«УТВЕРЖДАЮ»
Первый заместитель
Председателя Правления
АКБ «Микрокредитбанк»
«18» мая 2023 г.

Техническое задание
на поставку оборудования для модернизации центров обработки данных

Директор департамента
стратегии и развития

О.Шукурова _____

Директор департамента
информационных технологий

С.Козимов _____

Ташкент 2023 г.

СОДЕРЖАНИЕ

ГЛОССАРИЙ

АКБ	Акционерный коммерческий банк
ТСО	Total Cost of Ownership или совокупная стоимость владения
ЗИП	Запасные части, инструменты и принадлежности
ЦОД	Центр обработки данных
ОЦОД	Основной центр обработки данных
РЦОД	Резервный центр обработки данных
ГЦИ	Главный центр информатизации
IP	Internet Protocol — межсетевой протокол
ISP	Internet Service Provider или интернет-провайдер
VPN	Virtual Private Network или Виртуальная частная сеть
АБС	Автоматизированная банковская система
СХД	Система хранения данных
HA	High-Availability, высокая доступность
ОС	Операционная система
СУБД	Система управления базами данных
ЦПУ	Центральное процессорное устройство
ИИ	Искусственный интеллект
ISCSI	Internet Small Computer System Interface
IPS	Intrusion prevention system, программная или аппаратная система сетевой и компьютерной безопасности
МСЭ	Межсетевой экран
WAN	Глобальная компьютерная сеть
NAT	Network Address Translation, преобразование сетевых адресов
URL	Uniform Resource Locator, адрес, который выдан уникальному ресурсу в интернете
SSH	Secure Shell, безопасная оболочка
CLI	Command Line Interface, Интерфейс командной строки
SNMP	Simple Network Management Protocol, простой протокол сетевого управления
ОЗУ	Оперативное запоминающее устройство

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы

Полное наименование проекта – Поставка оборудования для модернизации центров обработки данных АКБ «Микрокредитбанк» (далее – Банк).

1.2. Заказчик

Заказчик – АКБ «Микрокредитбанк».

Адрес «Заказчика»: Республика Узбекистан, 100096 г. Ташкент, ул. Лутфий 14;

Тел.: 1285, 71-207-46-51;

1.3. Исполнитель

Исполнитель по данному проекту будет определен на основе результатов отбора наилучшего предложения.

Исполнитель должен иметь опыт работы в данном направлении.

Исполнитель должен предоставить информацию по реализации аналогичных проектов до начала настоящего проекта.

Исполнитель должен представить свое Техническое предложение по поставке оборудования и программного обеспечения, удовлетворяющие всем требованиям данного документа.

Исполнителем должна быть предоставлена следующая дополнительная информация:

– информационное письмо от производителя о наличии авторизованных сервисных центров на территории Республики Узбекистан;

– авторизационное письмо от производителя предлагаемого оборудования подтверждающее право участника на осуществление поставки в рамках данного проекта;

Исполниетель должен в рамках выделенного бюджета предоставить полностью укомплектованное и работоспособное оборудование, при необходимости предложить дополнительные модули, продукты, и услуги, по каким-либо причинам не учтенные Заказчиком, но обязательные для обеспечения полноты использования запрашиваемой конфигурации.

Для определения критериев технической оценки, Участником (Претендентом) должна быть предоставлена следующая дополнительная информация по:

- персональному составу проектной команды (подтверждение наличия специалистов (инженеров) в штате Исполнителя, подтвердивших свою квалификацию сертификатами от ведущих мировых поставщиков предлагаемого решения);

- совокупной стоимости владения ТСО (Total Cost of Ownership) за счет предлагаемого оборудования (лицензирование, расходы на техподдержку, подписка к сервисам, ЗИП), функционала, и т.п. уникальных решений производителя сроком на не менее 5 лет;

При этом, для расширения круга потенциальных участников в тендерных торгах, в рамках выделенного бюджета заказчиком будут рассматриваться аналогичные либо с превосходящими характеристиками оборудования, указанные в Техническом задании. В этой связи, в случае предоставления аналогичного решения необходимо предоставить:

- технико-экономическую информацию по результативности и эффективности;

- расчет финансовых затрат по взаимоинтеграции с существующей инфраструктурой (миграция, перенос или замена).

Монтаж, настройка и установка оборудования должны осуществляется сертифицированными производителем специалистами поставщика.

1.4. Плановые сроки начала и окончания работ

Плановые сроки реализации проекта:

Начало работ: в соотвествии со сроками указанными в договоре;

Завершение работ: в соотвествии со сроками указанными в договоре.

1.5. Источники финансирования

Источником финансирования проекта являются собственные средства банка.

1.6. Основания для реализации проекта

Основание для реализации проекта является:

- Постановление Президента Республики Узбекистан № ПП-3270 от 12.09.2017г. «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики Узбекистан»;
- Рещение Правления АКБ "Микрокредитбанк" №48-4 от 1 мая 2023 года.

1.7. Порядок оформления и предъявления результатов работ

С целью принятия результатов работ по проекту Заказчик имеет право создать в установленном порядке Приемочную комиссию.

Датой сдачи - приемки работ считают дату подписания акта Приемочной комиссией.

Совместно с предъявлением Приемочной комиссии Системы производится сдача разработанного Исполнителем комплекта документации, перечень и требования к оформлению, которые определяются в соответствии с ГОСТами, и иными стандартами, и руководящими документами, действующими на территории Республики Узбекистан, а также по взаимному согласованию Заказчика и Исполнителя.

2. НАЗНАЧЕНИЕ И ЦЕЛИ РЕАЛИЗАЦИИ ПРОЕКТА

2.1. Назначение проекта

Основным назначением проекта является модернизация имеющегося и приобретение нового оборудования в основном и резервном центре обработки данных банка.

В ходе реализации проекта должны быть решены следующие задачи:

- Обеспечение отказоустойчивости подсистемы хранения данных автоматизированной банковской системы АКБ «Микрокредитбанк» путём приобретения новой СХД в резервный центр обработки данных.
- Расширения доступных вычислительных ресурсов сегмента системных и бизнес-приложений Банка путём приобретения нового сервера в основной центр обработки данных.
- Устранение узких мест в инфраструктуре ядра корпоративной сети передачи данных путём приобретения двух новых межсетевых экранов (для защиты и сегментации ядра сети) и двух новых 48 портовых коммутаторов (для создания отказоустойчивого ядра сети) в основной центр обработки данных.
- Приобретение запасных частей для имеющегося оборудования с целью устранения текущих неисправности и улучшения производительности.

2.2. Цели реализации проекта

Основной целью реализации данного проекта является устранение критически важных проблем в аппаратной инфраструктуре Банка для обеспечения бесперебойной работы информационных систем.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1 Общие сведения

Акционерно-коммерческий банк «Микрокредитбанк», созданный Указом Президента Республики Узбекистан от 5 мая 2006 года №УП-3750 (О создании акционерного коммерческого банка «Микрокредитбанк» и Постановлением Кабинета Министров №78 от 6 мая 2006 года «О мерах по организации деятельности и укреплению материально-

технической базы акционерного коммерческого банка «Микрокредитбанк»», является одним из ведущих универсальных коммерческих банков Республики Узбекистан.

3.2. Корпоративная сеть передачи данных

Локальная вычислительная сеть банка построена на различном оборудовании производства Cisco Systems, Dlink, Chekpoint, TPLink, Fortinet.

Большинство эксплуатируемого оборудования является морально устаревшим, модернизация и дальнейшее наращивание производительности которого не представляется возможным, оборудование не имеет гарантии и требует замены на современное оборудование.

По причине выхода из строя эксплуатируемого оборудования и отсутствия возможности замены на аналогичные устройства, критически важные элементы не зарезервированы.

Корпоративная сеть в целом состоит из 4-х логических уровней, включающих уровень ядра, уровень доступа ЦОД, а также уровень доступа головного отделения и уровень ISP/VPN.

Соединение между ОЦОД и РЦОД реализована на двух L2/L3 коммутаторах CISCO 3750, соединенных между собой оптическим каналом;

Уровень ядра ОЦОД функционирует на базе одного L3 коммутатора CISCO 3560, который выполняет маршрутизацию между всеми сегментами локальной сети;

Уровень доступа ОЦОД представлен коммутаторами Dlink и TPLink. К данным коммутаторам подключено оборудование Основного ЦОД. Восходящим сетевым соединением коммутаторы подключены к коммутатору ядра ОЦ.

Уровень ядра РЦОД построен на базе одного коммутатора CISCO 3750, вычислительное оборудование, размещенное на площадке РЦОД, подключается к уровню ядра посредством единственного коммутатора CISCO 2960.

Защита периметра ОЦОД и Головного отделения обеспечивается одним межсетевым экраном Chekpoint.

Подключение сети ГЦИ осуществляется через межсетевой экран CISCO ASA 5520.

К коммутаторам ядра также подключены:

- Ethernet коммутаторы локальной сети, осуществляющие подключение конечных пользователей (уровень доступа)
- Маршрутизаторы и защищенные IP шлюзы, осуществляющие подключение к оператору БТС и операторам сети Internet (Уровень ISP/VPN).

