ЗАПРОС КОММЕРЧЕСКОГО И ТЕХНИЧЕСКОГО ПРЕДЛОЖЕНИЯ(RFP)

Цель запроса:

Поставка и внедрение системы безопасного удаленного доступа (VPN) и системы контроля доступа к сети
АО «Национальный Межбанковский Процессинговый Центр»

Разработал:
Директор департамента ИТ и Инфраструктуры: Холматов Н.
Согласовали:
Директор департамента ИБ: Гафуров. А

Ташкент, 2026г

Оглавление

Введение 3

1. Общая информация о проекте 3

2. Объем поставки и работ (Scope of Work) 3

3. Состав поставляемого оборудования 4

4. Общие требования к оборудованию и поставщику 4

5. Требования к архитектуре и отказоустойчивости 19

6. Требования к составу ответа (как поставщик должен оформить предложение) 21

7. Требования к коммерческому предложению (КП) 22

8. Требования к расчету совокупной стоимости владения (TCO) 22

9. Критерии оценки предложений 24

10. Требования к информационной безопасности поставляемого оборудования 25

11. Требования к приемке и вводу решения в эксплуатацию 26

12. Таблица соответствия техническим требованиям (Compliance Matrix) 27

13. Документация (исполнительная документация) 28

14. Требования к гарантийной и сервисной поддержке 29

15. Vendor Neutral Requirement 29

16. Формат и способ подачи предложения 30

17. Общие условия RFP (Disclaimers) 30

Введение

1. Общая информация о проекте

Акционерное общество «Национальный Межбанковский Процессинговый Центр» (далее — **Заказчик**) планирует модернизацию существующей инфраструктуры удаленного доступа пользователей.

Целью проекта является построение современной, безопасной и отказоустойчивой системы удаленного доступа пользователей к корпоративной сети, обеспечивающей:

- защищенный удаленный доступ пользователей;
- контроль доступа к сетевой инфраструктуре;
- соответствие требованиям информационной безопасности;
- централизованное управление политиками доступа.

В рамках проекта предполагается поставка, внедрение и интеграция:

- межсетевых экранов следующего поколения (NGFW);
- системы контроля доступа к сети (NAC);
- системы удаленного доступа пользователей (Remote Access VPN).

1.1 Исходные данные инфраструктуры Заказчика:

- у Заказчика 2 географически распределенных ЦОД;
- предполагается размещение 2 NGFW на каждой площадке в HA;
- существующая сетевая инфраструктура построена на оборудовании Cisco;
- требуется интеграция с AD/LDAP/RADIUS/SIEM;
- количество пользователей удаленного доступа — не менее 500;
- NAC — не менее 1000 одновременных подключений;
- виртуализация для NAC — VMware ESXi;
- требуется централизованное управление.

2. Объем поставки и работ (Scope of Work)

В рамках реализации проекта Поставщик должен обеспечить выполнение следующих работ и поставок:

• поставку активного сетевого оборудования в соответствии с требованиями настоящего RFP;

• монтаж, установку и подключение оборудования;

• интеграцию поставляемого оборудования с существующей сетевой инфраструктурой Заказчика;

• проведение пуско-наладочных работ (ПНР), включая настройку оборудования, тестирование и проверку работоспособности решения;

• ввод решения в промышленную эксплуатацию;

• подготовку и передачу Заказчику исполнительной документации.

Поставщик несет ответственность за корректную установку, настройку и функционирование поставляемого решения в соответствии с требованиями настоящего RFP и действующими отраслевыми стандартами.

3. Состав поставляемого оборудования

№	Описание	Ед. изм.	Количество
1	Система контроля доступа к сети (NAC)	шт.	2
2	Межсетевой экран следующего поколения (NGFW)	шт.	4

Примечание: предполагается построение отказоустойчивой инфраструктуры на базе двух географически распределенных центров обработки данных (ЦОД) Заказчика. Четыре единицы оборудования должны быть сконфигурированы в два кластера высокой доступности (HA) по схеме Active/Standby (по одному кластеру на площадку). Поставщик должен учесть данную архитектуру в своем предложении.

4. Общие требования к оборудованию и поставщику

4.1 Общие положения

Настоящий документ определяет технические требования к оборудованию и программным компонентам, предназначенным для модернизации системы безопасного удаленного доступа пользователей **АО «Национальный Межбанковский Процессинговый Центр».**

В рамках проекта предусматривается поставка, внедрение и интеграция следующих компонентов инфраструктуры информационной безопасности:

• межсетевые экраны следующего поколения (NGFW);

• система контроля доступа к сети (NAC);

Детальные технические требования к поставляемому оборудованию и программному обеспечению приведены в соответствующих разделах настоящего документа.

Технические требования представлены отдельно для каждого типа системы:

• Раздел 4.12 — Технические требования к системе контроля доступа к сети (NAC);

• Раздел 4.13 — Технические требования к межсетевым экранам следующего поколения (NGFW), включая функциональность организации защищенного удаленного доступа пользователей (Remote Access VPN).

Поставщик должен предложить оборудование, полностью соответствующее функциональным, техническим и эксплуатационным требованиям, указанным в настоящем документе.

Определения и сокращения

- Вендор — производитель оборудования.
- Поставщик — участник закупки, официальный партнёр Вендора.
- ПМИ – программа и методика испытания
- ПСИ – приемосдаточные испытания
- TAC — служба технической поддержки Вендора (Technical Assistance Center).
- RMA — процесс замены неисправного оборудования.
- NBD — следующий рабочий день.

4.2 Общие требования к оборудованию

1. Все поставляемое оборудование должно соответствовать следующим требованиям:

- оборудование должно быть **новым**, не бывшим в эксплуатации и не восстановленным (refurbished);
- оборудование не должно находиться в статусе End-of-Sale (EoS), End-of-Life (EoL) или End-of-Support на момент подачи предложения и в течение не менее 60 месяцев с момента ввода в эксплуатацию;
- производитель должен обеспечивать доступность **запасных частей, модулей и обновлений программного обеспечения** в течение не менее **5 лет** с момента ввода оборудования в эксплуатацию;
- оборудование должно поставляться через **официальные каналы производителя** и сопровождаться действующей гарантийной поддержкой;
- оборудование не должно быть снято с производства на момент подачи предложения.

Поставляемое оборудование должно обеспечивать построение единой, отказоустойчивой и масштабируемой инфраструктуры безопасного удаленного доступа.

Допускается использование оборудования одного или нескольких производителей при условии обеспечения полной функциональной совместимости компонентов решения, поддержки стандартных сетевых протоколов и технологий, а также возможности централизованного мониторинга и управления инфраструктурой. Участник закупки должен гарантировать корректную интеграцию всех компонентов предлагаемого решения и предоставить подтверждение совместимости используемого оборудования в составе предлагаемой архитектуры.

