-NODE
- **latest.tar.gz** – архив с пакетами E-NODE (на примере версии latest)

в **/home/$user$** на целевую операционную систему (Рисунок 3.1).

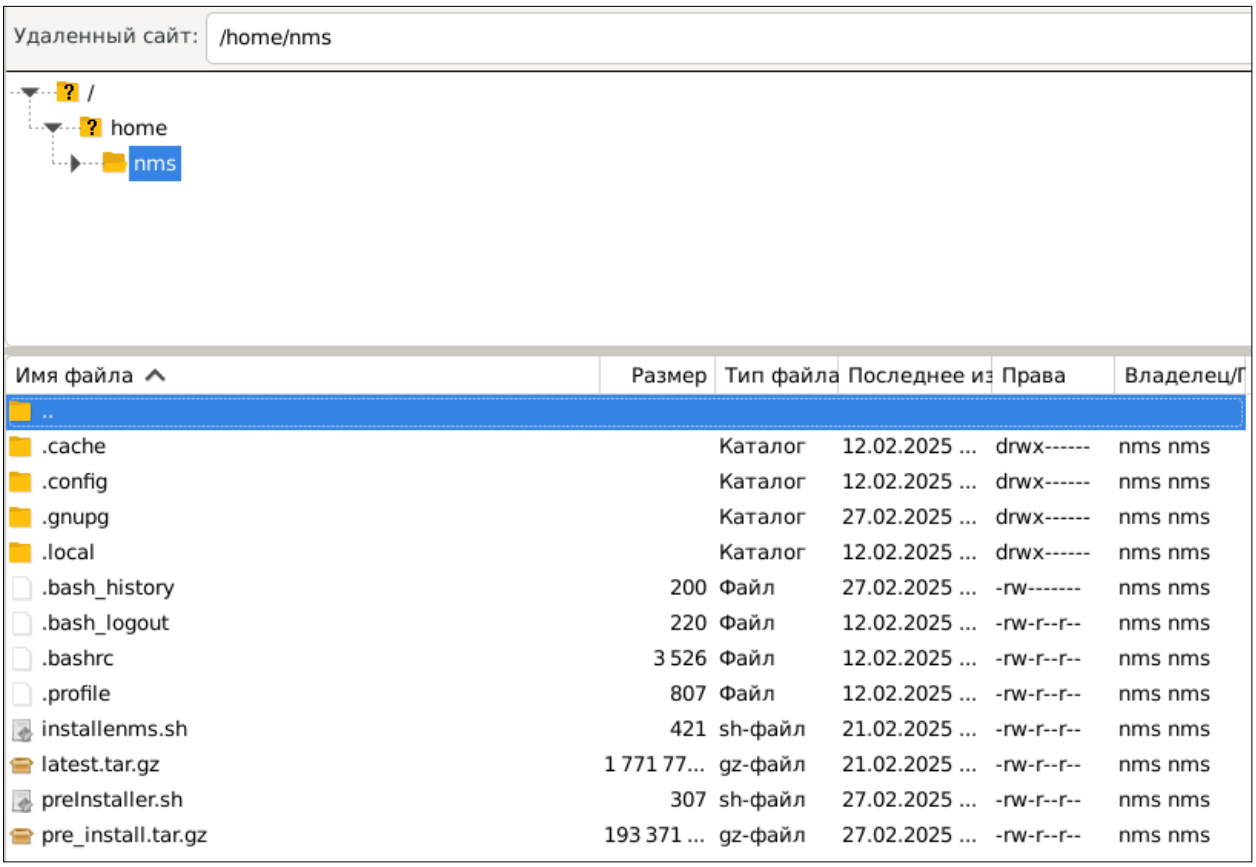

Рисунок 3.1

2. Подключиться по протоколу **SSH** и проверить расположение файлов командой `ls` (Рисунок 3.2).

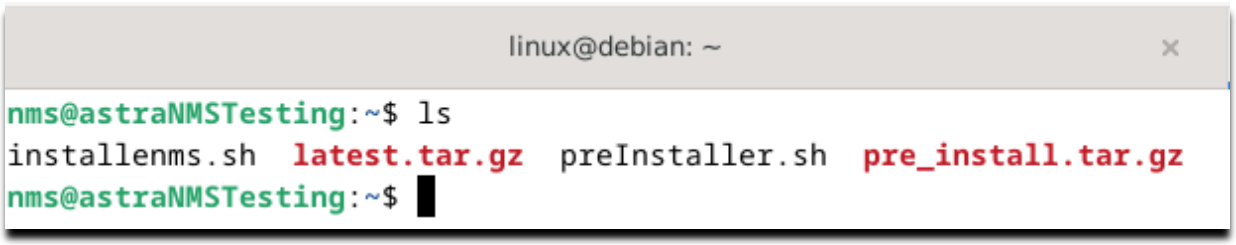

Рисунок 3.2

3. Запустить скрипт установки базовых пакетов, командой `bash preInsataller.sh pre_install.tar.gz astra` **(**на примере операционной системы **Astra Linux)** (Рисунок 3.3).

```
nms@astraNMSTesting:~$ bash preInstaller.sh pre_install.tar.gz astra
```

Рисунок 3.3

4. На рисунке 3.4 отображено **завершение установки**.

