«УТВЕРЖДАЮ»
АКБ «УЗПРОМСТРОЙБАНК»
Первый Заместитель
Председателя Правления

А.Эргашев

_____ 2024 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

по проекту «Модернизация центров обработки данных для бесперебойной работы критичных бизнес-приложений».

1. Общие сведения.

Настоящее техническое задание разработано АКБ «Узпромстройбанк» и показывает необходимость модернизации ИТ-инфраструктуры центров обработки данных для устранения единых точек отказа и обеспечения бесперебойной работы критичных бизнес-приложений банка.

Полное наименование проекта.

«Модернизация центров обработки данных для бесперебойной работы критичных бизнес-приложений».

Наименование Заказчика.

Заказчик – АКБ «Узпромстройбанк»
Адрес: Республика Узбекистан, г.Ташкент,100000, Юнусабадский район, ул. Шахрисабзская, дом №3; Тел.: (998-71) 120 45 00 (1094);
МФО: 00440; ИНН: 200 833 707, Расчетный счет: 19907000000000440600;
Наименование банка: ОПЕРУ при АКБ «Узпромстройбанк»
Адрес электронной почты: info@uzpsb.uz.

2. Основание для реализации проекта

Основанием для реализации проекта является:

1. Постановление Президента Республики Узбекистан № ПП-1730 от 21.03.2012 г. «О мерах по дальнейшему внедрению и развитию информационно-коммуникационных технологий»;
2. Положение «Об организации защиты электронной информации в банках Республики Узбекистан» №492 от 23.06.2001г. (Рег. №1047 от 09.07.2001 г.);
3. Положение «О защите информации в электронных системах Центрального банка и ответственности должностных лиц» (Рег. № 633 от 17.01.2006 г.);
4. Положение «О защите информации в электронных системах коммерческих банков Республики Узбекистан» (Рег. № 1552 от 13.03.2006г.);
5. Постановление Президента Республики Узбекистан № ПП-3270 от 12.09.2017 г. «О мерах по дальнейшему развитию и повышению устойчивости банковской системы Республики Узбекистан»;
6. Постановление Президента Республики Узбекистан № ПП-3620 от 23.03.2018 г. «О дополнительных мерах по повышению доступности банковских услуг»;
7. ИТ-Стратегия АКБ «Узпромстройбанк» на 2023-2027 гг.

3. Цели и задачи проекта.

Основной целью реализации данного проекта является модернизация ИТ-инфраструктуры центров обработки данных для обеспечения бесперебойной работы критичных бизнес-приложений АКБ «Узпромстройбанк».

В рамках проекта планируется:

- построение отказоустойчивого растянутого на две площадки кластера виртуализации, для обеспечения высокой доступности и производительности сервисов Банка;
- модернизация системы резервного копирования, путем организации хранения «горячих» резервных копий на специализированных системах хранения данных, распределенных по двум площадкам АКБ «Узпромстройбанк».

Закупаемый в рамках проекта программно-аппаратный комплекс необходим для решения следующих задач:

- исключение единых точек отказа в ИТ-инфраструктуре для бесперебойного функционирования критичных бизнес-приложений АКБ «Узпромстройбанк»;
- внедрение георезервированного кластера виртуализации с нулевым временем простоя, для обеспечения доступности бизнес-приложений АКБ «Узпромстройбанк»;
- модернизация текущей системы резервного копирования, для возможности быстрого восстановления данных, а также для организации архивного резервного копирования на магнитную ленту.

4. Источники финансирования.

Источником финансирования проекта являются собственные средства АКБ «Узпромстройбанк».

5. Требования к потенциальному Исполнителю.

Поставщик определяется на конкурсной основе, в установленном законодательством и нормативными актами порядке и должен соответствовать следующим требованиям:

- представить свое Техническое предложение по поставке оборудования и программного обеспечения, удовлетворяющее всем требованиям данного документа.