Текущая архитектура корпоративной сети передачи данных АКБ «Микрокредитбанк» имеет вид прямолинейной цепи, в которой каждый элемент представлен в единичном виде. Наблюдается высокий риск того, что при выходе из строя одного устройства, все информационные системы банка окажутся недоступны.

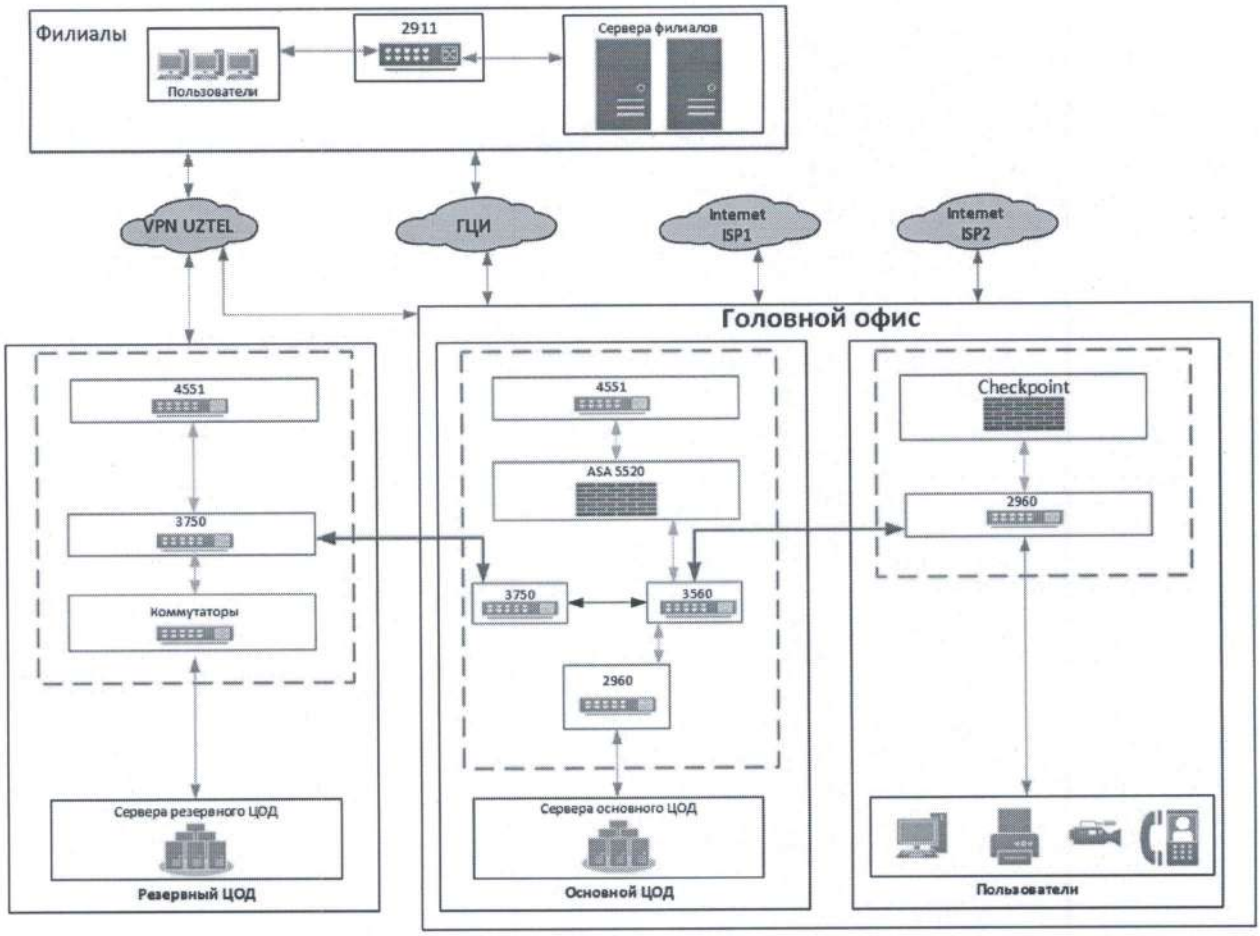

Рисунок №1 Логическая схема текущей корпоративной сети банка

Максимальная пропускная способность корпоративной сети данных на уровне ядра и на уровне доступа составляет не более 1 Гбит/с, это является узким местом в ИТ инфраструктуре банка, которое накладывает существенное ограничение на производительность информационных систем банка.

На сегодняшний день, централизованный мониторинг не осуществляется, а поиск и устранение неисправностей требует существенных временных затрат.

Безопасность подключений к корпоративной сети банка осуществляется одним межсетевым экраном Chekpoint, резервного оборудования для замены у банка нет.

3.3. Инфраструктура АБС

На сегодняшний день ключевая информационная система АКБ "Микрокредитбанк" – IABS (АБС) функционирует на базе серверов, систем хранения данных и коммутационного оборудования производства компании IBM.

Основная часть оборудования инфраструктуры, которое обеспечивает функционирование АБС, приобретена в 2016 году, модернизация оборудования была осуществлена в 2022 году. Серверы базы данных IBM Power 870 уже сняты с производства у производителя и их дальнейшая модернизация не представляется возможным.

В основном ЦОД для функционирования АБС эксплуатируется оборудование IBM Power 870 – сервера базы данных, IBM FlashSystem 7300 – система хранения данных для продуктивной среды АБС и IBM Storwize V7000 - система хранения данных резервного копирования базы данных АБС.

В резервном ЦОД эксплуатируется IBM Power 870 – резервный сервер базы данных который подключен к СХД находящимся в основном ЦОД (в связи с чем вопрос полноценного резервирования инфраструктуры АБС остаётся не решенным), IBM Power 740 – Standby сервер для АБС и IBM Storwize V7000 - система хранения данных для Standby сервера, на котором на сегодняшний день имеются неисправности.

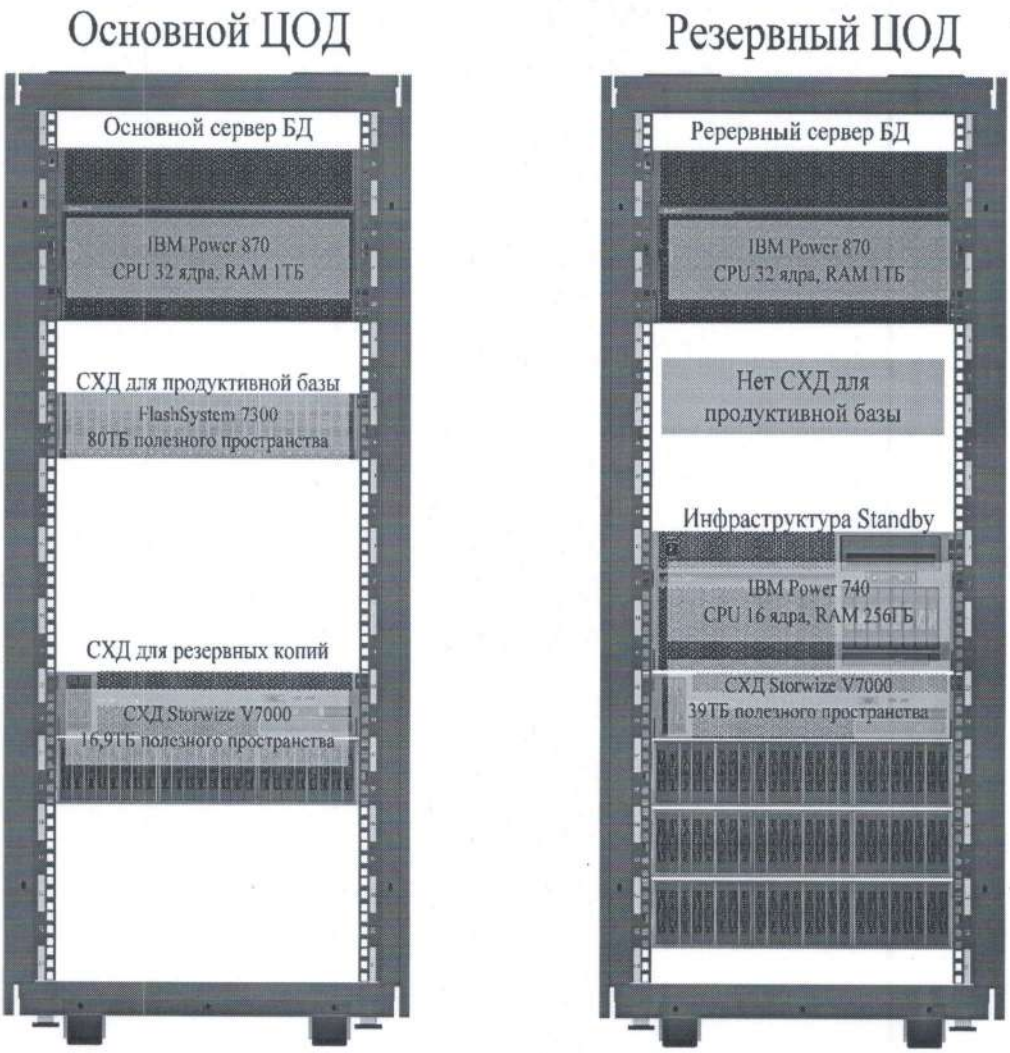

Рисунок № 2 Текущая инфраструктура АБС

На сегодняшний день общий объём базы данных АБС составляет более 20ТБ, а количество транзакций достигает более 3 млн. за один операционный день. Дальнейшее развитие банка путем внедрения новых информационных систем, выпуска новых банковских продуктов, а также расширение объёма предоставляемых услуг через цифровые каналы взаимодействия с клиентом, приведут к существенному увеличению количества транзакций в АБС и объёма базы данных, в перспективе ближайших трёх лет.