2. Оборудование должно быть оснащено **актуальной стабильной версией программного обеспечения, рекомендованной производителем для промышленной эксплуатации.**
3. Все программное обеспечение должно быть **лицензионным**.
4. Оборудование должно соответствовать международным стандартам и требованиям безопасности:
   - электромагнитной совместимости;
   - энергоэффективности;
   - экологической безопасности.
5. Поставщик должен выполнить комплекс работы по **поставке, установке и конфигурации оборудования**, включая интеграцию с существующей сетевой инфраструктурой Заказчика.
6. Оборудование должно обеспечивать возможность корректной интеграции с существующей инфраструктурой Заказчика, включая взаимодействие с системами каталогов пользователей (Active Directory / LDAP), системами централизованной аутентификации (RADIUS / TACACS+), системами централизованного мониторинга и анализа событий безопасности (SIEM) с использованием стандартных протоколов передачи событий (например, Syslog или API), а также поддерживать синхронизацию времени по протоколу NTP. Решение должно обеспечивать совместимость с используемым сетевым оборудованием Заказчика, включая коммутаторы Cisco, с использованием стандартных сетевых протоколов и технологий.
7. В состав поставки должны входить все необходимые лицензии для реализации заявленного функционала оборудования, включая:
   • функции межсетевого экрана уровня L3–L7;
   • систему предотвращения вторжений (IPS/IDS);
   • контроль приложений;
   • SSL/TLS инспекцию;
   • идентификацию пользователей;

• систему анализа угроз и репутационных сервисов;
• фильтрацию веб-ресурсов.
Срок действия лицензий должен составлять не менее 36 месяцев.

4.3 Требования к поставщику

1. Поставщик должен иметь статус официального или сертифицированного партнёра производителя предлагаемого оборудования, подтверждённый соответствующими документами.
2. Основным видом деятельности Поставщика должно являться предоставление услуг в области проектирования, внедрения и сопровождения:
   - телекоммуникационных решений;
   - сетевой инфраструктуры;
   - строительства или модернизации центров обработки данных (ЦОД).
3. Поставщик должен предоставить **официальное письмо авторизации (Authorization Letter)** от производителя предлагаемого оборудования, действительное на момент подачи предложения.
4. Поставщик должен обеспечить наличие авторизованной сервисной поддержки производителя на территории Республики Узбекистан либо через официального партнера производителя оборудования, обеспечивающей гарантийное обслуживание оборудования, диагностику, замену неисправных компонентов и выполнение обязательств по SLA.
5. Поставщик обязан обеспечить:
   - поставку оборудования;
   - монтаж и установку;
   - настройку и конфигурацию оборудования;
   - ввод оборудования в эксплуатацию.
6. Работы по внедрению должны выполняться квалифицированными инженерами, имеющими действующую сертификацию производителя по предлагаемому решению на уровне не ниже Professional либо на эквивалентном уровне, подтверждающем компетенции по внедрению и сопровождению предлагаемого решения.
7. По итогам внедрения Поставщик должен предоставить исполнительную документацию, включая:
   - логическую схему сети;
   - физическую схему подключения оборудования;
   - описание конфигурации оборудования и основных параметров настройки.
8. Поставщик должен обеспечить гарантийную техническую поддержку(замену оборудования) и сопровождение поставляемого оборудования в соответствии с требованиями настоящего RFP (включая требования разделов 4.4–4.5) сроком не менее **36 месяцев** с даты подписания акта ввода в эксплуатацию.
   Стоимость продления сервисной поддержки на 4-й и 5-й годы должна быть отдельно отражена в расчёте TCO, предоставляемом в составе коммерческого предложения.
9. В состав поставки должна входить следующая техническая документация:
   • паспорт оборудования или сертификат соответствия;

• руководство по установке и эксплуатации;
• схема коммутации оборудования;
• план адресации и сетевой архитектуры (по итогам ПНР);
• программа и методика испытаний (ПМИ);
• акт прохождения приемосдаточных испытаний (ПСИ);
• акт ввода оборудования в эксплуатацию.

4.4 Требования к лицензированию и комплектности

В состав поставки должны входить все необходимые лицензии для реализации заявленного функционала оборудования.

Лицензии должны обеспечивать функционирование следующих возможностей:
• межсетевой экран уровня L3–L7;
• систему предотвращения вторжений (IPS/IDS);
• контроль приложений;
• SSL/TLS инспекцию;
• идентификацию пользователей;
• систему анализа угроз и репутационных сервисов;
• фильтрацию веб-ресурсов.

Поставщик должен указать модель лицензирования (perpetual или subscription) и ограничения лицензий, включая:
• максимальную пропускную способность;
• количество одновременных сессий;
• количество VPN-подключений;
• количество интерфейсов или модулей.

4.5 Требования к технической поддержке и SLA

Поставщик должен обеспечить доступ к технической поддержке производителя оборудования (TAC).

Поддержка должна включать:
• регистрацию сервисных запросов;
• консультации по эксплуатации оборудования;
• обновления программного обеспечения;
• доступ к базе знаний производителя.

Время реакции службы технической поддержки должно соответствовать следующим уровням:

Severity 1 (критический инцидент) — не более 4 часов.

Severity 2 (деградация сервиса) — не более 8 часов.

Severity 3 (функциональные вопросы) — не более 12 часов.

При подтверждении неисправности оборудования должна применяться процедура замены оборудования (RMA).

Срок замены оборудования:
• критические компоненты — не позднее следующего рабочего дня (NBD);
• прочие компоненты — не более 5 рабочих дней.

4.6 Требования к обучению и передаче знаний

Поставщик должен провести обучение специалистов Заказчика по эксплуатации внедряемого решения.

Продолжительность обучения — не менее 24 академических часов.

Обучение должно включать:

• архитектуру решения;

• настройку политик безопасности;

• управление пользователями;

• мониторинг и анализ событий;

• резервное копирование и восстановление конфигурации.

4.7 Внедрение (ПНР) и приёмка

Проектные работы

Поставщик должен выполнить полный комплекс пуско-наладочных работ (ПНР), включая:

- монтаж и коммутацию оборудования;
- базовую и расширенную конфигурацию оборудования;
- интеграцию с системами аутентификации и управления доступом (AAA/AD/IdP);
- настройку синхронизации времени (NTP).

Приёмочные испытания

В рамках приёмосдаточных испытаний должны быть выполнены следующие тесты:

- проверка производительности оборудования (сквозная пропускная способность при включенных функциях IPS, Application Control и SSL/TLS инспекции) — показатели должны быть не ниже заявленных в техническом предложении поставщика;
- проверка функциональных сценариев:
  - отказ одного узла кластера HA;
  - отказ и восстановление сетевого соединения;
  - изменение политик безопасности;
  - генерация и обработка инцидента IPS;
  - проверка фильтрации веб-ресурсов;
- проверка резервного копирования и восстановления конфигурации.

По результатам испытаний оформляется **акт приёмки оборудования и протоколы тестирования**.

4.8 Требования по информационной безопасности

При внедрении оборудования должны соблюдаться требования информационной безопасности, включая:

- применение рекомендаций **CIS Benchmarks** или best practices производителя;
- отключение неиспользуемых сервисов;
- использование ролевой модели доступа (**RBAC**);
- ведение журналов событий безопасности;
- передачу логов в систему централизованного анализа событий (**SIEM**).