Исполнителем, в обязательном порядке, должна быть предоставлена следующая информация:

- сертификаты технических специалистов по предлагаемым решениям;
- наличие авторизаций от региональных структурных подразделений производителей предлагаемого оборудования и программного обеспечения для участия в конкурсе по данному проекту (MAF);
- информация от производителей оборудования об авторизованных сервисных центрах/складах запчастей на территории Республики Узбекистан для обеспечения гарантийного обслуживания;
- информация от производителя ПО резервного копирования о проведении предпроектного обследования и технического аудита после внедрения.

6. Порядок осуществления поставки.

С момента поступления оборудования на таможенный склад либо склад Заказчика, специалистами Заказчика проводится проверка комплектности и осмотр оборудования на предмет наличия повреждений. После успешного включения оборудования и проведения нагрузочного тестирования Заказчик подписывает Акт приемки товаров. Вместе с оборудованием должна быть передана документация по эксплуатации.

С целью принятия результатов работ (услуг), Заказчик имеет право создать в установленном порядке Приемочную комиссию.

Место поставки.

- для нерезидентов Республики Узбекистан до таможенного склада города Ташкент на условиях поставки CIP-Ташкент;
- для резидентов Республики Узбекистан до склада Заказчика с учетом налогов и таможенных платежей.

Срок поставки.

90 банковских дней со дня осуществления предоплаты.

Требования к страхованию.

Согласно условиям поставки.

7. Общие требования к оборудованию.

Производитель, присутствующий в Узбекистане, как минимум, в течение 3 лет.

Исполнитель должен предусмотреть в поставке необходимое количество адаптеров, кабелей, коннекторов, переходников, конвертеров, усилителей и прочих соединительных материалов для реализации проекта.

Все оборудование должно поставляться со всеми необходимыми программными инструментами, принадлежностями и руководствами, и соответствующими сертификатами.

Оборудование должно отвечать требованиям международных стандартов в отношении экологического воздействия, потребления энергии и электромагнитного излучения.

8. Требования к гарантийному обслуживанию.

Гарантийный срок - 36 месяцев после поставки.

Жизненный цикл предлагаемого решения на момент приобретения должен составлять не менее 5 (пяти) лет.

В гарантийную техническую поддержку должны быть включены следующие услуги:

- техническая поддержка от производителя/ей, направленная на поддержание и восстановление работоспособности, в случае возникновении отказов;
- предоставление обновленных информационных материалов (документации);
- в случае обнаружения несоответствия, брака и т.д. Поставщик обязан в минимально возможные сроки произвести замену оборудования.

9. Требования к комплектации.

Товар должен быть упакован и промаркирован в соответствии с требованиями действующего законодательства РУз. Товар поставляется в заводской упаковке. Стоимость тары и упаковки входит в цену товара.

Товар должен иметь полную комплектацию, в которую входит весь перечень заказываемых программных средств необходимых для полноценного функционирования предлагаемого решения в рамках текущего ТЗ.

10. Требования на соответствие товара нормативным документам в области технического регулирования.

Оборудование должно соответствовать действующим стандартам и нормам по пожарной, санитарной и электрической безопасности, а также электромагнитной совместимости, в соответствии с номенклатурой продукции, в отношении которой законодательными актами Республики Узбекистан предусмотрена обязательная сертификация с документальным подтверждением.

Товар должен соответствовать требованиям нормативных документов в области технического регулирования (O'zDSt 2815:2014, O'zDSt 2875-2014, ПУЭ (правил устройства электроустановок) и др.

11. Технические требования к поставляемому аппаратно-программному комплексу:

1.	**Система обработки и хранения данных (гиперконвергентная инфраструктура)**	комплект	**1**
	Технические характеристики и требования к оборудованию:		
	Физические параметры	• Гиперконвергентная инфраструктура должна устанавливаться в монтажный шкаф(ы) для серверного оборудования 19" и состоять из узлов «серверов» с физическим размером узла не большим 1U с процессорами архитектуры x86 с возможностью замены сервера без остановки работы всей системы. Серверы должны быть оборудованы кабельными органайзерами от производителя для удобства обслуживания.	
	Отказоустойчивость	• Аппаратное резервирование шин питания и ввода/вывода. Каждый узел системы должен комплектоваться блоками питания горячей замены с уровнем доступности 1+1. • Каждый узел системы должен комплектоваться вентиляторными модулями достаточной мощности в количестве, необходимом для отказоустойчивой работы системы с полным набором внутреннего оборудования. • Вентиляторные модули должны работать в режиме горячего резервирования (выход из строя части вентиляторов не должен приводить к остановке работы системы).	
	Управление гиперконвергентной системой	• Гиперконвергентная система должна комплектоваться всеми необходимыми программно-аппаратными средствами для реализации следующих основных возможностей: • Предоставление единого интерфейса управления всем включенным в систему оборудованием через Web. Ролевое ограничение прав администраторов. • Удаленное управление с помощью встроенных в серверы средств управления и мониторинга. • Мониторинг производительности установленных серверов. Возможность удаленной установки всего необходимого для работы сервера ПО, включая операционную систему. • Возможность простого восстановления сервера после серьезного сбоя (по восстановлению всего ПО и настроек соединений). • Управление на уровне политик интегрировано с VMware vSphere с возможностью контроля производительности сверху вниз.	

		• Система должна обеспечивать управление журналами событий и аналитикой причины возникновения инцидента. Система аналитики событий должна быть интегрирована в среду VMware. • Поддержка REST-API • Гиперконвергентная система должна иметь единый пользовательский интерфейс для управления жизненным циклом эксплуатации всего установленного в систему оборудования и ПО посредством Web-браузера; • Система управления должна быть отказоустойчивой и продолжать функционирование при аппаратном отказе одного из компонентов; • Полный выход из строя системы управления гиперконвергентной системы не должен приводить к простою в функционировании всего установленного в него оборудования и приложений; • Гиперконвергентная система должна поддерживать автоматический процесс установки и настройки всех основных компонентов виртуализации, управления СХД и сетевой инфраструктурой. Результатом процесса должен быть полностью готовый кластер под управлением VMware vCenter, в котором доступна возможность безопасного запуска виртуальных машин; • Максимальное время автоматического развёртывания для первого устройства не должно превышать 30 минут, для дополнительных устройств – 5 минут; • Гиперконвергентная система должна поддерживать автоматические процедуры обновления всех программных компонентов и микрокодов оборудования без остановки работы приложений; • Гиперконвергентная система должна обеспечивать непрерывную работу всех приложений и системы управления при выполнении операций по плановой замене любых компонентов одного узла; • Гиперконвергентная система должна поддерживать возможность выполнения безопасных процедур по замене дисковых накопителей и серверных узлов силами обслуживающего персонала заказчика.
	Требования к инфраструктуре доступа к данным	• Подсистема хранения данных должна базироваться на технологиях программно-определяемой архитектуры хранения данных с возможностью балансировки нагрузки и отказоустойчивости между всеми аппаратными компонентами на уровне ядра гипервизора и использовать технологии флэш-накопителей, дедупликации и компрессии в реальном времени. В случае невозможности реализации подсистемы на уровне гипервизора необходимо добавить дополнительно вычислительные ресурсы для виртуальных машин,

		которые должны обеспечивать данную функцию. Система должна включать не менее 368 ТБ RAW дискового пространства на флэш-накопителях. Подсистема хранения данных должно поддерживать следующие политики доступности данных: количество допустимых отказов равное 0, 1 или 2; erasure coding (RAID5, RAID6). • Подсистема хранения данных должна обеспечивать логическую сегментацию доступа к данным на уровне каждой виртуальной машины или файла виртуальной машины. (сбой доступа к данным одной виртуальной машины не должен сказываться на работе других). Возможность назначать уровень защиты и задавать приоритеты доступа к дисковым ресурсам (пропускная способность) на каждый файл виртуальной машины. Система хранения данных должна поддерживать создание единого кластера в масштабах двух ЦОД с одновременным доступом к данным на обеих площадках в режиме Active-Active. • Система хранения данных должна обеспечивать защиту данных на уровне выхода из строя как минимум одного диска или серверного узла. • Система должна иметь возможность масштабироваться в рамках каждого узла кластера и путем добавления дополнительных узлов. Количество узлов кластера должно масштабироваться не менее чем до 64. • Гиперконвергентная система должна включать возможность синхронной и асинхронной репликации между различными системами, как программно-определенными, так и классическими на основе контроллеров. В рамках решения должно предоставляться соответствующее решение репликации. • Поддержка шифрования данных на уровне datastore и виртуальных машин.
	Требования к платформе виртуализации	• Должно быть централизовано управление платформой виртуализации и автоматизация процессов администрирования. • Платформа должна поддерживать механизмы перераспределения нагрузки между узлами кластера без остановки работы виртуальных машин. • Платформа должна поддерживать механизмы изменения конфигурации виртуальных машин. • Платформа должна предоставлять механизмы создания мгновенных снимков гостевых операционных систем. • Платформа должна поддерживать интеграцию с системой управления виртуальными рабочими столами. • Поддержка распределенных виртуальных коммутаторов для серверов виртуализации, управляемых централизованно.

