Министерство образования и молодежной политики Свердловской области

государственное автономное профессиональное

образовательное учреждение Свердловской области

«Уральский радиотехнический колледж им. А.С. Попова»

ДОПУСТИТЬ К ЗАЩИТЕ

Зав. отделением

­\_\_\_\_\_\_\_\_\_\_\_О. В. Алферьева

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

РАЗРАБОТКА МАКЕТА IT-ИНФРАСТРУКТУРЫ

СОВРЕМЕННОЙ КОМПАНИИ

Пояснительная записка к дипломному проекту

РК 09.02.06 401 10 ПЗ

Рецензент Руководитель

Д. С. Апататьев Д. С. Апататьев

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г.

Консультант Разработчик

Д. С. Апататьев Т. И. Куваев

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г.

Нормоконтролер

Д. С. Апататьев

«\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2025 г.

2025

**Содержание**

[**Введение** 4](#_Toc196405350)

[**1 Теоретическая часть** 5](#_Toc196405351)

[1.1 Значение IT-инфраструктуры в современном мире 5](#_Toc196405352)

[1.2 Компоненты и составляющие IT-инфраструктуры 6](#_Toc196405353)

[1.3 Основные принципы проектирования 10](#_Toc196405354)

[1.4 Безопасность инфраструктуры 21](#_Toc196405355)

[1.5 Требования для построения инфраструктуры 21](#_Toc196405356)

[1.6 Выбор лабораторной среды для создания макета 21](#_Toc196405357)

[**2 Практическая часть** 22](#_Toc196405358)

[2.1 Определение ПО, сервисов и производителей, подходящих под требования 22](#_Toc196405359)

[2.2 Планирование и подготовка к реализации будущей инфраструктуры 22](#_Toc196405360)

[2.3 Настройка сетевого оборудования 22](#_Toc196405361)

[2.4 Настройка серверных ОС 22](#_Toc196405362)

[2.5 Развертывание сервисов 22](#_Toc196405363)

[2.6 Настройка пользовательских ОС 22](#_Toc196405364)

[2.7 Проверка соответствия представленным и законодательным требованиям 22](#_Toc196405365)

[3 Охрана труда и производственная санитария 23](#_Toc196405366)

[**Заключение** 24](#_Toc196405367)

[**Перечень сокращений и условных обозначений** 25](#_Toc196405368)

[**Список используемых источников** 26](#_Toc196405369)

[Приложение А 27](#_Toc196405370)

# **Введение**

Основные параметры документа согласно ГОСТ Р 2.105-2019:

* + текст шрифт Times New Roman, 12пт;
  + межстрочный интервал 1.5;
  + поля: слева 25 мм, справа 10 мм, сверху 15 мм, снизу 30 мм;
  + абзацный отступ 15 мм;
  + названия разделов выделять увеличенным размером шрифта (14пт), полужирным шрифтом, без точки в конце;
  + расстояние от заголовка раздела и подраздела до текста и от текста до заголовка должно быть равно 3 интервалам.

# **1 Теоретическая часть**

# 1.1 Значение IT-инфраструктуры в современном мире

ИТ-инфраструктура — это взаимосвязанные компоненты, из которых состоит информационная структура организации. В состав такой инфраструктуры входит техническое оборудование для выхода в интернет, выполнения рабочих задач и комфортной работы в офисе.

По мере распространения интернета и его доступности стали создаваться единые цифровые системы. Они необходимы для бесперебойной работы организации на всех уровнях.

Главная задача ИТ-инфраструктуры — обеспечить стабильную и безопасную работу организации, а значит, она решает множество актуальных вопросов. В первую очередь, важнейшим аспектом является защита информации. Сегодня, когда данные становятся наиболее ценным активом, грамотное управление ими критично важно. Организации разрабатывают системы, которые позволяют защищать конфиденциальную информацию от кибер-атак и утечек.

Еще одна важнейшая задача ИТ-инфраструктуры — это обеспечение отказоустойчивости. Никакой бизнес не может позволить себе длительные простои, и здесь на помощь приходят резервирование и автоматические решения для восстановления. Когда случаются сбои, возможность быстро вернуть работу системы в нормальный режим становится критически важной.

Оптимизация рабочих процессов — это значительное преимущество, которое дает современная ИТ-инфраструктура. Интеграция различных программных решений позволяет работникам получать доступ к нужной информации в любое время, что значительно облегчает выполнение задач. Поработав в такой системе, сотрудники быстро замечают, как снижается время, затрачиваемое на рутинные операции, и как повышается общая продуктивность.

По мере роста бизнеса возникает необходимость в гибкости и способности адаптироваться. ИТ-инфраструктура предоставляет возможность масштабировать ресурсы в зависимости от текущих потребностей. Компании могут увеличивать мощность своих систем, чтобы справляться с пиком загрузки, и, наоборот, снижать её в спокойные времена, что снижает затраты организации.

Кроме того, сегодня все чаще обсуждается такая тема, как мобильность и удаленная работа. ИТ-инфраструктура должна отвечать требованиям этого нового времени, позволяя сотрудникам иметь доступ к данным и приложениям независимо от места их нахождения.

Наконец, ИТ-инфраструктура не стоит на месте. Она требует постоянного обновления и адаптации к новым технологиям. Внедрение облачных сервисов, инструментов для анализа данных и средств, которые помогают обеспечить безопасность и конфиденциальность информации становится необходимостью.

# 1.2 Компоненты и составляющие IT-инфраструктуры

Любая ИТ-инфраструктура — это комплекс взаимосвязанных компонентов, где каждый элемент выполняет строго определенную роли. Без их совместной работы невозможны ни обработка данных, ни коммуникация, ни даже базовое функционирование организации. Условно компоненты делятся на несколько типов:

* + аппаратные;
  + программные;
  + сетевые.

Аппаратные компоненты можно подразделить на несколько подтипов:

* + системы хранения данных — обязательный элемент относительно продвинутых организаций и выше. От обычного сервера с жесткими дисками этот элемент отличается наличием специализированных решений, по типу NAS для файлового доступа или SAN, где данные передаются блоками через iSCSI/Fibre Channel. RAID-массивы в хранении данных являются абсолютным стандартом. Если один диск «умрет», данные не потеряются;
  + автоматизированное рабочее место — это всё, чем пользуются сотрудники: офисные ПК, инженерные станции, принтеры, телефоны. Главное правило — соответствие задачам. Для бухгалтерии хватит слабого ПК с офисным пакетом ПО, для специфических задач с обработкой графики — рабочая станция с GPU невероятной мощности;
  + сервер. В любой организации подобное оборудование можно грубо назвать «моторами» инфраструктуры. Бывают стоечные, блейд-сервера или Tower-сервера (по виду – обычный ПК). Их задача — не выключаться, поэтому всё идет с запасом: блоки питания, диски с горячей заменой и много других функций.

Аппаратные компоненты в инфраструктуре лишь некоторая часть. Поверх них работают программные компоненты, которые выполняют большую часть функций, необходимых организации.

Операционная система — фундамент, который превращает набор плат в компьютере в рабочую среду. Без неё сервера, ПК и смартфоны останутся бесполезными устройствами. ОС управляет ресурсами, распределяет память между программами, выделяет процессорное время, обеспечивает доступ к дискам и сети. Даже встроенные устройства (роутеры, например) имеют свою операционную систему — обычно сильно урезанные дистрибутивы Linux. Ключевая задача любой ОС — быть посредником, то есть принимать команды от программ, преобразовывать их в инструкции для процессора и гарантировать, что сбой одного приложения не сможет помешать остальным.

Системное программное обеспечение — это инструментарий для управления инфраструктурой. Оно не решает бизнес-задачи напрямую, но обеспечивает стабильность и контроль над аппаратными ресурсами. Если брать в пример гипервизоры, то увидим, что позволяют запускать на одном сервере десятки виртуальных машин, изолируя их друг от друга. Утилиты резервного копирования создают копии данных даже во время работы систем. Инструменты мониторинга следят за нагрузкой на процессор, диски и сеть, отправляя предупреждения при критических значениях. Отдельная категория — драйвера. Микропрограммы, которые «объясняют» аппаратной части, как взаимодействовать с ОС. Без них видеокарта не будет выводить изображение. Системное ПО работает в фоне, но его отсутствие парализует инфраструктуру, примерно, как отключение электричества на предприятии.

Прикладное программное обеспечение — это программы, которые непосредственно решают задачи бизнеса или пользователя. Например, офисные пакеты программ (Р7, Мой Офис) позволяет бухгалтеру формировать отчеты, CAD-программы помогают инженеру проектировать детали, а Paint дает возможность дизайнеру редактировать изображения. В корпоративной среде востребованы CRM-системы (Bitrix24, Salesforce) для учета клиентов, ERP-платформы (1С, SAP) для управления финансами и логистикой, ну и конечно, специализированные решения вроде САПР для машиностроения или медицинских информационных систем для больниц. Даже веб-браузер — часть прикладного ПО: без него сотрудник не откроет корпоративный портал. Эти программы зависят от системного ПО и ОС, но именно они создают ценность для бизнеса.

Ограничивается программное обеспечение последним типом – промежуточным ПО. Промежуточное программное обеспечение — это что-то вроде клея, который соединяет приложения друг с другом и с инфраструктурой, но при этом может выступать и в роли прикладного ПО, конкретное определение зависит от контекста эксплуатации. Используется подобное как правило в серверной части инфраструктуры, где имеется какое-то нагромождение сервисов. В качестве примера можно привести СУБД (PostgreSQL, MySQL и прочие), которая хранит данные для интернет-магазина, веб-сервер (Nginx, Apache) принимает запросы от покупателей и может передавать какую-то информацию дальше по системе. Без промежуточного ПО приложения не смогут взаимодействовать.

Программные компоненты обеспечивают логику работы инфраструктуры, но без сети, в большинстве случаев – мало полезны. Сервер не передаст данные в СУБД на другом сервере, сотрудник не отправит отчет коллеге. Сетевые компоненты — это что-то вроде кровеносной системы ИТ-инфраструктуры, которая соединяет устройства, маршрутизирует трафик.

Физический уровень — основа любой сети, по которой движутся данные: кабели, разъемы, сетевые карты и оборудование, преобразующее сигналы в электрические импульсы или световые сигналы. Самый распространенный вариант — Ethernet. Витая пара CAT5E дешевая, проста в монтаже и подходят для офисов, где расстояние между устройствами не превышает 100 метров. Для больших дистанций или высокой скорости используют витую пару с категорией выше или оптоволокно — световые сигналы в таких кабелях почти не затухают, всегда используется в глобальных магистралях.

Канальный уровень обеспечивает передачу данных между устройствами в рамках локальной сети, организуя их в структурированные блоки — кадры. На этом уровне к исходной информации добавляется служебная информация, MAC-адреса отправителя и получателя, контрольные суммы для проверки целостности и управляющие флаги. Без этой структуризации данные не могут быть корректно интерпретированы принимающей стороной.

Основная задача уровня — точная доставка кадров, где эту задачу решает MAC-адресация. Например, при отправке данных с компьютера на принтер коммутатор анализирует MAC-адрес получателя и перенаправляет фрейм только в соответствующий порт. Это исключает избыточную рассылку трафика, характерную для устаревших сетевых концентраторов.

Канальный уровень также отвечает за обнаружение и коррекцию ошибок передачи. Контрольная сумма (CRC), включенная в каждый кадр, выявляет искажения данных из-за помехам или сбоев. При обнаружении ошибки фрейм отклоняется, что инициирует повторную передачу со стороны отправителя.

На канальном уровне реализованы:

* + Ethernet (IEEE 802.3) — стандарт для проводных сетей, использующий MAC-адресацию и фреймы до 1500 байт;
  + Wi-Fi (IEEE 802.11) — беспроводная передача данных с механизмами минимизации помех;
  + VLAN (IEEE 802.1Q) — логическое разделение физической сети на изолированные сегменты (например, для отделов компании);
  + PPPoE — инкапсуляция данных для широкополосных подключений;
  + LLDP — обмен служебной информацией между сетевыми устройствами.

Сетевой уровень обеспечивает передачу данных между устройствами, находящимися в разных сетях, определяя оптимальные маршруты для их доставки. Его ключевая задача — преодолеть ограничения локальной коммуникации, организовав взаимодействие в масштабах глобальных сетей, включая глобальные сети. На этом уровне кадры инкапсулируются в пакеты, содержащие IP-адреса отправителя и получателя и прочую служебную информацию для управления маршрутизации.

Основной функцией уровня является маршрутизация — процесс выбора пути для пакетов через маршрутизаторы. Для этого нужны таблицы маршрутизации, где указаны направления к сетевым сегментам. Например, пакет, отправленный из офиса в Москве в филиал в Берлине, проходит через несколько маршрутизаторов, каждый из которых анализирует IP-адрес назначения и перенаправляет его дальше по оптимальному маршруту.

Сетевой уровень также отвечает за:

* + фрагментацию пакетов — разделение данных на части, если их размер превышает MTU (максимальный размер блока, поддерживаемый канальным уровнем);
  + логическую адресацию — использование IP-адресов (IPv4/IPv6) вместо MAC-адресов, что позволяет работать в гетерогенных сетях (Ethernet, Wi-Fi, спутниковая связь);
  + обработку ошибок — протоколы вроде ICMP отправляют уведомления о проблемах доставки (например, если узел недоступен).

На сетевом уровне работают:

* + IP (Internet Protocol) — основа интернета, обеспечивающая адресацию и маршрутизацию;
  + ICMP (Internet Control Message Protocol) — диагностика и уведомления об ошибках (например, ping);
  + NAT (Network Address Translation) — преобразование приватных IP-адресов в публичные для выхода в интернет;
  + VPN (Virtual Private Network) — создание защищенных туннелей между сетями;
  + OSPF, BGP — протоколы динамической маршрутизации.

# 1.3 Основные принципы проектирования

Проектирование ИТ-инфраструктуры – комплексный процесс, направленный на создание технологической основы для поддержки бизнес-процессов организации. Современные принципы проектирования информационных систем учитывают не только текущие потребности, но и обеспечивают возможность масштабирования и отказоустойчивости.

Современная инфраструктура должна проектироваться с учетом концепции "пирамиды надежности", где каждый уровень (аппаратный, программный, сетевой) обеспечивает резервирование и отказоустойчивость. Рассматривая этот момент чуть подробнее, стоит отметить – полная отказоустойчивость в большинстве случаев требует достаточно больших затрат, ведь сделать резерв всего иногда попросту невозможно, поэтому иногда приходится где-то сэкономить, опираясь на надежность имеющихся аппаратных и программных средств.

Выделяют несколько основных типов, которые выбираются в зависимости от задач и внешних требований организации:

* + традиционная;
  + облачная;
  + гибридная.

Традиционная ИТ-инфраструктура, основанная на локальных дата-центрах и физических серверах, на протяжении десятилетий оставалась преобладающей моделью для большинства предприятий. Несмотря на растущие тенденции к облачным решениям и виртуализации, эта модель по-прежнему сохраняет свою актуальность и востребованность в ряде секторов.

В основе традиционной инфраструктуры лежит концепция полного контроля организации над собственными информационными ресурсами. Выделенные серверные помещения, оснащенные надежными системами электропитания, охлаждения и физической безопасности, выступают фундаментом этой архитектуры. Оборудование приобретается в собственность компании и размещается на ее территории. За счет этого обеспечивается прямое управление аппаратными мощностями и данными. Данный подход обусловлен жесткими требованиями к безопасности информации, которые характерны, например, для сфер государственного управления, финансов, энергетики и прочих отраслей, которые могут содержать в себе объекты КИИ.

При проектировании традиционной инфраструктуры ключевыми аспектами являются:

* + обеспечение избыточности и отказоустойчивости с помощью кластерных решений, резервного оборудования и систем бесперебойного питания;
  + иерархическая структура сетевой инфраструктуры с ядром, распределительными коммутаторами и точками подключения клиентских устройств;
  + интеграция с унаследованными системами и обеспечение совместимости с существующими ИТ-ресурсами.

Классическая сетевая инфраструктура опирается на жесткую иерархию физических компонентов с жестко закрепленными функциями для каждого элемента. Основу формируют проводные соединения, создающие фиксированную топологию с централизованными управляющими узлами. Коммутационные устройства, размещенные в защищенных серверных помещениях, выполняют роль системного каркаса, обеспечивая взаимодействие между серверами, рабочими станциями и периферийными устройствами. Архитектура подразумевает строгое разделение на зоны: внутренние сегменты сети изолированы от внешних подключений физическими барьерами, а межзональный доступ регулируется через централизованные контрольные точки.

В отличие от гибких современных решений, управление трафиком здесь базируется на заранее заданных правилах, жестко прописанных в конфигурациях оборудования. Данные передаются по статическим маршрутам, оптимизированным для стандартных нагрузочных сценариев. Подобная схема гарантирует стабильность работы, однако плохо адаптируется к динамичным изменениям — резким скачкам числа подключений или неравномерному распределению запросов.

Система безопасности реализуется через многоуровневую изоляцию. Внешний периметр контролируется аппаратными фильтрами, блокирующими несанкционированные подключения на уровне сетевых пакетов. Внутренние сегменты дополнительно разделяются по функциональному принципу для ограничения горизонтального перемещения угроз. Серверы баз данных, к примеру, могут располагаться в отдельном физическом контуре с ограниченным доступом для определенных групп пользователей. Централизованная реализация аутентификации упрощает администрирование, одновременно создавая риски единых точек отказа.

Масштабирование инфраструктуры связано с физическим расширением — установкой новых коммутаторов, прокладкой кабельных трасс, настройкой дополнительных портов. Подобные операции усложняют топологию и повышают эксплуатационные расходы. Интеграция новых узлов требует проверки совместимости оборудования, обновления таблиц маршрутизации и тестирования на предмет возникновения узких мест. Подключение облачных сервисов осуществляется через выделенные шлюзы, что увеличивает задержки передачи данных.

Надежность сети обеспечивается дублированием критических элементов: резервных линий связи, избыточных источников питания и зеркальных устройств. Несмотря на резервирование, часть мощностей часто остается невостребованной в штатных режимах, а перенастройка под меняющиеся условия требует остановки работы для физического переподключения компонентов.

Облачная инфраструктура представляет собой современный подход к организации вычислительных ресурсов, где все компоненты – серверы, хранилища и сети, предоставляются как сервис через интернет. В отличие от традиционных локальных решений, она исключает необходимость закупки и обслуживания собственного оборудования, перекладывая эти задачи на облачного провайдера.

Современные облачные системы строятся на принципе абстракции аппаратных ресурсов, преобразуя их в гибкие логические сервисы. Фундаментом этой модели выступает гипервизор — технология, разделяющая вычислительные мощности сервера на изолированные виртуальные среды. Каждая виртуальная машина функционирует независимо, получая выделенные параметры CPU, RAM и хранилища, что устраняет зависимость между ОС и физическим «железом». В отличие от традиционных дата-центров с фиксированным распределением ресурсов, облака позволяют динамически перераспределять мощности: незадействованная память одной ВМ может быть мгновенно передана соседнему экземпляру без прерывания работы сервисов.

Эластичность инфраструктуры усиливается за счет программно-определяемых сетей (SDN). Их ключевая инновация — декомпозиция управления: контроллер верхнего уровня (control plane) централизованно задает правила маршрутизации, тогда как коммутаторы (data plane) выполняют только транспортировку пакетов. Используя открытые протоколы вроде OpenFlow, система адаптирует топологию под текущие задачи — от автоматического создания изолированных сегментов для клиентов до глобальной балансировки нагрузки между дата-центрами. Такой подход не только минимизирует зависимость от вендорного оборудования, но и позволяет мгновенно блокировать кибератаки на уровне всей сети.

Следующий уровень абстракции — виртуализация хранилищ. Технологии распределенных файловых систем (Ceph, GlusterFS) объединяют дисковые массивы серверов в единый пул с автоматическим восстановлением данных. Информация дробится на блоки, которые реплицируются между узлами, а метаданные управляются кластерными службами. При отказе диска система перенаправляет запросы к другим копиям, сохраняя доступность данных.

Сегодня существует два основных варианта построения облачной инфраструктуры:

* + частные облака — выделенные ресурсы для одной организации;
  + публичные облака — общие ресурсы у провайдера.

Частное облако – это модель локальных облачных вычислений, которая предоставляет выделенные ресурсы, включая вычислительную мощность, хранилище и сеть, ограниченному числу пользователей в рамках одной организации. Большинство компаний выбирают частное облако в тех случаях, когда они хотят иметь огромный контроль над своей информацией и быть в безопасности. Это могут быть виртуальные облака, такие как VMware Cloud и OpenStack, а также облачные решения, предоставляемые поставщиками частных платформ.

Публичное облако – тип облака, которое провайдер предоставляет в аренду на время. Используется для созданий пул ресурсов, выделенного под конкретный проект или задачу. Можно создавать несколько виртуальных серверов и управлять ими, однако физического доступа к оборудованию у компании не будет. Оставшиеся ресурсы, достаточные, чтобы выделить железо, будут использоваться уже другими компаниями. То есть, вашими виртуальными соседями будут сервисы других организаций.

Ресурсы в публичном облаке будут использоваться по модели pay-as-you-go — по мере потребления. В случае пиковых нагрузок (акции, распродажи) облако будет расходовать больше ресурсов и плата за них возрастает. Но когда нагрузка вновь стабилизируется, облако продолжит работать на обычных мощностях и плата снизится. Публичные облака выросли из частных облаков провайдеров, которые накопили экспертизу и поняли, что ее можно предлагать в форме продукта. Так же, как и частное облако, публичное представляет собой инфраструктуру по типу IaaS.

Рассматривая российский рынок облачных услуг, самыми крупными провайдерами являются:

- Timeweb;

- VK Cloud;

- Yandex Cloud;

- MTS Web Services;

- Cloud.ru.

Чтобы детальнее понять разницу между этими двумя типами, нужно чуть углубиться в документации различных провайдеров.

Термин «частное облако» был введен, чтобы провести различие между этими внутренними облачными средами и публичными облачными сервисами сторонних производителей. Пользователи как публичных, так и частных облачных сервисов имеют определенные сходства.

И публичные, и частные облака абстрагируют и совместно используют вычислительные ресурсы, такие как аппаратное обеспечение, сети, программное обеспечение, обычные серверы и серверы хранения данных. Пользователи могут выделять и освобождать ресурсы по мере необходимости и управлять конфигурацией инфраструктуры.

Оба типа облачных сред используют схожие базовые технологии. Они используют виртуализацию для абстрагирования базового оборудования и его предоставления через API. Они также обеспечивают автоматическое масштабирование, автоматическую оркестровку, отказоустойчивость и улучшенные системы резервного копирования.

Как публичные, так и частные облака обеспечивают операционную эффективность ИТ-инфраструктуры компании. Компании могут сократить расходы за счет централизованного управления инфраструктурой. Быстрее масштабируются и быстрее выводят на рынок новые продукты. Существующие мощности используются более эффективно, а затраты снижаются.

Опыт малых и средних предприятий показывает, что во многих случаях публичные облака значительно эффективнее частных.

Гибридное облако — смесь публичного и частного. Кратко говоря – берутся две инфраструктуры, связываются через VPN или прямые каналы связи (что не получило сильного распространения) и организация по итогу этих действий получает фиксированные мощности с возможностью расширения.

При таком подходе также важно учесть совместимость API, одинаковые сетевые настройки. Иногда ставят шлюзы для синхронизации — чтобы приложения с обоих сторон видели друг друга как одну систему. Также играет роль финансовая составляющая – локальная инфраструктура все также требует вложений, но в меньшем количестве, но затраты на облачную инфраструктуру заметно сокращаются из-за модели оплаты по факту использования, вплоть до почти нулевых значений, когда нет сильной нагрузки и локальная инфраструктура справляется сама.

Если рассматривать такой подход с точки зрения безопасности, то появляется возможность обрабатывать критичные данные — внутри, а различные функции и сервисы, не требующие специфических условий – перенести в публичное облако. Аудит доступа в таких случаях проводится везде, даже если части облака физически в разных местах.

Как выбирать какой-то определенный тип?

Итоговое сравнение всех моделей приведено в таблице 1.1.

Таблица. 1.1 – Сравнение моделей

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Частная | Публичная | Гибридная |
| Уровень контроля | Высокий | Ограниченный | Высокий |
| Гибкость и масштабируемость | Ограниченная | Высокая | Очень высокая |
| Теоретическая стоимость инфраструктуры | Высокая | Низкая | Высокая |
| Уровень безопасности данных | Высокий | Зависит от поставщика. Потенциально – низкий | Зависит от реализации и поставщика. Потенциально – высокий |
| Возможность соблюдения требований регуляторов | Высокая | Зависит от поставщика. Потенциально – низкая | Зависит от реализации и поставщика. Потенциально – высокая |
| Производительность | Низкая | Количество возможных ресурсов зависит от поставщика. Потенциально – очень высокая | Очень высокая |

Развивая тему облачных моделей, стоит отметить модель управления инфраструктурой под названием IaC (инфраструктура как код). Условно говоря, это подход, с помощью которого инфраструктура управляется через конфигурационные файлы и код. Вместо ручной настройки серверов, виртуальных машин и прочих необходимых сервисов, системный администратор может написать несколько файлов, в которых опишет что, в каком формате и на каких устройствах хочет получить. Почти та же ручная настройка – но фактически не выходя из консоли.