Передача исходных конфигураций, административных доступов и паролей должна осуществляться по акту передачи через защищённый канал.

4.9 Отчётность и KPI

Поставщик обязан предоставлять **ежемесячный отчёт** в период гарантийной поддержки, включающий:

- список открытых и закрытых сервисных кейсов;
- среднее время реакции и восстановления;
- статус обновлений программного обеспечения;
- загрузку ресурсов оборудования;
- информацию об инцидентах безопасности.

Целевые показатели качества обслуживания:

- соблюдение SLA реакции — **не менее 95 % случаев**;
- доступность сервисного центра — **не менее 99 % рабочего времени**.

4.10 Ответственность и штрафные санкции

- За нарушение сроков поставки или замены оборудования применяется штраф в размере **0,1 % от стоимости просроченной части поставки за каждый календарный день**, но не более **10 % от стоимости договора**.
- В случае несоблюдения SLA реакции по инцидентам уровня **P1 или P2** более двух раз в течение месяца может применяться штраф **1 % от стоимости договора за соответствующий месяц**.

4.11 Перечень подтверждающих документов в составе заявки

В составе конкурсной заявки поставщик должен предоставить:

1. подтверждение партнёрского статуса и письмо-авторизацию производителя на территории Республики Узбекистан;
2. сертификаты инженеров;
3. перечень реализованных проектов (референсы с контактами заказчиков);
4. гарантийное письмо о сроках EoS/EoL и доступности запасных частей;
5. описание сервисного центра в г. Ташкенте и наличие склада запасных частей;
6. шаблон SLA и регламент работы с TAC/RMA;
7. учебную программу курса и формат проведения обучения.

4.12 Технические требования к системе контроля доступа к сети (NAC)

Наименование требований	Технические требования
Количество	2 экземпляра
Тип продукта	Система контроля доступа к сети (Network Access Control, NAC)
Реализация	Система должна поддерживать развертывание в виде виртуальной машины на платформе виртуализации VMware ESXi
Управление	Управление системой должно осуществляться через встроенную WEB-консоль администрирования без необходимости установки дополнительного программного обеспечения для управления, мониторинга и формирования отчетности
Количество одновременных сессий	Система должна обеспечивать не менее 1000 одновременных пользовательских сессий / подключений

Отказоустойчивость	Система должна поддерживать отказоустойчивую схему развертывания 1+1 (Active/Standby) либо эквивалентную архитектуру высокой доступности
Контроль доступа	Система должна реализовывать функции контроля доступа к сети для проводного и беспроводного сегментов сети, а также для удаленных пользователей, подключающихся по технологии Remote Access VPN
Поддержка 802.1X	Система должна поддерживать работу согласно стандарту IEEE 802.1X и выполнять функции AAA (Authentication, Authorization, Accounting)
Поддержка RADIUS	Система должна поддерживать протокол RADIUS для аутентификации и авторизации пользователей и устройств
Поддержка RADIUS CoA	Система должна поддерживать механизм RADIUS Change of Authorization для динамического изменения уровня доступа пользователей
Поддержка EAP	Система должна поддерживать протоколы аутентификации EAP (EAP-TLS, PEAP, EAP-MSCHAPv2 или эквивалентные методы)
Пользовательская и машинная аутентификация	Система должна поддерживать одновременную аутентификацию пользователя и устройства (user + device authentication)
Использование сертификатов	Система должна поддерживать использование различных атрибутов сертификатов (CN, SAN, Serial Number, SAN-Email, SAN-DNS или эквивалентных) для идентификации пользователей
Локальная база пользователей	Система должна поддерживать локальную базу пользователей
Локальная база устройств	Система должна поддерживать локальную базу устройств на основе MAC-адресов
Интеграция с каталогами	Система должна поддерживать интеграцию с Active Directory или LDAP-совместимыми каталогами
Авторизация по группам	Система должна обеспечивать авторизацию пользователей на основе принадлежности к группам Active Directory
Приоритет источников аутентификации	Система должна поддерживать настройку последовательности проверки источников аутентификации
Обнаружение устройств	Система должна обеспечивать обнаружение и мониторинг подключающихся к сети конечных устройств
Предотвращение несанкционированного доступа	Система должна обеспечивать предотвращение несанкционированного доступа к сети
Назначение VLAN	Система должна поддерживать назначение VLAN-идентификаторов для пользователей и устройств

Назначение ACL	Система должна поддерживать применение списков контроля доступа (ACL)
Мониторинг и диагностика	Система должна обеспечивать наличие встроенных инструментов мониторинга и диагностики подключений
Проверка ОС	Система должна поддерживать проверку версии операционной системы пользовательского устройства
Проверка антивирусного ПО	Система должна поддерживать проверку наличия и состояния антивирусного программного обеспечения
Проверка приложений	Система должна поддерживать проверку наличия необходимых приложений
Проверка параметров безопасности	Система должна поддерживать проверку параметров системы и конфигурации безопасности
Количество проверяемых устройств	Система должна обеспечивать проверку не менее 1000 пользовательских устройств одновременно
Политики безопасности	Система должна поддерживать применение политик доступа в зависимости от статуса соответствия устройства требованиям безопасности
Определение типа устройства	Система должна поддерживать автоматическое определение типа подключаемого устройства
Определение ОС	Система должна поддерживать определение операционной системы подключаемого устройства
Определение версии ПО	Система должна поддерживать определение версии программного обеспечения подключаемого устройства
Совместимость	Система должна быть совместима с существующим сетевым оборудованием (коммутаторы, устройства безопасности, контроллеры беспроводной сети)
Используемые протоколы	Взаимодействие должно осуществляться с использованием стандартных сетевых протоколов
Интеграция с SIEM	Система должна поддерживать передачу событий безопасности во внешние системы мониторинга и анализа (SIEM или эквивалент)
Административный доступ	Система должна поддерживать аутентификацию и авторизацию администраторов при доступе к сетевому оборудованию
Поддержка Conditional Access	Система должна поддерживать применение политик условного доступа (Conditional Access) на основе атрибутов пользователя, устройства, способа аутентификации, сетевого сегмента и статуса соответствия устройства требованиям информационной безопасности.
Динамическое изменение уровня доступа	Система должна обеспечивать возможность динамического изменения уровня доступа пользователя или устройства по результатам аутентификации и проверки состояния устройства, включая полный, ограниченный, гостевой доступ либо отказ в доступе.