		• Поддержка создания иерархической структуры пулов вычислительных ресурсов (CPU/RAM) физических серверов с назначением приоритетов или выделенного резерва по ресурсам. • «Горячее» добавление процессоров и оперативной памяти для работающей гостевой ОС (для поддерживаемых ОС – без остановки работы гостевой ОС). • Возможность создания клонов работающих виртуальных машин с измененными параметрами сети и вводом в домен MS AD. • Архитектурная возможность использования собственной виртуализации сети. • Система виртуализации должна поддерживать ПО антивирусной защиты на уровне гипервизора без необходимости установки агентов внутрь виртуальной машины.
	Лицензии ПО VMware которые должны быть включены в состав комплекса	• VMware vSphere Standard для всех процессоров программно-аппаратного комплекса. • ПО подсистемы программно-определяемого хранения VMware vSAN Enterprise с функционалом дедупликации, компрессии и метро кластера для всех процессоров и предложенного дискового пространства программно-аппаратного комплекса. • В комплект поставки должно входить программное обеспечение VMware vCenter редакции Standard • Тип лицензий: постоянные с технической поддержкой на 3 года или аналогичная подписка с технической поддержкой на 3 года, с возможностью продления
	Суммарное количество процессорных ядер в серверах кластера (без учета технологии Intel Hyper-Threading или аналогичной)	• Не менее 1536 физических процессорных ядер.
	Требования к процессорам по архитектуре и продуктивности	• Не хуже Intel® Xeon® Platinum 8462Y+ 2.8G, 32C/64T, 16GT/s, 60M Cache, Turbo, HT (300W) DDR5-4800.
	Суммарное количество оперативной памяти в кластере	• Не менее 49152 ГБ оперативной памяти не хуже DDR5-4800.
	Суммарный RAW объем дисковой подсистемы кластера	• Не менее 368ТБ All-Flash, количество дисков на каждом сервере не должно быть меньше восьми без учёта кэш уровня. • Дополнительно должны быть предусмотрены накопители 1.6TB Enterprise NVMe Mixed Use для организации кэш-уровня и создания двух дисковых групп на каждом сервере кластера