3.4. Инфраструктура сервисных и бизнес-приложений банка

На сегодняшний день инфраструктура сегмента бизнес-приложений состоит из 7 серверов HPE Proliant и 3 систем хранения данных HPE MSA. Всё оборудование эксплуатируется только в основном ЦОД. В резервном ЦОД вычислительные ресурсы под задачи сегмента бизнес-приложений не предусмотрены.

Всё оборудование, эксплуатируемое в данном сегменте, поставлялась не через официальный канал поставки производителя, в связи с чем отсутствует гарантия на комплектующие, установленные в оборудовании.

Отсутствует разделение оборудования для сред тестирования, разработки и продуктивного программного обеспечения. Работы по разработке и тестированию осуществляются на том же оборудовании, на котором функционируют информационные системы, находящие в промышленной эксплуатации.

Также отсутствует система резервного копирования и система распределения нагрузки, что создаёт риск перегрузки отдельных элементов инфраструктуры, которая может привести к временным перебоям в работе критически важных для банка информационных систем, а также существенно усложняет процесс восстановления работоспособности систем.

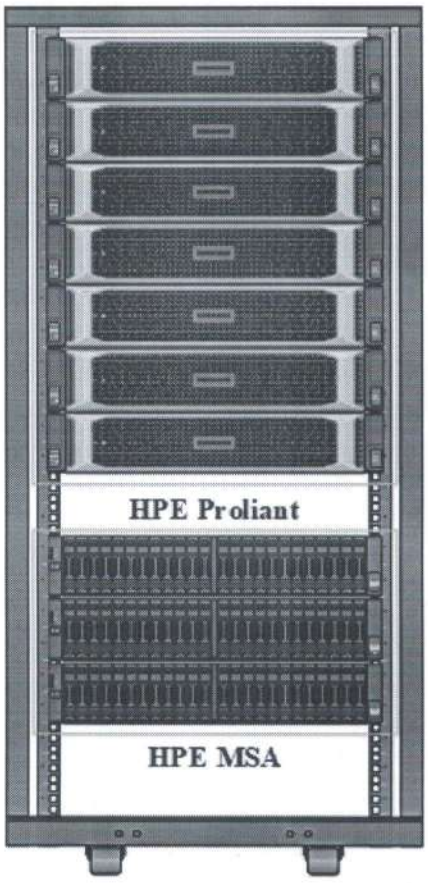

Рисунок № 3 Текущая инфраструктура сегмента сервисных и бизнес-приложений

Наблюдается нехватка вычислительных ресурсов имеющегося оборудования, оперативная память большинства серверов перегружена, что сказывается на производительности функционирования информационных систем (Коллектив, мобильное приложение и прочее) банка.

4. ТРЕБОВАНИЯ К ПОСТАВЛЯЕМОМУ РЕШЕНИЮ

Проект должен быть реализован в следующем направлении:

1. **Инфраструктура сегмента сервисных и бизнес приложений**

   Приобретение нового сервера архитектуры x86 для сегмента системных и бизнес-приложений Банка.

2. Инфраструктура АБС

Приобретение новой Системы хранения данных для резервного сервера базы данных.

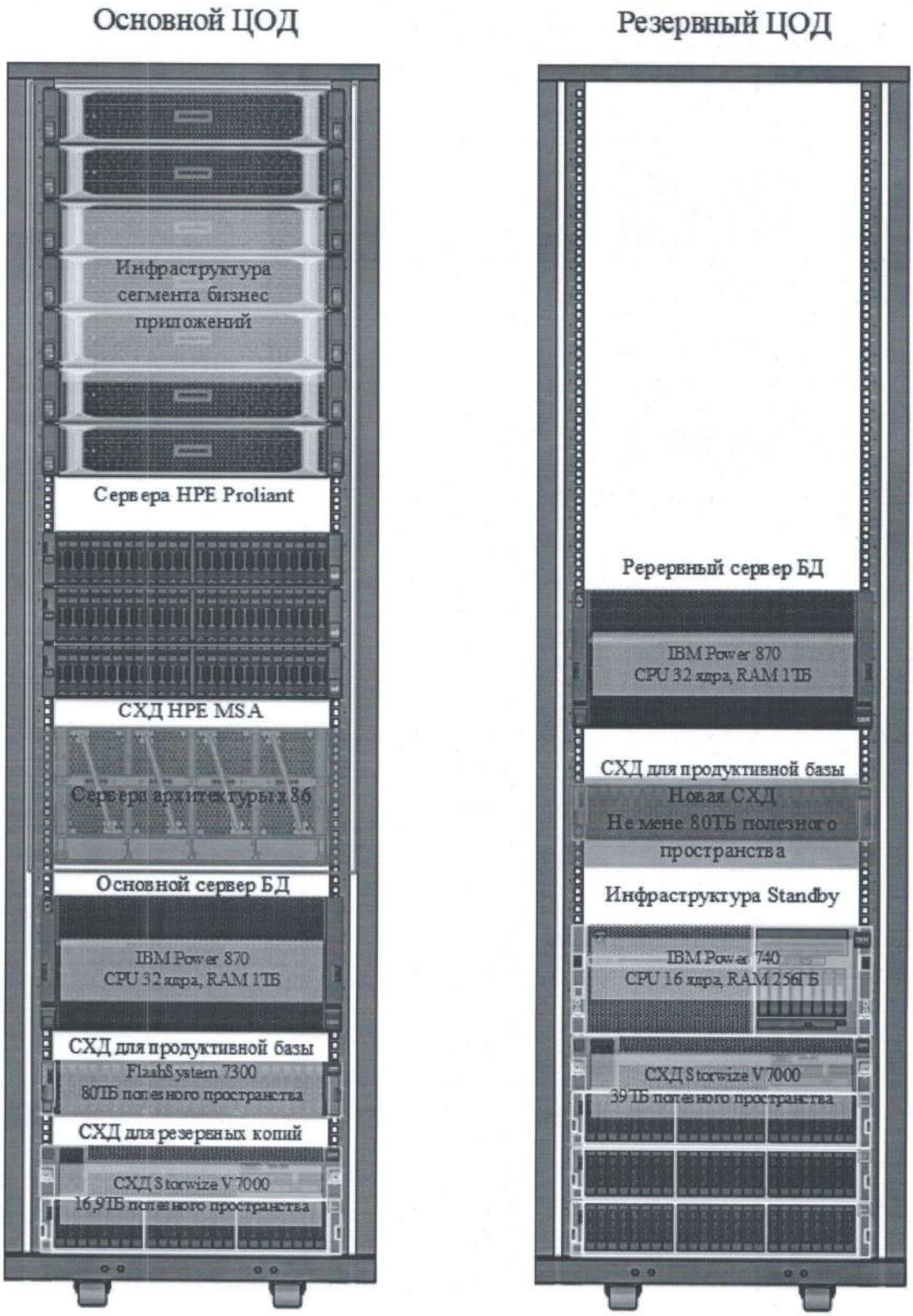

Рисунок № 4 Предлагаемая будущая инфраструктура ЦОДов

3. Корпоративная сеть передачи данных

Приобретение двух межсетевых экранов в основной ЦОД.
Приобретение двух 48 портовых медных коммутаторов.