Контроль команд	Система должна обеспечивать возможность авторизации выполняемых команд на сетевом оборудовании
Журналирование	Система должна обеспечивать ведение журнала действий администраторов
Лицензирование	Лицензии на программное обеспечение должны быть предоставлены сроком не менее 36 месяцев
Сервисная поддержка	Сервисная поддержка производителя и/или авторизованного сервисного партнера должна быть предоставлена сроком не менее 36 месяцев
Совместимость с существующей инфраструктурой	*Предлагаемое решение должно обеспечивать совместимость и корректную работу с существующей сетевой инфраструктурой Заказчика. В инфраструктуре Заказчика используются коммутаторы Cisco. Решение должно поддерживать взаимодействие с оборудованием Cisco с использованием стандартных протоколов (включая 802.1X, RADIUS, SNMP, TACACS+, Syslog или эквивалентные механизмы).* ***Дополнительно: система NAC должна обеспечивать сбор расширенной информации о конечных устройствах (тип ОС, версия ОС, наличие и статус антивирусного ПО, наличие и статус межсетевого экрана) с использованием стандартных и/или вендорских механизмов интеграции сетевого оборудования (например, механизмы сбора телеметрии сетевого оборудования (Cisco Device Sensor или аналогичные механизмы других производителей)). Рассматривается как преимущество сбор информации без установки дополнительного агента на рабочую станцию пользователя.***
Интеграция с сетевым оборудованием	*Система должна поддерживать интеграцию с сетевыми коммутаторами для реализации функций контроля доступа к сети (802.1X, MAC Authentication Bypass, VLAN assignment, Dynamic ACL или эквивалентные механизмы).*

4.13 Технические требования к межсетевому экрану следующего поколения пользовательского сегмента сети.

Наименование требований	Технические требования
Кол-во	4 комплекта
Тип продукта	Межсетевой экран
Форм-фактор	Установка в стандартные 19" монтажные шкафы, должен занимать не более 1U.
Количество встроенных интерфейсов	Не менее 8 медных портов 1 Гбит/с RJ45 и не менее 4 оптических портов 1/10 Гбит/с SFP+ либо эквивалентная комбинация интерфейсов.
Порты управления	Наличие консольного порта управления (Serial console) — не менее 1. Management port 1Гбит/с RJ45– не менее 1шт.
Наличие USB 3.0 портов	Не менее 1 порта

Дисковый накопитель	Наличие встроенного накопителя ёмкостью не менее 400 ГБ (SSD, NVMe или эквивалентный тип энергонезависимой памяти) для хранения системных данных, журналов событий и сигнатур безопасности.
Требования к производительности межсетевого экрана.	Пропускная способность межсетевого экрана в режиме инспекции трафика не менее 13 Гбит/с. Пропускная способность межсетевого экрана в режиме инспекции трафика, контроля приложений и системы предотвращения вторжений не менее 9 Гбит/с Пропускная способность межсетевого экрана в режиме IPSec VPN не менее 13 Гбит/с Количество одновременных сессий не менее 400 000. Количество создаваемых новых сессий в секунду — не менее 50 000. Производительность инспекции TLS/SSL-трафика — не менее 2,5 Гбит/с.
Требования к функционалу межсетевого экрана.	Межсетевой экран следующего поколения должен обеспечивать следующий функционал: • **Поддержка механизма безопасной загрузки (Secure Boot)** либо эквивалентного механизма, предотвращающего запуск неоригинального программного обеспечения или несанкционированную модификацию прошивки устройства. • **Поддержка сервисов безопасности уровня NGFW**, включая: • контроль приложений (Application Control); • систему предотвращения вторжений (IPS/IDS); • фильтрацию веб-ресурсов (URL Filtering); • защиту от вредоносного программного обеспечения (Anti-Malware / Threat Prevention). • **Поддержка режимов работы**: • прозрачный режим (Transparent Mode); • режим маршрутизации (Routed Mode). • **Поддержка протоколов IPv4 и IPv6**, включая применение политик безопасности, контроля приложений, IPS и URL-фильтрации для трафика IPv6. • **Поддержка протоколов динамической маршрутизации**, включая: • OSPF; • BGP (версии 4 и 6). • **Поддержка механизма Bidirectional Forwarding Detection (BFD)** для повышения скорости обнаружения отказов маршрутов при использовании протокола BGP. • **Поддержка механизмов трансляции сетевых адресов (NAT)**: • статический NAT;

	• динамический NAT; • PAT (Port Address Translation). • **Поддержка механизма идентификации и классификации сетевых приложений (Application Control)** с возможностью распознавания не менее нескольких тысяч приложений. • **Возможность управления использованием приложений** на уровне отдельных пользователей или групп пользователей, включая интеграцию с внешними системами каталогов пользователей (например, Active Directory, LDAP или эквивалент). • **Поддержка классификации приложений** по уровню риска и категории использования. • **Поддержка механизмов управления полосой пропускания и качества обслуживания (QoS)**. • **Поддержка локального и централизованного управления**, включая: • управление непосредственно на устройстве; • управление через систему централизованного управления. • **Поддержка механизмов высокой доступности (High Availability)** в режиме Active/Standby либо эквивалентном режиме производителя. • **Поддержка Policy-Based Routing (PBR)** с возможностью контроля доступности маршрута. • **Поддержка виртуализации маршрутизации**, включая наличие не менее **10 независимых таблиц маршрутизации (VRF)**. • Поддержка интеграции с overlay-средами и современными механизмами сегментации (VXLAN, GENEVE или эквивалент) — при необходимости интеграции в существующую инфраструктуру Заказчика. • **Поддержка построения виртуальных частных сетей (VPN)** с количеством не менее **500 VPN-пиров (site-to-site peers)**. Решение должно поддерживать различные топологии site-to-site VPN, включая point-to-point, hub-and-spoke и mesh, а также поддерживать route-based VPN и/или иные функционально эквивалентные механизмы построения VPN. Поддержка policy-based VPN рассматривается как дополнительное преимущество. • **Поддержка Policy-based VPN** (без использования выделенных туннельных интерфейсов). • **Поддержка подключения VPN-узлов с динамическими IP-адресами**. • **Поддержка Route-based VPN**, включая использование статических и динамических туннельных интерфейсов.
Требования к построению виртуальных частных сетей удаленного доступа	Наличие клиента виртуальных частных сетей удаленного доступа с поддержкой операционных систем Windows, MacOS, Linux, Android и iOS.

	Поддержка передачи данных удаленных клиентов виртуальных частных сетей по протоколам IPSec-IKEv2, TLS и DTLS. Поддержка ограничения списка приложений, которым разрешен доступ к VPN на мобильных устройствах Android и iOS. Поддержка централизованной аутентификации пользователей с помощью имени и пароля по протоколам AD, LDAP, и RADIUS. Поддержка использования в политиках безопасности атрибутов пользователя, включая идентификатор пользователя, членство в группах и иные атрибуты, полученные от внешних систем аутентификации. Поддержка смены пользовательского пароля с истекшим сроком действия в процессе подключения. Поддержка аутентификации пользователей в режиме Single Sign-On по протоколу SAML 2.0. Поддержка аутентификации пользователей с помощью сертификатов. Поддержка одновременной аутентификации пользователей по паролю и с помощью сертификата. Поддержка одновременной аутентификации пользователей через SAML SSO и с помощью сертификата. Поддержка одновременной аутентификации пользователей и устройств по нескольким сертификатам. Поддержка многофакторной аутентификации пользователей. Поддержка балансировки нагрузки между несколькими узлами виртуальной частной сети удаленного доступа. Поддержка механизма выборочной маршрутизации трафика удалённых пользователей (Split Tunneling), в том числе на основе доменных имен (DNS/FQDN) или эквивалентных механизмов. Поддержка централизованного управления настройками VPN-клиента и параметрами подключения удалённых пользователей. Поддержка гибкой настройки атрибутов LDAP для авторизации пользователей. Поддержка назначения клиентского адреса сервером RADIUS. Поддержка динамического назначения профиля доступа по атрибуту от сервера RADIUS. Поддержка назначения пользователю, загружаемого с сервера RADIUS списка контроля доступа. Поддержка динамического изменения авторизации пользователя и механизма RADIUS Change of Authorization (RADIUS CoA). Поддержка динамических политик контроля доступа по результатам проверки рабочей станции на