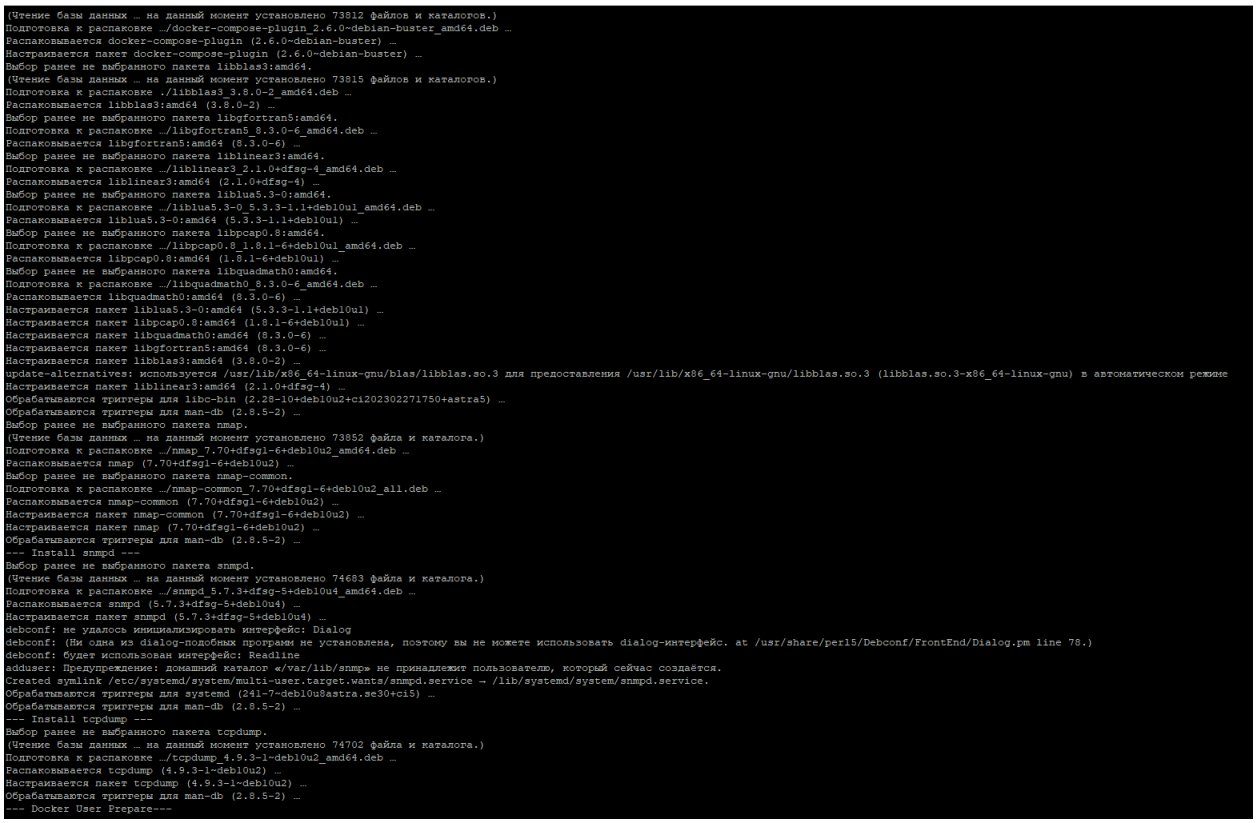

Рисунок 3.4

Далее необходимо:

5. Проверить установку `docker` (Рисунок 3.5).

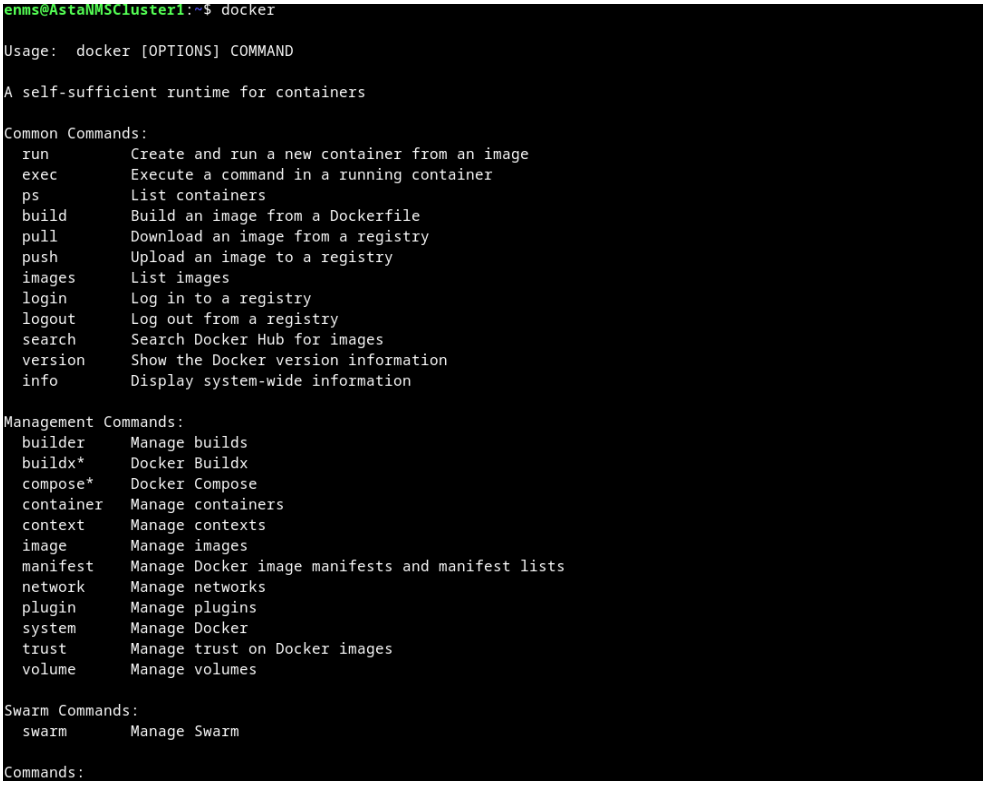

Рисунок 3.5

6. Проверить установку `snmp` (Рисунок 3.6).

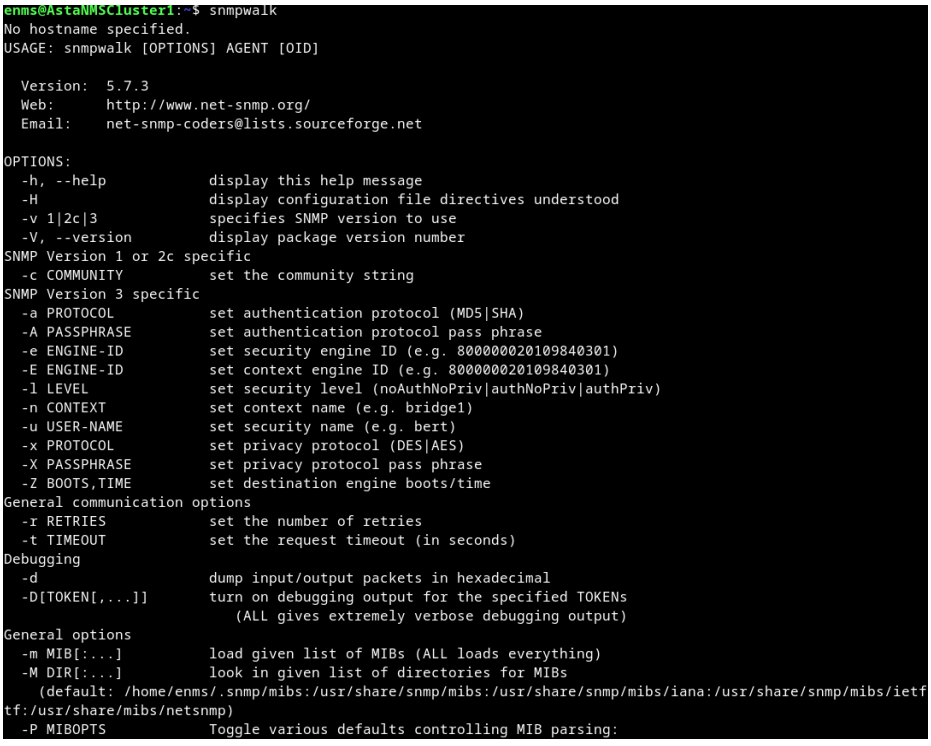

Рисунок 3.6

7. Проверить установку `nmap` (Рисунок 3.7).

```
enms@AstaNMSCluster1:~$ nmap
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
```