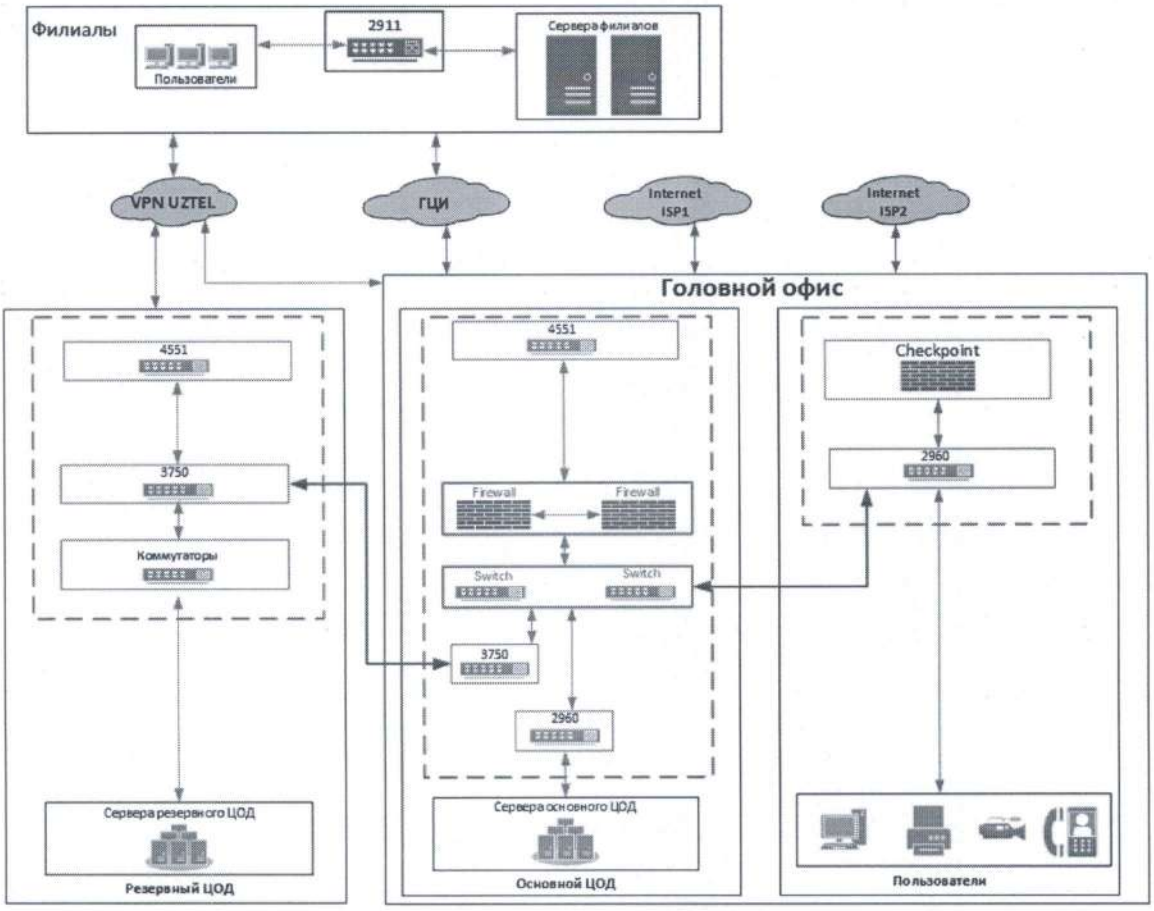

Рисунок № 5 Предлагаемая будущая архитектура сети

4. Приобретение комплекта запасных частей для имеющихся серверов и систем хранения данных в целях дальнейшего обслуживания этого оборудования.

4.1. Общие требования

Все предлагаемые товары должны полностью соответствовать требованиям Технического Задания.

Все предлагаемые товары должны быть новыми, не использованными и изготовленным не ранее 2023 года.

Все предлагаемые товары должны функционировать при следующих условиях:

- параметры электропитания (220 V +/- 20 V, 50 Hz +/- 1 Hz); возможны резкие скачки напряжения;

- температура окружающей среды: от +10 С0 до +32 С0; относительная влажность от 10% до 80%; запыленность до 0.4 г/м3; уровень шума не должен превышать 55 Дб, если нет специальных требований.

Все необходимые Руководства пользователя должны быть на русском языке. Техническая документация должна быть на русском или английском языке. Во всех случаях

недопустимо предоставление Технической документации и Руководств пользователя в виде ксерокопий.

4.2. Требования к поставке и выбору оборудования

Поставляемое оборудование, комплектующие части, расходные материалы, аксессуары и программное обеспечение не должны вызывать ненадлежащее функционирование или отказ существующего оборудования и ранее установленного программного обеспечения.

Поставляемое оборудование всех марок должно производиться серийно к моменту открытия торгов.

4.3. Обязательные требования к гарантийному обслуживанию

Предлагаемое оборудование и программное обеспечение должно быть новым (не бывшим в употреблении, не снятым с производства), производства не ранее 2023 г. и соответствовать мировым стандартам.

Гарантия на все оборудование должна быть не менее 3 лет.

Исполнитель должен учесть в стоимости предложения техническую поддержку в течении 1-го (первого) года с момента запуска программно-аппаратного комплекса в эксплуатацию.

Помимо гарантийной поддержки оборудования, Исполнитель в течение действия гарантийных обязательств должен обеспечить необходимую информационно-консультационную помощь специалистам Заказчика.

Гарантийное сервисное обслуживание всего оборудования должно осуществляться по месту эксплуатации, специалистами авторизованного производителем сервис-центра в Республике Узбекистан.

4.4. Требования к доставке и установке

Для отечественных компаний: Доставка осуществляется до склада Покупателя, расположенного по адресу: 100096 г. Ташкент, ул. Лутфий 14.

Для иностранных компаний: Поставка оборудования осуществляется на условиях DAT Международный Аэропорт Ташкента имени Ислама Каримова (Incoterms 2010).

Доставка, монтаж и запуск в эксплуатацию поставляемой техники осуществляется Поставщиком.

Запуск в эксплуатацию оборудования включает в себя установку и пуско-наладку, включая установку программного обеспечения.

Все поставляемое оборудование должно быть сертифицировано в соответствии с законодательством или эквивалентными международными стандартами, что должно подтверждаться соответствующими документами.

4.5. Требования к инсталляции, настройке, монтажу.

Поставщик должен выполнить следующие работы:

- Осуществить поставку оборудования
- Установить оборудование в шкаф;
- Проложить кабели питания и сети;
- Провести процедуру регистрации оборудования на портале производителя;
- Прописать и настроить IP-адреса;
- Настроить работу оборудования в кластере и режиме HA;
- Выполнить работы по устновке, настройке и запуску всех предполагаемых к поставке систем на предоставленное оборудование.

4.6. Требования к составу поставляемого оборудования.

Перечень оборудования, планируемого для покупки приведен ниже:

1. Новый сервер архитектуры x86 для сегмента системных и бизнес-приложений Банка - 1 шт.
2. Система хранения данных для резервного сервера базы данных – 1 шт.
3. Межсетевые экраны для основного ЦОД – 2 шт.
4. 48 портовые медные коммутаторы – 2 шт.
5. Дополнительные детали для существующих систем хранения данных HPE MSA 1050 - шт.
6. Дополнительные детали для существующих систем хранения данных HPE MSA 2050 - шт.
7. Дополнительные детали для существующих систем хранения данных HPE MSA 2060 - шт.
8. Дополнительные детали для существующих серверов HPE DL360 Gen10 - шт.
9. Дополнительные детали для существующих серверов HPE DL380 Gen10 - шт.
10. Дополнительные детали для существующих серверов HPE DL380 Gen10 Plus - шт.
11. Дополнительные детали для существующих систем хранения данных IBM Storwize V7000 – 2 шт.

4.6.1. Общие требования к функционалу сервера.

Предлагаемое решение должно поддерживать возможность установки в стойку.

Сервер должен поддерживать процессоры Intel Xeon SP 83XX (Platinum) и 63XX

Сервер должен иметь модульную архитектуру, при этом каждый модуль масштабируется до архитектуры 4Sockets. Возможности масштабирования и обновления должны быть достигнуты за счет добавления дополнительных строительных блоков модулей 4Socket без необходимости предварительных инвестиций в большое шасси.

Предлагаемое решение должно поддерживать последние операционные системы и программное обеспечение, такое как:

- Microsoft Windows Server
- Red Hat Enterprise Linux (RHEL)
- SUSE Linux Enterprise Server (SLES)
- Oracle Linux/Oracle UEK
- Vmware

Сервер должен дать возможность Заказчику беспрепятственно наращивать емкость или переходить от горизонтального масштабирования к вертикальному масштабированию или наоборот без необходимости повторной платформизации.

Шасси должен поддерживать не менее 48 слотов DIMM, обеспечивающих до 12 ТБ памяти DDR4 на шасси с поддержкой ECC, Adaptive Double Device Data Correction (ADDDC) и Single Device Data Correction (SDDC) для защиты от ошибок. Все каналы памяти для каждого процессора должны быть заполнены для оптимальной производительности. Система должна поддерживать сочетание модулей DIMM емкостью 32 ГБ и 256 ГБ.

Сервер должен поддерживать энергонезависимую память с емкостью DIMM 128 ГБ/256 ГБ/512 ГБ. Поддержка должна быть только для прямого режима приложения, чтобы обеспечить тесную интеграцию с рабочими нагрузками и обеспечить наилучшую производительность памяти и согласованность данных.

Шасси сервера должен поддерживать до десяти (10) отсеков для 2,5-дюймовых

дисков на шасси для поддержки дисков типа SATA/SAS/NVMe/SSD.

Сервер должен иметь опциональную поддержку оптического привода DVD-ROM.

Сервер должен поддерживать все прямые каналы ввода-вывода PCI-e от ЦП, чтобы обеспечить полную скорость, разблокировку и подключение ввода-вывода с малой задержкой.

Сервер должен поддерживать не более 16 полно скоростных интерфейсов ввода-вывода PCI-e 3.0 для конфигурации 4S и 32 интерфейса для конфигурации 8S.

Сервер должен поддерживать горячую замену резервных блоков питания, обеспечивающих минимальную эффективность не менее 91% при 100% нагрузке и эффективность не менее 94% при 50% нагрузке.

Сервер должен поддерживать дополнительный комплект с 2 источниками питания, который рекомендуется, если требуется N+N.

Предлагаемое решение должно поддерживать Redfish® API. Решение должно поддерживать вариант встроенной консоли и консоли управления для конфигурации 4S и 8S. Должна быть также поддержка устройства консоли управления для больших конфигураций.

Сервер должен быть интегрирован в структуру централизованного управления, где его можно будет тщательно контролировать и установить автоматическую связь с персоналом службы поддержки производителя, а также автоматически инициировать действия для беспрепятственного взаимодействия с пользователем.