	соответствие политике информационной безопасности. ***Если для реализации функции удаленного доступа требуется лицензирование пользователей, Поставщик должен предусмотреть лицензии не менее чем на 500 уникальных пользователей удаленного доступа. Лицензии на пользователей удаленного доступа должны предоставляться по постоянной модели лицензирования (perpetual). Подписочная (subscription-only) модель лицензирования пользователей удаленного доступа не допускается. Подписка на обновления программного обеспечения, обновления безопасности и техническую поддержку должна быть предусмотрена сроком не менее 36 месяцев.***
Поддержка сервисов репутации и анализа угроз	Межсетевой экран должен обеспечивать возможность передачи событий безопасности, журналов активности пользователей, сетевых сессий и событий системы предотвращения вторжений во внешние системы мониторинга и анализа безопасности (SIEM/SOC) с использованием стандартных протоколов (например, Syslog, API или эквивалентных механизмов). Должна поддерживаться возможность передачи логов в режиме реального времени.
Поддержка инспекции зашифрованного трафика (TLS/SSL Inspection)	Межсетевой экран должен поддерживать возможность расшифровки и анализа TLS/SSL-трафика (SSL Inspection) для применения функций безопасности, включая IPS, контроль приложений и фильтрацию веб-ресурсов. Система должна поддерживать: • расшифровку входящего и исходящего TLS/SSL-трафика; • использование корпоративного сертификата для расшифровки пользовательского трафика; • возможность исключения доверенных ресурсов из инспекции; • применение политик безопасности к расшифрованному трафику.
Threat Intelligence / Reputation	Межсетевой экран должен поддерживать использование сервисов репутации IP-адресов, доменов и URL-ресурсов, предоставляемых производителем оборудования или его облачными сервисами. Система должна обеспечивать возможность автоматического обновления баз угроз, сигнатур атак и репутационных баз данных.
Требования к системе централизованного управления.	Возможность анализа сетевых сессий и содержимого трафика в объеме, необходимом для расследования событий безопасности, в пределах функциональных возможностей системы.

	Встроенные механизмы создания пользовательских отчетов произвольного содержания по событиям, содержащимся в базе данных. Возможность быстрого формирования отчетов на основе настраиваемых информационных панелей и шаблонов. Поддержка различных форматов выгрузки отчетов (PDF, HTML, CSV). Возможность произвольного поиска по базе данных событий. Возможность создания и сохранения пользовательских шаблонов поиска. Поддержка ролевой модели управления доступом к системе централизованного управления. Возможность интеграции с внешними системами аутентификации (RADIUS, LDAP, AD). Поддержка открытых API для взаимодействия внешних систем с системой централизованного управления. Единая платформа централизованного управления сервисами межсетевого экрана, системы предотвращения вторжений, контроля приложений, фильтрации веб-запросов пользователей по URL, платформы для предотвращения проникновения вредоносного кода. Поддержка взаимодействия со сторонними системами в результате корреляции различных условий (возможность инициировать действие в сторонней системе как результата корреляции различных условий). Возможность экспорта и доступа к данным событий через API, системные интерфейсы или другие механизмы интеграции.
Дополнительные требования к сервисам обеспечения информационной безопасности.	Требования к сервису предотвращения вторжений Сервис предотвращения вторжений должен обеспечивать анализ сетевых устройств, сервисов и сетевого трафика для повышения точности обнаружения угроз. Сервис предотвращения вторжений должен поддерживать механизмы корреляции событий безопасности. Сервис предотвращения вторжений должен поддерживать приоритизацию событий безопасности с учетом контекста защищаемой среды. Сервис предотвращения вторжений должен обеспечивать выявление признаков компрометации устройств или сетевых сегментов на основе анализа нескольких событий безопасности. Сервис предотвращения вторжений должен обеспечивать возможность формирования рекомендаций по настройке политик безопасности или применения эквивалентных механизмов

	повышения эффективности защиты. Сервис предотвращения вторжений должен поддерживать задание белых списков устройств, операционных систем, приложений и сервисов. Сервис предотвращения вторжений должен поддерживать возможность задания правил корреляции событий. Сервис предотвращения вторжений должен поддерживать возможность инициирования действий внешними системами на основании правил корреляции. Сервис предотвращения вторжений должен поддерживать API для интеграции и получения дополнительной информации об оконечных устройствах из внешних источников. Сервис предотвращения вторжений должен поддерживать возможность просмотра и редактирования существующих правил и сигнатур. Сервис предотвращения вторжений должен поддерживать возможность создания пользовательских сигнатур и правил обнаружения вторжений на основе открытых или документированных форматов сигнатур. Сервис предотвращения вторжений должен поддерживать автоматическую загрузку и обновление черных и белых списков IP-адресов, URL-адресов и DNS-имен из источников производителя и пользовательских источников. Сервис предотвращения вторжений должен поддерживать механизм перенаправления DNS-запросов к вредоносным доменам (DNS sinkhole или эквивалентный механизм). **Требования к сервису защиты от вредоносного программного обеспечения** Возможность повторного анализа ранее переданных файлов при обновлении сигнатур угроз. Возможность формирования политик безопасности на уровне типов файлов. Использование нескольких методов обнаружения вредоносного кода (сигнатурный анализ, поведенческий анализ, репутационные сервисы и иные методы), а также возможность использования облачных сервисов анализа угроз или эквивалентных механизмов. Возможность отслеживания распространения файлов и связанных событий безопасности в пределах защищаемой инфраструктуры. Возможность регистрации, хранения и последующего анализа файлов с различным уровнем доверия и статусом проверки. Возможность выявления источника и точки

	первоначального появления вредоносного программного обеспечения в защищаемой инфраструктуре.
Подписка на обновление сигнатур сервисов предотвращения вторжений, защиты от вредоносного программного обеспечения и фильтрации веб-ресурсов	Не менее 36 месяцев
Сервисная поддержка	Не менее 36 месяцев
Требования к резервному копированию	Оборудование (NGFW) и система централизованного управления должны поддерживать автоматическое резервное копирование конфигурации по расписанию на внешний SFTP/SCP-сервер. Должна быть предусмотрена возможность восстановления конфигурации на устройство (включая процедуру восстановления "с нуля" на новое устройство RMA) без участия инженеров Поставщика/Вендора (на основе инструкции).

5. Требования к архитектуре и отказоустойчивости

Предлагаемое решение должно обеспечивать построение отказоустойчивой, масштабируемой и географически распределенной инфраструктуры безопасности, соответствующей требованиям Заказчика по обеспечению непрерывности сервисов.