К самым распространенным средствам эксплуатации такого подхода относят:

* + Ansible. При привычном подходе нужно вручную прописывать каждую команду или скрипт и по кругу запускать их на серверах. Когда серверов много, это процесс становится сложным и трудоёмким, а вот уже с помощью Ansible всю настройку можно прописать в одном конфигурационном файле, который программа разошлёт на большое количество машин. Пример файла конфигурации можно увидеть на рисунке №.
  + Terraform. Этот продукт уже не занимается как таковой настройкой инфраструктуры, он ее только разворачивает в определенной среде. Если у организации имеется какое-то облако или несколько серверов, выделенных под виртуализацию – развернуть и настроить все виртуальные машины можно ровно также через несколько файлов.

Есть еще много другого ПО, которое позволяет автоматизировать управление инфраструктурой организации: Puppet, Chef, Vagrant, SaltStack и многие другие. Но как правило, все они используются в связке с первыми двумя средствами, чтобы как можно меньше лезть в сами сервера и минимизировать ручную настройку.

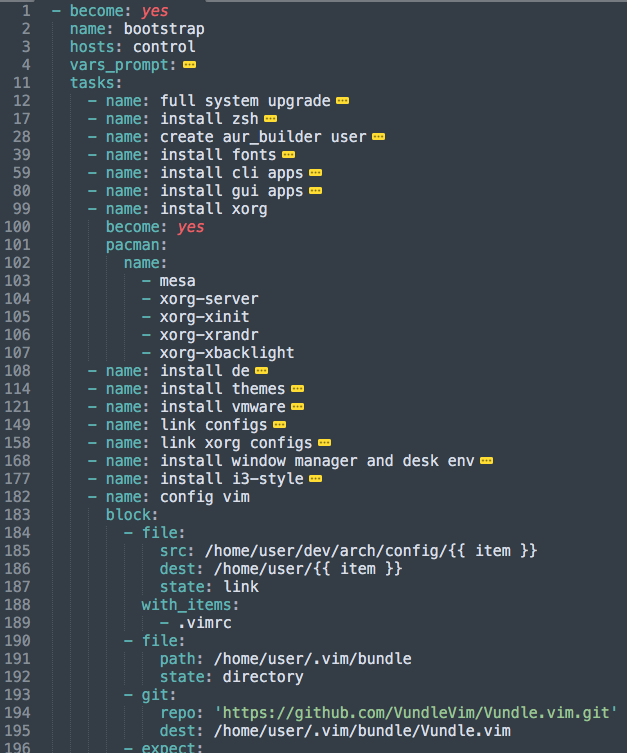


Рисунок № – пример Ansible-плейбука

Самым важным моментом при проектировании инфраструктуры являются сервисы, ПО и задачи, которые они будут выполнять. Эффективность итоговой инфраструктуры в большей части определяется не новизной и новыми технологиями, а наличием отказоустойчивых базовых элементов, которые обеспечивают жизнеспособность всего ПО и иногда аппаратной части инфраструктуры. Ключевая особенность такой архитектуры заключается в способности обеспечивать непрерывность процессов при сохранении гибкости для адаптации к изменяющимся условиям.

К обязательным компонентам любой инфраструктуры в первую очередь относят, конечно, IP-адресацию и организацию сети. Обосновывать такое, в целом, бессмысленно. Без нее ничего в ИТ-инфраструктуре работать никогда не будет.

Организация сети начинается с проектирования её логической структуры. Основой служит разделение на подсети — либо по VLAN, либо через физическую изоляцию. Например, отдельная подсеть для серверов, клиентских устройств и управляющего оборудования. Маршрутизация между ними настраивается на L3-коммутаторах или маршрутизаторах, где прописываются правила доступа (ACL). Для защиты периметра используются межсетевые экраны, блокирующие нежелательный трафик по портам или IP-адресам. Внутри сети часто применяется 802.1X для аутентификации устройств: если компьютер не прошел проверку — доступ в VLAN ограничивается. Отдельное внимание уделяется резервированию: два независимых маршрутизатора с VRRP или HSRP гарантируют, что выход одного из строя не парализует инфраструктуру. Для Wi-Fi сетей аналогично — несколько точек доступа с общим SSID и быстрым роумингом. Всё это требует строгой документации: схемы адресации, таблицы VLAN, политики безопасности. Без этого даже незначительное изменение конфигурации может привести к коллизиям или уязвимостям.

Продолжая тему IP-адресации и организации сети, нельзя упустить DHCP – протокол динамической настройки хостов. Позволяет автоматически присваивать настройки сети хостам, которые отправляют запросы на получение адреса. В основном используются для устройств, которые по большей части принимают трафик, а не получают. Обуславливается это тем, что подобным устройствам в сети нужно чего-то получать, делать что-то и после куда-то опять отсылать данные. Под такую роль подходят именно различные клиентские ПК. Также для связи с каким-то устройством надо знать его IP-адрес (или доменное имя, которое тоже преобразуется в IP-адрес), что при получении адреса через DHCP достаточно затруднительно. Эту проблему могут решать DDNS и статические адреса, выдаваемые по MAC-адресам.

На этом моменте инфраструктура, пускай и откровенно плохая – но будет работать. Хорошим тоном всегда будет настроить систему доменных имен. Задача простая – переводить доменное имя в IP-адрес, чтобы никаких лишних чисел с точками работникам запоминать не приходилось. Есть много других функций, по типу DNSSEC, TXT-записей, которые передают метаданные, но они играют роль обеспечения работоспособности других сервисов, например – почтовых серверов (MX и SPF-записи). Как правило, имена присваиваются только сервисам и серверам, к которым часто приходится обращаться – локальное ПО для конференций, сервисы, взаимодействие с которыми происходит через веб-интерфейс. Для обычных рабочих станций такое обычно не настраивается, они только получают различные записи с DNS-серверов. Но в случае если такое вдруг понадобится – DDNS снова в помощь. Это функция, которая позволяет DHCP серверам при очередной аренде вносить на один или несколько DNS-серверов изменения. Составляются они из имени устройства и обслуживаемой зоны.

Иногда администратору не приходится вручную настраивать DNS – этим занимается контроллер домена. Это как раз тот сервис, который не может работать без доменных имен. Добавляются служебные SRV записи, которые по большей части необходимы для Kerberos-аутентификации. Сам домен строится в большинстве случаев из LDAP (места, где хранятся все объекты домена), DNS и Kerberos. В случае использования AD-совместимого домена, все это разворачивается автоматически. И записи для всех клиентов, и в том числе, что немаловажно – централизованная аутентификация. Существуют и другие реализации: FreeIPA и ее производные (ALD PRO). Эти системы в основном ориентированы на Linux и Unix, но и Windows поддерживают. Также контроллеры домена реализуют общие сетевые папки (netlogon, например), политики доступа к ПК, сетевым папкам и почти всему, что есть в используемом домене. Доменов может быть несколько – корневой, дочерний, несколько дочерних, у которых в свою очередь еще пару дочерних доменов. Задачу аутентификации в таких решают доверительные отношения. Администратор вручную указывает, какие домены могут передавать данные от клиента на другие контроллеры домена.

Вслед за доменом и сетевыми папками приходит проблема износа комплектующих в серверах и в особенности – накопителей. Эту проблему успешно решают RAID-массивы и резервные копии на другие сервера. Проблему, когда из строя выходит сервер с резервными копиями, решают незамысловато - третьим сервером. Продуктов, которые предоставляют функции резервного копирования – несметное множество. От rsync до проприетарного ПО с немыслимым функционалом.

С вышеописанным функционалом работает огромное большинство организаций, будь то облачная инфраструктура или традиционная. Все что выстраивается дополнительно необходимо для обеспечения работы ПО специфичного для определенной отрасли организации или для ускорения каких-то процессов (любое ПО для этого и служит). Но даже резервные копии и RAID не спасут от проблем, которые не видны.

Решения вроде Zabbix или связки Prometheus c Grafana – обязательный минимум для организаций покрупнее. Они следят за нагрузкой на процессор, диски, сеть, предупреждают о критических сбоях или аномалиях. За логами тоже следят – через Elasticsearch или Graylog. Без этого админ узнает о проблеме только когда сотрудники начнут негодовать.

Следующий шаг для оптимизации инфраструктуры – уменьшить количество физических серверов. Не полностью, но большую часть можно заменить виртуальными машинами. Виртуализация дает несколько плюсов: можно быстро масштабировать ресурсы, мигрировать ВМ между хостами, изолировать сервисы. Да и с точки зрения энергопотребления такой подход гораздо выгоднее.

Если уж говорить о виртуализации – нельзя обойти гипервизоры. Proxmox здесь вне конкуренции для небольших и средних инфраструктур. Весь функционал – live-миграция, распределенное хранилище (CEPH), HA-кластеры и прочее идут в составе по умолчанию. Достаточно настроить ноды, прописать общее хранилище – и падение одного хоста останется незамеченным для пользователей. Также имеется встроенная сетевая организация: мосты, VLAN, SDN. Конечно, SDN в Proxmox не может конкурировать с Cisco ACI, но для базовых сценариев функционала хватает. Например, отделить трафик виртуальных машин от управляющего трафика гипервизоров или создать изолированные подсети для тестовых стендов.

Когда инфраструктура начинает достаточно разрастаться, появляются проблемы масштабирования и организации сети. Обычно эти проблемы решаются самыми первыми – еще на этапе создания примерного макета сети, путем выбора одной из распространенных сетевых архитектур.

Стандартная трехуровневая архитектура (также известная как иерархическая модель) — базовая модель для большинства корпоративных сетей. Выделяют уровни ядра, распределения и доступа. Ядро отвечает за маршрутизацию между подсетями, распределение — за агрегацию трафика и применение политик (ACL, QoS), доступ — за подключение конечных устройств. Такая архитектура масштабируется вертикально: добавление новых коммутаторов на уровне доступа не затрагивает ядро. Однако при росте устройств возникают узкие места — например, STP-блокировки или перегрузка L3-интерфейсов. Пример такой архитектуры представлен на рисунке №

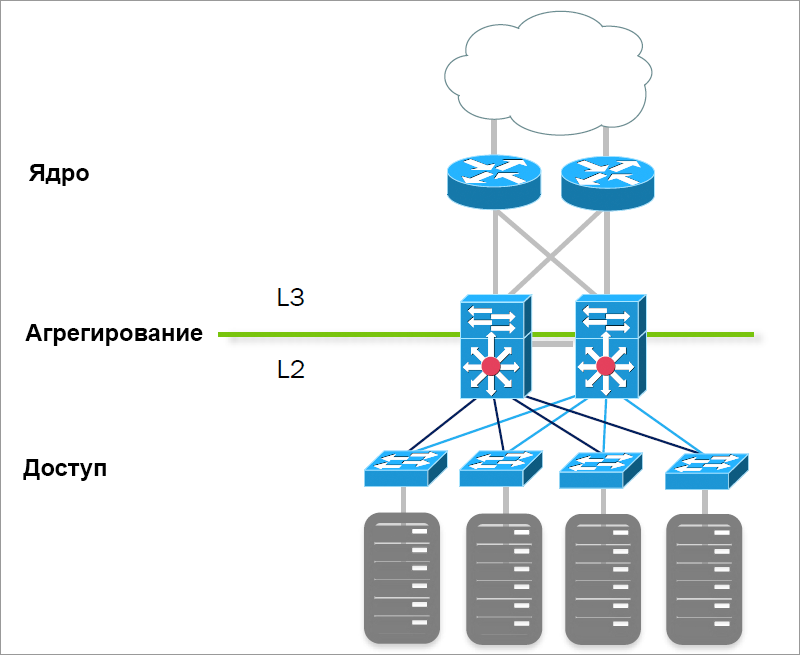


Рисунок № – Иерархическая модель сети

Leaf-spine — архитектура для ЦОД и высоконагруженных сред. Все leaf-коммутаторы (доступ) соединены с каждым spine-коммутатором (ядро), образуя сетку с фиксированной задержкой. Маршрутизация — только L3, что исключает петли и STP. Плюсы: горизонтальное масштабирование, балансировка нагрузки через ECMP, отказоустойчивость (выход из строя spine-узла не влияет на связность). Из мнусов такого подхода выделяют стоимость каждого порта на коммутаторах и невероятную сложность миграции с устаревших сетей. Подходит для кластеров и распределенных СХД. Пример такой архитектуры представлен на рисунке №.

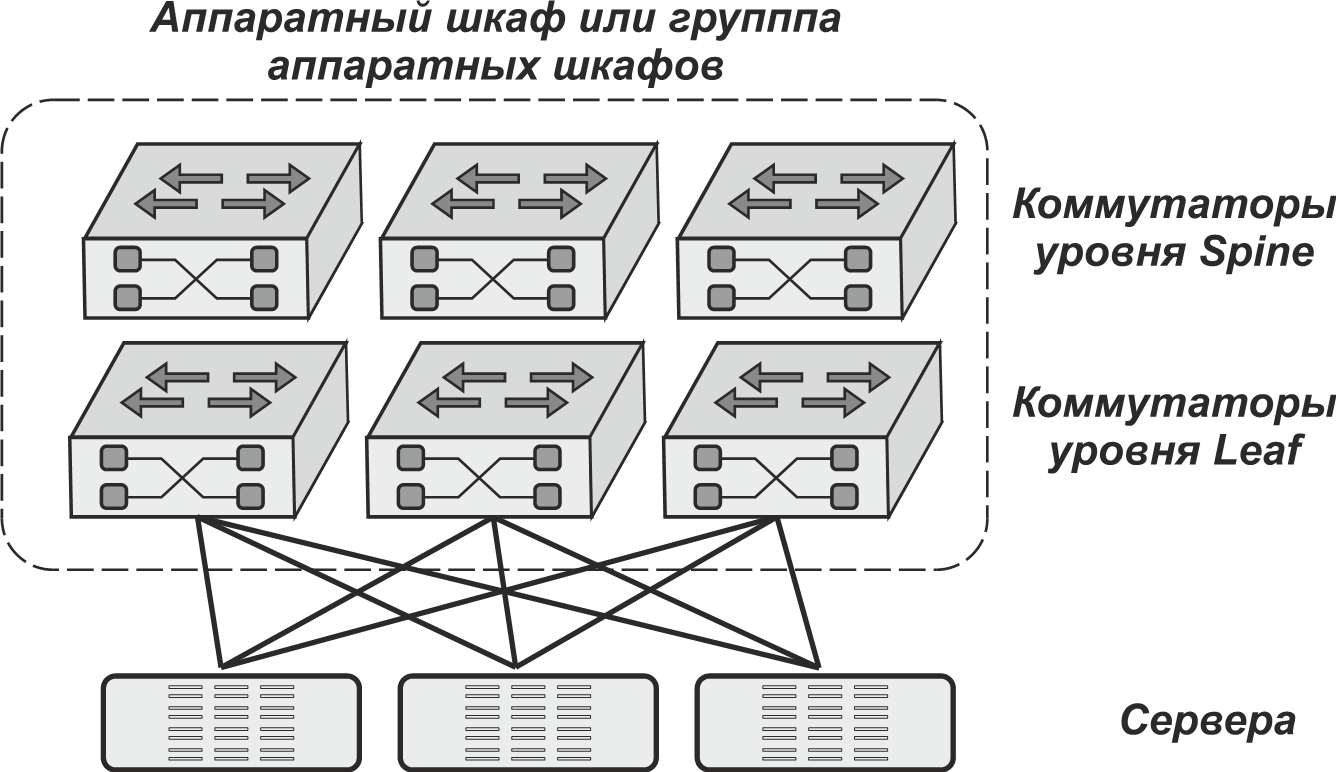


Рисунок № – Архитектура leaf-spine

Гибридные модели — комбинации подходов. Например, трехуровневая архитектура в офисе и leaf-spine в ЦОД. Или spine-уровень на основе VXLAN, что позволяет расширить L2-домены поверх L3-сети. Пример гибридной модели представлен на рисунке №



Рисунок № – Гибридная архитектура

Такие решения часто встречаются в гибридных облаках, где часть инфраструктуры размещена локально, часть — у облачного провайдера.

# 

# 1.4 Безопасность инфраструктуры

Информационная безопасность направлена на обеспечение конфиденциальности, целостности и доступности данных. Безопасность ИТ‑инфраструктуры предполагает комплексную защиту всех её элементов: сетей, серверов, центров обработки данных, рабочих станций и клиентских устройств, где каждый компонент инфраструктуры должен быть изолирован и контролируем, поскольку сбой или компрометация одной части могут вызвать цепную реакцию по всем элементам сети. Ключевыми принципами являются разграничение прав доступа, многоуровневая защита и постоянный мониторинг.

Угрозы безопасности ИТ-инфраструктуры разнообразны и включают в себя как внешние, так и внутренние факторы. Основными источниками угроз являются киберпреступники, стремящиеся нарушить работу систем и похитить данные, а также сотрудники организации, умышленно или по неосторожности использующие свои привилегии во вред компании. В совокупности именно действия персонала являются причиной примерно 66% всех инцидентов безопасности, причём для 14% инцидентов сотрудники становятся «точкой входа» для внешних атак. Среди классических видов угроз выделяются:

* + несанкционированный доступ к конфиденциальной информации (например, через взлом пароля или уязвимость системы);
  + вредоносное ПО (вирусы, шпионские программы, программы-вымогатели);
  + атаки на отказ в обслуживании, фишинг и социальная инженерия;
  + аппаратные и программные сбои (отказы серверов, сбои накопителей, сбои электропитания и т.п.).

Целевые атаки могут быть направлены на нарушение конфиденциальности данных, нарушение их целостности (например, удаление или искажение информации) или доступности ресурсов и служб предприятия. Полноценная защита инфраструктуры требует анализа всех перечисленных типов угроз и своевременного реагирования на инциденты.

Современные системы безопасности инфраструктуры включают круглосуточный мониторинг и анализ событий специалистами по ИБ. К основным техническим средствам защиты ИТ‑инфраструктуры относятся:

* + сегментация сети. Локальная сеть разбивается на изолированные сегменты с ограниченным обменом данными между ними. При таком подходе компрометация одного сегмента слабо затрагивает другие, что существенно снижает риски распространения атаки. Например, отдельные VLAN или подсети для административного, пользовательского и гостевого трафика. Такой многоуровневый доступ не обеспечивает полного разделения ресурсов, но все-таки позволяет внедрить другие инструменты для проверки и разграничения трафика;
  + межсетевые экраны и фильтрация трафика. На границах периметра и между сегментами устанавливаются МЭ, анализирующие пакеты на основе установленных правил. Новое поколение фаерволов (NGFW) может фильтровать трафик на уровне приложений, применять DPI и интегрироваться с IDS или IPS. МЭ ограничивает входящий/исходящий трафик по источнику, назначению, протоколу и содержимому, предотвращая неавторизованные соединения. В сочетании с VPN он защищает удалённый доступ сотрудников к ресурсам организации;
  + антивирусы и EDR. На рабочих местах и серверах устанавливаются антивирусные и EDR-системы, обнаруживающие известные вирусы, сложные вредоносные программы, а также отслеживающие подозрительное поведение;
  + системы обнаружения и предотвращения вторжений (IDS/IPS). IDS/IPS анализируют сетевой трафик в режиме реального времени, выявляя атакующие активности и аномалии. По сравнению с «традиционными» средствами (антивирус, межсетевые экраны), IDS/IPS обеспечивают более высокий уровень защиты сети. Важна комбинированная установка: сети внутреннего периметра, периметра ЦОД, конечных машин, что позволит обнаруживать сложные угрозы, даже если злоумышленник уже прошёл начальный рубеж;
  + шифрование данных. Данные важно защищать как «в покое», так и «в движении». Для передачи информации следует применять защищённые каналы (TLS/SSL или VPN, или все вместе) с современными алгоритмами (в приоритете, конечно, отечественные стандарты и алгоритмы). Хранение конфиденциальных данных должно выполняться в зашифрованном виде. Также все больше распространяется использование сертифицированных криптографических модулей (по типу «КриптоПро») для обеспечения криптографической защиты, даже в организациях без требований к защите такого уровня;
  + системы контроля доступа и аутентификации. Всегда необходимо жёстко ограничивать привилегии пользователей по принципу наименьших прав. Для этого используют централизованные решения для управления идентификацией (например, отечественные IdM/IGA-системы – Solar inRights или аналогичные), которые позволяют реализовать ролевой подход и автоматизировать выдачу и отзыв прав. Обязательны надёжные политики паролей, двухфакторная аутентификация для критичных ресурсов и журналы аудита. Также в совокупности с предыдущими практиками приветствуется регулярный анализ логов (с применением SIEM) для выявления попыток НСД и нарушения политик безопасности.

При проектировании инфраструктуры предпочтительно использовать отечественное или открытое программное обеспечение. Например, ОС Astra Linux SE имеет сертификат соответствия ФСТЭК России (запись №2557 в реестре) и соответствует профильной защите ОС первого класса. Также стоит упомянуть операционную систему Alt Linux СП, которая также имеет встроенные средства защиты информации, сертифицирована ФСТЭК (№ 3866). Вместо проприетарного ПО можно внедрять Zabbix для мониторинга сети и серверов (имеет открытый исходный код), OpenVPN для построения VPN и так далее, вообще все решения во всех сферах имеют отечественные или открытые аналоги.

Говоря об операционных системах, с 2017 введены стандарты, разработанные ФСТЭК, которые касаются операционных систем, предназначенных для функционирования в условиях, где необходима повышенная безопасность обрабатываемых данных. Это означает, что теперь любая ОС, если она претендует на использование в государственных или критически важных системах, должна соответствовать конкретным требованиям, которые описаны в нормативной базе. Собственно, с этого момента в реестре сертифицированных средств защиты информации стали появляться операционные системы, соответствующие этим требованиям. На сегодняшний день в перечне таких продуктов насчитывается 18 ОС, причём 15 из них получили сертификаты по схеме, которая допускает серийное производство и реализацию.

ФСТЭК предложил следующую классификацию операционных систем, разделяя их на три ключевых типа, исходя из характера задач и особенностей среды применения:

* + тип «А» включает в себя так называемые универсальные или, проще говоря, операционные системы общего назначения. Под этим термином скрываются привычные системы, которые используются в рабочих станциях, серверном оборудовании, а также на мобильных устройствах. Их основное назначение — обеспечить гибкое выполнение широкого спектра пользовательских задач;
  + тип «Б» охватывает встраиваемые операционные системы. Эти ОС проектируются не для повседневного взаимодействия пользователя с техникой, а для жёстко регламентированных функций в составе какого-либо оборудования. То есть они «живут» внутри систем видеонаблюдения, промышленных контроллеров, систем управления на транспорте и так далее. Грубо говоря, везде, где от системы требуется стабильность и предсказуемость в условиях ограниченных ресурсов;
  + тип «В», в свою очередь, представляет собой операционные системы реального времени (ОСРВ). Их особенность в том, что они должны гарантированно реагировать на события в строго заданный промежуток времени. Зачастую подобные системы применяются в авиации, оборонной сфере или в робототехнике, где задержка даже в миллисекунду может привести к сбоям или авариям.

Каждая операционная система в рамках требований ФСТЭК получает определённый класс защищённости. Эти классы, которых всего шесть, представляют собой своего рода «рейтинговую шкалу», где шестой класс — это минимально допустимый уровень защиты, а первый — максимальный:

* + 6 класс предназначен для информационных систем, не предполагающих хранения или обработки особо чувствительных данных. Такие ОС могут использоваться в государственных системах 3 или 4 классов защищённости, в АСУ ТП 3 класса, а также в информационных системах персональных данных с необходимостью 3 и 4 уровней защищённости;
  + 5 класс применяется в более ответственных системах, например, во 2 классе защищённости государственных информационных систем, аналогичных по уровню АСУ ТП, и в ИСПДн с 2 уровнем защищённости;
  + 4 класс относится к системам, где обрабатываются особенно важные данные. Это может быть 1 класс защищённости для государственных ИС, автоматизированные системы критических объектов, а также ИСПДн с максимальным, 1 уровнем защищённости;
  + классы 1–3 ужe предполагают работу со сведениями, составляющими государственную тайну. Их применение требует соответствующего допуска и особого порядка работы с такими системами.

Технических средств защиты недостаточно без адекватных организационных мер. Необходимо разработать и внедрить политику информационной безопасности, определяющую правила работы с ресурсами, а именно требования к учётным записям, классификация информации, процедуру инцидент-менеджмента, ответственность сотрудников. Политику необходимо регулярно пересматривать и актуализировать. Важные положения нужно закрепить во внутренних документах (регламентах, инструкциях) и доводить до персонала.