Сервер должен иметь проверенные Unix-подобные функции RAS с доступностью отдельной системы до 99,999%. Он должен обеспечивать комплексные возможности RAS, в том числе:

- Архитектура, ориентированная на микропрограммное обеспечение, при анализе предупреждений, ошибок и выполнении действий
- Автоматическая регистрация ошибок
- Автоматическое самовосстановление (движок анализа)
- Отключение/деконфигурация неисправных FRU
- Бортовой анализатор неисправностей
- Автоматический перезапуск
- Расширенная обработка ошибок процессора (eMCA Gen2)
- Расширенная отказоустойчивость памяти (ADDDC)
- Повышенная отказоустойчивость оптики (адаптивная маршрутизация)
- Расширенное восстановление после ошибок PCIe (LER)
- Онлайн обновление прошивки

Система должна поддерживать горячую замену резервных вентиляторов.

В предлагаемом решении должно быть интегрированное кластерное решение высокой доступности для Linux вместе с аппаратным обеспечением, предпочтительно от одного производителя для всей инфраструктуры, включая аппаратное обеспечение, ОС и решение высокой доступности для простоты интеграции и ответственности служб поддержки. Кластерное решение должно предоставлять наборы инструментов для интеграции БД/приложений, чтобы облегчить интеграцию и услуги поддержки. Наборы инструментов должны охватывать популярные корпоративные приложения, такие как СУБД Oracle, приложения и т. д.

Система должно позволять объединять несколько систем в более крупный комплекс для масштабирования, гибкости и защиты инвестиций.

В предлагаемом решении должно быть интегрированное решение безопасности с учетом рабочей нагрузки для ОС и приложений Linux. Решение должно обеспечивать соответствие требованиям безопасности благодаря простоте внедрения и администрирования, а также эффективному автоматизированному выполнению большинства задач.

Предлагаемое решение должно поддерживать следующие требования к безопасности:

- Поддержка UEFI Secure Boot и Secure Start.
- Защита от отката прошивки для исправления критических уязвимостей.
- Immutable SRT, решение Cyber Catalyst от Marshsm
- Обновления без несанкционированного доступа — компоненты имеют цифровую подпись и проверены
- Безопасное восстановление — восстанавливает критическое микропрограммное обеспечение до заведомо исправного состояния при обнаружении скомпрометированного микропрограммного обеспечения.
- Поддержка TPM (Trusted Platform Module) 2.0 - защищен от несанкционированного доступа и припаян для всех систем
- Обнаружение проникновения в корпус (опционально)
- Обновление встроенного ПО защищено аутентификацией администратора RMC
- Управляемость с воздушным зазором
- Надежные готовые пароли
- Управление доступом к каталогу (LDAP/Active Directory)
- Альтернативы PXE (направленная загрузка по локальной сети, загрузка по

- Возможность отключения портов HOST USB

Система должна поддерживать несколько серверов с перекрывающимися IP-адресами, создавать и управлять политиками безопасности и применять их ко всей среде.

В системе не должны использоваться агенты, которые могут потреблять ресурсы ЦП, но активируются вручную для выполнения задач.

Система должна поддерживать управление доступом на основе ролей. Различные роли для выполнения различных функций, таких как определение политик соответствия и выполнение заданий аудита.

В системе должна быть информационная панель для отображения общего статуса соответствия.

Сканирование соответствия и исправление должны поддерживаться в одной и той же системе.

Система должна поддерживать добавление новых пользователей с определенной ролью для операций безопасности.

Система должна предоставлять стандартные отраслевые тесты безопасности, такие как политика CIS для соответствия операционной системе.

Система должна иметь авторизованную роль для настройки политики в соответствии с определением политики CSIO и обеспечения ее доступности для развертывания в соответствующих ОС.

Система должна обеспечивать возможность развертывания нескольких политик в ОС, относящихся к организациям, ИТ и политикам отделов. Изменения политики и история должны быть сохранены для целей аудита.

Система должна поддерживать исправление на основе утвержденной политики, которая также может быть определена в определении политики соответствия.

Система должна предоставить список всех активных и неактивных политик, настроенных в среде центра обработки данных.

Система должна поддерживать ручной запуск сканирования соответствия.

Система должна поддерживать сканирование на соответствие одной политике или всем политикам, настроенным в ОС.

Система должна поддерживать последовательный откат последней операции исправления безопасности в ОС до тех пор, пока она не достигнет исходного состояния.

Система должна генерировать полный отчет о сканировании, включая сбои и

подробный отчет о том, как исправить ситуацию в среде для повышения оценки соответствия.

Производитель должен быть в состоянии предложить гибкий режим развертывания с оплатой по факту использования, позволяющий локально распределять ИТ-ресурсы, при этом корректируя затраты на ИТ в соответствии с фактическим использованием в режиме

Должна быть сквозная поддержка от основного производителя инфраструктуры: аппаратное обеспечение, ОС и системное решение высокой доступности.

4.6.2. Общие требования к функционалу систем хранения данных.

Предлагаемый массив хранения должен быть массивом All Flash - NVMe и должен быть основан на технологии PCI Gen4 последнего поколения.

Предлагаемое хранилище должно быть флагманским массивом All NVMe - Flash от организации и должно быть четко опубликовано на их веб-сайте.

Массив хранения должен поддерживать ведущие в отрасли платформы операционных систем и кластеризацию, включая: Windows Server 2019 и 2022, VMware 7, операционные системы Linux и UNIX и т. д.

Предлагаемый массив хранения должен быть гибким как при вертикальном масштабировании, так и при горизонтальном масштабировании с использованием технологии кластеризации, встроенной в микропрограмму массива.

Технология горизонтального масштабирования должна выходить за рамки технологии федерации, поскольку она должна иметь возможность чередовать тома по всем масштабируемым контроллерам системы хранения.

Операции записи должны быть полностью защищены, и в случае сбоя питания не должно быть потери данных. Этот механизм не должен полагаться на батарейки.

Предлагаемый массив хранения должен быть сконфигурирован без единой точки конфигурации, включая карту контроллера массива, кэш-память, вентилятор, источник питания и т. д.

Не должно быть ухудшения характеристик из-за отказа одного компонента или контроллера. Производитель должен предоставить документальное подтверждение этого.

Предлагаемый массив хранения должен поддерживать различные емкости флэш-накопителей NVMe.

Предлагаемый массив хранения должен поставляться с сертифицированным шифрованием AES-256 XTS FIPS на уровне Granular LUN без использования зашифрованных флэш-накопителей NVMe.

Предлагаемый массив хранения должен быть обеспечен защитой от отказа трех дисков одновременно. В случае, если производитель не поддерживает это, размер массива должен быть максимально 6D+2P.

Для достижения максимальной емкости дисков — у производителя должна быть возможность разместить все предлагаемые диски в одном пуле дисков.

Если у производителя нет возможности единого пула, необходимо предоставить и настроить 20% дополнительной необработанной емкости.

Не должно быть ухудшения характеристик из-за отказа одного компонента или контроллера. Производитель должен предоставить документальное подтверждение этого.

Не должно быть снижения производительности во время критически важных действий по поддержке, таких как обновление микропрограммы, обновление исправлений и т. д.

Предлагаемый массив хранения должен предлагать контрольные суммы, выходящие за рамки стандарта T10-PI. Контрольные суммы автоматически обнаруживают и предотвращают ошибки, возникающие в результате потерянных/неуместных операций чтения или записи, которые T10-PI и аналогичные системы контрольного суммирования не

могут исправить.

Предлагаемое хранилище должно иметь облачный мониторинг, поддержку искусственного интеллекта и аналитический механизм для упреждающего управления хранилищем. Все необходимые лицензии должны быть включены в предложение.

Облачный мониторинг, поддержка ИИ и механизм аналитики должны обеспечивать следующее:

- Предоставление рекомендаций по обновлению встроенного ПО и обновлению исправлений заблаговременно и с учетом периферийной инфраструктуры, подключенной к массиву.
- Автоматически предотвращать установку прошивки массива, которая может конфликтовать с другими элементами инфраструктуры, подключенными к массиву.
- Предоставление чрезвычайно детального поминутного анализа емкости и тенденций производительности по умолчанию без необходимости включения дополнительного ведения журнала, установки каких-либо устройств (физических или виртуальных) или установки какого-либо программного обеспечения.
- Аналитика производительности должна иметь возможность разбивать ввод-вывод на гистограммы размера ввода-вывода, определять последовательный и случайный ввод-вывод и давать рекомендации на основе ИИ для устранения проблем с производительностью.
- Избавьтесь от необходимости для клиента предоставлять журналы массива для поддержки, так как служба поддержки будет автоматически получать необходимую информацию из массива.
- Должен предоставить историю обращений в службу поддержки, зарегистрированных группой поддержки, с оперативной эффективностью. Он должен ясно демонстрировать процент обращений в службу поддержки, закрытых автоматически по сравнению с ручным.
- Должен быть в состоянии предоставить единую исполнительную панель мониторинга, охватывающую различные критические и обязательные аспекты экономии места за счет технологий сокращения данных, готовности к защите данных (как RPO, так и периода хранения) для классифицированных приложений, работающих в хранилище, и готовности к аварийному восстановлению для приложений.
- Предоставляет полную диаграмму здоровья массива и позволяет гибко определять правило здоровья на основе определенных условий.
- Предоставлять рекомендации по автоматическому обновлению как программного, так и аппаратного обеспечения с конкретными инструкциями относительно того, что необходимо обновить и в какой степени.