5.1. Общие архитектурные принципы

Предлагаемое решение должно соответствовать следующим принципам:

- **Отсутствие единой точки отказа (SPOF).** Архитектура решения не должна содержать единых точек отказа. Отказ любого отдельного компонента оборудования (блок питания, вентилятор, интерфейсный модуль и т.п.) либо отказ целого узла (сервер, сетевое устройство, межсетевой экран) не должен приводить к полной недоступности сервисов безопасности.
- **Резервирование ключевых компонентов.** Все критически важные компоненты инфраструктуры безопасности должны быть зарезервированы. Для межсетевых экранов нового поколения (NGFW) обязательно наличие отказоустойчивой схемы эксплуатации в режиме **Active/Standby** или **Active/Active** с обязательным описанием выбранного режима работы.
- **Масштабируемость.** Архитектура решения должна обеспечивать возможность горизонтального и вертикального масштабирования: увеличение производительности, добавление новых узлов, расширение кластеров, а также подключение дополнительных площадок без существенного изменения логической схемы и без длительной остановки сервисов.
- **Непрерывность работы.** Решение должно обеспечивать непрерывность функционирования сервисов безопасности при отказе отдельных компонентов оборудования и/или отдельных узлов.

5.2. Требования к распределенной архитектуре (Multi-DC)

С учетом наличия у Заказчика двух географически распределенных центров обработки данных (ЦОД) предлагаемое решение должно соответствовать следующим требованиям:

- **Независимость кластеров по площадкам.** На каждой площадке ЦОД должен быть развернут собственный отказоустойчивый кластер NGFW, способный функционировать независимо от кластера другой площадки. Плановые работы, деградация сервиса или отказ оборудования на одной площадке не должны влиять на работоспособность кластера на другой площадке.
- **Корректная работа при асимметричной маршрутизации.** Решение должно предусматривать возможность обработки сценариев асимметричного прохождения трафика между площадками и обеспечивать корректную работу Stateful Inspection в таких условиях. Необходимо описать, каким образом решение обрабатывает трафик, входящий через одну площадку и выходящий через другую, включая применяемые механизмы: синхронизацию состояния сессий, особенности маршрутизации, ограничения и рекомендуемую топологию.
- **Синхронизация состояний сессий.** Поставщик должен явно описать механизм синхронизации состояний сессий (session state) между узлами кластера в пределах площадки, а также, при наличии такой возможности, между площадками. Если межплощадочная синхронизация состояний архитектурой решения не поддерживается, Поставщик обязан предложить альтернативные сценарии обеспечения непрерывности пользовательских и прикладных сессий при переключении на резервную площадку.
- **Централизованное управление.** Решение должно обеспечивать централизованное управление всей распределенной инфраструктурой безопасности из единой консоли, включая управление политиками безопасности, объектами, журналированием, обновлениями и мониторингом для всех устройств и кластеров с учетом различий между площадками (адресные пространства, VRF, локальные маршруты, локальные политики и иные параметры).

5.3. Требования к составу архитектурного предложения

В составе технического предложения Поставщик должен предоставить:

- архитектурную схему предлагаемого решения в логическом и физическом представлении (logical diagram и physical diagram) отдельно по каждой площадке ЦОД;
- описание ролей каждого элемента инфраструктуры, межсоединений и логики обеспечения отказоустойчивости;
- схемы прохождения трафика (flow diagrams) для следующих сценариев:
    - штатный режим работы;
    - отказ одного узла внутри кластера;
    - отказ одной площадки целиком;
    - возврат в штатный режим после восстановления.

5.4. Минимальные требования к отказоустойчивости

- **HA-кластеризация.** На каждой площадке должен быть реализован отказоустойчивый кластер NGFW с автоматическим переключением (failover) при отказе активного узла.
- **Минимизация разрыва сессий.** Время переключения на резервный узел не должно приводить к существенному нарушению работы критичных приложений и

сервисов. Поставщик должен указать ожидаемое время переключения и отдельно описать влияние переключения на уже установленные сессии, включая TCP/UDP-соединения, VPN-туннели и иные критичные сервисы. Рекомендуемое целевое время переключения — **не более 10–30 секунд**, если иное не обосновано архитектурой решения.

- **Механизмы обнаружения отказов.** Поставщик должен описать применяемые механизмы обнаружения отказа и инициирования переключения, включая, при наличии, **BFD, link monitoring, path monitoring, hello/heartbeat messages** и иные используемые средства.
- **Сохранение сервисов безопасности при отказах.** Работа основных сервисов безопасности, включая межсетевое экранирование, IPS/IDS, VPN и иные заявленные функции, должна сохраняться при отказе отдельных аппаратных компонентов, а также при отказе одного узла кластера.
- **Отказоустойчивость по питанию и интерфейсам.** Оборудование должно поддерживать резервирование по питанию и отказоустойчивость сетевых подключений в соответствии с рекомендуемой производителем архитектурой.

5.5. Требования к пояснениям со стороны Поставщика

Поставщик в явном виде должен указать в техническом предложении:

- поддерживается ли межплощадочная синхронизация session state;
- допускается ли работа решения в условиях асимметричной маршрутизации без потери stateful-функциональности;
- какие ограничения имеются у предлагаемой архитектуры;
- требуется ли использование дополнительных компонентов, лицензий или выделенных каналов связи для реализации отказоустойчивости и централизованного управления;
- какие действия потребуются от Заказчика для эксплуатации и сопровождения решения в двух ЦОД.

6. Требования к составу ответа (как поставщик должен оформить предложение)

Поставщик должен предоставить два отдельных документа:

- **Техническое предложение;**
- **Коммерческое предложение.**

6.1 Техническое предложение

Должно включать:

- описание предлагаемой архитектуры решения и состава оборудования;
- подтверждение соответствия требованиям настоящего RFP (см. Compliance Matrix);
- описание используемых лицензий, подписок и сервисов производителя;
- план внедрения (этапы, сроки, последовательность работ и зависимости);
- требования к инфраструктуре площадки (стойки, питание, охлаждение, кабельная инфраструктура — при необходимости);
- перечень допущений/ограничений (если есть);
- архитектурную схему предлагаемого решения (logical и physical diagram);
- описание механизмов отказоустойчивости и обеспечения высокой доступности;
- описание требований к эксплуатации и администрированию решения.

Поставщик должен предоставить календарный план реализации проекта с указанием сроков поставки, ПНР, тестирования, обучения и ввода в промышленную эксплуатацию.

6.2 Коммерческое предложение (КП)

Коммерческое предложение предоставляется отдельно от технического предложения и оформляется в соответствии с требованиями раздела 7 настоящего RFP.

Коммерческое предложение не должно содержать технических параметров, влияющих на оценку соответствия техническим требованиям.