Не менее важна обученность сотрудников. Из статистики, приведенной ранее, нужно вспомнить, что 66% всех инцидентов ИБ вызваны непреднамеренными действиями сотрудников. Это как раз таки подчёркивает, что без осведомленности пользователей в вопросах защиты информации обеспечить ее невозможно. Например, регулярное обучение и повышение осведомлённости о киберугрозах (фишинг, инженерия, безопасная работа в сети) существенно снизит долю ошибок из-за человеческого фактора. В программу обучения включают изучение корпоративных процедур ИБ, правил работы с удалёнными подключениями и средствами обмена информацией. Как правило, процедуры обучения рабочего персонала по темам безопасности информации проводятся регулярно и иногда сопровождаются работами по проверке знаний.

Также хорошей, но весьма трудной практикой является определение прав доступа и ролевой подход. Сотрудникам назначают только необходимые для работы полномочия, исключая одновременное владение конфликтующими правами (также называют SoD – разделение обязанностей). Желательно наличие периодических аудитов учётных записей и ревизия выданных прав. Важной практикой является ведение журналов действий и их анализ. Только таким образом возможно выявить злоупотребление привилегиями и своевременно отреагировать на подозрительные события.

Наряду с организационными и физическими мерами защиты в ИТ-инфраструктуре критически важно соблюдать законодательные требования по защите информации. В РФ действует множество нормативных актов, определяющих права и обязанности участников информационных процессов, способы защиты данных и ответственности за их нарушение, но рассмотрены будут только некоторые основные.

Федеральный закон №152-ФЗ «О персональных данных» - этот закон регулирует сбор, хранение и обработку персональных данных граждан. Под персональными данными понимается любая информация, непосредственно или косвенно относящаяся к конкретному физическому лицу (субъекту персональных данных). Закон вводит понятие оператора – лица (госоргана, компании или ИП), самостоятельно или совместно обрабатывающего персональные данные и определяющего цели такой обработки. Оператор обязан обрабатывать ПД только законным образом, в частности – на основании явного согласия субъекта или других установленных законом оснований

Перед сбором данных оператор должен информировать субъектов персональных данных о целях и условиях обработки, указывать своё наименование и адрес, перечень собираемых данных и права субъекта (например, право отозвать согласие). При необходимости получения согласия оператор обязан разъяснить гражданину последствия отказа. Если же персональные данные получены не от самого субъекта, оператор до начала обработки должен уведомить его обо всех указанных сведениях. Таким образом обеспечивается принцип прозрачности и информированности.

Закон закрепляет строгие требования к защите персональных данных. Оператор при обработке обязан принимать необходимые правовые, организационные и технические меры для защиты ПД от несанкционированного доступа, утраты, уничтожения и иных неправомерных действий. В частности, требуется выявлять угрозы безопасности в информационных системах, применять сертифицированные средства защиты, оценивать эффективность мер до ввода системы в эксплуатацию и контролировать любые инциденты. Оператор также обязан обеспечить быстрое восстановление данных в случае нарушения их целостности. Если обработка персональных данных ведётся в рамках государственных функций или оказания услуг (например, базы клиентов или работников), Базы данных должны располагаться на территории России, а передача данных за рубеж допускается лишь при соблюдении особых условий и защиты.

Его влияние на ИТ-инфраструктуру особенно заметно в части локальных систем хранения и обработки данных. Закон требует, чтобы информационные системы, обрабатывающие персональные данные граждан РФ, находились на территории Российской Федерации, что ограничивает использование зарубежных серверов, хостинга и средств телекоммуникации. Это делает обязательным развёртывание собственных серверов или аренду сертифицированных дата-центров внутри страны. Дополнительно необходимо реализовать физическую и программную изоляцию сегментов сети, где производится обработка ПДн, от других элементов ИТ-инфраструктуры.

Закон также влечёт за собой необходимость закупки и внедрения сертифицированного ПО и технических средств защиты информации, соответствующих требованиям ФСТЭК и ФСБ. Это касается, например, межсетевых экранов, средств шифрования, антивирусной защиты, журналирования и резервного копирования. Всё это увеличивает общую стоимость сопровождения локальной ИТ-инфраструктуры и потребует отдельного учета при проектировании систем.

Федеральный закон №149-ФЗ «Об информации, информационных технологиях и о защите информации» – этот закон устанавливает общие принципы правового регулирования информационных отношений. Под информацией он понимает любые сведения (данные, сообщения) независимо от формы представления. Информационные технологии – это процессы поиска, сбора, хранения, обработки и передачи информацииconsultant.ru. Закон определяет понятие информационной системы как совокупность информации в базах данных и средств её обработки (программные и технические). Оператор информационной системы – это обычно её владелец или организация, эксплуатирующая оборудование и базы данных.

Закон вводит понятие конфиденциальности информации – обязательство лица, получившего доступ к данным, не передавать их третьим лицам без разрешения владельца. Он различает общедоступную и ограниченную информацию, устанавливает порядок ограничения доступа и обеспечения открытости там, где это необходимо (например, экологические сведения должны быть доступными). Также закон диктует основные требования к защите информации. Защита понимается как комплекс правовых, организационных и технических мер, направленных на:

* + предотвращение несанкционированного доступа, искажения или уничтожения данных;
  + соблюдение конфиденциальности ограниченной информации;
  + реализацию права на доступ к сведениям.

Этот закон прямо требует, чтобы базы данных, содержащие персональные данные граждан РФ, находились на территории страны. Приказы ФСТЭК России (в частности, №17, №21, №235, №239, №76) конкретизируют эти общие требования, устанавливая правила классификации информации, порядок организации защиты локальных ИТ систем, процедур аудита и санкции за несоблюдение.

Если рассматривать его роль в рамках только проектирования инфраструктуры, то он влияет на архитектуру и эксплуатацию, так как требует обеспечения целостности, конфиденциальности и доступности информации в любых ИС. В локальных ИС это требует детальной проработки механизмов разграничения прав доступа, шифрования данных, устойчивости к отказам оборудования и обеспечения физической безопасности серверов.

Также закон ограничивает использование неконтролируемого программного обеспечения. В рамках исполнения требований закона в государственных и корпоративных инфраструктурах запрещается использование несертифицированного ПО, что требует полной инвентаризации установленного программного обеспечения и соответствия требованиям ФСТЭК.

Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры РФ» – посвящён защите объектов критической информационной инфраструктуры (КИИ), то есть ИТ систем и сетей, имеющих особое значение для устойчивости общества и государства. Под КИИ понимаются совокупности объектов, информационных систем и сетей электросвязи, обеспечивающие функционирование жизненно важных сфер (энергетика, транспорт, связь, финансы, оборона). КИИ делится на значимые объекты – те, что имеют присвоенную категорию значимости и включены в реестр значимых объектов КИИ РФ.

Закон устанавливает категорирование объектов КИИ: каждому объекту присваивается одна из трёх категорий (первая, вторая, третья) по степени его критичности. Критерии значимости включают оценки потенциального ущерба здоровью людей, функционированию инфраструктуры, экономике, обороне и прочим важным факторам. Ответственность за проведение категорирования несут субъекты КИИ – государственные органы и организации, владеющие или эксплуатирующие такие объекты.

Субъекты КИИ обязаны соблюдать особые правила безопасности и информировать государство о происшествиях. В частности, они незамедлительно уведомляют уполномоченный федеральный орган о любых компьютерных инцидентах. Для значимых объектов вводятся ещё более жёсткие требования: необходимо выполнять предписания по безопасности, проводить регулярный аудит, обеспечивать восстановление работоспособности в случае инцидентов и допускать проверяющих на объекты в любой момент. В совокупности с остальными приведенными законами влияние на инфраструктуру остается аналогичным.

# 1.5 Требования для построения инфраструктуры

Главным специалистом отдела аналитики и архитектуры государственной единой облачной платформы и государственной информационной системы мне были предоставлены требования, которые необходимо учесть при проектировании и разработке макета.

# 1.6 Выбор лабораторной среды для создания макета

Для создания и тестирования сетевых макетов в рамках проекта необходима лабораторная среда, обеспечивающая реалистичную эмуляцию или симуляцию сетевой инфраструктуры. Выбор подходящей платформы зависит от множества факторов, включая функциональные возможности, требования к ресурсам, совместимость с реальными устройствами, уровень сложности настройки и поддержки, наличие встроенных инструментов для анализа сетевого трафика и диагностики. Основные инструменты, примерно подходящие под требования описаны в этом разделе.

Cisco Packet Tracer — Это симулятор, разработанный Cisco для обучения базовым сетевым концепциям. Он имитирует поведение устройств Cisco (роутеры, коммутаторы) через упрощенные алгоритмы. Внутренняя архитектура основана на визуальном моделировании логических и физических слоев сети, включая автоматическую генерацию кабелей и упрощенную эмуляцию протоколов (RIP, OSPF, DHCP и прочие протоколы). Каждое устройство — программная модель с ограниченным набором команд, которые не включают полный функционал аналогичного физического устройства.

Из явных плюсов выделяются:

* + относительная простота использования;
  + поддержка лабораторных работ внутри интерфейса;
  + не требователен к ресурсам;

Минусов слегка больше:

* + изолированность в экосистеме Cisco;
  + отсутствие возможности взаимодействия со сторонними программами;
  + ограничения на количество узлов в одном проекте;
  + не бесплатен;
  + только достаточно устаревшие модели оборудования;

Переходя к следующим симуляторам, можно упомянуть малоизвестный Mininet. Это эмулятор сетей, использующий встроенные средства Linux и OpenFlow для создания виртуальных устройств. На всех устройствах в рамках проекта можно полноценно пользоваться утилитами из ядра.

С основной задачей в построении сети этот инструмент справится, но с нюансами. Для сетевых устройств используются OpenFlow-контроллеры, что встречается только в SDN и особой популярностью не пользуются и получается, что и пользы в реализации данного проекта – не несет.

Следующий инструмент имеет подобный функционал и гораздо большее применение. ContainerLab – инструмент, который также используется для создания и тестирования сетей. Топология строится не в графическом интерфейсе, а описывается в yml файле, почти идентичному файлу docker-compose, а после управляется через терминал.

Инструмент воссоздает нужную сетевую инфраструктуру используя docker-контейнеры и стандартные средства по типу виртуальных пар интерфейсов и мостов в Linux. Так как в docker’е можно запустить практически все что угодно, за исключением специфических устройств, то и в этом инструменте их тоже можно использовать. В поддержке имеются все самые используемые linux-дистрибутивы, также есть возможность запуска сетевого оборудования Cisco, Huawei (сильно урезанные подобия VRP), MikroTik, Arista и многих других. Пример использования представлен на рисунке 1.1



Рисунок № – пример использования ContainerLab

Из интересных моментов также выделяется возможность запуска Windows, но только сильно странных редакций для интернета вещей. Ресурсов оно расходует очень мало, так как не требуется полная виртуализация устройств, они работают просто как отдельный процесс в системе. В рамках проекта следующий пункт роли не играет, но также имеется возможность интеграции в процесс автоматического развертывания при разработке какого-либо продукта в команде.

Подводя итог, инструмент имеет потенциал, в виде:

* + быстрого развертывания проекта;
  + отличной интеграции с облачными технологиями;
  + ресурсоемкости;
  + большой поддержки числа производителей.

Минусов слегка больше:

* + непрактичное управление;
  + сложность управления и построения больших сетей;
  + малая функциональность в сравнении с другими продуктами.

Следующий эмулятор – EVE-NG. Представляет из себя набор инструментов для работы с виртуальными устройствами, построением сетей, коммутацией с реальным оборудованием. Возможности данного продукта позволяют легко использовать, управлять, коммутировать моделируемое сетевое оборудование. Имеет две редакции – бесплатную, с ограничениями в виде 64 узлов в проекте (что в целом и немало) и платную – без ограничений, с поддержкой контейнеров в одном проекте с виртуальными машинами. В отличии от прошлых инструментов – используется полная виртуализация используемых устройств, что позволяет производителям в образах устройств вместить все функции, которые используются в реальном оборудовании. Пример топологии представлен на рисунке №.

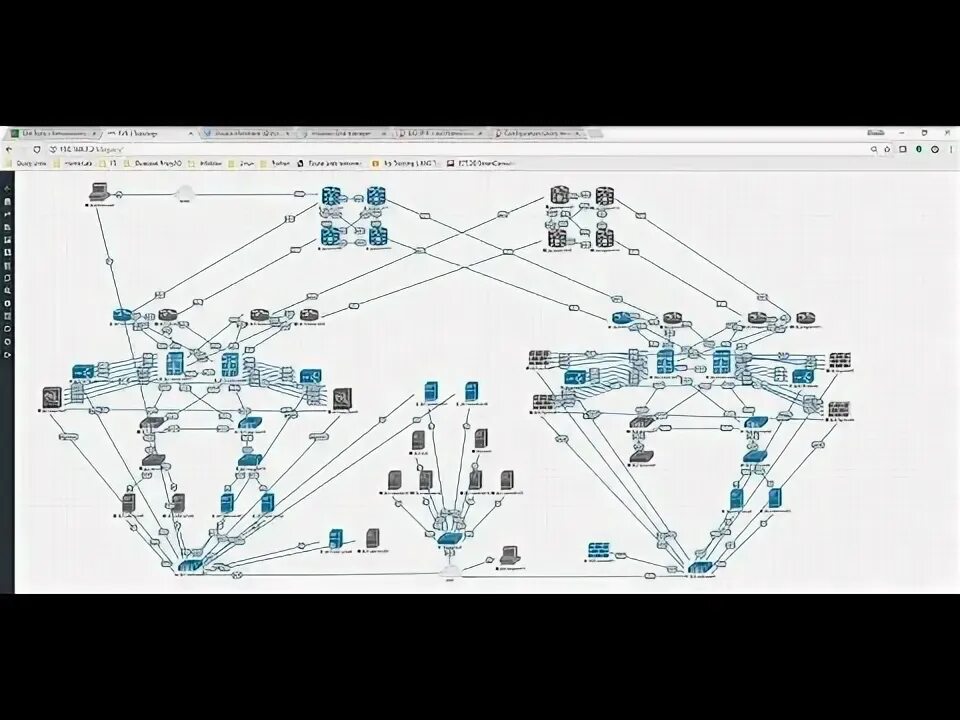


Рисунок № – пример топологии в EVE-NG

Продукт сильно серьезный, так как до определенного момента использовался в исследованиях ФСТЭК в рамках исследований и тестирований уязвимостей. Имеет поддержку вообще всех производителей, которые представляют программные образы своих устройств, используется через веб-интерфейс, а управляется – через терминал. Также позволяет прослушивать весь трафик на абсолютно всех соединениях, которые имеются в проекте, через WireShark. Интересный нюанс - при должном понимании работы EVE-NG можно прекрасно интегрировать проект с физической инфраструктурой, даже в случае, когда просто требуется проверить совместимость. Развертывается данный инструмент может в качестве виртуальной машины или сразу на физическое оборудование и поставляется в виде установщика, по типу обычной ОС.

Последний инструмент, и по мнению сотен тысяч людей – самый перспективный из всех вышеописанных – GNS3. Если дословно – графический симулятор сети, но говоря правильно – эмулятор. Инструмент абсолютно бесплатен, не имеет ограничений в сравнении с прошлым инструментом. Так как проект открытый, то и технической поддержки не предоставляется, что заставляет различные организации посмотреть в сторону EVE-NG.

Развертываться он может в качестве виртуальной машины и также в качестве хостовой ОС, но первое, что его отличает от остальных инструментов – это возможность запуска еще и на любой ОС, без необходимости развертывания виртуальной машины. Имеет полную поддержку всех функций остальных инструментов. Также выделяется возможность запуска машин в проекте на разных серверах, чем не может порадовать EVE-NG. Получается что-то вроде объединения мощностей серверов как в облачной инфраструктуре, но только для запуска ВМ в рамках проекта. Среди всех этих преимуществ есть и минус – для построения топологий больше, чем пара устройств, потребуется неплохое количество ресурсов.

GNS3 имеет веб-интерфейс, представленный на рисунке №, но достаточно скудный.

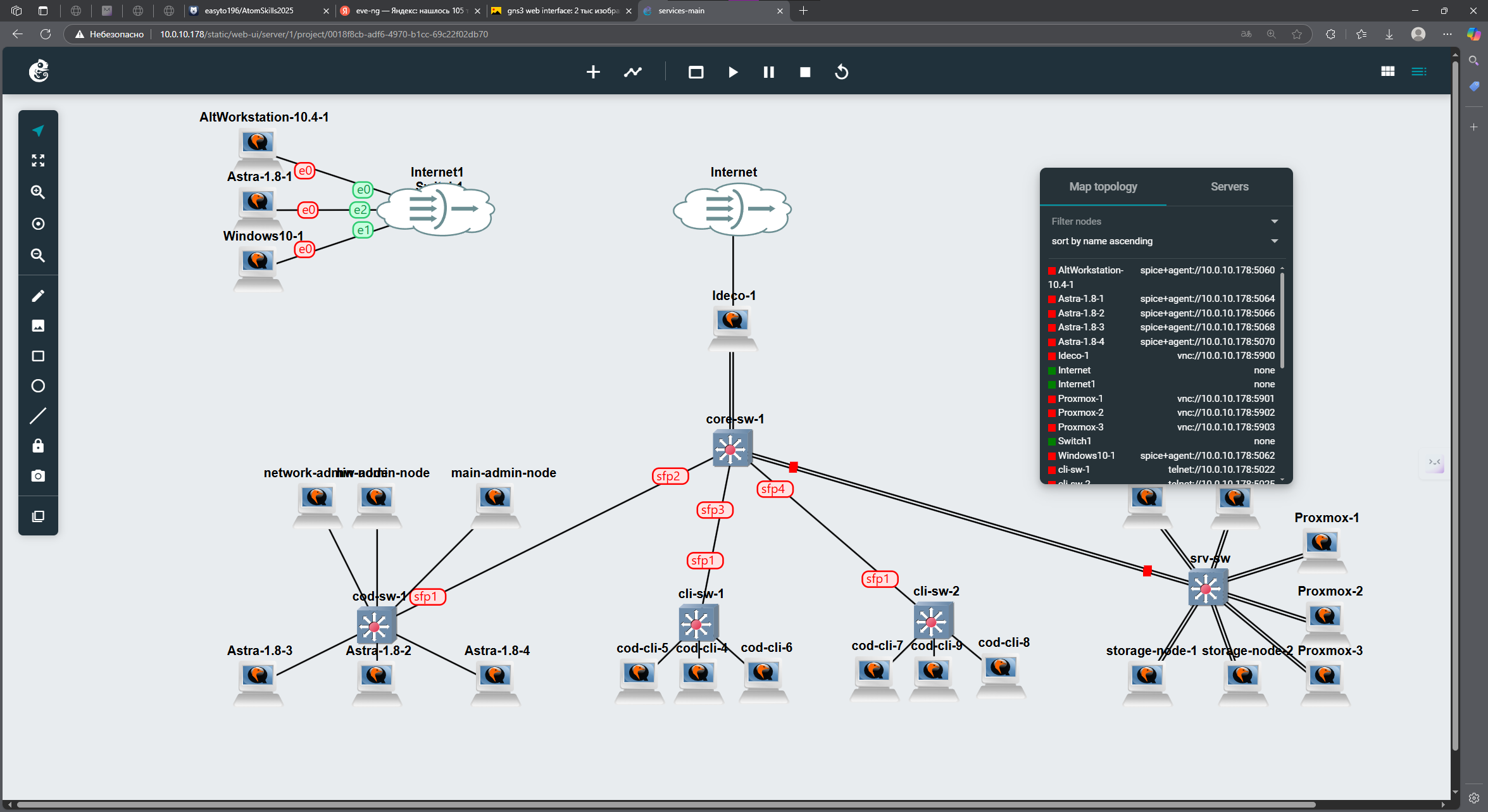


Рисунок № – внешний вид веб-интерфейса

Лучшим вариантом использования является клиент, который включает в себя сразу и сервер. Внешний вид клиента представлен на рисунке №. В одном проекте возможна совместная работа сразу нескольких людей, все изменения в проекте отображаются с минимальной задержкой.

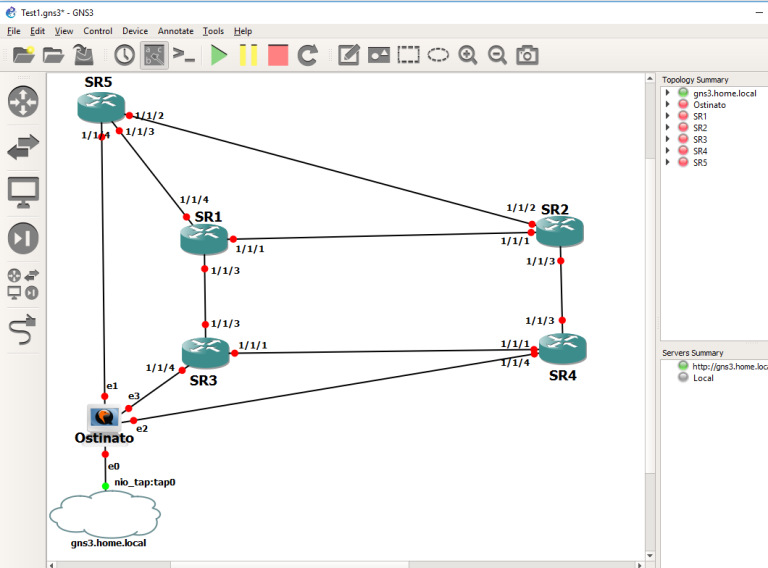


Рисунок № – внешний вид клиента GNS3

Подводя итог – GNS3 показал существенные преимущества, что и делает его фаворитом во многих сферах. Каждый инструмент имеет свои уникальные особенности, подходящие для разных целей и условий работы. Однако, исходя из потребностей, предъявляемых к будущему проекту и характеристик рассматриваемых инструментов, можно сделать вывод, что GNS3 является наиболее подходящей платформой для создания сложных и детализированных сетевых топологий. Большое количество функциональных возможностей, поддержка полноценных ОС и возможность настройки делают его идеальной лабораторной средой.

# **2 Практическая часть**

# 2.1 Определение ПО, сервисов и производителей, подходящих под требования

Компьютеры в АРМ пользователей в этом проекте выбираются заказчиком, исходя из требований к специализированным решениям, которое не были рассмотрены в ТЗ. Выбор итогового сетевого оборудования рассматривается далее, но на стороне заказчика также остается возможность замены, с единственным требованием к поддержке технологий, которые реализуются в данном проекте. Но перед выбором сетевого оборудования стоит точнее определить сетевую архитектуру и требования к функциональности устройств.

За основу проектируемой сети будет взята архитектура Collapsed Core, несколько измененная стандартная иерархическая модель. Данное решение обусловлено следующими ключевыми факторами, делающими стандартную трехуровневую модель неоптимальной для данного проекта:

* прогнозируемый масштаб сети и объем межсегментного трафика не достигают значений, требующих выделения специализированного, высокопроизводительного и дорогостоящего уровня ядра. Использование отдельного уровня ядра при текущих требованиях привело бы к значительным неоправданным капитальным затратам на оборудование с избыточной мощностью и усложнению физической инфраструктуры;
* Collapsed Core обеспечивает существенное снижение совокупной стоимости владения – исключается закупка дорогих коммутаторов ядра, уменьшается количество необходимых устройств, оптимизируется СКС и энергопотребление, упрощается лицензирование;
* архитектура централизует критически важные функции маршрутизации между VLAN, ACL, QoS и фильтрации трафика на меньшем количестве устройств уровня распределения (функционально совмещающего роль ядра). Это значительно упрощает конфигурирование, мониторинг, администрирование сети и повышает предсказуемость ее работы.
* современные управляемые L3 коммутаторы уровня агрегации обладают достаточной производительностью на L2 и L3, портовой плотностью (включая uplink-порты по 10G), а также поддержкой необходимых технологий (маршрутизация, QoS, резервирование протоколами типа STP/RSTP/MSTP, Stacking) для эффективного выполнения функций объединенного уровня Distribution/Core в рамках заданных требований проекта.

В итоге Collapsed Core является практически единственной допустимой архитектурой для данного проекта, обеспечивающей соответствие требованиям при оптимальных затратах и управляемости, и уже на ее основе будет производится выбор оборудования и настройка.

В качестве коммутаторов на уровень доступа в первую очередь нужно рассмотреть решения от Eltex - MES1124M (очень бюджетный вариант) и MES2324. Сравнительная таблица коммутаторов представлена в таблице №.