Механизм аналитики с поддержкой облака должен иметь возможность предоставлять следующее:

- Должен иметь возможность глобального обучения — механизм аналитики должен собирать контрольную информацию как минимум из более чем 25 000 массивов по установленной базе производителя для значимого вывода. Производитесь должен предоставить документальное подтверждение этого.
- Механизм аналитики должен иметь возможность проактивных рекомендаций для устранения проблем / проблем, обнаруженных в другой базе установки производителя после выявления проблемной подписи.

Для облачной интеграции механизма мониторинга и аналитики с гипервизором должны быть учтены следующее:

- Предлагаемый облачный механизм мониторинга и аналитики должен быть тесно интегрирован с уровнем гипервизора и должен быть сертифицирован для работы как минимум с VMware и Hyper-V.
- Интеграция с гипервизором должна обеспечивать сквозной мониторинг центра обработки данных гипервизора, хранилища данных, узла гипервизора и виртуальных машин, работающих в центре обработки данных гипервизора, и должна иметь возможность связываться с предлагаемым массивом хранения.
- Инструмент облачного мониторинга и интеграции должен обеспечивать подробный анализ конфликтов ЦП, памяти, операций ввода-вывода для каждой виртуальной машины, включая задержку.
- Инструмент облачного мониторинга и интеграции должен предоставлять рекомендации на основе ИИ для улучшения состояния инфраструктуры гипервизора.
- Инструмент облачного мониторинга и интеграции должен иметь возможность определять основные виртуальные машины, которые способствуют максимальному количеству операций ввода-вывода и задержке.
- Если производитель не поддерживает предлагаемые выше функции, производитель должен предоставить корпоративную лицензию на пакет VMware vRealize или лицензию Microsoft System center Operations Manager как минимум на 20 физических серверов, каждый из которых работает с двумя физическими процессорами и 16 ядрами.

Предлагаемый массив хранения должен иметь встроенную облачную консоль данных для управления неограниченным количеством массивов. Облачная консоль должна обеспечивать следующие функции:

- Общая панель мониторинга для всех, кто управляет несколькими массивами через единую облачную консоль данных.
- Главная информационная панель должна предоставлять информацию об общем количестве массивов, томов, хостов, емкости и информации о производительности основных массивов и томов.
- Общий контроль доступа на основе ролей для управления несколькими массивами через единую консоль данных вместо создания пользователей и назначения ролей индивидуально для каждого массива.
- Общее управление аудитом для всех массивов
- Должен иметь возможность пометить том хранилища для заданных хост-приложений, чтобы можно было построить диаграммы производительности для экземпляра приложения для упрощения управления и устранения неполадок.
- Предлагаемая консоль должна сообщить о размещении приложения в наиболее подходящей системе на основе рабочей нагрузки после тегирования приложения.
- Должен иметь возможность предоставлять контекстно-зависимые обновления программного обеспечения для массива хранения.
- Должна быть возможность предлагать управление и настройку хранилища как услугу вместо контроля, установки исправлений и обновлений приложения управления командой на месте.

Приложение управления должно быть действительно облачным, чтобы не было необходимости настраивать, обновлять, исправлять приложения управления в течение жизненного цикла контракта на поддержку, и оно должно предлагаться как услуга.

В случае, если производителю нужны какие-либо дополнительные услуги, такие как кластеризация / федерация для управления несколькими массивами с одной консоли и нет собственной облачной консоли данных, тогда все необходимые аксессуары, такие как двойные коммутаторы Ethernet, кабели, по крайней мере, двойной сервер управления в HA и другие должны быть предоставлены заранее как минимум для 16 массивов.

Предлагаемое хранилище должно масштабироваться без прерывания работы до серий массивов хранения более высокого поколения в данном семействе без какой-либо модернизации вилочным погрузчиком.

При обновлении хранилища до модели следующего поколения не должно быть простоев.

Все предлагаемые сетевые карты должны быть способны работать на линейных скоростях.

Для оптимальной производительности — каждый интерфейсный слот PCI должен иметь не менее 8 линий PCI Gen4 или пропускную способность 16 Гбит/с.

Предлагаемый массив хранения должен поддерживать распределенное глобальное «горячее» резервирование для предлагаемых дисковых накопителей.

Глобальный горячий резерв должен быть настроен в соответствии с отраслевой практикой.

Предлагаемый массив хранения должен поддерживать качество обслуживания (QoS) для выборочного управления IOPS и МБ/с для данного LUN.

Предлагаемый массив хранения данных должен автоматически выполнять QoS, чтобы одна рабочая нагрузка не перевешивала производительность массива.

Предлагаемое хранилище должно поддерживать критически важные функции эффективности хранения — встроенную дедупликацию, сжатие, тонкое выделение ресурсов на уровне контроллера.

Предлагаемое хранилище должно поддерживать как недублированные, так и дублированные тома одновременно в пределах массива.

Предлагаемое хранилище должно одновременно поддерживать как несжатые, так и сжатые тома в массиве.

Предлагаемое хранилище должно иметь возможность категорировать домены для приложений, поддерживающих различные рабочие нагрузки, для эффективной дедупликации и сжатия. Например, должна быть возможность иметь рабочую нагрузку базы данных в одном домене или группе защиты и рабочую нагрузку виртуализированного приложения в другом домене или группе защиты для эффективной дедупликации и сжатия.

Предлагаемый массив хранения должен поддерживать более 1000 снэпшотов на LUN/том. Производитель должен использовать эффективные технологии производительности, такие как перенаправление при записи или лучше.

Предлагаемый массив хранения должен быть тесно интегрирован с VMware и сертифицирован для VVOL:

- Должен быть сертифицирован для репликации на основе vVol
- Должен поддерживать как сжатие, так и дедупликацию.
- Должен быть квалифицирован для работы как с Fibre Channel, так и с ISCSI.
- Должен поддерживать запланированный моментальный снимок и качество обслуживания.
- Должен поддерживать шифрование.

Производитель должен ежеквартально проводить всестороннюю оценку на основе облачных технологий, по крайней мере, для среды VMware, и учитывать необходимые для этого услуги.

Оценка должна предоставить подробный анализ хостов VMware — использование ЦП и памяти, анализ хранилища и соответствующие выводы о конфликтах, ВМ-преступниках и жертвах в среде, подключенной к предлагаемому хранилищу. Предлагаемая оценка также должна провести полный анализ лицензирования.

Предлагаемый массив хранения должен быть интегрирован с Red-hat OpenShift, bernetes и другой отраслевой контейнерной платформой на базе K8 через набор драйверов CSI. Производитель должен поддерживать как минимум следующие функции посредством интеграции CSI/CSP:

- Должен поддерживать как статическую, так и динамическую подготовку
- Должна быть возможность расширять и изменять размер постоянных томов, предоставленных приложениям с сохранением состояния.
- Должна быть возможность создавать и удалять снимки.
- Должен поддерживать блочный том CSI Raw, а также клонирование тома CSI.
- Поддержка как Fibre Channel, так и ISCSI.

Предлагаемое хранилище должно поддерживать как синхронную, так и асинхронную репликацию на основе хранилища между центрами обработки данных для эффективной защиты данных.

Предлагаемый массив хранения должен иметь отдельную политику резервного копирования моментальных снимков между рабочей площадкой и площадкой аварийного восстановления.

Предлагаемый массив хранения должен иметь возможность репликации только добавочных изменений между двумя площадками (основной и вторичной).

Предлагаемый массив хранения должен поддерживать несколько моментальных снимков, клонов или сеансов репликации без какого-либо влияния на производительность.

Предлагаемый массив хранения должен иметь возможность репликации данных из Flash в Hybrid Flash или наоборот в пределах данного семейства массивов.

Предлагаемое хранилище должно поддерживать асинхронную репликацию FAN out из первичного массива как минимум в два вторичных массива для данного тома. Он должен обеспечивать гибкость для определения отдельного расписания для каждого отношения репликации.

Производитель должен предоставить лицензию на все критически важные функции, такие как моментальный снимок, клонирование, репликация, QOS, конфигурация и управление LUN и т. д. для максимальной поддерживаемой емкости массива. Для будущего увеличения емкости не требуется дополнительных лицензий на программное обеспечение. Любая дополнительная лицензия, необходимая для соответствия спецификации RFP, также должна быть предложена заранее.