7. Требования к коммерческому предложению (КП)

Коммерческое предложение должно включать:

- спецификацию оборудования (Bill of Materials, BoM) с количеством, артикулами, лицензиями и сроками поставки;
- стоимость оборудования, лицензий, подписок, работ по внедрению и сервисной поддержки (отдельными строками);
- условия оплаты;
- срок действия коммерческого предложения (не менее 60 календарных дней);
- все стоимости должны быть указаны с явным указанием валюты, наличия или отсутствия НДС а также условий поставки (INCOTERMS — при необходимости);
- сроки поставки оборудования.

Коммерческое предложение предоставляется отдельно от технического предложения.

8. Требования к расчету совокупной стоимости владения (TCO)

Поставщик обязан предоставить расчет совокупной стоимости владения (Total Cost of Ownership, TCO) для предлагаемого решения с учетом всех затрат, необходимых для приобретения, внедрения, эксплуатации и сопровождения решения.

В расчет TCO должны быть включены все лицензии, подписки, сервисы и иные компоненты, необходимые для корректной эксплуатации решения в соответствии с требованиями настоящего RFP.

Расчет TCO должен быть представлен на два периода эксплуатации:

- 3 года эксплуатации
- 5 лет эксплуатации

Цель расчета TCO — предоставить Заказчику полную оценку всех затрат, связанных с приобретением, внедрением, эксплуатацией и сопровождением предлагаемого решения.

Все значения TCO должны быть указаны с явным указанием валюты расчётов и наличия или отсутствия НДС.

Поставщик должен представить расчет TCO **в табличной форме с разбивкой по годам эксплуатации.**

8.1 Состав TCO

Расчет TCO должен включать следующие категории затрат:

Капитальные затраты (CAPEX)

- стоимость поставляемого оборудования;
- стоимость базовых лицензий (если применимо);
- стоимость модулей, трансиверов, кабелей и иных компонентов;
- стоимость работ по внедрению и настройке оборудования;

- стоимость обучения специалистов Заказчика (при наличии);
- стоимость поставки и логистики оборудования (при наличии);
- стоимость дополнительных аппаратных модулей и интерфейсов (если применимо).

Операционные затраты (OPEX)

- стоимость подписок на сервисы информационной безопасности (IPS, Anti-Malware, URL Filtering, Sandbox или эквивалентные сервисы);
- стоимость лицензий и подписок на программное обеспечение;
- стоимость продления лицензий и подписок;
- стоимость сервисной поддержки поставщика;
- стоимость технической поддержки производителя;
- стоимость продления технической поддержки производителя (при необходимости).

8.2 Требования к расчету TCO

Расчет TCO должен:

- учитывать все расходы, необходимые для полноценной эксплуатации решения;
- учитывать стоимость продления лицензий и подписок после окончания первоначального срока действия;
- включать стоимость лицензий и подписок, необходимых для выполнения требований настоящего RFP;
- быть представлен в виде **структурированной таблицы**;
- содержать итоговую стоимость владения на 3 и 5 лет.

8.3 Формат предоставления TCO

Расчет TCO должен быть предоставлен в формате Excel с возможностью редактирования формул и проверки структуры расчета.

Поставщик обязан явно указать срок действия лицензий и подписок, включенных в состав предложения.

Категория затрат	Ед. изм.	К-во	Стоимость за единицу (валюта)	CAPEX	OPEX (год)	Итого 3 года	Итого 5 лет	Комментарий
Оборудование								
Лицензии								
Подписки безопасности (по типам по строкам)								
Поддержка производителя								
Внедрение и настройка								
Обучение								

В случае если срок действия лицензий или подписок отличается от 3 или 5 лет, поставщик обязан указать стоимость их продления.

Поставщик должен указать итоговую совокупную стоимость владения (TCO) для предлагаемого решения на горизонте 3 и 5 лет эксплуатации.
Все расходы, необходимые для корректной работы предлагаемого решения, должны быть включены в расчет TCO. Дополнительные платежи, не указанные в коммерческом предложении, не допускаются.

9. Критерии оценки предложений

Оценка предложений участников осуществляется на основании анализа технических и коммерческих параметров предложенного решения.

Критерий	Описание	Вес
Соответствие техническим требованиям	Полнота и корректность соответствия предлагаемого решения требованиям настоящего RFP	50 %
Совокупная стоимость владения (TCO)	Общая совокупная стоимость владения решением на период 3 и 5 лет эксплуатации	30 %
Опыт поставщика	Наличие опыта реализации аналогичных проектов	10 %
Сроки поставки и внедрения	Сроки поставки оборудования и внедрения	10 %

Минимальный проходной балл, по технической оценке, составляет 80%

9.1 Техническая оценка

На первом этапе проводится анализ технических предложений участников.

Предложения, не соответствующие ключевым техническим требованиям настоящего RFP, могут быть отклонены на этапе технической оценки.

К ключевым техническим требованиям, в частности, относятся требования по:

- построению отказоустойчивой архитектуры NGFW на каждой площадке ЦОД;
- наличию централизованной системы управления;
- поддержке защищенного удаленного доступа пользователей (Remote Access VPN);
- интеграции с системами аутентификации (Active Directory / LDAP / RADIUS или эквивалентными механизмами);
- возможности передачи журналов и событий безопасности во внешние системы мониторинга и анализа (SIEM / Syslog / API или эквивалентными механизмами);
- совместимости с существующей сетевой инфраструктурой Заказчика;
- наличию лицензий и сервисной поддержки сроком не менее 36 месяцев;
- предоставлению таблицы соответствия техническим требованиям (Compliance Matrix).

Поставщик обязан предоставить таблицу соответствия техническим требованиям (Compliance Matrix) в соответствии с требованиями настоящего RFP.

9.2 Коммерческая оценка

К коммерческой оценке допускаются только предложения, получившие статус **«Соответствует»** по ключевым техническим требованиям.
На втором этапе проводится анализ коммерческих предложений участников, включая:

- стоимость оборудования;
- стоимость лицензий;
- стоимость внедрения;

- стоимость технической поддержки;
- расчет ТСО.

9.3 Право Заказчика

Заказчик оставляет за собой право:

- запросить дополнительные разъяснения;
- провести переговоры с участниками;
- запросить демонстрацию решения;
- отклонить любое предложение в соответствии с внутренними процедурами Заказчика.

9.4 Методика оценки определяется Заказчиком.

При этом:

- по критерию “Соответствие техническим требованиям” оценивается полнота и достоверность соответствия **предлагаемого решения** требованиям настоящего RFP, подтвержденная официальной документацией производителя;
- по критерию “Совокупная стоимость владения (ТСО)” преимущество получает предложение с наименьшей совокупной стоимостью владения на горизонте 5 лет при условии соответствия ключевым техническим требованиям;
- по критерию “Опыт поставщика” оценивается подтвержденный опыт реализации аналогичных проектов, сопоставимых по масштабу и сложности;
- по критерию “Сроки поставки и внедрения” оценивается общий срок поставки оборудования, выполнения работ по внедрению и ввода решения в промышленную эксплуатацию (go-live).

В случае равенства итоговых баллов преимущество получает предложение с наименьшей совокупной стоимостью владения (ТСО).