Таблица. 1.1 – Сравнительная таблица коммутаторов

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование характеристики | MES1124M | MES2324 | Единица измерения |
| Производитель | Eltex | | |
| Общая пропускная способность коммутатора | 12,8 | 128 | Гбит/сек |
| Количество портов 1G (RJ-45) | 0 | 24 | Шт |
| Количество портов 100M (RJ-45) | 24 | 0 | Шт |
| Количество портов 1G (SFP) | 4 | 0 | Шт |
| Количество портов 10G (SFP) | 0 | 4 | Шт |
| Объем ОЗУ | 128 | 512 | МБ |
| Поддержка L3-функций | Нет | Есть | - |
| Исполнение | 19”, 1U | | |

Внешний вид коммутаторов представлен на рисунках №.

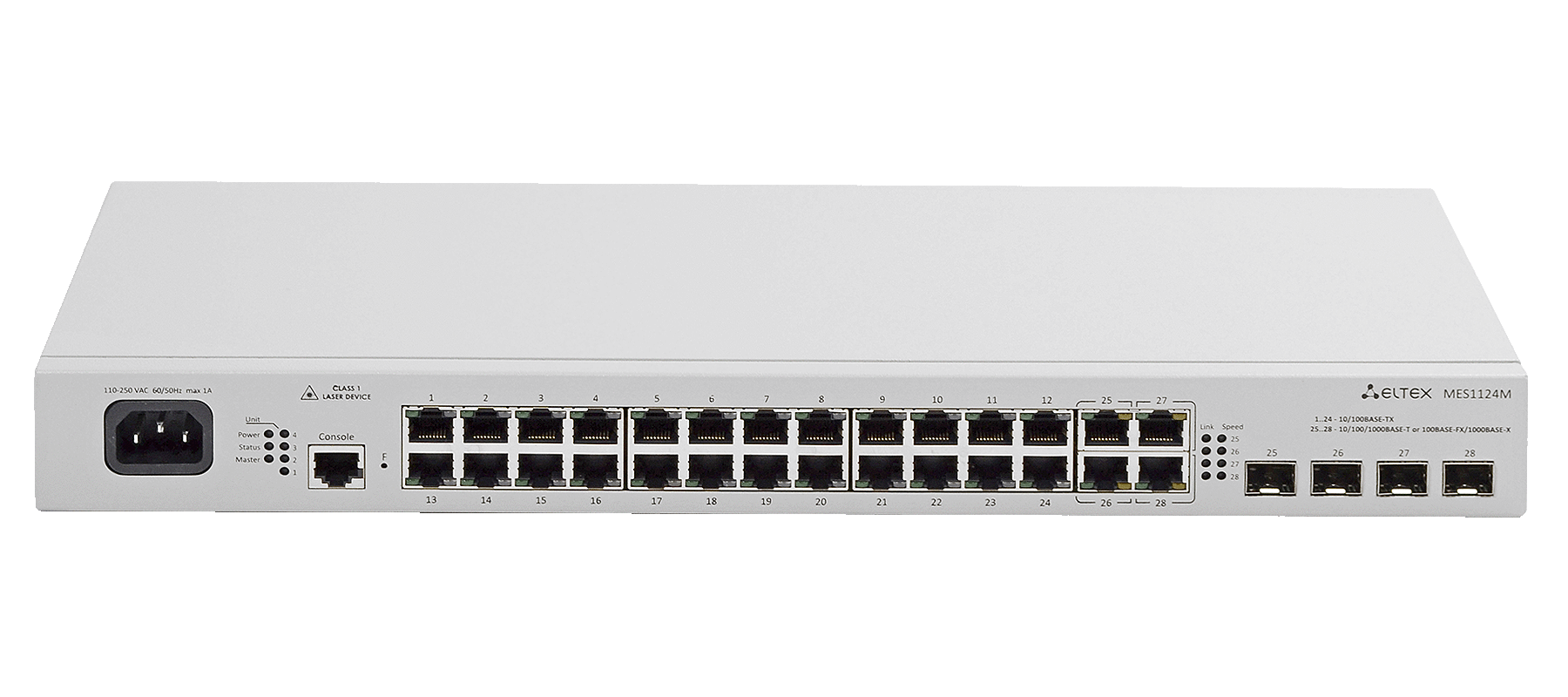


Рисунок № – Коммутатор MES1124M

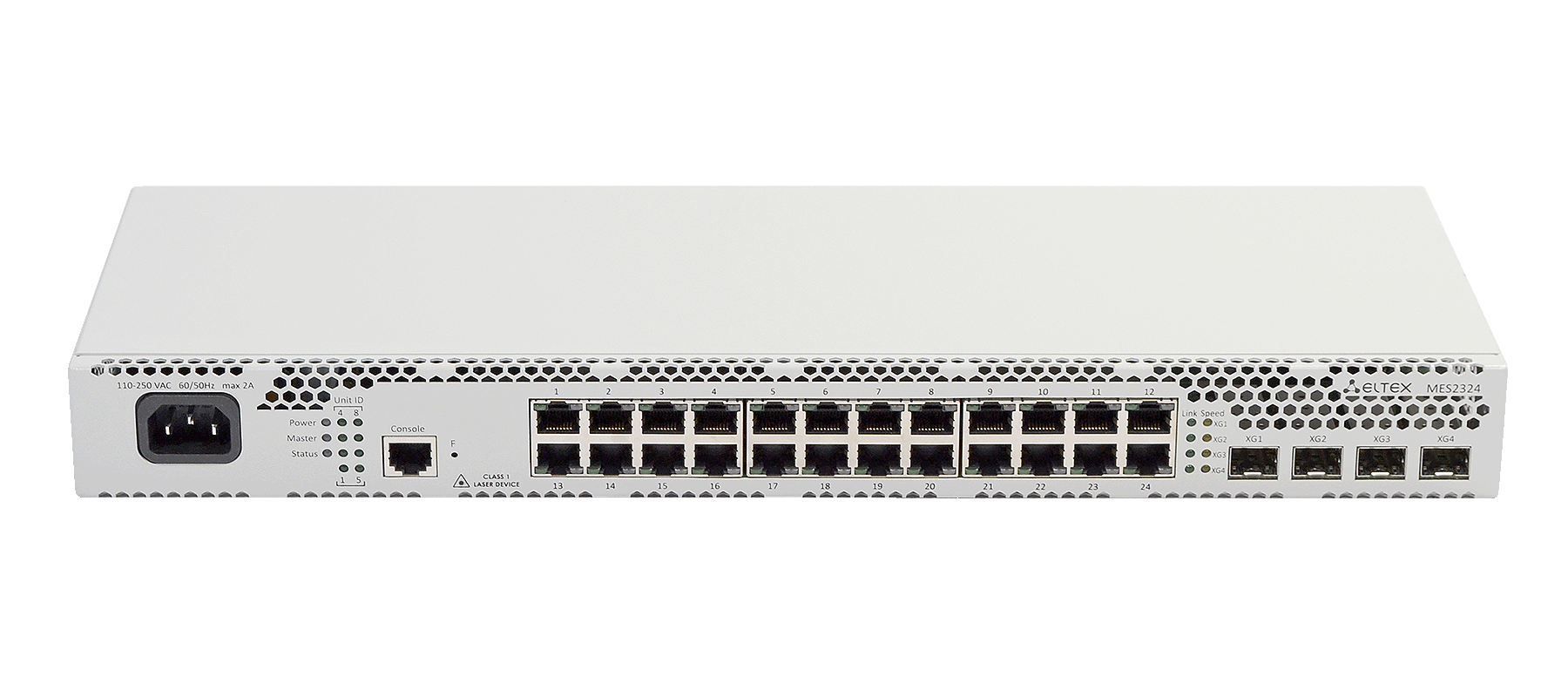


Рисунок № – Коммутатор MES2324

Так как четких данных о планируемых нагрузках представлено не было, в макете на уровне доступа будет использоваться виртуальная версия коммутатора MES1124M, без поддержки L3 функционала.

В случае изменения архитектуры с объединенным уровнем агрегации и ядра на полноценную трехуровневую модель – на уровень ядра подходит MES5324, для агрегации - MES2324F. Основное требование к уровню ядра – скорость маршрутизации и поддержка протоколов динамической маршрутизации.

Рассматривая модель с Collapsed Core дальше – ввиду того, что трафик в сети по большей части будет направлен только к остальным офисам организации или в Интернет, то решения с uplink-портами по 10 Гбит/сек и более (которые больше подходят к центрам обработки данных, например - MES5324) будут чересчур избыточными. Лучшим вариантом будет переносить не уровень агрегации в ядро, а ядро в агрегацию, что позволит сэкономить большое количество бюджета и избежать простоя мощностей оборудования. Поэтому в качестве устройств на Collapsed Core уровне будет использоваться виртуальный образ, похожий на MES2324F.

Говоря о безопасности трафика, нужно отметить, что в мире МСЭ появилось много различных решений. Основные, которые стоит внести в рассмотрение:

* Ideco NGFW;
* UserGate;
* Континент 4;
* xFirewall.

Из предложенного списка стоит сразу отмести Континент, так как действительно серьезных законодательных требований и требований к безопасности представлено не было, что и делает это решение сильно избыточным. Также это решение очень специфично в настройке, чем стоит заниматься квалифицированным специалистам, имеющим опыт в работе с таким оборудованием.

UserGate – самый многофункциональный NGFW из всех представленных. Данное решение закрывает практически все потребности, которые может закрывать МСЭ. Также существует реализация для ЦОД – UserGate DCFW. За огромный функционал придется платить стабильностью и очень квалифицированными специалистами, которые будут заниматься в организации только администрированием UserGate.

Ideco – МСЭ, особо не выделяющийся из множества остальных. Для организаций плюсом будет то, что продукт до невероятного прост в настройке, с этим справится абсолютно каждый человек с небольшой базой теории. Также отличается огромной стабильностью, но за эти плюсы придется пожертвовать функциональностью. Предоставляется возможность контроля трафика на уровнях до L7, но не так гибко, как в остальных продуктах. Имеет только базовые возможности от маршрутизаторов – например, нет того же VRRP и его иных реализаций.

xFirewall является также очень специфичным продуктом, даже больше, чем Континент. Ключевым моментом является то, что продукт направлен в первую очередь на внедрение в сети с VipNet. Обуславливается это тем, что для администрирования xFirewall нужен Coordinator, который тоже сам по себе является МСЭ, но без IPS, но с функциями криптографии, которых лишен xFirewall.

Исходя из сравнения, выбор в данном проекте стоит отдать Ideco NGFW. Решение закрывает необходимый функционал по фильтрации и защите трафика, но отсутствие функциональности не влияет в данном проекте.

Подводя итог проектирования, необходимо подытожить планируемые технологии и протоколы, их местоположение в инфраструктуре.

На границе сети существует вариант сделать или один МСЭ, или кластер из двух МСЭ. Для экономии бюджета, с предположительными нагрузками сможет справится и один NGFW. При росте нагрузки и трафика самым простым решением будет добавить еще один межсетвой экран и настроить балансировку. Решение достаточно простое и лаконичное, потому что никаких изменений в основу сети вносить не придется, не будет даже простоя.

Далее – сердце сети. Использоваться будет именно Collapsed Core, так что на уровне ядра изначально можно оставить два коммутатора. Так как сеть не высоконагруженная, а также не планируется рост числа пользователей, на двух коммутаторах останется запас и по ресурсам, и по общей пропускной способности. Масштабируется такое решение будет аналогично – необходимо добавить еще один коммутатор, добавить все интерфейсы в VRRP группу и настроить анонс маршрутов. С подключениями все немного сложнее – каждый коммутатор доступа должен иметь минимум два подключения к вышестоящим, но при добавлении третьего это решение не играет особой роли. В таком случае будет необходимо проводить подключения не ко всем коммутаторам доступа, а только к новым, которые добавляются при расширении количества пользователей.

На уровне доступа все немного проще. Так как не указано точное число пользователей, будет настроено лишь небольшое количество, для грубой демонстрации работоспособности решения.

Итого, при увеличении количества пользователей, лучшим вариантом будет возвращаться к полноценной трехуровневой модели или делать дополнительные каналы в агрегации и добавлять устройств на уровень доступа и ядра. При первом варианте огромной проблемой станет потребность в полной переработке сети, что приведет и к большим затратам, и к долгому простою сети. При втором варианте исчезает вероятность простоя сети, но возникают другие проблемы:

* капитальные затраты на новое оборудование;
* большое количество роста подключений.

На плакате 1 представлена итоговая сетевая архитектура. Все подключения к ядру дублированы, чтобы соблюсти особенности изначальной сетевой модели. Для максимальной экономии, чтобы избежать единой точки отказа был добавлен второй канал от провайдера, но без дублирования (как правило, очень дорогих) МСЭ, который заходит напрямую в ядро. Такое решение можно было бы назвать большим ударом по безопасности, но суть при таких размытых требованиях к безопасности все же остается в максимальной отказоустойчивости за наименьшие деньги.

Каналы от серверной части в макете планируются в виде LAG, но при использовании платформ с uplink-портами более чем в 1 Гбит/сек такое решение можно назвать избыточным. Планируется туннель до основного офиса, куда будут анонсироваться локальные сети отдела. Также динамическая маршрутизация не будет мешать между уровнем ядра и NGFW (в таком случае при масштабировании и ядра, и МСЭ на границе сети потребуется минимальное количество времени), даже при условии, что количество сетей слишком маленькое.

Вся локальная сеть сегментирована на:

* VLAN 201 – клиентский сегмент (если рассматривать его уже реализованным в физической инфраструктуре, то этот сегмент придется дробить для функционального разделения всех работников и их прав);
* VLAN 100 – сегмент администраторов (при рассмотрении макета в физическом виде, сюда будут относиться также устройства для СКУД и прочие сетевые решения, используемые для администрирования);
* VLAN 101 – общий серверный сегмент;
* VLAN 102 – сегмент для OOB-интерфейсов, управления сетевым оборудованием.

Количество серверов в макете можно назвать минимально необходимым, особенно для основных задач отдела. Решения ALD PRO вынесены на отдельные физические машины для обеспечения точной и полной работоспособности и изолированности от остальных сервисов организации. Для хранения используется две машины для обеспечения полной отказоустойчивости хранения данных.

Между машинами добавлено отдельное подключение, которое никак не функционирует и не задевается в основной сети. Как правило, сервера, СХД поставляются с дополнительными сетевыми картами (2.5 или 10 Гбит/сек). В случае без них – среднебюджетный вариант не будет стоить больших денег. Именно по этому подключению будет происходить синхронизация всех хранимых файлов, образов виртуальных машин между серверами хранения.

Планируется три сервера виртуализации, объединенных в кластер. Три – минимальное количество, при котором можно обеспечить абсолютную отказоустойчивость всех виртуальных машин, работающих на серверах. Подводя итог, можно сказать – при таких условиях будет обеспечена очень хорошая возможность масштабирования, что в условиях макета (постоянное изменение, добавление, тестирование новый решений в инфраструктуре) очень важно.

# 2.2 Планирование и подготовка к реализации будущей инфраструктуры

При создании макета с виртуальными машинами, сначала всегда требуется создать шаблоны ВМ, из которых все будет разворачиваться. Первым делом будет создан шаблон Astra Linux обеих версий (1.7 и 1.8). Конфигурации шаблонов показаны на рисунках №. 4 ГБ и 4 vCPU были выбраны, так как данный объем считается избыточным для макета и тестирования инфраструктуры. Также играют роль минимальные требования и клиентских ПК, и серверов, ПО которых должно запустится и функционировать.

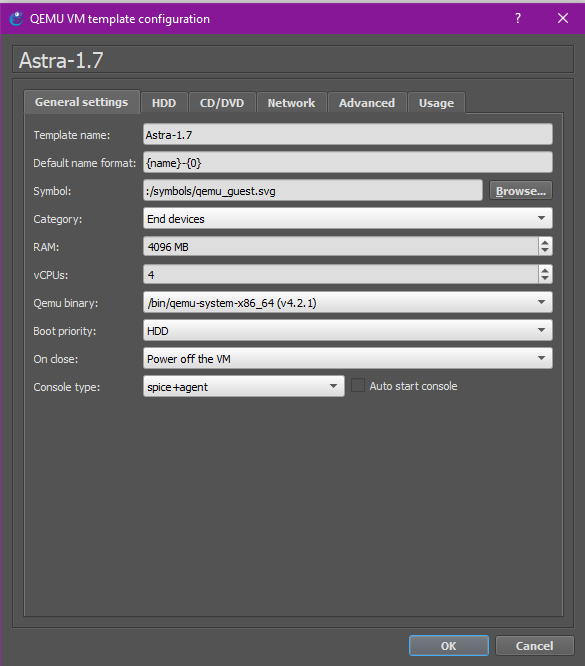


Рисунок № – Настройки шаблона Astra Linux 1.7

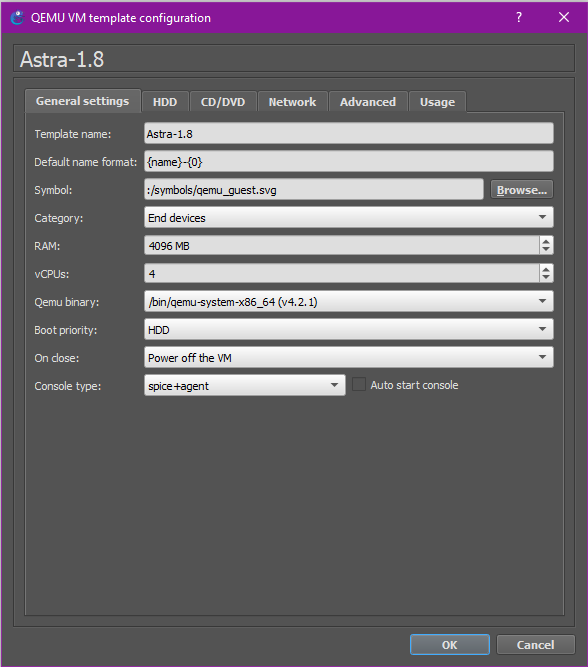


Рисунок № – Настройки шаблона Astra Linux 1.8

Далее для шаблонов необходимо создать диск и установить саму операционную систему. Ключевые моменты процесса установки показан на рисунках №. После успешной загрузки установочного образа необходимо придумать имя для учетной записи администратора.

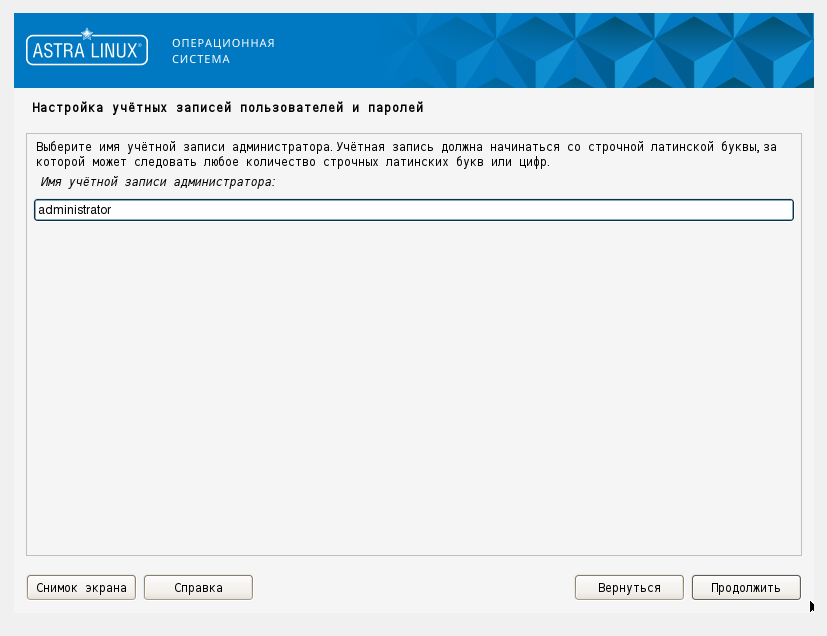


Рисунок № – Создание аккаунта администратора

Дальше необходимо два раза повторить пароль для нашего пользователя. Пароль в рамках макета выставляется одинаковым везде, ради ускорения развертывания. После ввода пароля и нескольких шагов по настройке системы появится этап разметки диска. Ввиду отсутствия требований можно выбрать «Авто», что автоматически создаст загрузочный раздел и раздел подкачки.

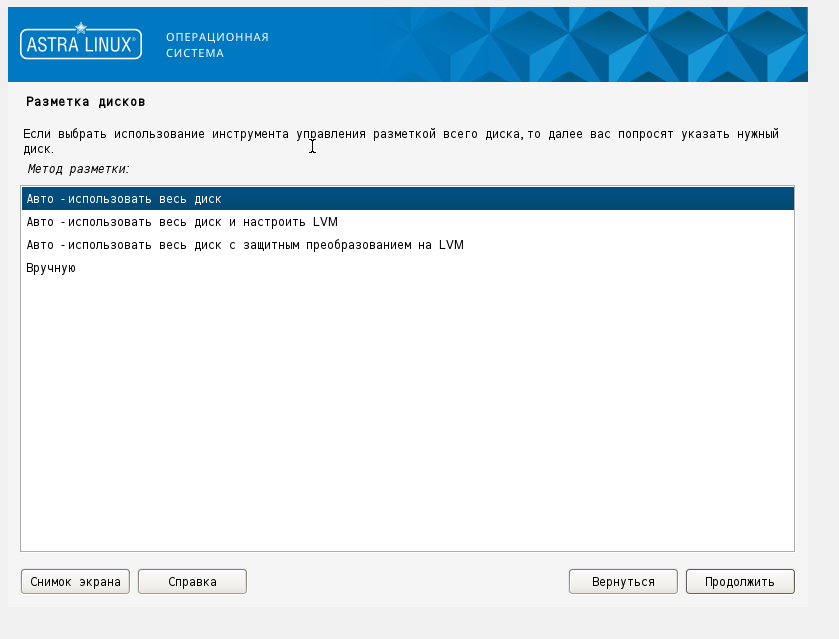


Рисунок № – Выбор метода разметки

Далее, если был выбран метод «Авто», появится окно выбора схемы. Необходимо просто выбрать «Все файлы в одном разделе», так как второй в данном случае никакой роли не играет.

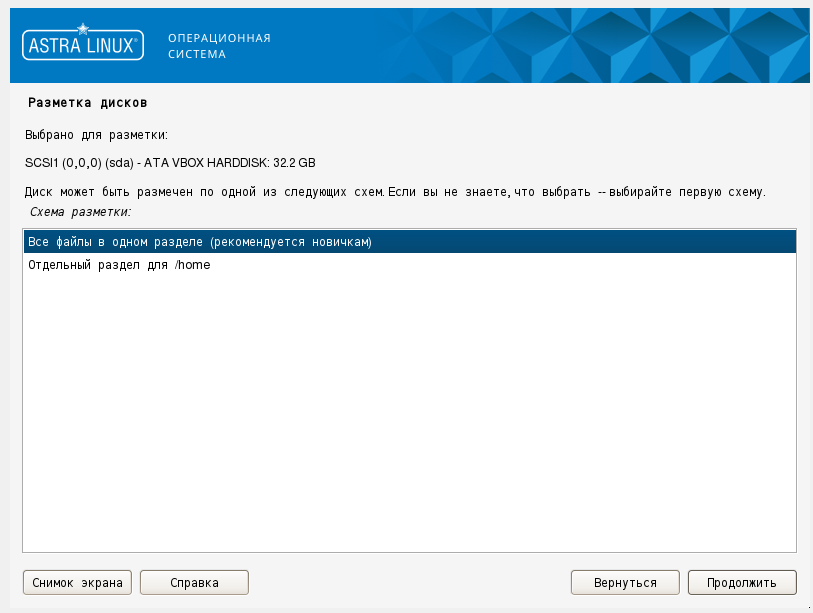


Рисунок № – Выбор метода разметки

После разметки идет следующий важный шаг в виде выбора ПО, которое будет установлено сразу же, без ручного вмешательства. Для полноты и упрощения последующей работы необходимо выбрать пункты:

* + графический интерфейс;
  + средства работы с Интернет;
  + консольные утилиты;
  + средства удаленного подключения SSH.

Пункт с ядром не выбирается ввиду отсутствия совместимости многого ПО с ядром «hardened».