Рисунок 3.7

8. Проверить установку `tcpdump` (Рисунок 3.8).

```
enms@AstaNMSCluster1:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
14:10:24.798128 IP 192.168.2.138.ssh > 192.168.2.254.55414: Flags [P.], seq 558265208:558265396, ack 1530984
14:10:24.798495 IP 192.168.2.138.35462 > netsrv.entcor.domain: 12269+ PTR? 254.2.168.192.in-addr.arpa. (44)
14:10:24.799034 IP netsrv.entcor.domain > 192.168.2.138.35462: 12269 NXDomain* 0/1/0 (98)
14:10:24.799117 IP 192.168.2.138.43428 > netsrv.entcor.domain: 43714+ PTR? 138.2.168.192.in-addr.arpa. (44)
```

Рисунок 3.8

9. Запустить скрипт установки E-NODE командой `bash installenms.sh`. Результат выполнения команды представлен на рисунке 3.9:

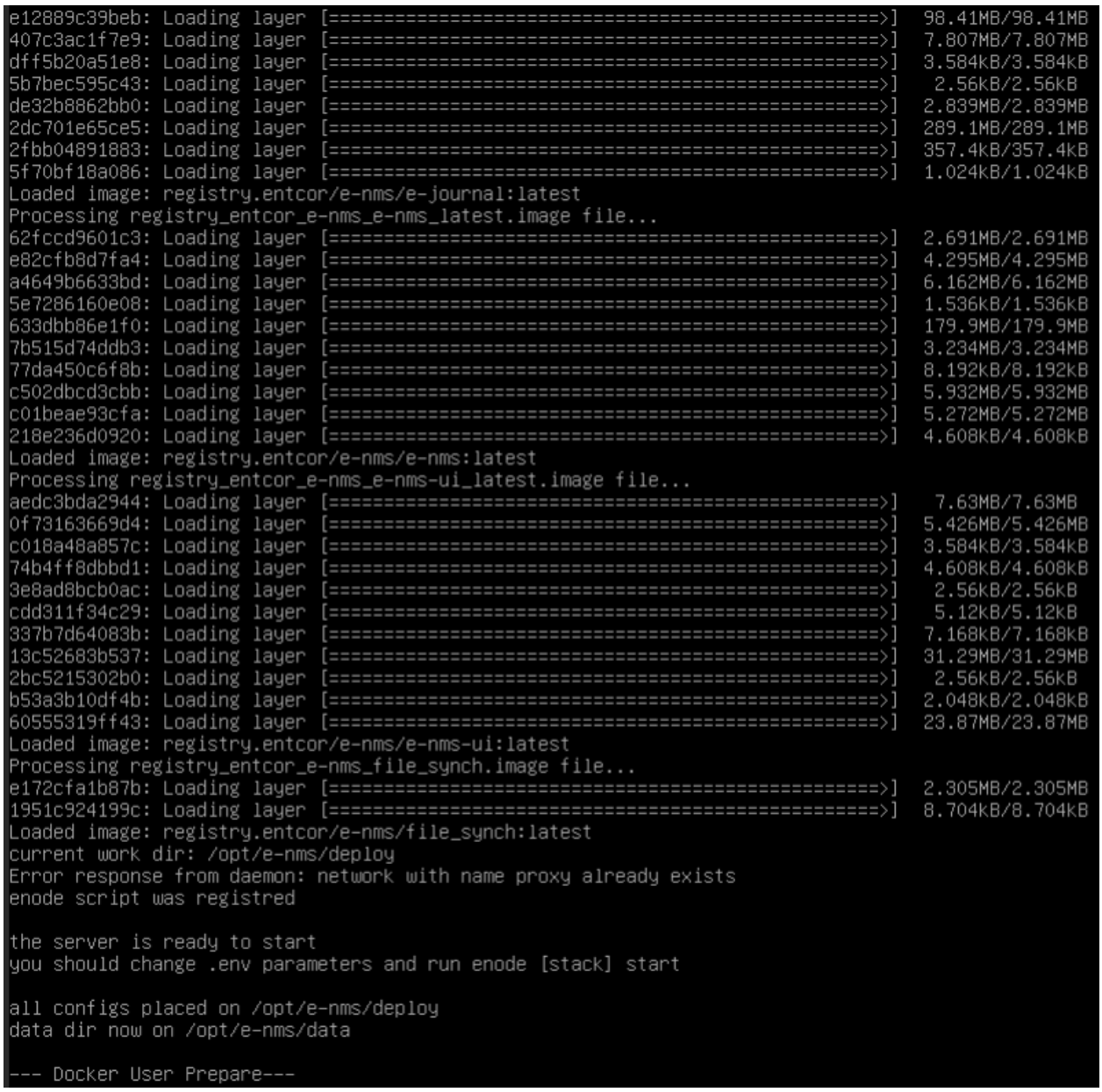

Рисунок 3.9 – Результат выполнения команды `bash installenms.sh`

10. Последовательно выполнить следующие команды:

- `E-NODE app start` (Рисунок 3.10);
- `E-NODE E-NODE start` (Рисунок 3.11);
- `E-NODE analytic start` (Рисунок 3.12);
- `E-NODE e-cvs start` (Рисунок 3.13).