4.6.3. Общие требования к функционалу межсетевых экранов

Предлагаемое сетевое оборудование должно соответствовать следующим требованиям:

- Лицензирование системы должно осуществляться для неограниченного количества пользователей.
- Система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя.
- Система должна поддерживать объединение в кластер не менее 4 устройств с

возможностью создания типов кластеров:

- с холодным резервом (active/passive);
- с горячим резервом (active/active);
- кластер балансировки;

- Система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений.
- Система должна иметь функциональность балансировки нагрузки.
- Система должна иметь функциональность управления полосой пропускания трафика (traffic shaping).
- Система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol).
- Система должна обеспечивать анализ SSH трафика (ssh inspection).
- Система должна обеспечивать динамическую маршрутизацию IPv4, IPv6.
- Система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента).
- Система должна обеспечивать оптимизацию WAN соединений.
- Система должна иметь функционал защиты от утечек данных DLP.
- Система должна обеспечивать антивирусную защиту с аппаратным ускорением;
- Система должна обеспечивать защиту от спама (антиспам).
- Система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением.
- Система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов.
- Принудительное включение режима безопасного поиска в популярных поисковых системах.
- Система должна иметь функциональность контроля приложений.
- Система должна иметь функциональность WEB proxy.
- Система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию.
- Система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика.
- Система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз.
- Система должна иметь возможность помещать инфицированные сообщения в карантин.
- Система должна иметь возможность блокировки передачи файлов в зависимости от размера.
- Система должна иметь возможность блокировки передачи файлов в зависимости от типа.
- Система должна поддерживать соединения множества WAN сетей.
- Система должна поддерживать протокол PPPoE и L2TP.
- Система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”.
- Система должна поддерживать маршрутизацию на основе политик.
- Система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP.
- Система должна поддерживать использование зон безопасности.
- Система должна поддерживать маршрутизацию между зонами.
- Система должна поддерживать маршрутизацию между виртуальными сетями.

- Система должна поддерживать администрирование на основе ролей.
- Система должна поддерживать несколько уровней администраторов и пользователей.
- Система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс.
- Система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО.
- Система должна поддерживать аутентификацию пользователей посредством внутренней базы данных.
- Система должна поддерживать Kerberos аутентификацию пользователей.
- Система должна поддерживать аутентификацию пользователей посредством Windows Active Directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей.
- Система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP.
- Система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу.
- Система должна поддерживать аутентификацию на основе групп пользователей.
- Система должна поддерживать функции NAT, PAT, «прозрачный» (мост).
- Система должна поддерживать функции NAT на основе политик.
- Система должна поддерживать функции VLAN Tagging (802.1Q).
- Система должна поддерживать функции SIP/H.323 NAT Traversal.
- Система должна поддерживать настройку профилей безопасности;
- Система должна иметь возможность блокировки по URL/ключевому слову/фразе.
- Система должна поддерживать «Белые» списки URL.
- Система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX.
- Система должна уметь предотвращать не менее 4000 типов сетевых атак.
- Система должна иметь возможность настройки списка сигнатур атак.
- Система должна поддерживать автоматическое обновление базы атак и сигнатур
- Система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев.
- Система должна поддерживать проверку заголовков MIME.
- Система должна поддерживать фильтрацию электронной почты, по ключевым словам, и фразам.
- Система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов.
- Система должна иметь возможность отсылки логов на удаленный syslog сервер.
- Система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла.
- Система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах.
- Система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках.
- Система должна поддерживать протокол VRRP.
- Система должна поддерживать интеграцию с IBM QRadar SIEM.
- Система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности.
- Система должна поддерживать обнаружение и контроль использования служб

- мгновенных сообщений.
- Система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам.
- Система должна поддерживать управление через Web интерфейс.
- Система должна иметь возможность интеграции с системами централизованного управления и построения отчетов.
- Система должна поддерживать протоколы NetFlow, sFlow.
- Система должна обеспечивать режим обратного прокси-сервера (reverse proxy).
- Система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy).
- Система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки.
- Система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях.
- Система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа.
- Система должна обеспечивать возможность управления беспроводными точками доступа.
- Система должна обеспечивать возможность управления коммутаторами.

Шлюзы безопасности должны иметь подписки на сервисы в течение 3 лет:
- Контроль приложений
- IPS
- AV
- Botnet IP/Domain
- Mobile Security
- Web Filtering
- Antispam
- Sandbox Cloud

4.6.4. Общие требования к функционалу коммутаторов

Коммутатор должен обеспечивать исключительную безопасность, производительность и управляемость.

Решение должно быть надежным, простым и масштабируемым.

Предоставляемое оборудование должно иметь возможность тесной интеграции в платформе, где обеспечивается комплексная, интегрированная и автоматизированная защита по всей поверхности цифровых атак, защищая критически важные устройства, данные, приложения и подключения от центра обработки данных до облака и домашнего офиса.

Предлагаемый коммутатор должен иметь возможность управления непосредственно из знакомого специально выделенного интерфейса.

Коммутатор должен иметь возможность настройки из командной строки.

Коммутатор должен быть оснащен как минимум одним портом USB Type-A с возможностью подключения съемных переносных носителей памяти для копирования с/на них файлов конфигурации и программного обеспечения и возможностью подключения электронных USB-ключей.

Коммутатор должен быть оснащен как минимум 48 портами типа BASE-T для передачи и приема информации.

Коммутатор должен поддерживать технологию агрегация каналов с несколькими шасси (MCLAG).

Предлагаемое оборудование должно поддерживать следующие функции канального уровня передачи данных (Уровень 2):

- Jumbo кадры
- Автосогласование скорости порта и дуплекса
- MDI/MDIX Автокроссовер
- IEEE 802.1D MAC-мост/STP
- Протокол быстрого связующего дерева IEEE 802.1w (RSTP)
- Протокол множественного связующего дерева IEEE 802.1s (MSTP)
- Корневая защита STP
- Защита STP BPDU
- Пограничный порт/порт Fast
- Маркировка VLAN IEEE 802.1Q
- Частная виртуальная локальная сеть
- Агрегация каналов IEEE 802.3ad с LACP
- Баланс одноадресного/многоадресного трафика через транкинговый порт
- (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac)
- Агрегация каналов IEEE 802.1AX
- Экземпляры связующего дерева (MSTP/CST)
- Управление потоком IEEE 802.3x и противодавление

Предлагаемое оборудование должно поддерживать следующие функции сетевого уровня передачи данных (Уровень 3):

- Статическая маршрутизация (аппаратная)
- Протоколы динамической маршрутизации: OSPFv2, RIPv2, VRRP, BGP, ISIS
- Многоадресные протоколы: PIM-SSM
- ECMP
- Обнаружение двунаправленной пересылки (BFD)
- DHCP-ретранслятор
- Обнаружение конфликта IP-адресов и уведомление
- DHCP-сервер
- Одноадресная переадресация обратного пути — uRPF
- Фильтрация маршрутов IPv6
- Фильтрация карт маршрутов на основе протокола маршрутизации

Коммутатор должен поддерживать следующие функции безопасности и видимости:

- Безопасность и видимость
- Зеркалирование портов
- Аутентификация администратора через RFC 2865 RADIUS
- Аутентификация IEEE 802.1X на основе порта
- Аутентификация IEEE 802.1X на основе MAC
- Обход MAC-доступа IEEE 802.1X (MAB)
- Назначение динамической VLAN IEEE 802.1X
- Radius CoA (Смена органа власти)
- ACL-список

Предлагаемый коммутатор должен поддерживать следующие функции качества обслуживания:

- Организация очереди приоритетов на основе IEEE 802.1p
- Организация очереди приоритетов на основе IP TOS/DSCP
- IEEE 1588 PTP (прозрачные часы)
- Явное уведомление о перегрузке
- Маркировка приоритета выхода
- Контроль процентной ставки

Предлагаемый коммутатор должен поддерживать следующие функции управления:

- Управление IPv4 и IPv6
- Телнет/SSH
- HTTP / HTTPS
- SNMP v1/v2c/v3
- SNTP
- Стандартный CLI и веб-интерфейс GUI
- Загрузка/выгрузка программного обеспечения: TFTP/FTP/GUI
- Управляется из FortiGate
- Поддержка HTTP REST API для
- Конфигурация и мониторинг

4.6.5. Требования к техническим характеристикам сервера

Наименование	Технические характеристики
Количество	1 шт.
Технические требования	
Форм фактор	Не более 5U
Количество поддерживаемых ЦПУ	До 8
Количество установленных ЦПУ	Не менее 4
Параметры ЦПУ	Не менее 3,9 ГГц; Не менее 8 ядер; Не менее 16 потоков; Не менее 35 мб Кэш памяти;
Количество поддерживаемых слотов ОЗУ	Не менее 48
Количество заполненных слотов ОЗУ	Не менее 24
Параметры установленной ОЗУ	Не менее DDR4 3200 МГц; Не менее 2 ТБ;
Контроллер жестких дисков	Не менее 8 портов типа SAS 12G Не менее 2 Гб Кэш памяти Поддержка уровней RAID не менее 0, 1, 5 и 10.
Тип дисков	Не менее 6G SATA SSD Mixed Use
Диски	Не менее 2 х 480 ГБ
Сетевые адаптеры	Не менее 4 портов 16 Гбит FC Не менее 16 портов 1 Гбит BASE-T
Трансиверы	Не менее 4 х 16 Гбит SFP+
Охлаждение	Не менее 8 вентиляторов
Блок питания	Не менее 4 х 1600 Вт
Сертификация БП	Не менее Platinum
Горячая замена БП	Обязательно

Горячая замена вентиляторов	Обязательно
Комплект обнаружения проникновения в корпус	Обязательно
Лицевая защитная панель	Обязательно
Комплект крепежей	Обязательно