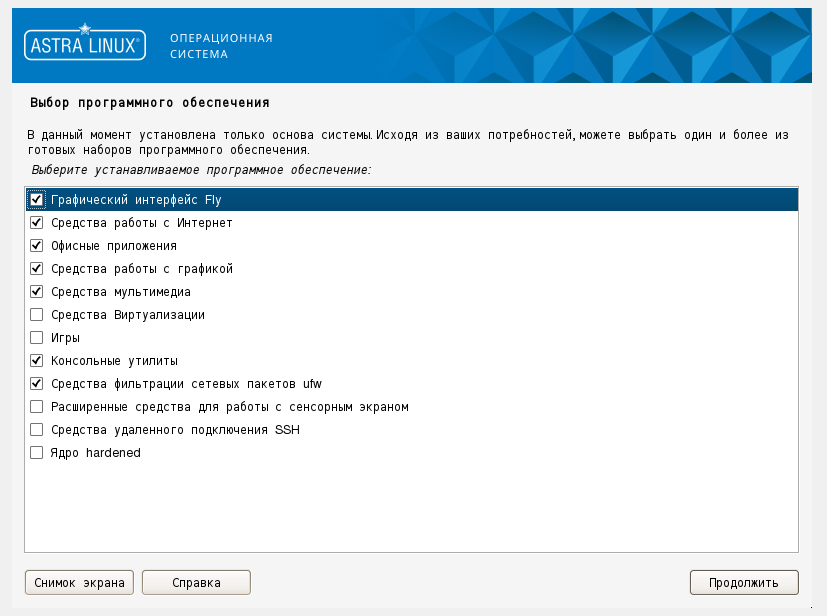


Рисунок № – Выбор программного обеспечения

После идет завершающий этап основных настроек – выбор режима работы ОС. Режимы отличаются функциональностью, которая отвечает за безопасность информации.

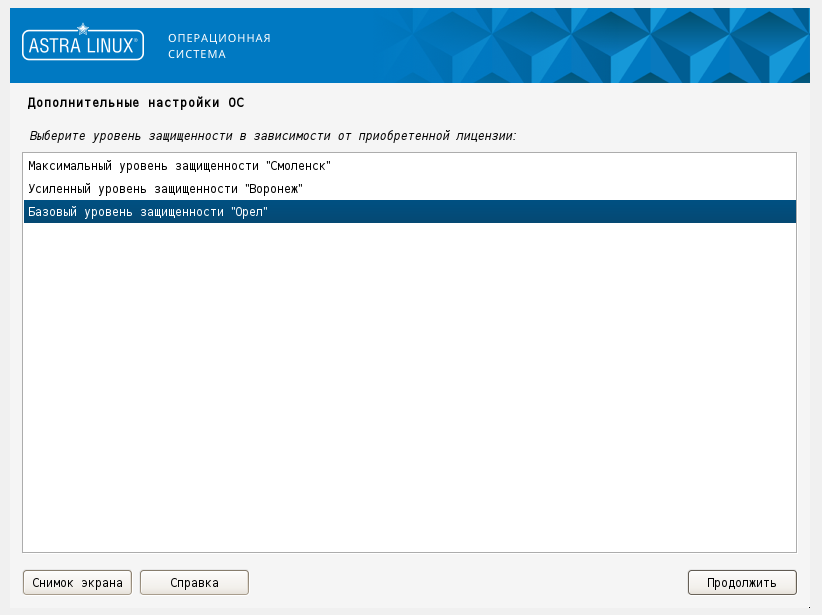


Рисунок № – Выбор режима работы ОС Astra Linux

Режим выбирается в соответствии с приобретенной лицензией, но в данном случае нужно выбрать базовый уровень защищенности, чтобы без особых проблем с функциями безопасность базово настроить ОС. После установки уровень защищенности также можно сменить. Настройка Astra Linux SE 1.8 выглядит аналогично и требует абсолютно аналогичных настроек, поэтому освещение этого процесса не несет особо смысла.

После необходимо создать шаблон Ideco NGFW. Минимальные требования для установки – 150 ГБ места на накопителе и 16 ГБ оперативной памяти, после установки ресурсы будут снижены до 8ГБ ОЗУ для увеличения производительности самого сервера. Технические детали шаблона представлены на рисунке №. Общий процесс установки, только для шагов играющих роль в работе в рамках макета, показан в рисунках №.

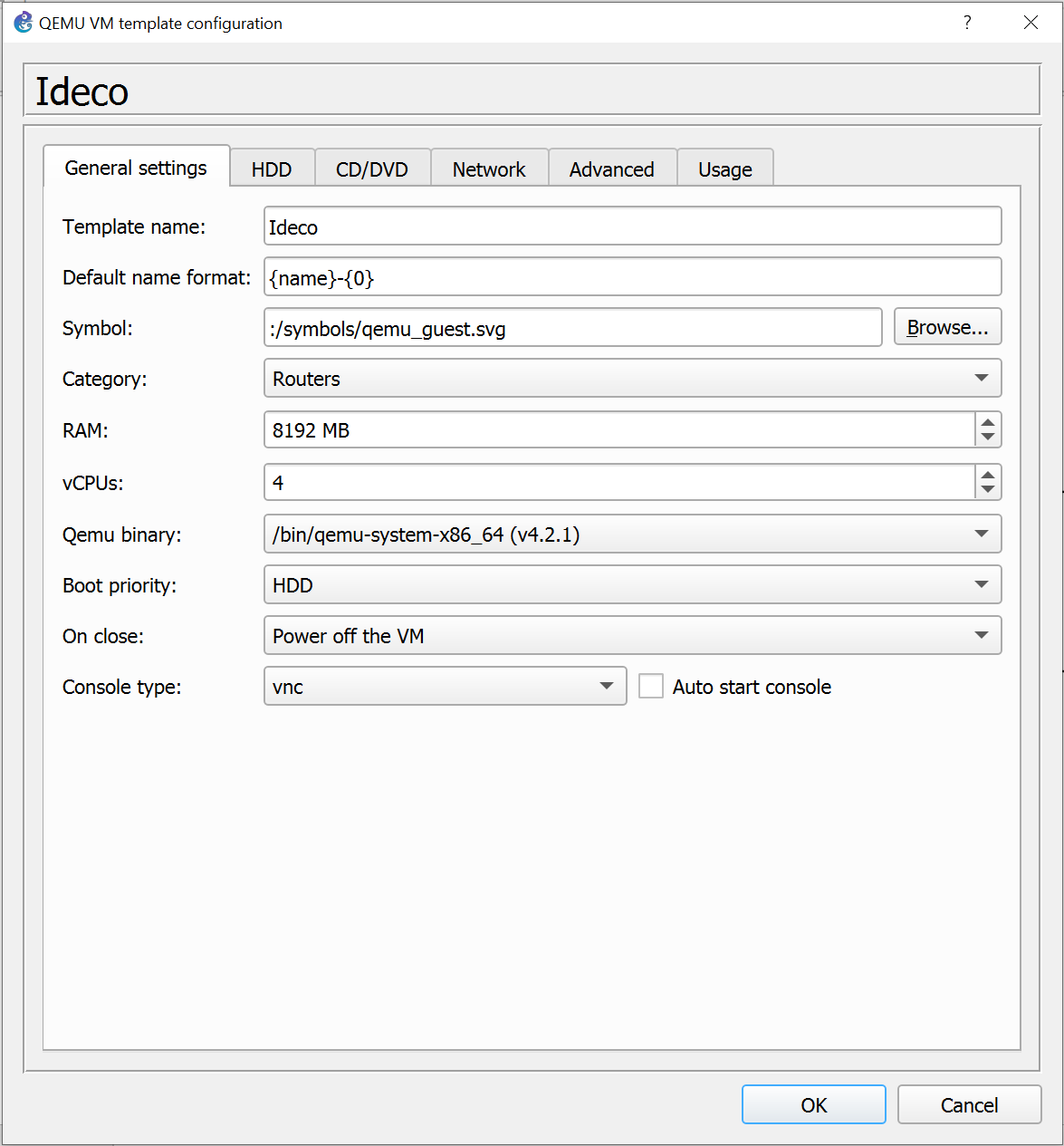


Рисунок № – Выбор режима работы ОС Astra Linux

После создания жесткого диска необходимо установить саму операционную систему. Необходимо загрузиться с указанного образа, в первом меню выбрать «Install Ideco NGFW»



Рисунок № – Меню загрузчика GRUB

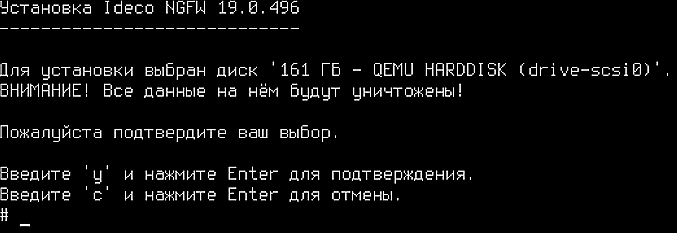


Рисунок № – Выбор накопителя для установки ОС

После выбора диска необходимо настроить временную зону, подтвердить настройки. После этого нужно загрузиться с уже установленной ОС и произвести начальную настройку. Нужно отказаться от предложения сделать устройство второй нодой кластера и приступить к созданию аккаунта администратора.

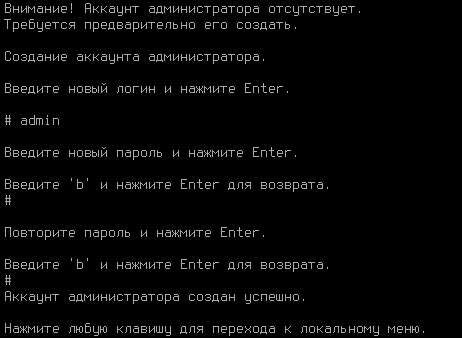


Рисунок № – Создание аккаунта администратора

После этого нужно войти и приступить к настройке локального интерфейса, для доступа в веб-интерфейс. Ideco NGFW не поощряет настройку через командную строку и в случае конфигурирования именно таким образом – снимает с себя ответственность за работоспособность устройства. Важное замечание - при использовании сетевых карт одного производителя могут возникнуть трудности при идентификации сетевой карты для настройки сетевого интерфейса. Для корректной идентификации сетевой карты нужно использовать ее MAC-адрес.

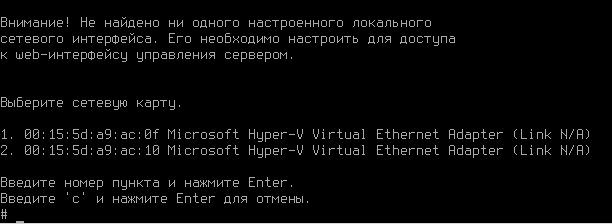


Рисунок № – Настройки сетевых интерфейсов

После выбора интерфейса можно выбрать тип IP адреса – статический или динамический. В случае шаблона это не имеет значения, поэтому необходимо выбрать динамический, чтобы при развертывании без особых проблем изменить на требуемый по топологии. На этом процесс установки Ideco NGFW завершен.

Остальные ОС необходимо установить с заявленными минимальными требованиями, в процессе установки нужно выполнить аналогичные шаги с аналогичными значениями.

После установки ОС необходимо собрать топологию в проекте и подключить устройства в соответствии со схемой на плакате 1.

# 2.3 Настройка сетевого оборудования

После создания топологии в проекте стоит приступить к настройке сетевых устройств и адресации на серверах и клиентских ПК. Сначала нужно настроить межсетевой экран, только для обеспечения связности между устройствами – трансляция адресов, динамическая маршрутизация. Процесс настройки МСЭ представлен на рисунках №. Первым делом надо перенастроить сетевые реквизиты на нужном интерфейсе.

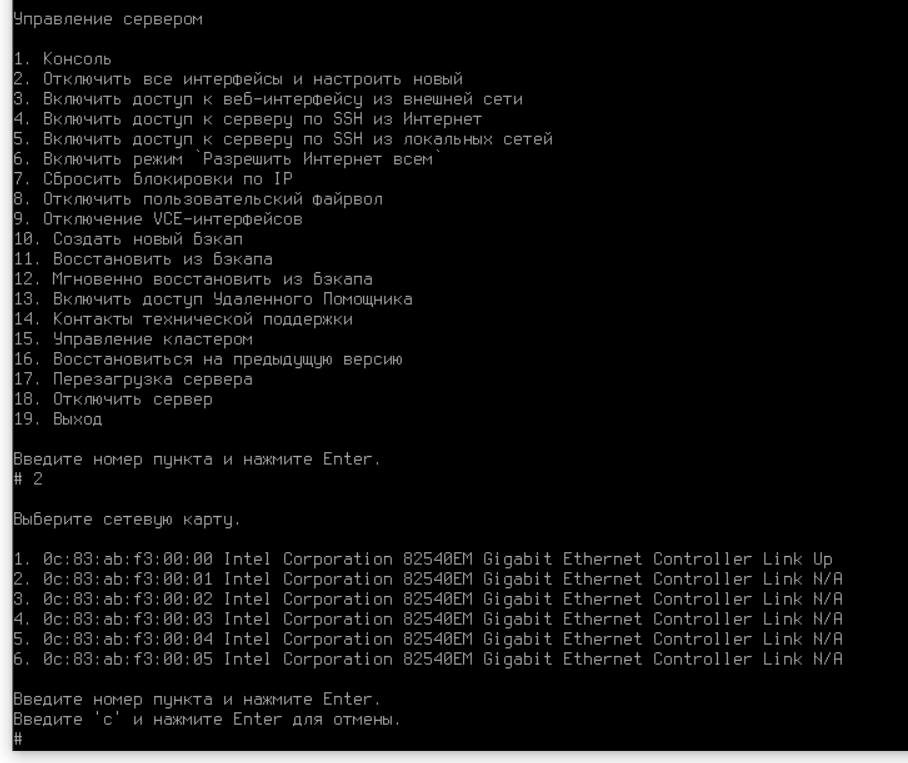


Рисунок № – Новая настройка сетевых интерфейсов

Далее в интерактивном опросе, следует настроить автоматическое получение IP-адреса (или иначе, если того требует провайдер). VLAN-тег в данном случае – оставить пустым.

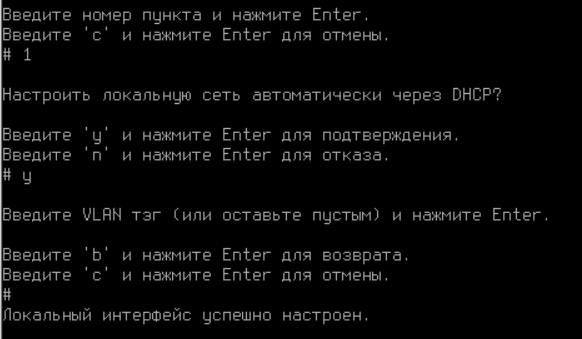


Рисунок № – Продолжение настройки сетевых интерфейсов

После следует перепроверить IP-адрес и найти его среди прочих системных интерфейсов.

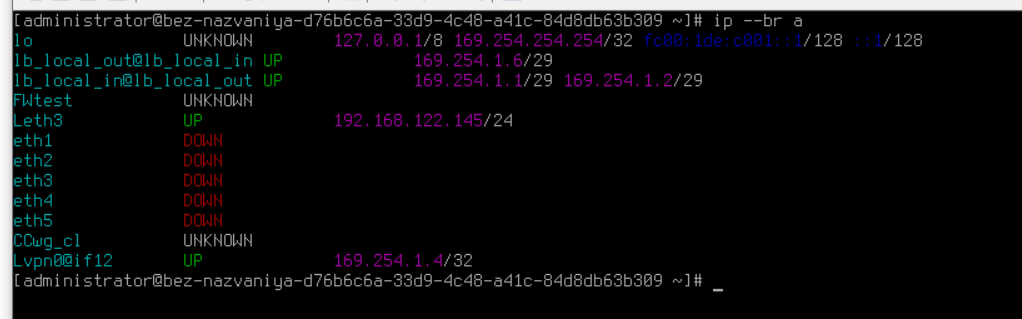


Рисунок № – Проверка IP-адресов на интерфейсах

После надо зайти в веб-интерфейс по IP-адресу от провайдера, с портом 8443 и войти с учетными данными, созданными при установке ОС.

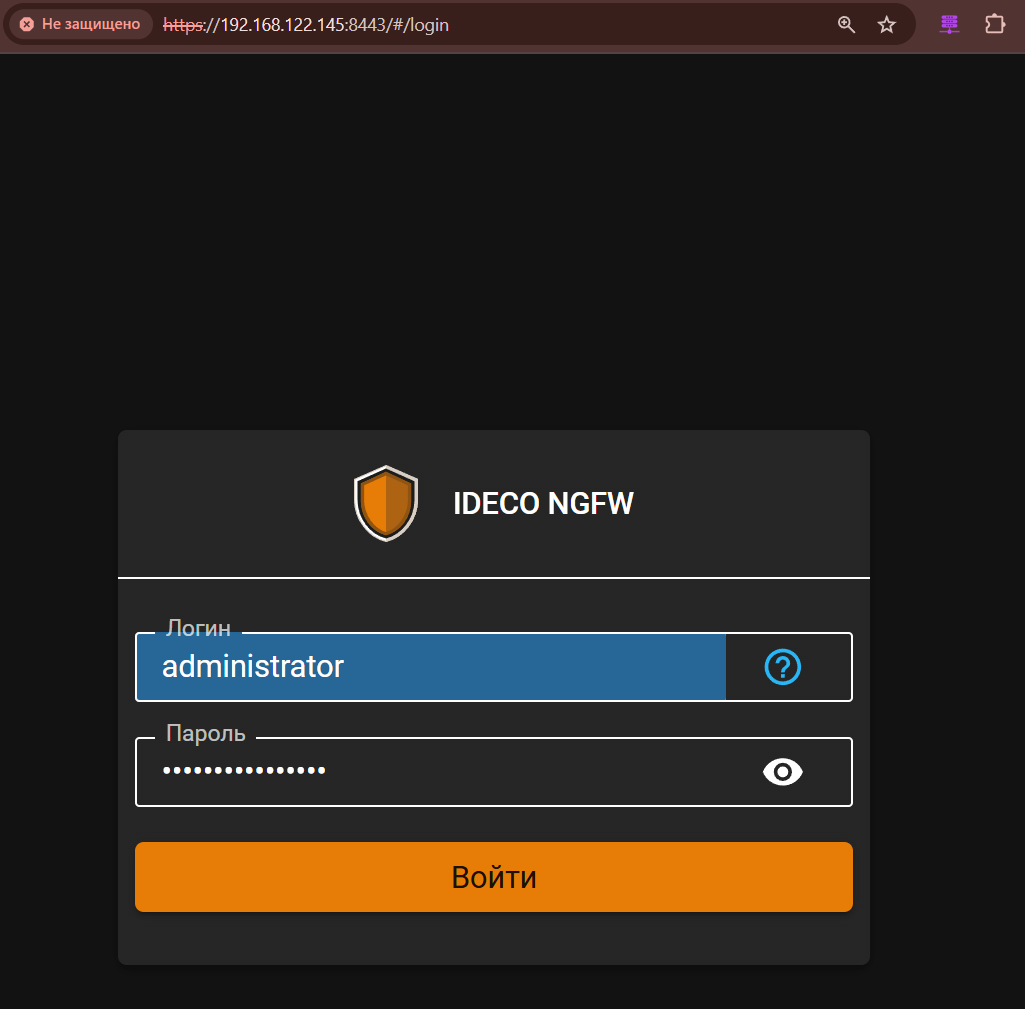


Рисунок № – Страница входа в интерфейс управления

На главной странице пользователь сможет увидеть управление модулями, графики о загруженности межсетевого экрана и статистику трафика от пользователей.

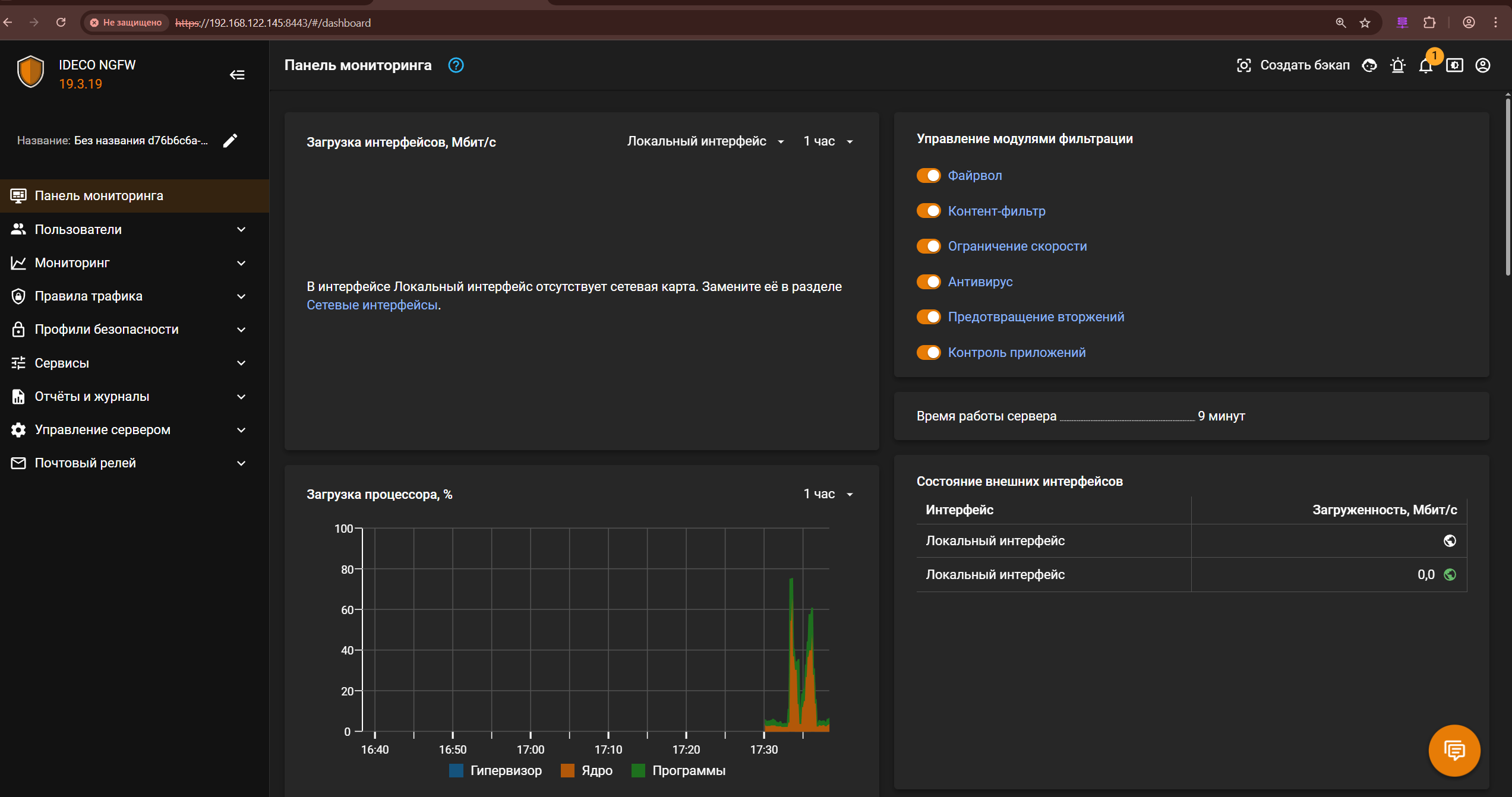


Рисунок № – Дашборд с модулями и графиками

После входа необходимо настроить адресацию на интерфейсах, создать пользователей и авторизацию по подсетям, прикрепив созданных пользователей к нужным подсетям. В итоге весь результат анализа трафика будет отсылаться на пользователей, которые были настроены до этого.

Сначала нужно зайти в раздел «Сетевые интерфейсы» и выбрать создание агрегированного канала. После дать название, выбрать интерфейсы, которые будут добавлены в LAG и сделать описание. Аналогично, в соответствии с созданной L1 схемой необходимо настроить второй LAG.

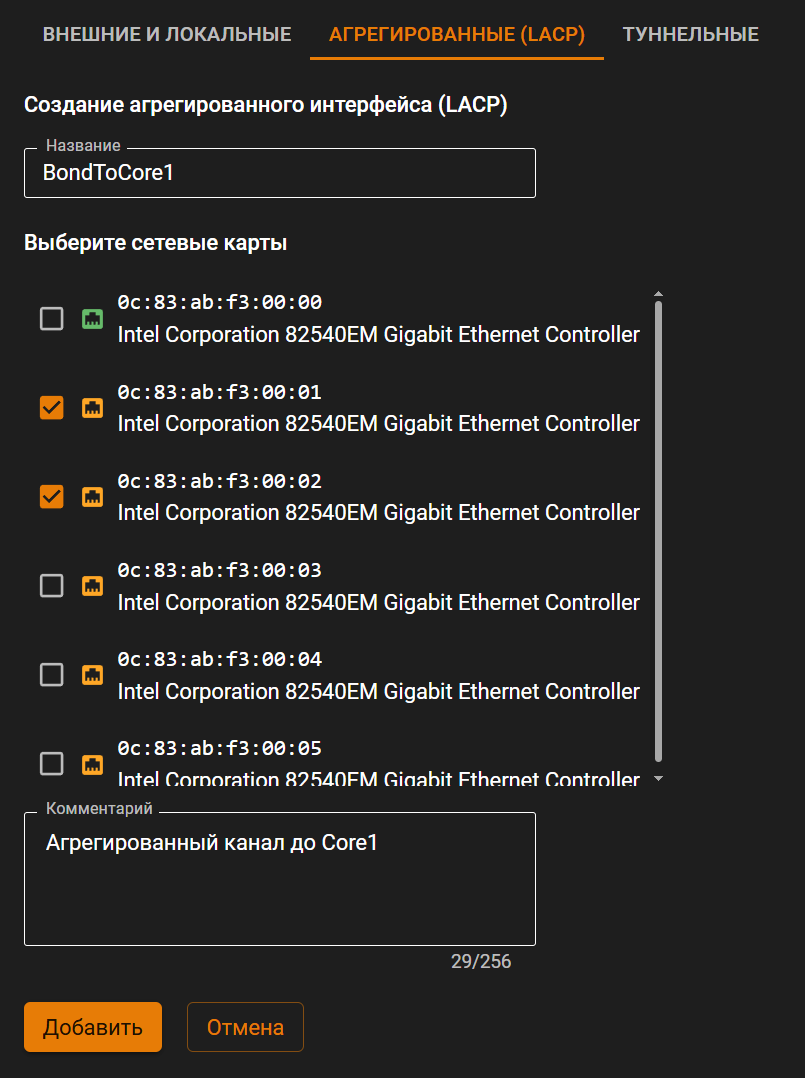


Рисунок № – Создание агрегированного канала

В результате, после создания в разделе агрегированных интерфейсов появятся новые. Здесь же доступно управление – включение, переназначение участников группы и так далее.