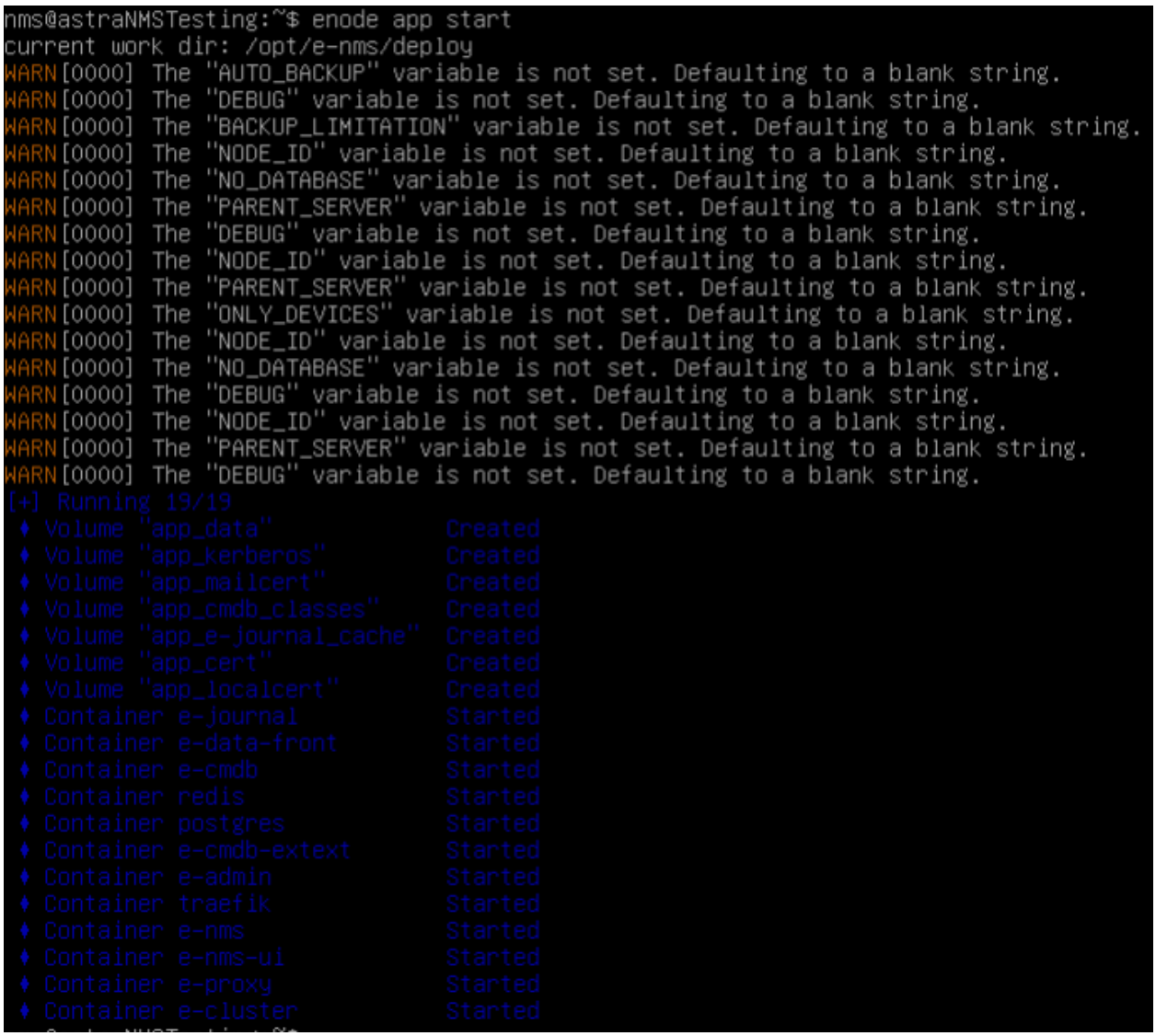

Рисунок 3.10 – Результат выполнения команды `E-NODE app start`

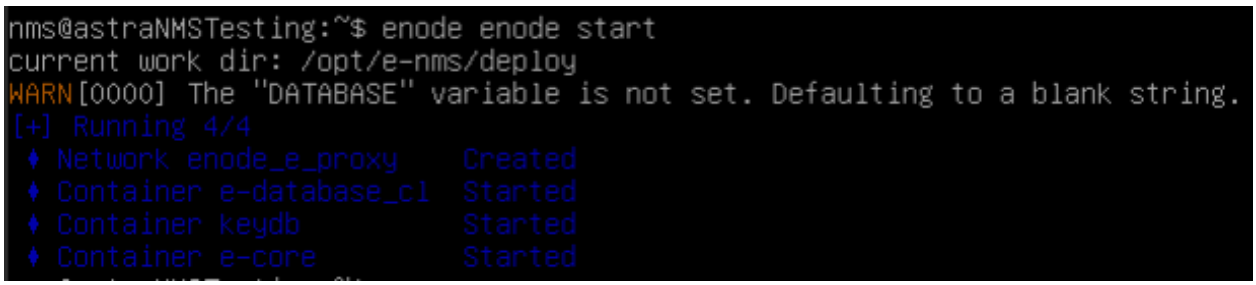

Рисунок 3.11 – Результат выполнения команды `E-NODE E-NODE start`

Рисунок 3.12 – Результат выполнения команды `E-NODE analytic start`

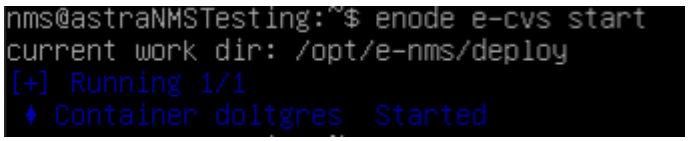

Рисунок 3.13 – Результат выполнения команды `E-NODE e-cvs start`

11. После выполнения всех команд необходимо проверить доступность Web-интерфейса по IP-адресу целевой системы (Рисунок 3.14):