10. Требования к информационной безопасности поставляемого оборудования

Поставляемое оборудование должно соответствовать требованиям информационной безопасности Заказчика, а также современным отраслевым практикам обеспечения безопасности сетевой инфраструктуры.

Оборудование должно обеспечивать следующие механизмы защиты:

• защиту целостности программного обеспечения устройства (Secure Boot либо эквивалентный механизм);

• защиту от несанкционированного изменения или подмены программного обеспечения и прошивки устройства;

• возможность обновления программного обеспечения только из официальных источников производителя;

• наличие механизма проверки подлинности и цифровой подписи обновлений программного обеспечения;

• поддержку безопасного процесса обновления программного обеспечения (secure upgrade);

При отсутствии документального подтверждения в официальной документации производителя соответствующее требование может считаться неподтвержденным.

Ответы вида

«Поддерживается»;

«Будет поддерживаться»;

«Аналогичная функция»;

без пояснения способа реализации, ограничений, лицензионных условий и ссылок на документацию производителя **не допускаются**.

В случае если требование поддерживается частично, поставщик обязан подробно описать:

• ограничения;

• условия реализации;

• необходимые лицензии или дополнительные компоненты.

12.3 Основания для отклонения предложения

Предложение участника может быть отклонено на этапе технической оценки в следующих случаях:

- отсутствие таблицы соответствия;
- неполное заполнение таблицы;
- отсутствие ссылок на документацию производителя;
- указание недостоверной информации;
- предоставление неполной или вводящей в заблуждение информации.

13. Документация (исполнительная документация)

Поставщик обязан предоставить комплект документации по результатам поставки и внедрения, включая:

- логическую схему сети;
- описание архитектуры решения;
- физическую схему подключения оборудования;
- таблицу используемых IP-адресов, VLAN и сетевых сегментов (при наличии в проекте);
- описание конфигурации оборудования и резервные копии конфигураций устройств;
- инструкции по эксплуатации и базовым операциям администрирования.

Документация должна отражать **фактически внедренное решение (as-built documentation).**

Формат предоставления документации

Документация должна быть предоставлена:

• в электронном виде (PDF / Word);

• в виде исходных редактируемых файлов схем (Visio, draw.io или эквивалентный формат);

• в виде файлов конфигурации оборудования (при наличии).

Сроки предоставления документации

Исполнительная документация должна быть передана Заказчику **не позднее даты приемки выполненных работ**, если иное не согласовано сторонами.

Требования к соответствию документации

Конфигурационные файлы, резервные копии конфигураций, схемы и инструкции должны:

• полностью соответствовать фактически внедренному решению;

• отражать текущую конфигурацию оборудования на момент передачи решения в промышленную эксплуатацию;

• быть достаточными для последующей эксплуатации и администрирования системы.

14. Требования к гарантийной и сервисной поддержке

Поставщик должен обеспечить гарантийную и сервисную поддержку поставляемого оборудования в соответствии с требованиями настоящего RFP:

- базовая гарантийная поддержка на аппаратную часть оборудования — **не менее 36 месяцев**;
- сервисная поддержка производителя и/или авторизованного сервисного партнера — **не менее 36 месяцев**;

в течение срока действия гарантии и/или подписок должны быть доступны:

- обновления программного обеспечения;
- обновления сигнатур безопасности (при наличии соответствующих сервисов);
- исправления выявленных уязвимостей и критических ошибок;
- минимальный уровень сервисного обслуживания — **8×5, NBD (Next Business Day)**, включая реакцию на инцидент и замену неисправного оборудования на следующий рабочий день либо эквивалентный уровень сервиса производителя;
- поставщик должен обеспечить возможность регистрации сервисных обращений (TAC / Service Desk) и взаимодействия с технической поддержкой производителя.

Продление сервисной поддержки

Стоимость продления сервисной поддержки и подписок на **4-й и 5-й годы эксплуатации** должна быть отражена:

• в коммерческом предложении;

• в расчете совокупной стоимости владения (**TCO**).

Поставщик должен гарантировать возможность продления сервисной поддержки и подписок для обеспечения эксплуатации оборудования и доступности запасных частей **в течение не менее 5 лет**, в соответствии с требованиями настоящего RFP.

15. Vendor Neutral Requirement

Настоящий RFP является **вендорно-независимым**.

Поставщик может предложить оборудование любого производителя при условии полного соответствия функциональным, техническим и эксплуатационным требованиям настоящего RFP.

Допускается использование оборудования **одного или нескольких производителей**, при условии обеспечения:

• полной функциональной совместимости компонентов решения;

• поддержки стандартных сетевых протоколов и технологий;

• возможности централизованного мониторинга и управления инфраструктурой;

• корректной интеграции всех компонентов решения.

Указание конкретных технологий, протоколов или архитектурных подходов в настоящем документе используется **исключительно для описания требуемого функционала**.

Допускается предоставление **эквивалентных решений**, при условии подтверждения их соответствия и функциональной сопоставимости требованиям настоящего RFP.

Поставщик несет полную ответственность за:

• корректную интеграцию всех компонентов предлагаемого решения;

• совместную работу оборудования различных производителей (при их использовании);

• соответствие предлагаемого решения требованиям настоящего RFP.

16. Формат и способ подачи предложения

Предложения участников должны быть предоставлены **в электронном виде**.

В состав предложения должны входить следующие документы:

Техническое предложение

• формат: **PDF**

• дополнительно допускается предоставление редактируемой версии (**Word**)

Коммерческое предложение (КП)

• формат: **PDF**

• расчетные таблицы и спецификации должны быть предоставлены в формате **Excel**

Таблица соответствия техническим требованиям (Compliance Matrix)

• формат: **Excel** (обязательно)

Расчет совокупной стоимости владения (TCO)

• формат: **Excel** (обязательно)

Требования к языку документов

Документы предложения должны быть предоставлены на одном из следующих языков:

• **русский язык**

• **узбекский язык**

Подписание предложения

Предложение должно быть подписано **уполномоченным представителем Поставщика**.

При необходимости Заказчик вправе запросить документы, подтверждающие полномочия лица, подписавшего предложение.

17. Общие условия RFP (Disclaimers)

Настоящий документ RFP направлен на сбор предложений от потенциальных поставщиков и не является предложением о заключении договора или обязательством

Заказчика заключить договор с каким-либо участником.

Заказчик оставляет за собой право:

• изменить, дополнить или уточнить требования настоящего RFP;

• запросить у участников дополнительные разъяснения, документы или информацию по представленным предложениям;

• провести дополнительные переговоры с одним или несколькими участниками;

• запросить презентацию или демонстрацию предлагаемого решения;

• отклонить любое или все предложения без объяснения причин;

• отменить или приостановить процедуру рассмотрения предложений полностью или частично.

Предоставление предложения участником означает согласие участника с условиями настоящего RFP.

Расходы, связанные с подготовкой и подачей предложения, несет участник.

Заказчик не компенсирует участникам расходы, понесенные в связи с участием в процедуре рассмотрения предложений.

Заказчик вправе использовать информацию, содержащуюся в представленных предложениях, исключительно в целях оценки и выбора решения, соответствующего требованиям настоящего RFP.