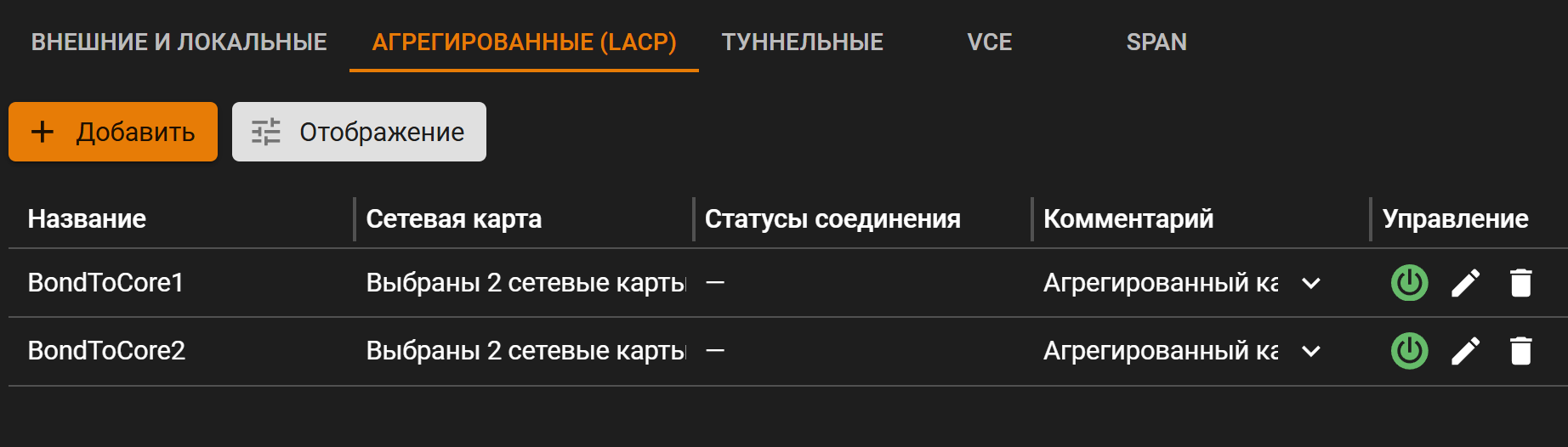


Рисунок № – Результат создания двух LAG

Далее необходимо назначить IP-адреса Bond-интерфейсам. Для этого необходимо также в разделе «Сетевые интерфейсы» зайти во «Внешние и локальные» и начать создание. Это создаст некое «соответствие» физического и логического интерфейса. Необходим такой подход потому, что логических интерфейсов на физическом может гораздо больше одного (например, реализация Router-on-a-Stick). Необходимо задать название, физический интерфейс и IP-адрес, остальное оставить по умолчанию. Аналогично в соответствии с L3 схемой нужно задать остальные IP-адреса на МСЭ.

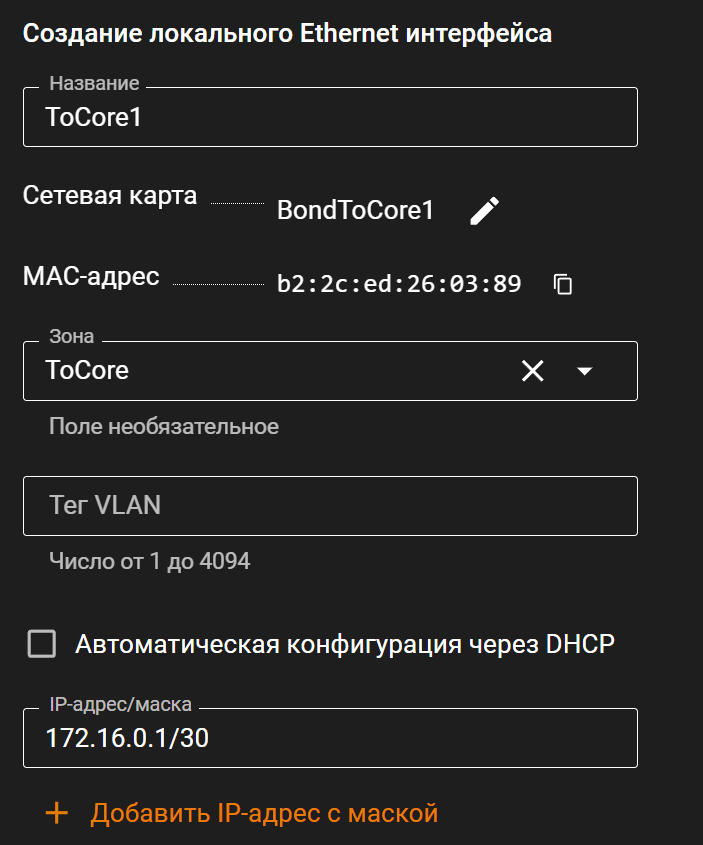


Рисунок № – Назначение адресов агрегированным группам

По итогу настройки в разделе «Внешние и локальные» можно будет увидеть новые интерфейсы.

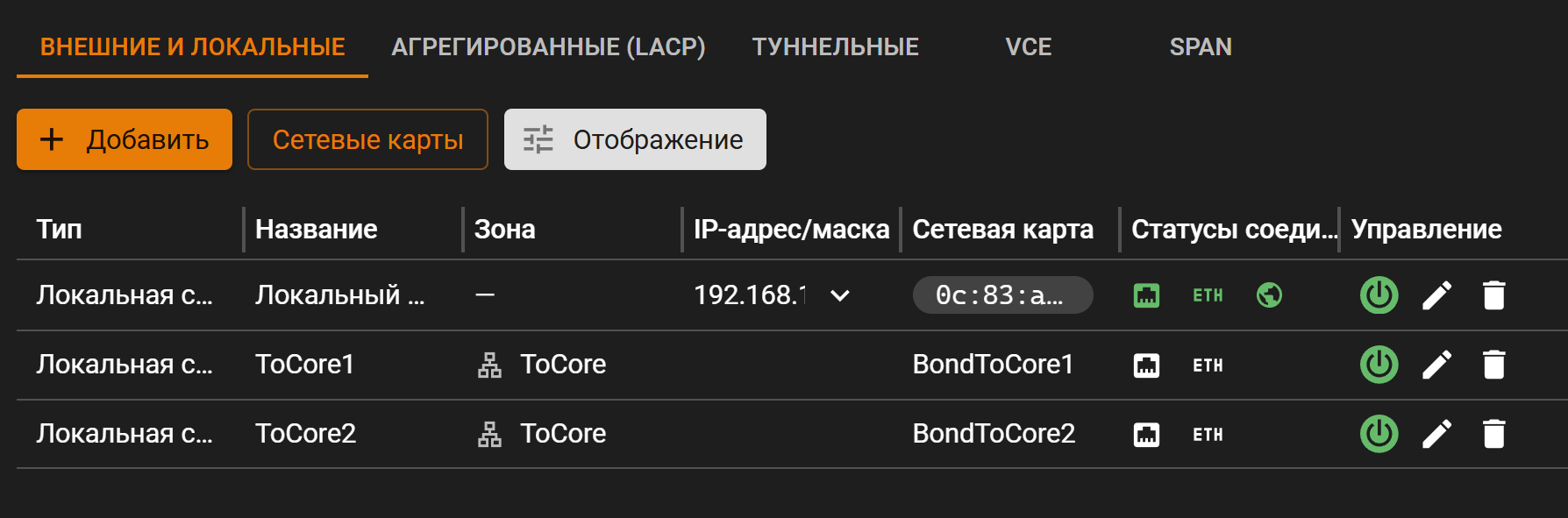


Рисунок № – Все сетевые интерфейсы

После базовой адресации нужно позаботиться о том, чтобы трафик клиентов мог проходить через NGFW, по умолчанию весь трафик фильтруется и отбрасывается.



Рисунок № – Создание пользователей

После создания необходимых пользователей должна получиться структура, как на рисунке №.

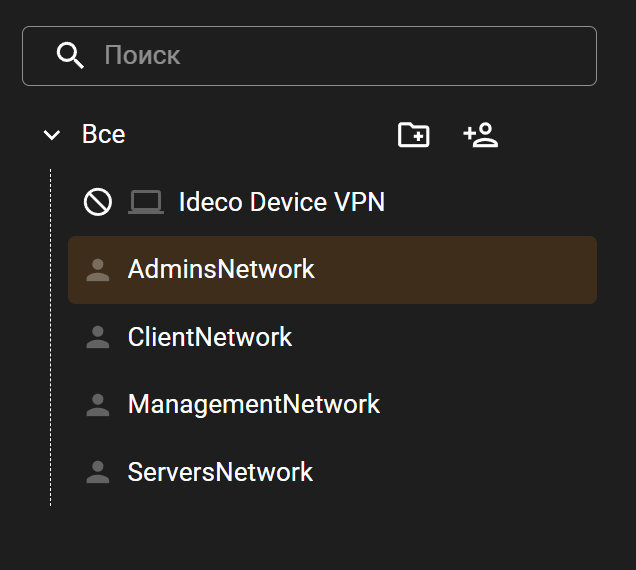


Рисунок № – Итоговое количество пользователей

Далее нужно зайти в раздел «Авторизация» в меню «Авторизация по подсетям» и присвоить каждому пользователю свою сеть.

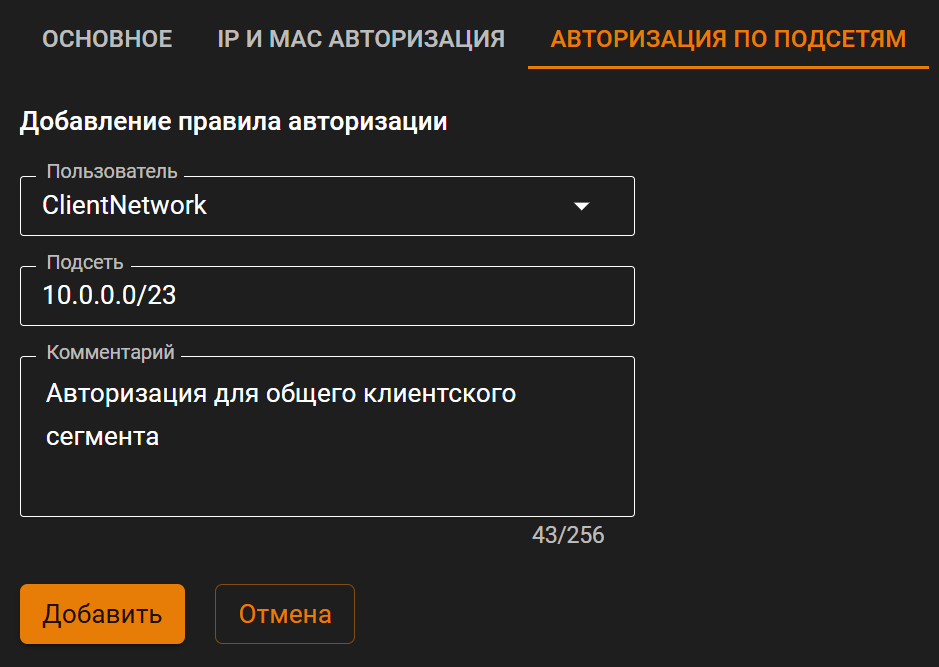


Рисунок № – Назначение сетей пользователям для авторизации

В результате должна получиться структура, как на рисунке №.

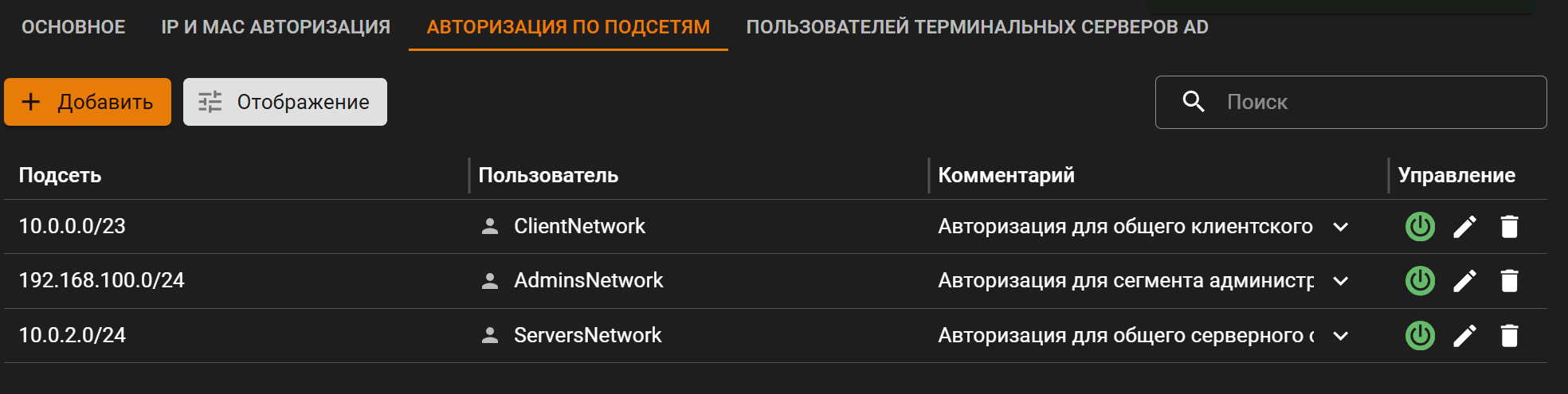


Рисунок № – Результат настройки авторизации по подсетям

После необходимо настроить подключение к VPN организации и обеспечить динамическую маршрутизацию, чтобы обмениваться маршрутами с коммутаторами уровня ядра и остальными офисами организации.

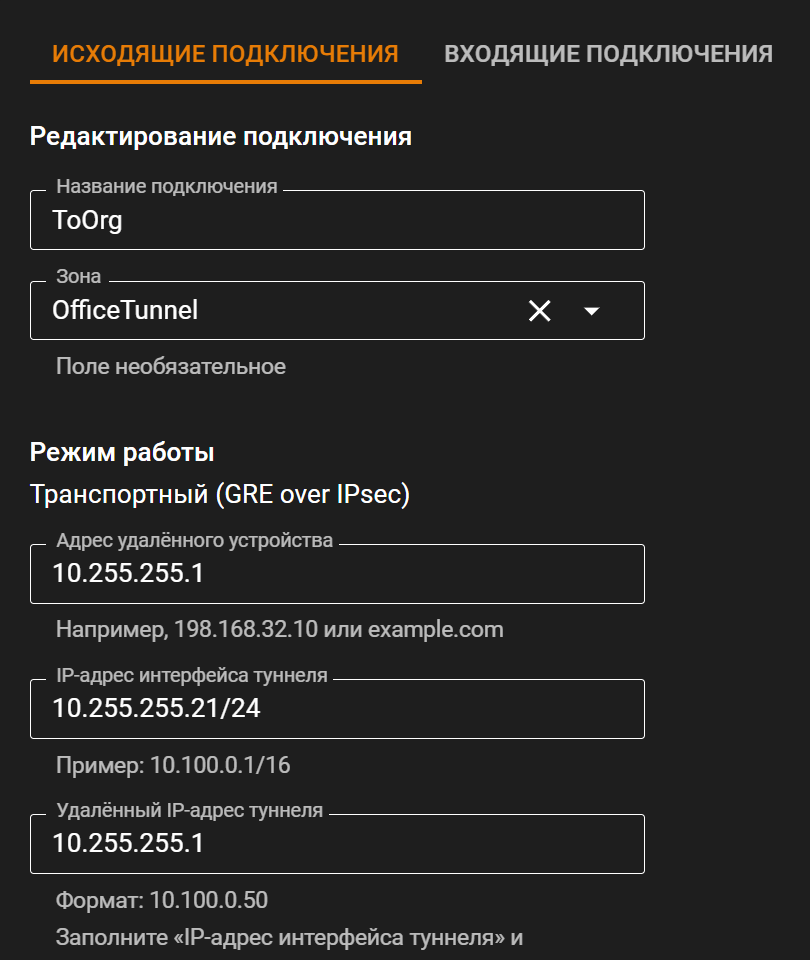


Рисунок № – Создание IPsec туннеля до сети в главном офисе

После создания туннеля и указания необходимых настроек, согласованных с администратором второго конца туннеля, в разделе исходящих подключений можно будет увидеть новый, идущий к основному офису организации.



Рисунок № – Созданный IPsec-туннель

Чтобы основной офис и клиенты из нового отдела могли общаться между собой, необходимо настроить маршрутизацию. Офис небольшой, но предусматривая момент роста сети, необходимо настроить динамическую маршрутизацию. Для этого надо перейти в раздел «OSPF» настроить зону на интерфейсе туннеля, а после отдельно на двух локальных интерфейсах, чтобы получать основные локальные маршруты от ядра сети и передать их дальше.

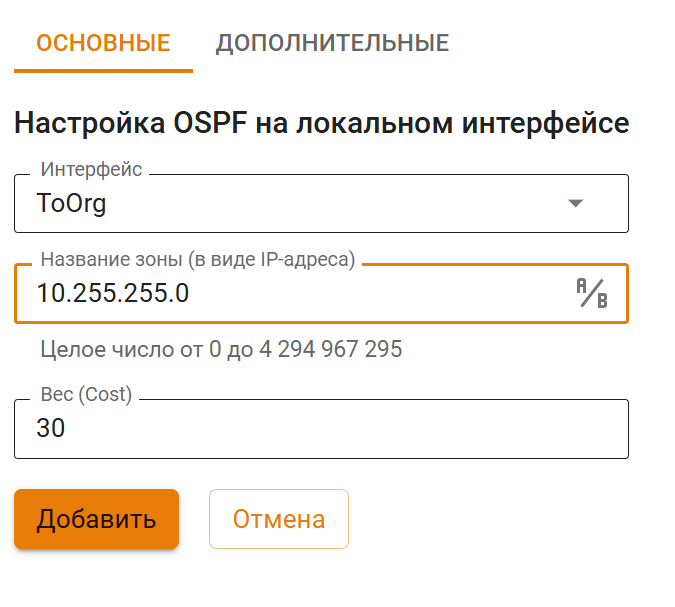


Рисунок № – Настройка анонса локальных маршрутов в туннеле

После выполненных настроек, должны появиться все интерфейсы участвующие в маршрутизации и их зоны.

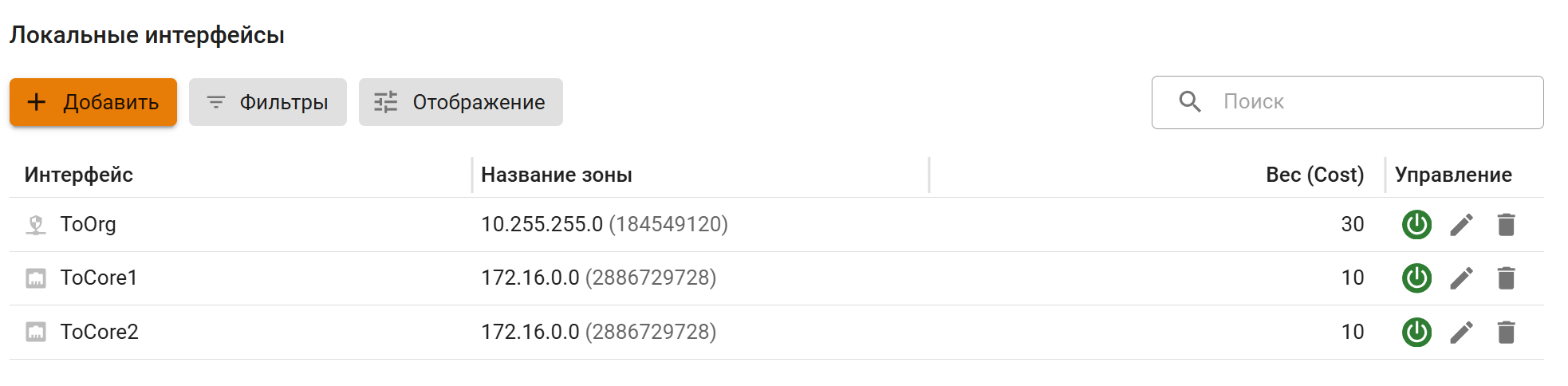


Рисунок № – Все интерфейсы, участвующие в маршрутизации

После настройки межсетевого экрана необходимо приступить к настройке коммутаторов уровня ядра. Нужно настроить IP-адреса, агрегацию каналов, динамическую маршрутизацию в сторону МСЭ и маршрутизацию между VLAN. Процесс выполнения описанных шагов показан на рисунках №.

Настройка агрегации на коммутаторах Eltex очень схожа с Cisco. Нужно создать группу, добавить в нее необходимы интерфейсы. Так как Ideco NGFW поддерживает только LACP (active-backup), то стоит задать приоритет интерфейсов в LAG. На рисунках показаны настройки для первого коммутатора, на втором необходимо произвести аналогичные настройки, учитывая составленные схемы.

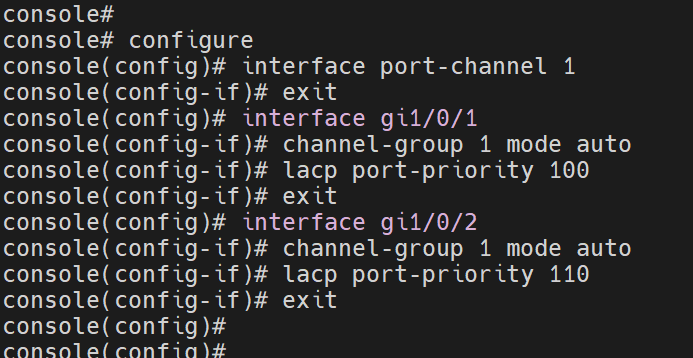


Рисунок № – LAG на CORE-1 к Ideco NGFW

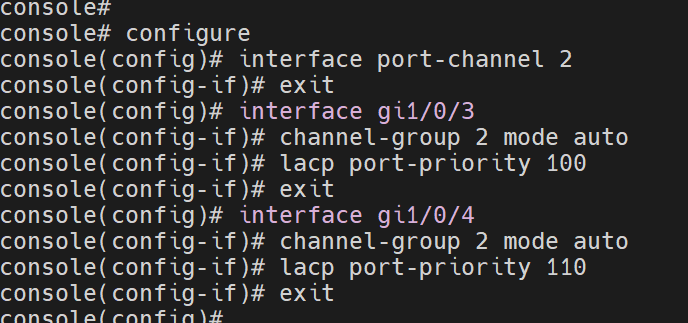


Рисунок № – LAG на CORE-1 до серверного коммутатора

После настройки агрегации нужно приступить к назначению IP-адресов на VLAN-интерфейсы на всех коммутаторах уровня ядра, чтобы маршрутизировать трафик между VLAN. Для этого надо просто создать VLAN, а после назначить им адреса. На первом коммутаторе все адреса будут иметь 253 адрес, на втором – 254. При масштабировании ядра адреса необходимо выставлять в убывающем порядке.