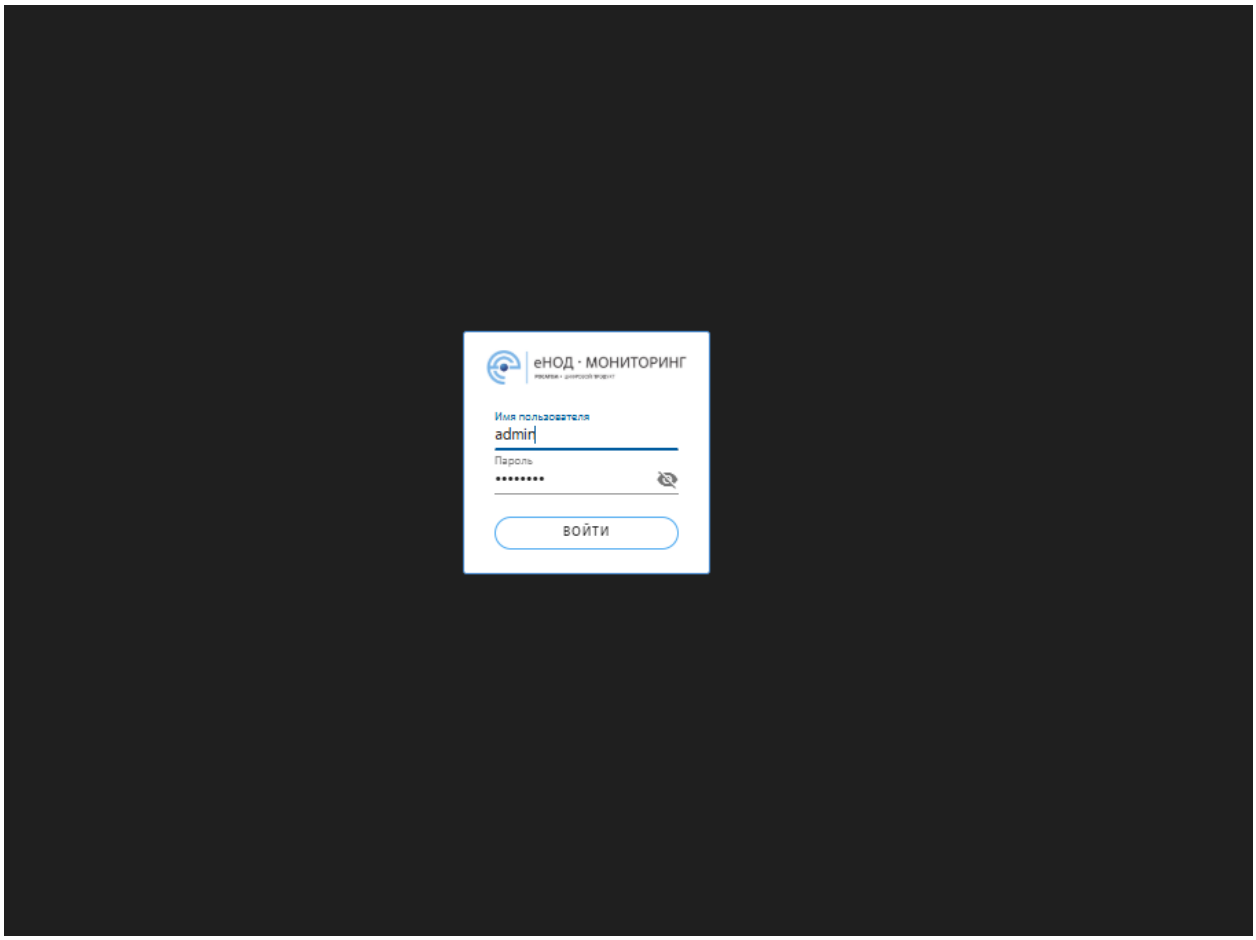

Рисунок 3.14 – Проверка доступности веб интерфейса

3.3. Установка синхронизации времени

3.3.1. Общие положения

Для полноценной работы Системы синхронизация времени должна осуществляться между следующими компонентами E-NODE:

- сервер E-NODE:
  - отдельностоящий (standalone) в случае одномашинной конфигурации Системы;
  - кластер серверов в случае применения кластерной конфигурации Системы;
- клиентские места E-NODE:
  - рабочие места под управлением ОС Windows;
  - рабочие места под управлением ОС Linux.

Для обеспечения единого времени на компонентах E-NODE используется протокол NTP (network time protocol) – сетевой протокол для синхронизации часов в компьютерных системах по сетям передачи данных с коммутацией пакетов и переменной задержкой (латентностью). Одним из ключевых преимуществ протокола является возможность передачи меток времени непосредственно по сети передачи данных, что позволяет отказаться от отдельной шины точного времени.

3.3.2. Варианты построения системы синхронизации

Для обеспечения единого времени на всех компонентах возможно использование следующих вариантов построения системы синхронизации.

Вариант 1 (предпочтительный). Использование сервера (источника) точного времени, имеющегося на предприятии (Рисунок 3.15).

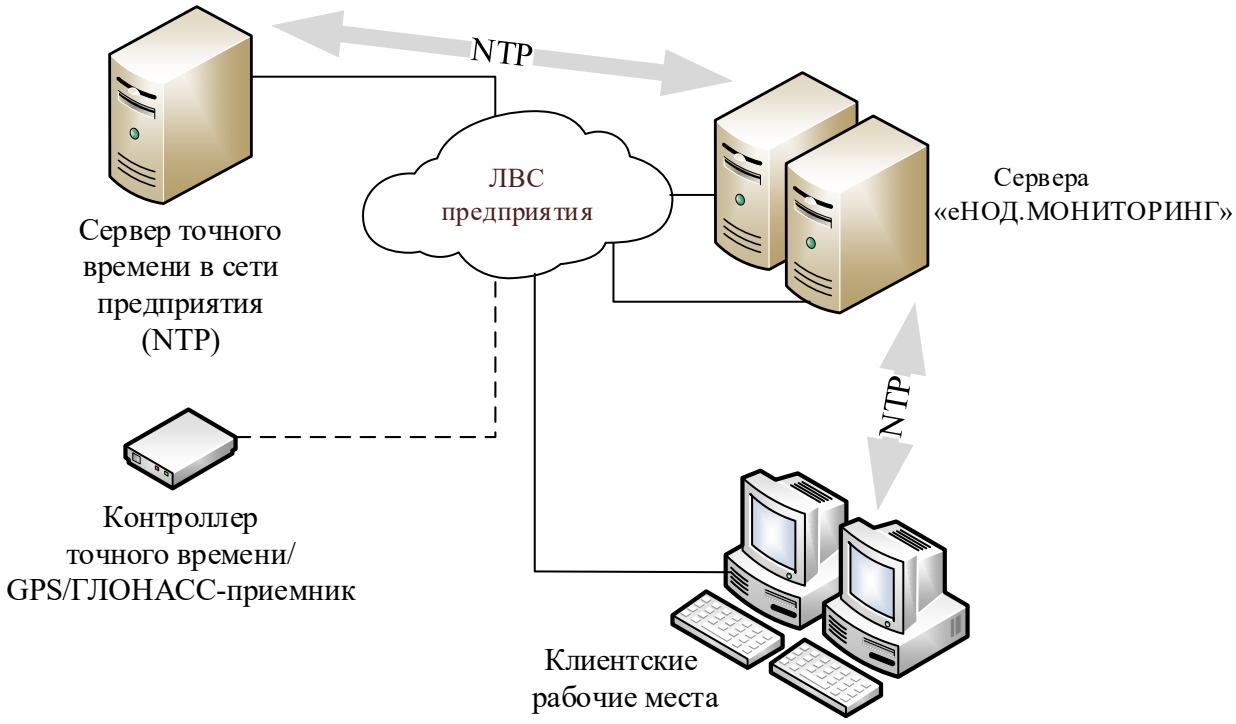

Рисунок 3.15 – Использование сервера (источника) точного времени, имеющегося на предприятии

При данном варианте построения системы синхронизации источником точного времени для серверов E-NODE является сервер (сервера) точного времени, расположенный(ые) в сети предприятия.
В качестве серверов точного времени могут выступать:

- выделенные (NTP) сервера точного времени;
- сервера службы каталога (к примеру, котроллеры домена Active Directory), развернутой в сети предприятия;
- сервера системы часофикации;
- GPS/ГЛОНАСС-приемники, используемые для синхронизации времени технологического оборудования;
- телекоммуникационное оборудование, поддерживающее функцию источника точного времени.

Клиентские рабочие места получают точное время от серверов E-NODE.

Вариант 2. Использование сети Интернет в качестве источника точного времени (Рисунок 3.16).