4.6.6. Требования к техническим характеристикам системы хранения данных

Наименование	**Технические характеристики**
Количество	1 шт.
Технические требования	
Форм фактор	Не более 4U
Тип массива	All Flash – NVMe
Доступность	Не менее 99,9999%
Контроллер	Не менее 2 Не менее 128Гб Кэш памяти на каждый контроллер
Поддерживаемые RAID уровни	RAID Triple+ Parity
Интерфейсы	Не менее 4 портов 32 Гбит FC на контроллер Не менее 8 портов 1 Гбит BASE-T
Трансиверы	Не менее 4 х 32 Гбит FC SFP+
Тип дисков	Не менее NVMe SSD
Диски	Не менее 24 х 3,84 Тб
Блок питания	Не менее 4 х 800 Вт
Сертификация БП	Не менее 80 PLUS Platinum
Горячая замена БП	Обязательно
Поддержка полок расширения	Обязательно
Количество поддерживаемых полок расширения	Не менее 2
Объем поддерживаемых накопителей NVMe учитывая все полки расширения	Не менее 72
Поддержка кластеризации массива	Обязательно
Объем поддерживаемых накопителей NVMe учитывая кластеризацию	Не менее 280
Комплект крепежей	Обязательно

4.6.7. Требования к техническим характеристикам аппаратных межсетевых экранов

Наименование	**Технические характеристики**
Количество	2 шт.
Технические требования	
Форм фактор	Не более 1U.
Пропускная способность с контролем состояния соединений (1518 / 512 / 64 byte UDP пакетов)	Не менее 10 / 10 / 6 Гбит/с.
Задержка при обработке пакетов	Не более 5 Мкр сек.
Пропускная способность по количеству пакетов	Не менее 9 000 000 пакетов/сек.

Производительность IPsec VPN	Не менее 6.5 Гбит/с.
Количество VPN-тунелей (точка-точка)	Не менее 200
Количество VPN-тунелей (клиент-точка)	Не менее 500
Производительность IPS	Не менее 1.4 Гбит/с
Производительность SSL VPN	Не менее 900 пакетов/сек.
Application Control Throughput (HTTP 64K)	не менее 1.8 Гбит/с.
Threat Protection Throughput Enterprise Mix	не менее 700 Мбит/с.
Количество SSL VPN пользователей	Не менее 200.
Количество новых сессий в секунду	Не менее 35 000.
Количество одновременных сессий	Не менее 700 000.
Производительность в режиме инспекции SSL-трафика	Не менее 630 Мбит/с.
Количество политик безопасности	Не менее 10 000.
Встроенные интерфейсы	Не менее 2 портов GE RJ45 WAN; Не менее 1 порта GE RJ45 DMZ; Не менее 7 портов GE RJ45 Internal; Не менее 1 порта RJ45 Console; Не менее 1 порта USB Port.
Количество виртуальных контекстов безопасности	Не менее 10.
Блок питания	100–240V AC, 50–60 Hz.

4.6.8. Требования к техническим характеристикам коммутаторов

Наименование	**Технические характеристики**
Количество	2 шт.
Технические требования	
Форм фактор	Не более 1U.
Количество/тип портов	- не менее 48 портов 10/100/1000 RJ45; - не менее 4 слотов SFP+; - не менее 1 консольного порта RJ45; - не менее 1 порта USB 2.0;
Пропускная способность	не менее 176 Гбит/с
Производительность коммутатора при обработке IPv4/IPv6 пакетов	Не менее 260 Mpps
Объем оперативной памяти	не менее 512 MB
Объем постоянной памяти (Flash)	не менее 64 MB
Размер таблицы маршрутизации, Unicast IPv4	Не менее 500 маршрутов

Размер таблицы маршрутизации, Unicast	Не менее 400 маршрутов
ACL	Не менее 768 записей
Количество поддерживаемых подсетей	Не менее 4096
Количество экземпляров протокола	Не менее 16
Блок питания встроенный	AC 100–240V AC, 50–60 Hz
Энергопотребление Вт	не более 57 Вт
Вес	не более 3.46 кг
Диапазон температуры хранения	-20 - 70 C
Диапазон температур в рабочем режиме	0 - 45 C
Диапазон относительной влажности при эксплуатации (без образования конденсата)	от 10 до 90%
Коммутатор должен поддерживаться технической поддержкой производителя в режиме	24x7 не менее 3 лет

4.6.9. Требования к дополнительным деталям для существующего оборудования

Наименование оборудования	Описание деталей	Кол-во
HPE MSA 1050	Блок питания 595 Вт (814665-001)	1 шт.
HPE MSA 1050	Контроллер MSA 1050 SAN (880098-001)	1 шт.
HPE MSA 1050	Диск 1.2ТБ 12G SAS 10K 2.5 HDD (EG001200JWJNK)	2 шт.
HPE MSA 2050	Контроллер MSA 2050 SAN (876127-002)	1 шт.
HPE MSA 2050	Диск 2.4ТБ 12G SAS 10K 2.5 HDD (EGO02400JWJNT)	2 шт.
HPE MSA 2050	Диск 800ГБ 12G SAS 2.5 SSD (XS800LE70084)	2 шт.
HPE MSA 2060	Блок питания 580 Вт (P12954-001)	1 шт.
HPE MSA 2060	Контроллер MSA 2060 FC (P12948-001)	1 шт.
HPE MSA 2060	Диск 2.4ТБ 12G SAS 10K 2.5 HDD (ST2400MM0129)	2 шт.
HPE DL360 Gen10	Блок питания 580 Вт Platinum (866729-001)	1 шт.
HPE DL360 Gen10	Диск 600ГБ 12G SAS 10K 2.5 DP HDD (EG000600JWJNP)	2 шт.
HPE DL360 Gen10	Сетевой адаптер HPE SN1200E 16Gb 2p FC HBA	1 шт.
HPE DL380 Gen10	Блок питания 800 Вт Platinum (866730-001)	1 шт.
HPE DL380 Gen10	Диск 300ГБ 12G SAS 10K 2.5 DP HDD (EG000300JWEBF)	2 шт.
HPE DL380 Gen10	Сетевой адаптер HPE SN1100Q 16Gb 2p FC HBA	1 шт.
HPE DL380 Gen10 Plus	Блок питания 800 Вт Platinum (P39385-001)	1 шт.
HPE DL380 Gen10 Plus	Диск 300ГБ 12G SAS 10K 2.5 DP HDD (EG000300JWEBF)	2 шт.
HPE DL380 Gen10 Plus	Сетевой адаптер HPE SN1100Q 16Gb 2p FC HBA	1 шт.
IBM Storwize V7000	Диск 600ГБ 12G SAS 15K 2.5 HDD (00AR323)	2 шт.

5. ПОРЯДОК КОНТРОЛЯ И ПРИЁМКИ СИСТЕМЫ

Контроль и приемка Системы должны проводиться в соответствии с требованиями O‘zDSt 1986:2018 Информационная технология. Информационные системы. Стадии создания.

Контролю, испытаниям и приемке могут подвергаться как Система в целом, так и ее отдельные очереди (пусковые комплексы), подсистемы и отдельные задачи.

Для Системы устанавливают следующие основные виды испытаний:

- предварительные испытания;
- эксплуатация.

6. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ СИСТЕМЫ К ВВОДУ В ДЕЙСТВИЕ.

К моменту окончания периода опытной эксплуатации обслуживающий персонал системы должен полностью овладеть практическими навыками работами с программно-техническим комплексом МКБ.

Для подготовки объекта к вводу Системы Заказчику необходимо выполнить следующие работы:

- разработать и реализовать, совместно с организацией - исполнителем, план мероприятий по подготовке объекта модернизации к внедрению Системы (подсистем);
- разработать, совместно с организацией-разработчиком, и утвердить дополнения и изменения в должностных инструкциях, определяющих работу персонала в условиях функционирования Системы;
- подготовить и оформить необходимую организационно-распорядительную документацию;
- обеспечить решение организационных вопросов по консультации и повышению квалификации сотрудников, которые будут работать с Системой;
- организовать изучение пользовательской документации Системы всеми вовлеченными отделами и подразделениями уполномоченного органа;
- обеспечить изучение пользователями эксплуатационной документации;
- подготовить нормативно-справочную и иную информацию и занести ее в соответствующие базы данных;
- провести контрольные испытания Системы (подсистем) совместно с исполнителем на рабочем месте администратора Системы.

Для подготовки объекта к вводу Системы организация-исполнитель обязана:

- разработать и реализовать совместно с организацией-заказчиком, план мероприятий по подготовке объекта к внедрению Системы (подсистем);
- разработать и обеспечить пользователей необходимой эксплуатационной документацией для работы с прикладным программным обеспечением Системы;
- провести контрольные испытания Системы (подсистем, задач) совместно с Заказчиком на рабочем месте администратора Системы;
- провести консультацию ключевых пользователей Системы

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Перечень подлежащих разработке комплектов и видов документов, соответствующих требованиям O’zDSt 1985:2018 Исполнитель согласовывает с Заказчиком на основании протоколов.

Вместе с отгруженным товаром Поставщик должен направить Заказчику нижеперечисленные документы:

- счет-фактура (инвойс) на сумму общей стоимости отгруженного товара на имя Заказчика;

- упаковочные листы;

- техническое описание аппаратного обеспечения на русском или английском языке

Передаваемая Заказчику документация должна быть выполнена в бумажном и электронном виде на носителе, предоставляемом Заказчиком.

Разработчик технического задания
Директор департамента
информационных технологий

С.Козимов _____
«18» мая 2023 г.