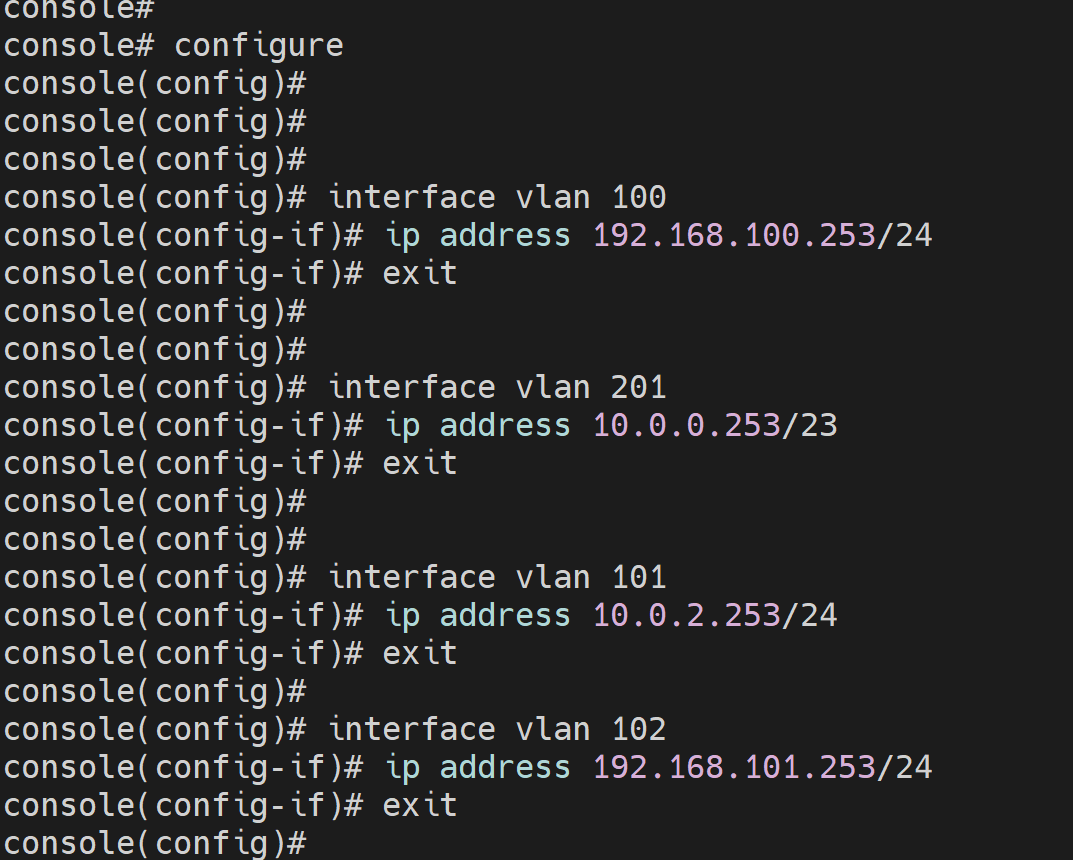


Рисунок № – Настройка VLAN-интерфейсов на CORE1

Дальше нужно назначить адреса на физические интерфейсы, идущие к МСЭ. По умолчанию включен Firewall и ICMP-запросы блокируются. Для этого везде надо их отключить.

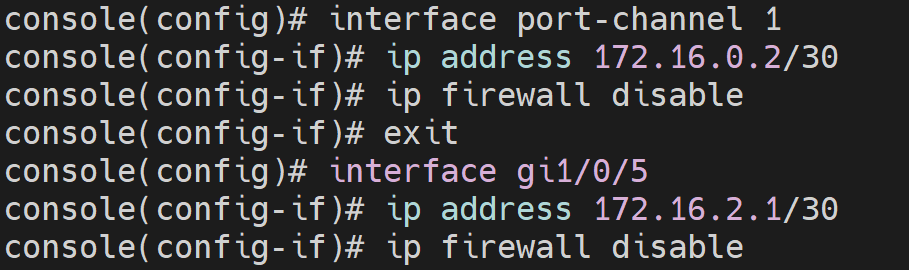


Рисунок № – Настройка IP-адресов на физических интерфейсах на CORE1

Аналогично, опираясь на составленную логическую схему, следует настроить второй коммутатор.

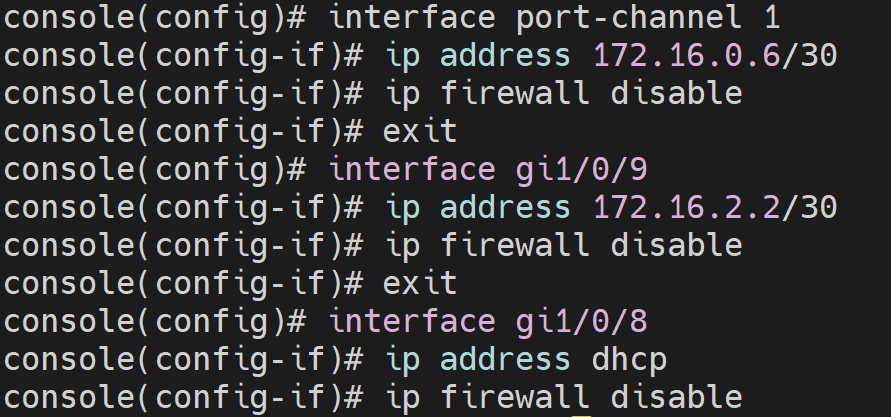


Рисунок № – Настройка IP-адресов на физических интерфейсах на CORE2

Чтобы ограничить возможности пользователей в сети на всех коммутаторах ядра надо прописать списки доступа, откуда и куда трафик не может ходить. Для того, чтобы запретить клиентский сети маршрутизироваться в сеть для управления и сеть администраторов (только в одну сторону), надо создать правило и применить его на необходимый VLAN-интерфейс.

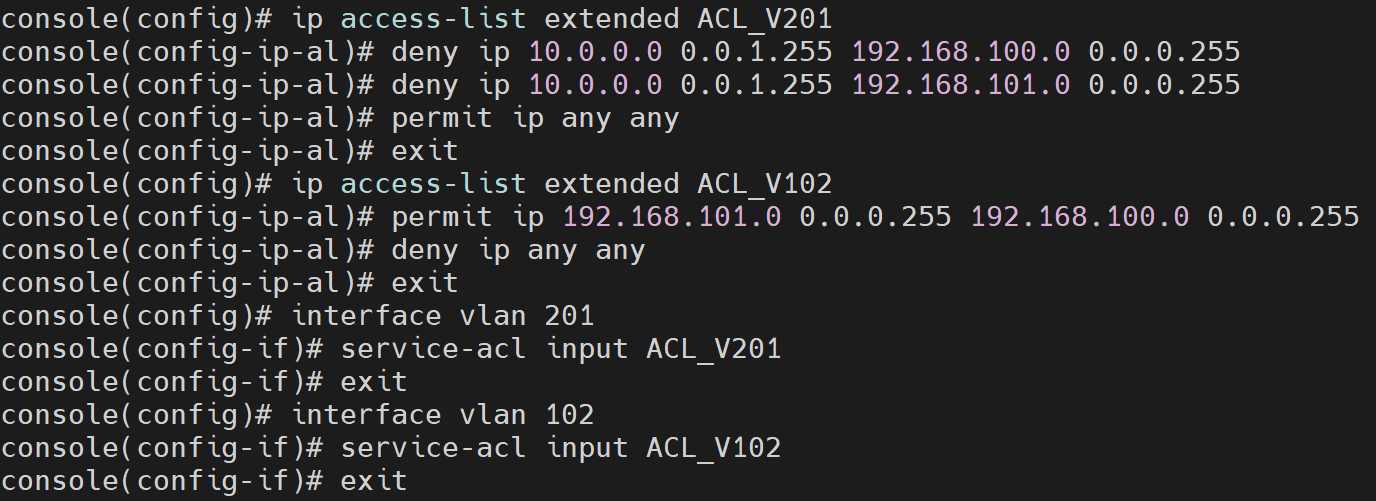


Рисунок № – Настройка ACL на коммутаторах ядра

Так как в сети существует второй провайдер, то надо реализовать и необходимые правила, чтобы использовать оба шлюза. Так как второй провайдер заходит сразу в ядро, то использоваться данный шлюз будет только в очень крайнем – случае, а именно в случае отказа межсетевого экрана. Для этого на всех коммутаторах ядра (если их больше, чем 2), не имеющих подключения к провайдеру надо указать плавающий маршрут – если отказывает NGFW, весь трафик перенаправлять на CORE2. На самом CORE2 аналогичный маршрут, но только на интерфейс, идущий к провайдеру.

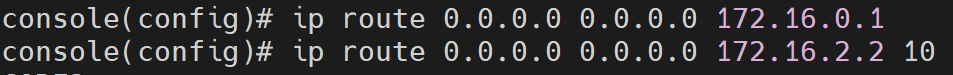


Рисунок № – Настройка основного и резервного маршрута на CORE1

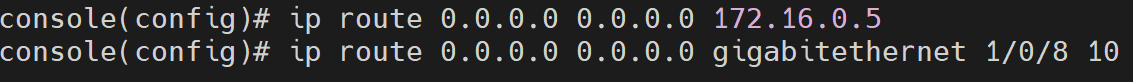


Рисунок № – Настройка основного и резервного маршрута на CORE2

Так как трафик в случае отказа будет маршрутизироваться через CORE2, на нем следует настроить сетевую трансляцию адресов. Для этого нужно создать зону безопасности и объекты, в которых указать адреса всех локальный сетей.

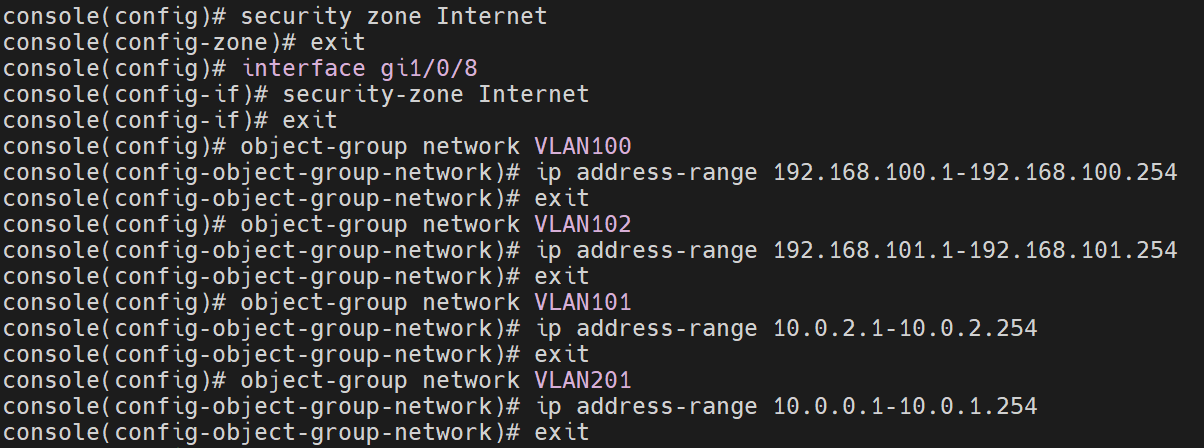


Рисунок № – Создание зоны безопасности и групп объектов

После следует создать набор правил с любым названием и в нем определить правила, которые будут подменять IP-адрес ранее созданных локальных сетей на внешний.

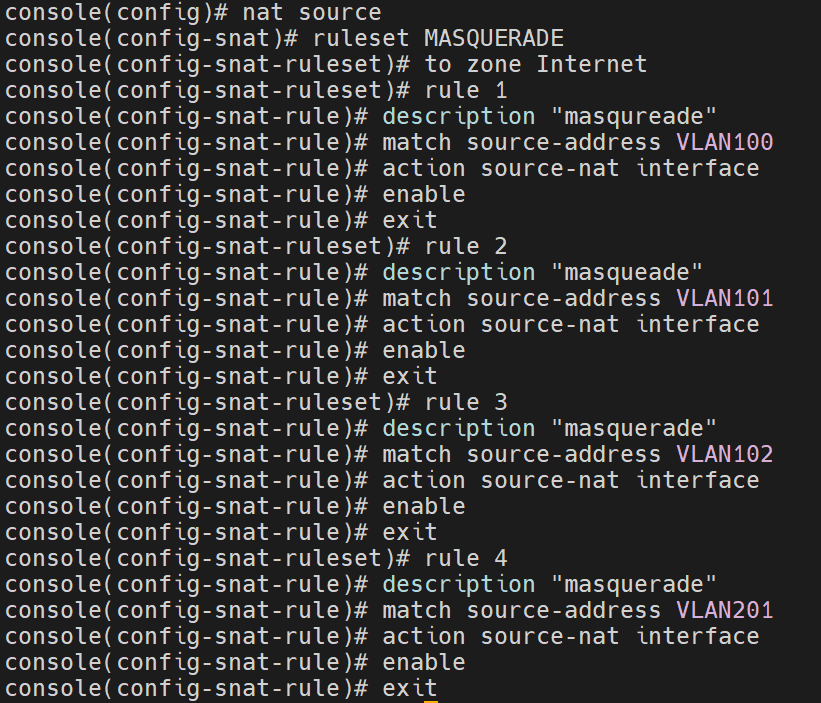


Рисунок № – Создание правил SNAT для каждой сети.

Далее на уровне ядра надо определить магистральные порты и разрешить VLAN, которые могут по ним проходить. Аналогичные настройки произвести на всём уровне ядра, в соответствии с L1 схемой.

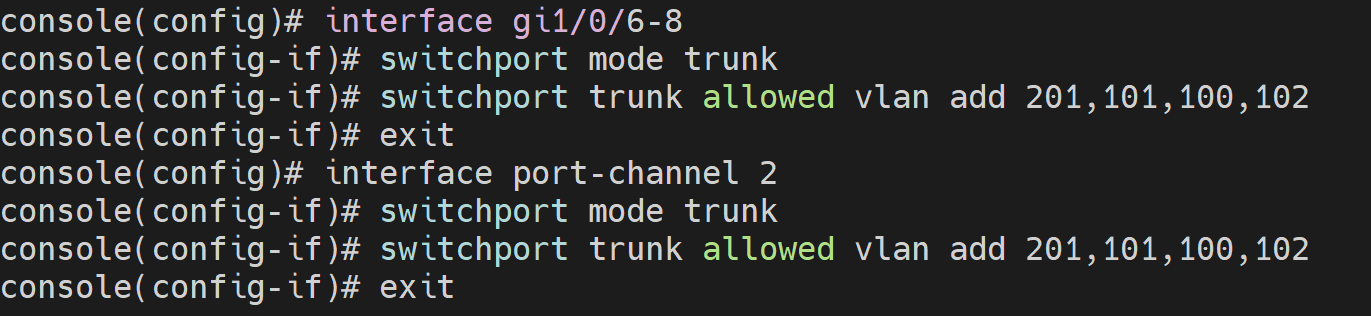


Рисунок № – Настройка магистральных портов на CORE1

Так как МСЭ еще не знает о локальных сетях, надо анонсировать ему маршруты. Аналогично требуется сделать на всех устройствах уровня ядра.

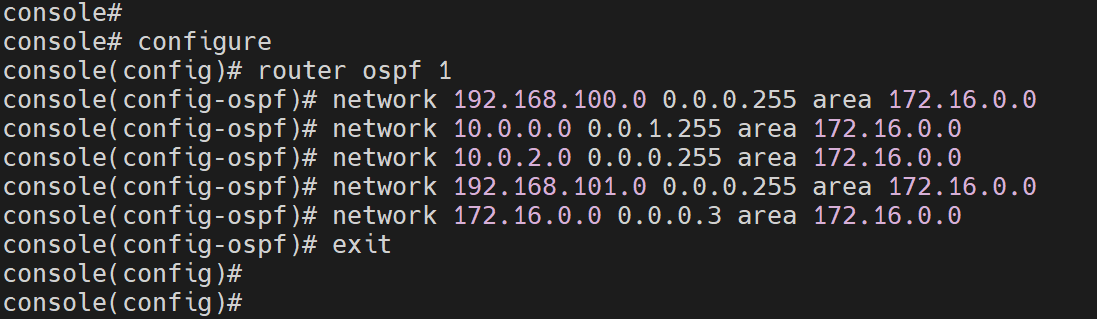


Рисунок № – Настройка OSPF на CORE1

Последним шагом на коммутаторах ядра нужно настроить VRRP, чтобы избежать дополнительной точки отказа на NGFW. Ранее именно для этого указывались последние адреса из диапазонов, чтобы виртуальный адрес имел привычный формат.

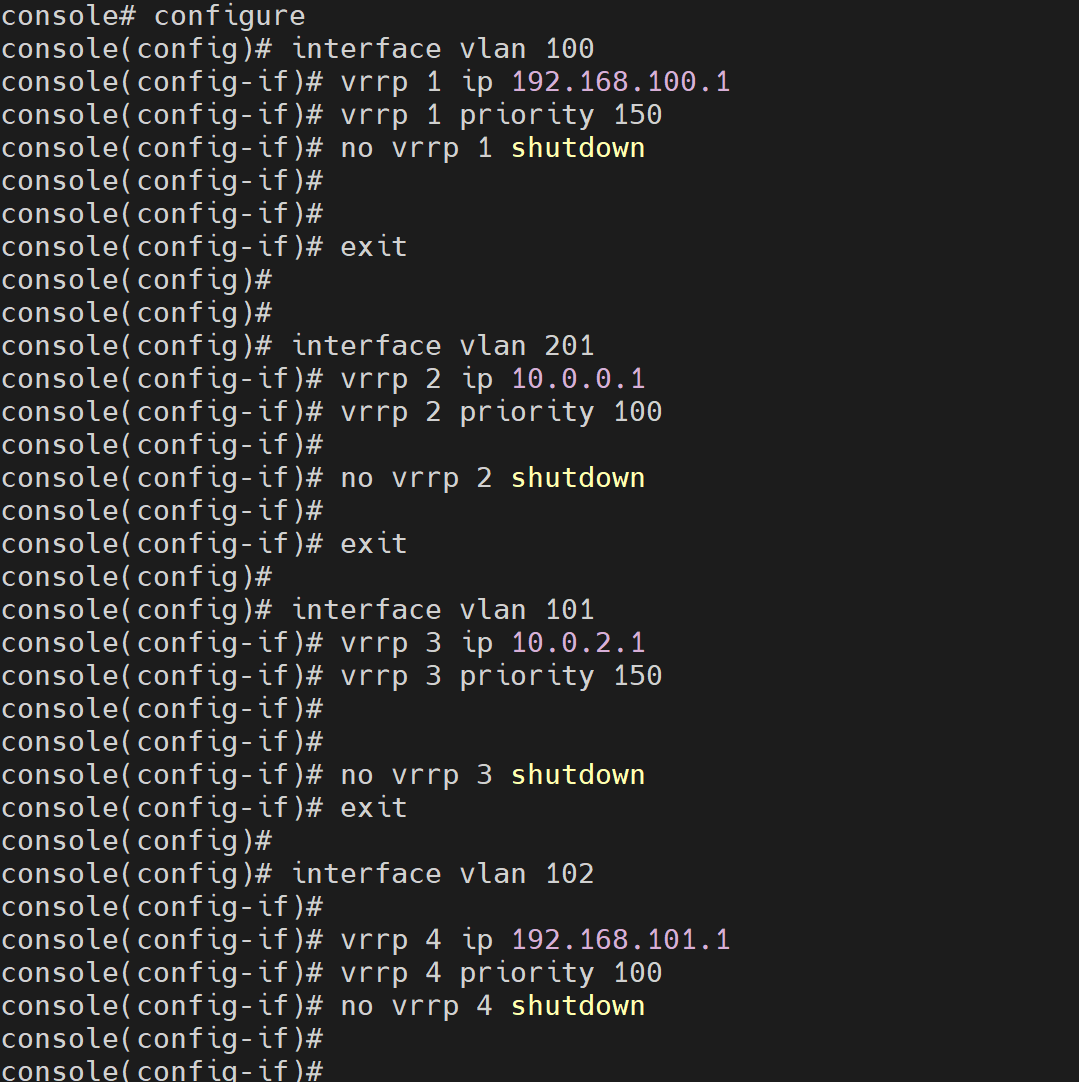


Рисунок № – Настройка VRRP на CORE1

Также можно заметить, что на разных устройствах указывается разный приоритет. Делается это для того, чтобы разбалансировать нагрузку в нормальном состоянии устройств. Если из строя выйдет один – второй будет обрабатывать свои два VLAN, а после возьмет еще два от другого коммутатора.

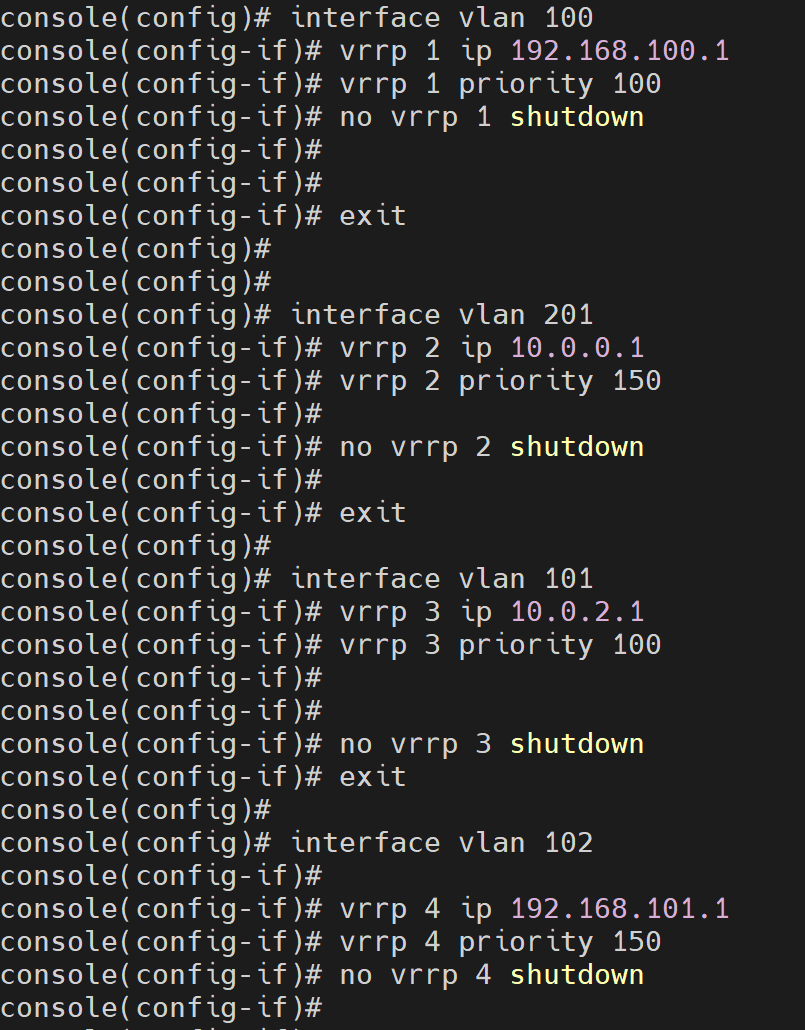


Рисунок № – Настройка VRRP на CORE1

В последнюю очередь необходимо настроить коммутаторы доступа, которые первые обрабатывают трафик от пользователей и серверов. Процесс настройки коммутаторов доступа показан на рисунках №. На каждом коммутаторе необходимо настроить uplink-порты так, чтобы они могли пропускать несколько VLAN. Остальные порты сделать портами доступа и распределить в соответствии с L3 схемой. Агрегацию на серверном коммутаторе необходимо настроить также, как на коммутаторах ядра.

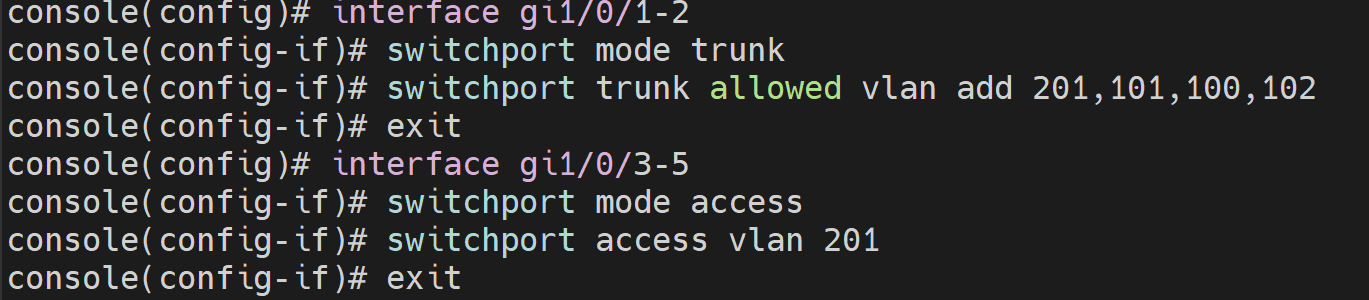


Рисунок № – Настройка магистральных и портов доступа на access-sw-2

Заканчивается настройка сети назначением адресов для удаленного доступа к коммутаторам, в VLAN 102, задача которого – обрабатывать трафик, связанный с управлением сетевого оборудования, серверов и если рассматривать физическую инфраструктуру, то и Out-Of-Band портов. Аналогично первому следует настроить остальной уровень доступа, включая серверный коммутатор.