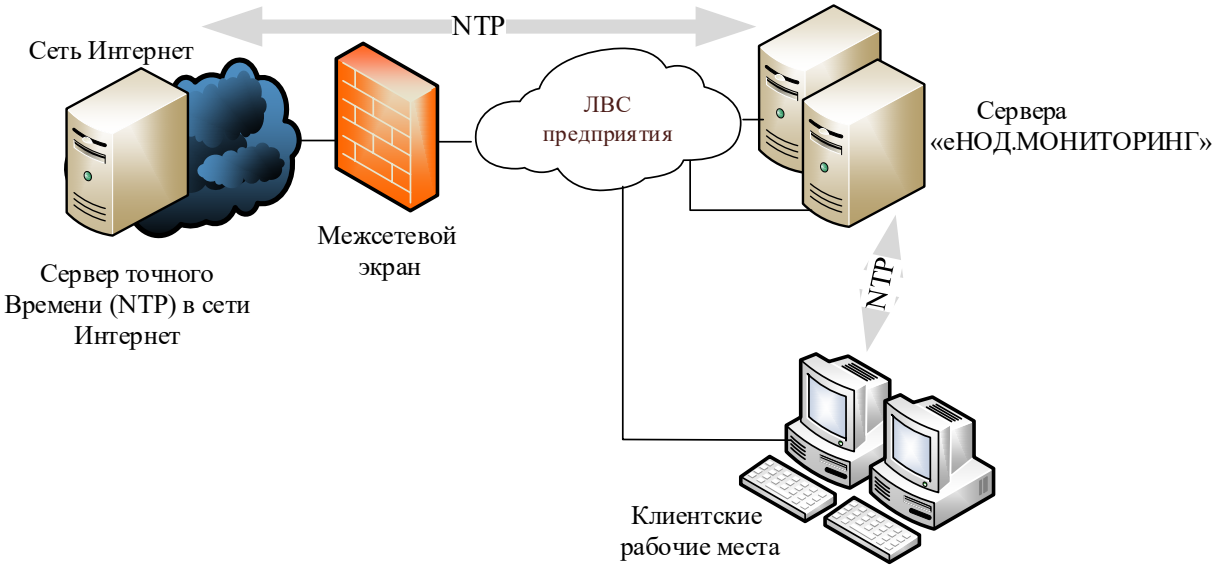

Рисунок 3.16 – Использование сети Интернет
в качестве источника точного времени

При данном варианте построения системы синхронизации источником точного времени для серверов E-NODE являются сервера точного времени, расположенные в сети Интернет. Клиентские рабочие места получают точное время от серверов E-NODE.

Вариант 3. Изолированная система (Рисунок 3.17).

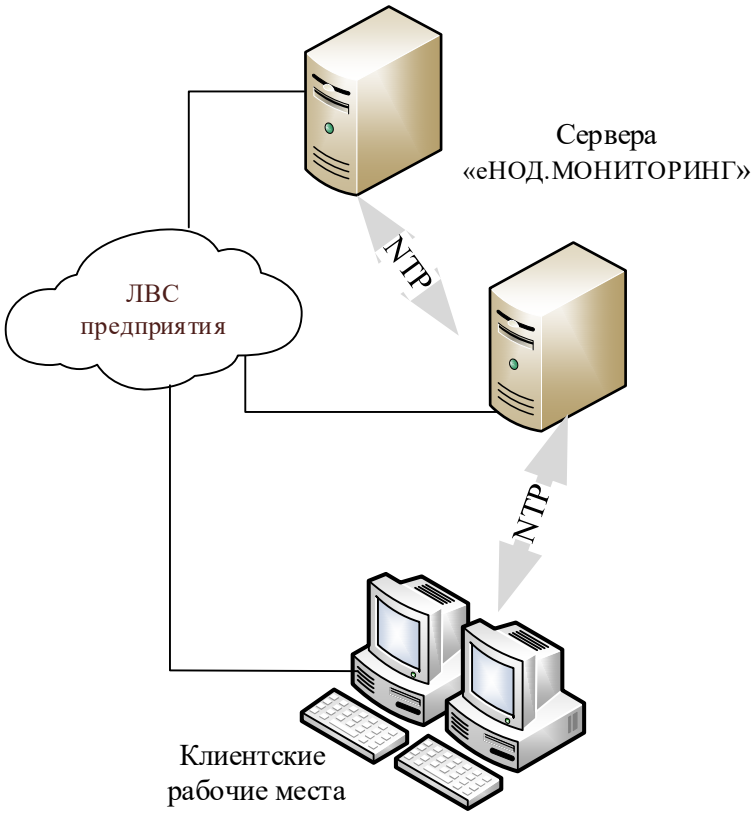

Рисунок 3.17 – Изолированная система точного времени

При данном варианте построения системы синхронизации источником точного времени для компонентов E-NODE являются внутренние часы одного из серверов E-NODE. Второй сервер получает точное время от первого, являющегося источником точного времени для всех компонентов. Клиентские рабочие места получают точное время от серверов E-NODE.

3.3.3. Настройка компонентов системы точного времени

3.3.3.1. Настройка серверов E-NODE

Установка и запуск пакетов, обеспечивающих работу системы синхронизации времени (NTP), выполняется на этапе установки базовых компонентов E-NODE. Дальнейшая настройка серверной части системы точного времени выполняется путем редактирования конфигурационного файла ntp.conf, расположенного в каталоге /etc/. В процессе инсталляции Комплекса по заданному пути размещается конфигурационный файл с типовыми настройками.

В случае использования сервера (источника) точного времени, имеющегося на предприятии (вариант 1), в конфигурационный файл (ntp.conf) необходимо внести информацию об адресах серверов точного времени в сети предприятия (Рисунок 3.18).

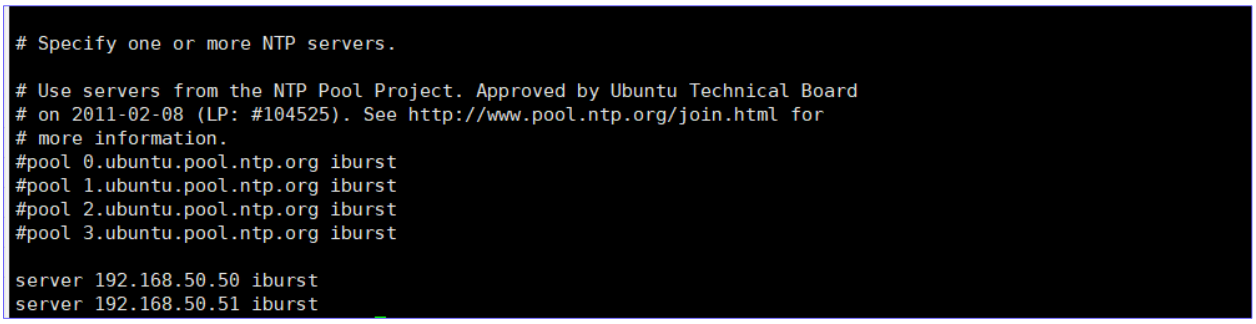

Рисунок 3.18 – Внесение информация в конфигурационный файл об адресах серверов точного времени сети предприятия

В случае использования сети Интернет в качестве источника точного времени (вариант 2) в конфигурационном файле (ntp.conf) необходимо отключить использование внутренних серверов точного времени в сети предприятия, и включить использование пула серверов ntp, расположенных в сети Интернет (Рисунок 3.19).

Рисунок 3.19 – Отключение в конфигурационном файле использования внутренних серверов точного времени

В случае построения изолированной системы точного времени (вариант 3) в конфигурационном файле (ntp.conf) сервера 2 необходимо внести информацию об адресе первого сервера, являющегося источником точного времени для компонентов системы (рис. Рисунок 3.20).

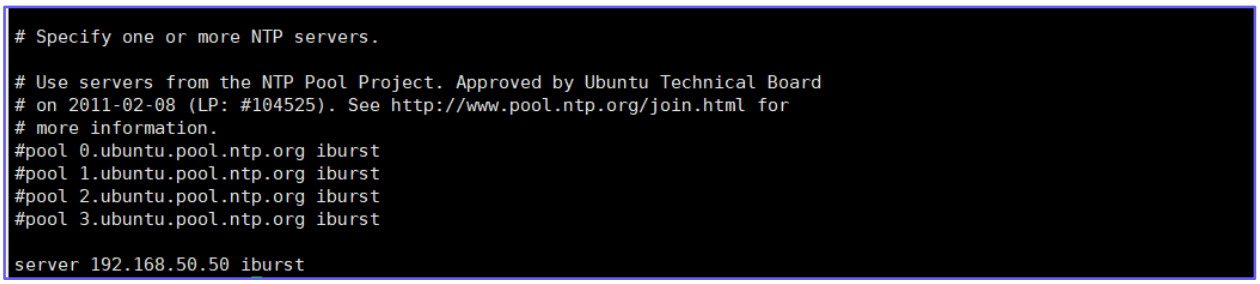

Рисунок 3.20 – Внесение информации об адресе первого сервера в конфигурационный файл сервера 2

В приведенном примере первый сервер имеет адрес «192.168.50.50».

3.3.3.2. Настройка клиента Windows 10

Применимо для Windows 10. Для настройки необходимо:

1. Нажать на кнопку [Пуск] и в выпавшем окне – на значок шестерёнки «Параметры» (Рисунок 3.21).

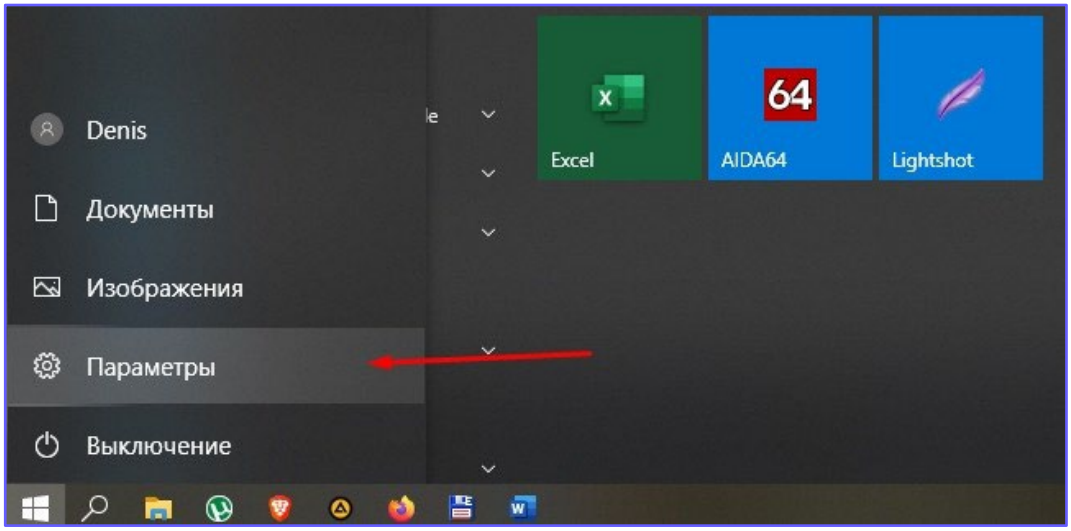

Рисунок 3.21 – Выбор «Параметры»

2. В открывшемся окне найти и нажать на иконку «Время и язык» (Рисунок 3.22).

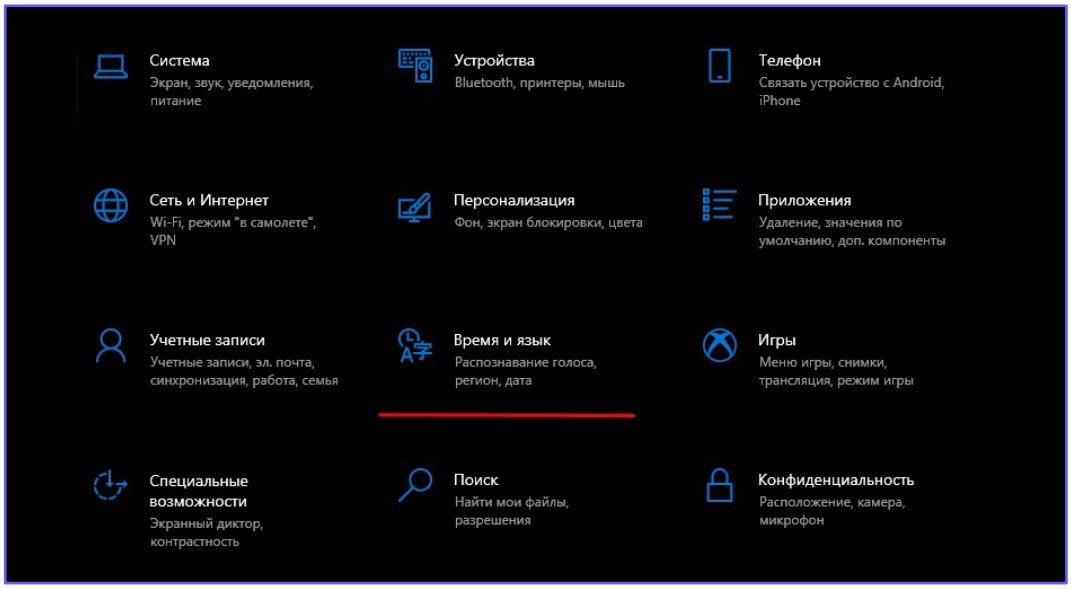

Рисунок 3.22 – Выбор «Время и язык»

3. После перехода вкладка будет разделена на две части. В левой найти и открыть раздел «Дата и время». В правой поставить галочку в пункте: «Установить время автоматически» на включенный режим, если она не активна (Рисунок 3.23).