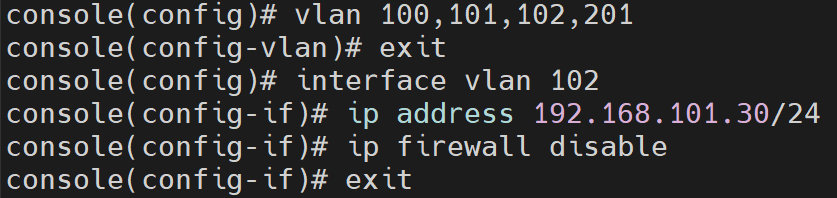


Рисунок № – Настройка IP-адреса управления на access-sw-0

После выполнения всех вышеописанных шагов процесс настройки сетевых устройств закончен.

# 2.4 Настройка серверных ОС

На рисунках № показан процесс стандартной базовой настройки. Сначала следует полностью зайти в root-пользователя, так как в процессе настройки отключится sudo, из-за манипуляций с именем устройства. Нужно установить требуемое имя устройства, обновить текущую оболочку. Проверить настройки можно командой hostnamectl. Далее стоит отключить сервис управления сетевыми интерфейсами – NetworkManager, так как он конфликтует с основным во многих дистрибутивах, а именно ifupdown2.



Рисунок № – Команды настройки и проверки изменений

В командах выше редактируется файл /etc/network/interfaces, в котором стоит описать сетевые реквизиты и прочие настройки для сетевых интерфейсов.

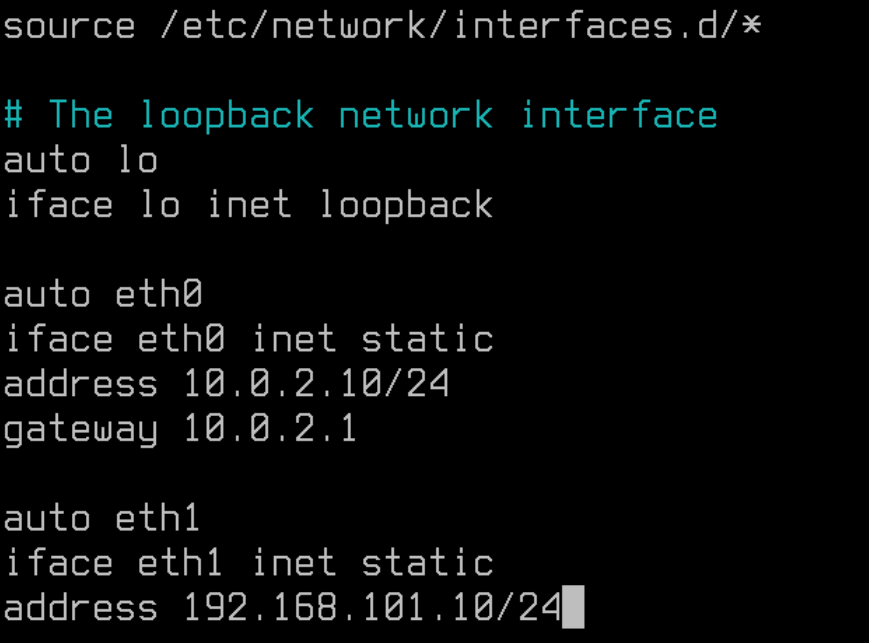


Рисунок № – Файл сетевых настроек устройства

Также в процессе был отредактирован файл /etc/hosts, который как раз таки и нарушал работу sudo. Чтобы все привести к рабочему виду, нужно указать соответствие нового полного доменного и короткого имени устройства на внешний адрес.

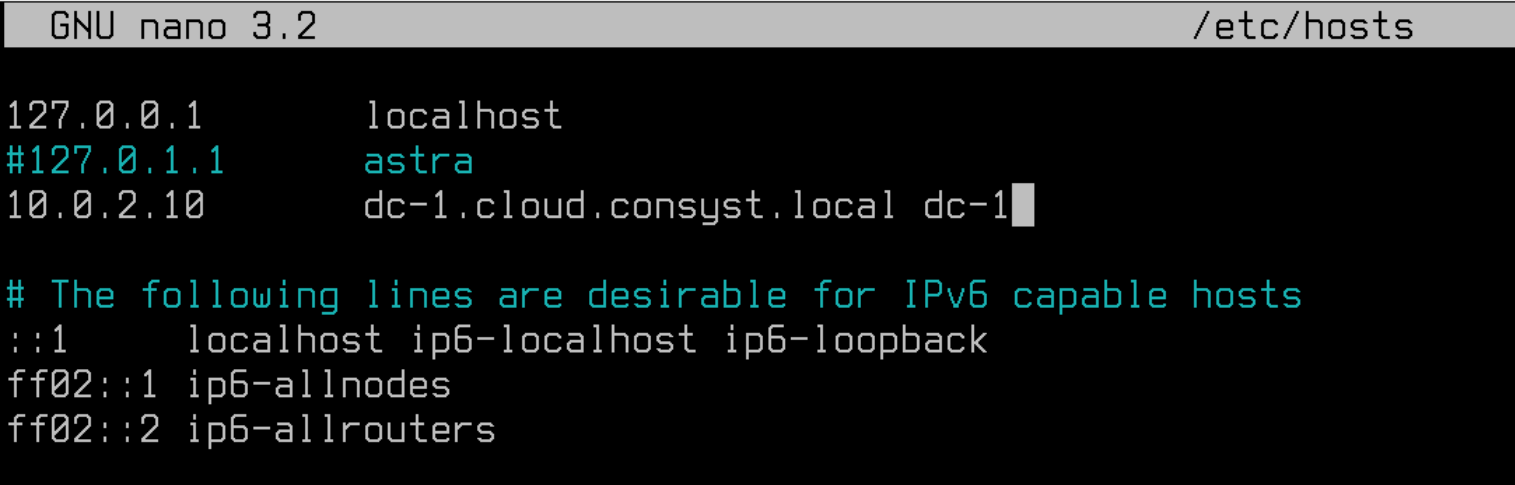


Рисунок № – Исправленный файл /etc/hosts

Сетевые настройки на машинах, ответственных за хранение данных будут немного отличаться. Так как между ними добавлено подключение, для него тоже следует указать свои реквизиты.

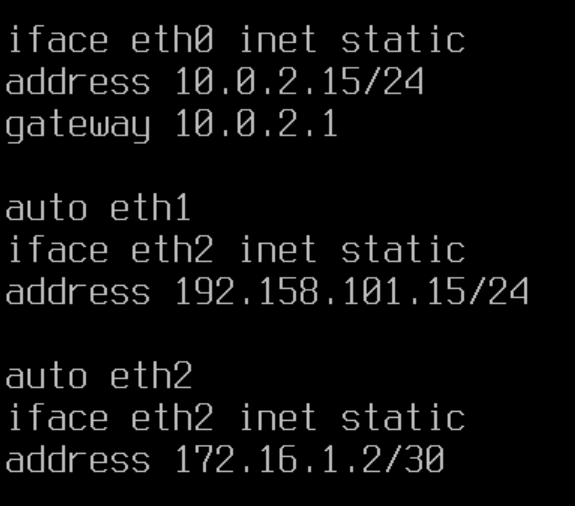


Рисунок № – Сетевые реквизиты на машинах хранения данных.

Все остальные устройства, работающие под управлением ОС Astra Linux 1.7 должны быть настроены аналогичным образом, но с учетом составленных физической и логической схем.

Настройки PVE

Настройка + включение SSH (Только MGMT)

# 2.5 Развертывание сервисов

- ЦС – + на видике

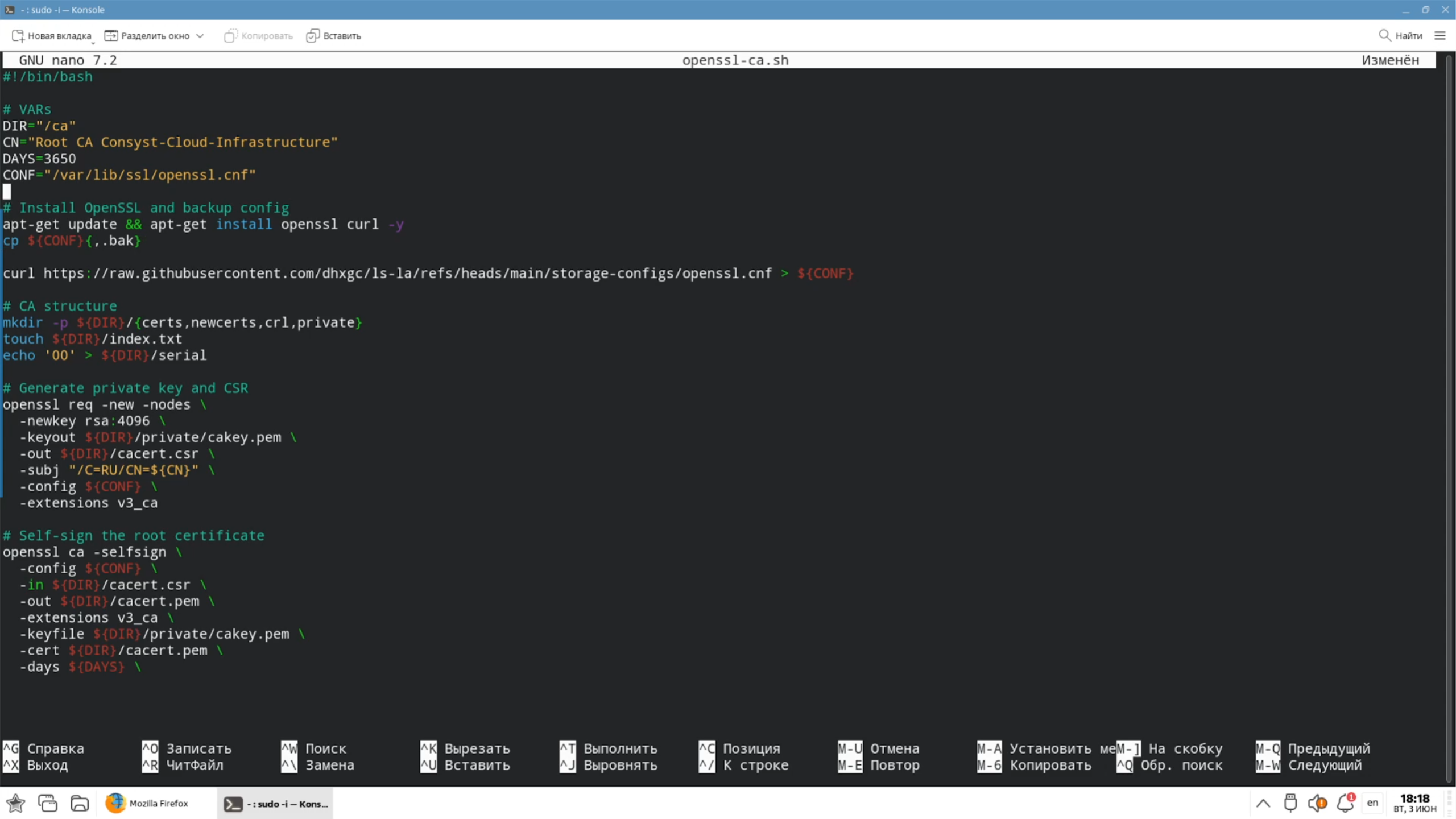


Рисунок № – Код скрипта

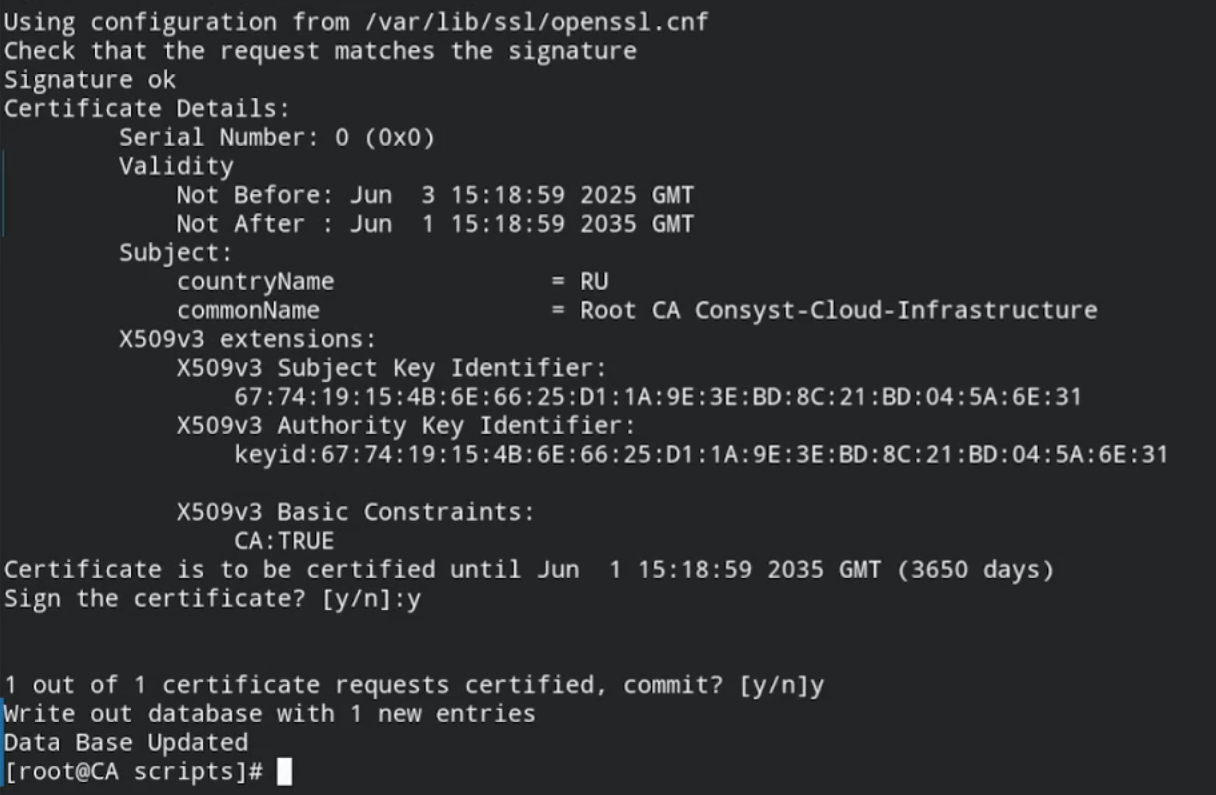


Рисунок № – Результат выполнения скрипта

- Выпуск сертов для сервисов

\* zabbix

\* kanboard

\* bookstack

- BookStack

- KanBoard

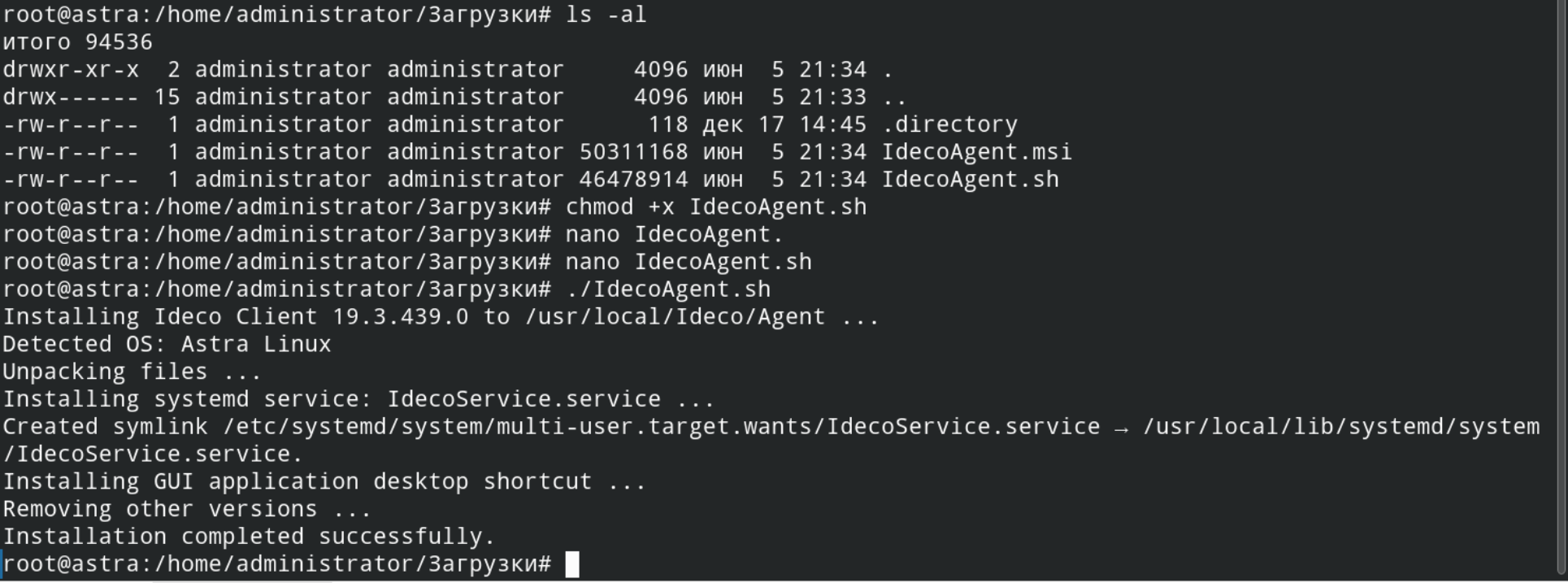
- ALD PRO, подсистемы

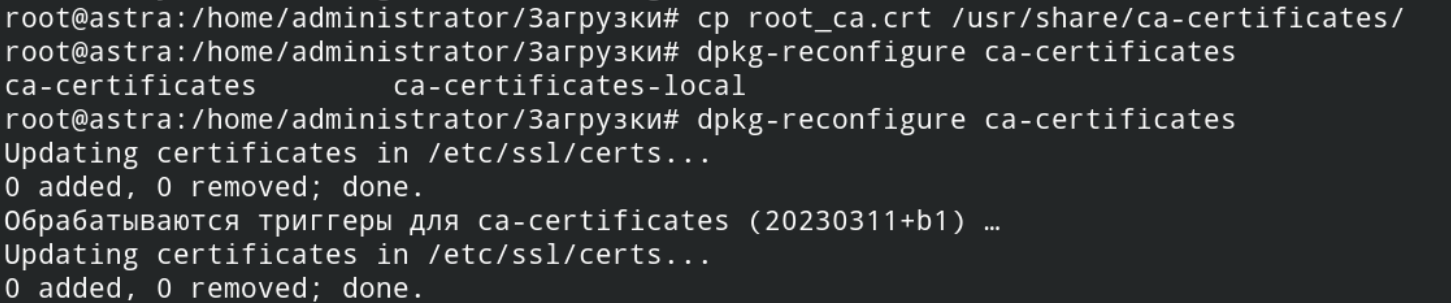
- Zabbix, хосты

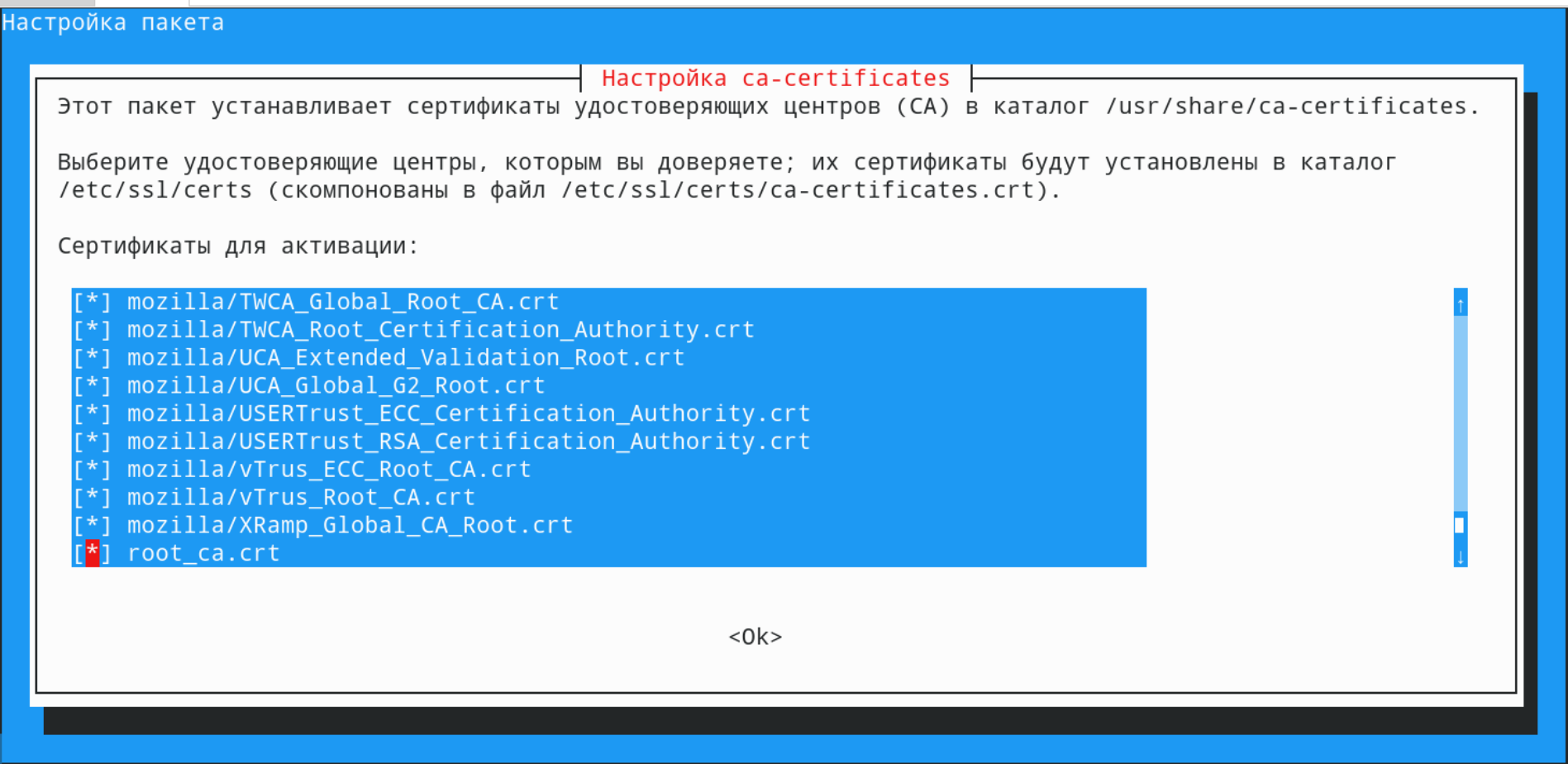
- DHCP

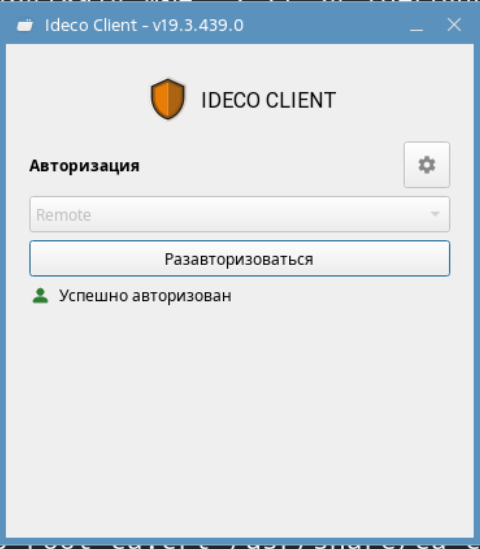
# 2.6 Настройка пользовательских ОС

- Удаленные клиенты









- Адресация, уровень защищенности

- Введение в домен, настройка сертов (+ на видике)

# 2.7 Проверка соответствия представленным и законодательным требованиям

Текст

### 3 Охрана труда и производственная санитария

Текст

# **Заключение**

Текст

# **Перечень сокращений и условных обозначений**

ГБ – гигабайт

ГГц - гигагерц

Ссылаюсь только на ГОСТ 2.32-2017 п. 6.15 «Перечень сокращений, условных обозначений, символов, единиц физических величин и определений должен располагаться столбцом без знаков препинания в конце строки. Слева без абзацного отступа в алфавитном порядке приводятся сокращения, условные обозначения, символы, единицы физических величин, а справа через тире - их детальная расшифровка.»

# **Список используемых источников**

Приведенный ниже список используемых источников выполнен исходя из ГОСТа Р.105-2019 п. 6.4.2 «Элемент «Библиография» размещают перед листом регистрации изменений. Выполнение элемента и ссылки на него в тексте — согласно требованиям к элементу «Список использованных источников» по ГОСТ 7.32.»

ГОСТ 7.32 п. 6.16 «Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте отчета и нумеровать арабскими цифрами с точкой и печатать с абзацного отступа.»

# Приложение А

(обязательное)

**Прайс-лист с ценами**