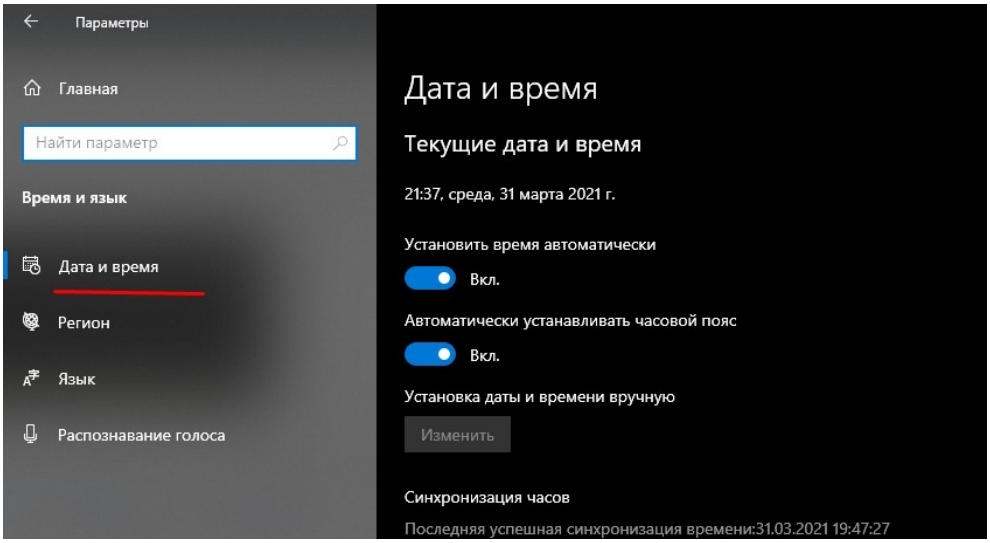

Рисунок 3.23 – Выбор вкладки «Дата и время»
→ флаг «Установить время автоматически»

4. Если синхронизация не произошла, в том же разделе найти пункт: «Формат даты, времени и региона» или в более старой версии «Дополнительные параметры даты и времени, региональные параметры», после чего открыть его.

5. В открывшейся панели нажать «Дата и время».

6. В новом окне нажать на вкладку «Время по интернету», затем на кнопку [Изменить параметры]».

7. Теперь нужно поставить галочку в разделе: «Синхронизировать с сервером времени в интернете». Ниже появится выпадающее окошко, в котором можно выбрать NTP-сервер или прописать свой, если предложенные ОС не проходят (Рисунок 3.24).

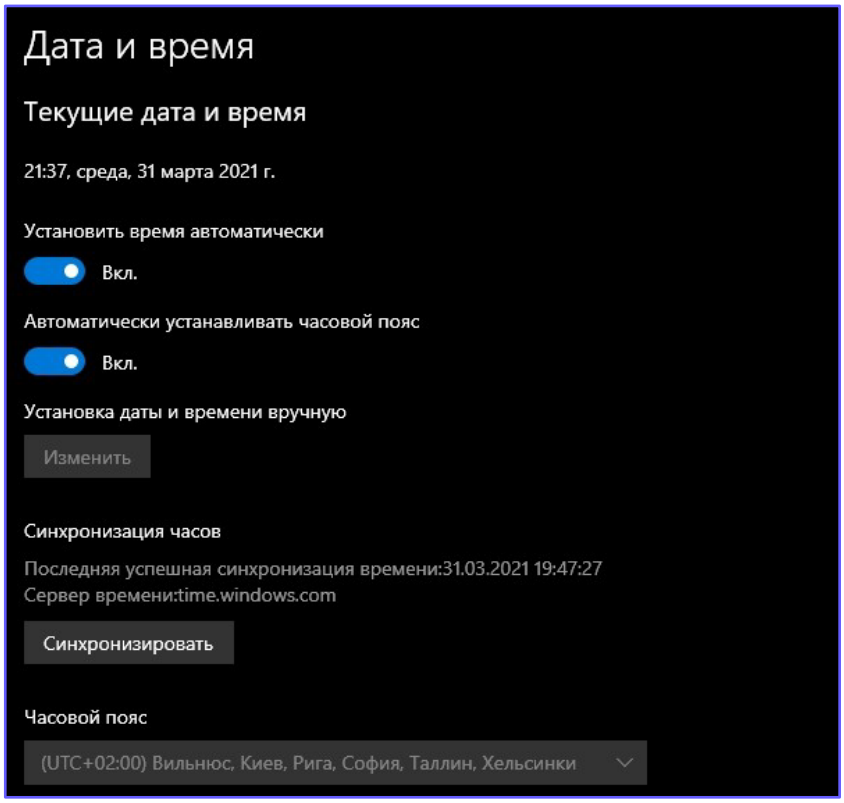

Рисунок 3.24 – Синхронизация часов

8. Нажать на кнопки [Обновить сейчас] и [Ok].

9. Во вкладке «Дополнительные часы» можно добавлять еще пункты, если требуется возможность время по другим поясам.

3.3.3.3. Настройка клиента под управлением ОС Linux Ubuntu

По умолчанию в ОС Linux Ubuntu служба синхронизации времени представлена сервисом `systemd timesync`, предоставляющим реализацию NTP, который управляется в контексте `systemd`. Он устанавливается и запускается по умолчанию в Ubuntu. Проверить состояние сервиса можно командой:

```
systemctl status systemd-timesyncd
```

Файл конфигурации для systemd-timesyncd – это /etc/systemd/timesyncd.conf.

```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=192.168.50.50
#FallbackNTP=ntp.ubuntu.com
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Единственный раздел, который он содержит, кроме комментариев, это [Time]. Все остальные строки закомментированы. Эти значения по умолчанию, их не нужно менять (если у вас нет для этого причин). Сервер NTP являющийся источником точного времени определяется в строке «NTP = …». В данном примере в качестве сервера NTP описан сервер с адресом «192.168.50.50». После внесения изменений в конфигурацию необходимо выполнить рестарт сервиса:

```
systemctl restart systemd-timesyncd
```

и проверить состояние службы синхронизации времени (Рисунок 3.25):

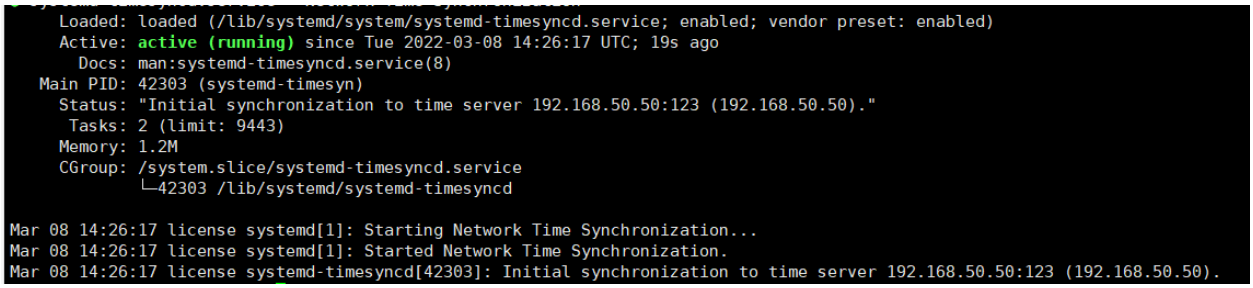

Рисунок 3.25 – Проверка службы синхронизации времени

```
systemctl status systemd-timesyncd
```