Серверные узлы в составе гиперконвергентной инфраструктуры -24 шт.	
Процессор(ы)	• Наличие не менее двух процессоров Intel® Xeon® Platinum 8462Y+ 2.8G, 32C/64T, 16GT/s, 60M Cache, Turbo, HT (300W) DDR5-4800 или эквивалент.
Память	• Наличие не менее 2048 ГБ, модулями памяти не меньше 64GB RDIMM 4800MT/s. • Возможность увеличения объема памяти до 4096 GB при полной замене установленных модулей. Память не хуже RDIMM 4800MT/s.
Накопители/жесткие диски	• Наличие не менее 2 (двух) накопителей 1.6TB Enterprise NVMe Mixed Use AG Drive U.2 Gen4, с поддержкой возможности “горячей” замены. • Наличие не менее 8 (восьми) накопителей 1.92TB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD, с поддержкой возможности “горячей” замены.
Диски для загрузки ОС/гипервизора	• Наличие не менее чем 2 (двух) накопителя M.2 960GB (в RAID 1)
Блоки питания	• Наличие не менее 2х блоков питания мощностью не менее 1100W 100-240V, с поддержкой возможности “горячей” замены и подключением кабелями C13-C14 к PDU. Кабели питания 2 шт. Rack Power Cord 2M (C13/C14 10A) должны в комплекте поставки. • Эффективность блоков питания не хуже чем Titanium
Подключения к сети Ethernet	Наличие не менее чем: • 2 (два) сетевых адаптера Dual Port 10/25GbE SFP28, один из которых не должен занимать слот PCIe (в комплекте должны быть соответствующие модули 25Gbe SFP28); • 1 (один) сетевой адаптер Dual Port 1GbE Optional LOM, который не должен занимать слот PCIe.
Требования по управлению и мониторингу	• В сервере (узле) должны быть предусмотрены программно-аппаратные средства от производителя сервера для конфигурирования управления и мониторинга работы всех компонентов
Механизмы управления узлами в условиях отсутствия физического доступа к ним (устройство удаленного присутствия)	• Графический интерфейс. • Удаленное управление питанием. • Платформо-независимая текстовая или графическая консоль для отображения управления активностью удаленного сервера. • Интерфейс командной строки и сценариев. • Шифрование SSL. • Возможность диагностики CPU и сервера. • Поддержка DNS\DHCP.

		• Возможность обновления микрокода IPMI через локальную сеть. • Возможность подключения образов в качестве локальных дисковых устройств.		
	Поддержка гипервизоров и сред управления виртуализации	• VMware ESXi версий не менее 8.x		
	Гарантия и техническая поддержка	• Не менее 36 месяцев (от изготовителя оборудования). • Обслуживание в режиме NBD (на следующий рабочий день). • Возможность регистрации обращений к технической поддержке по схеме: 24x7x365. • Гарантийное восстановление работоспособности оборудования или устранение технических неисправностей в работе оборудования должно быть обеспечено по месту эксплуатации оборудования (on-site). • Наличие единого колл-центра и/или web-портала производителя оборудования для приема сервисных обращений.		
2.	**Система хранения резервных копий**		шт	**2**
	Технические характеристики и требования к оборудованию:			
	Конструкция	• Для установки в шкаф 19”, монтажный набор должен быть в комплекте поставки		
	Аппаратные ресурсы	• наличие не менее 150 ТВ доступного дискового пространства (без учета дедупликации); • возможность расширения дискового пространства до не менее чем 280ТВ. • система должна адресовать локальный логический объём резервных копий в размере не менее 18 ПБ; • наличие не менее 2 шт. выделенных SSD объемом не менее 1,92ТВ для обслуживания каталога метаданных дедупликации и операций ускорения восстановления резервных копий. • наличие выделенного интерфейса для подключения к сети управления; • наличие не менее 4 (четыре) интерфейсов 16GB FC для подключения к продуктивной сети (в комплекте должны быть соответствующие модули SFP); • наличие не менее 4 (четыре) интерфейсов 25G (в комплекте должны быть соответствующие модули SFP) • наличие не менее 8 кабелей типа OM4 Fibre Cable LC-LC длиной 5 метров		
	Функциональность системы хранения резервных копий	• поддержка управления системой через WEB и CLI; • обеспечение ролевого доступа; • поддержка протоколов CIFS, NFS, NDMP;		

		• поддержка одного из протоколов распределенной дедупликации: OST, DDBoost, Accent; • поддержка эмуляции ленточных библиотек (VTL); • поддержка глобальной дедупликации хранящихся данных, система должна выявлять и устранять дубликаты данных независимо от использованного протокола и способа, которым они были записаны на систему хранения. • поддержка дедупликации с идентификацией блоков данных переменной длины; • наличие специализированного аппаратного адаптера, отвечающего за сжатие данных. В случае отсутствия такого адаптера предусмотреть в системе дополнительное полезное дисковое пространство в размере 45 ТВ (30% от 150 ТВ) поддержка репликации данных на уровне систем хранения с возможностью репликации только уникальных (дедуплицированных) данных; • поддержка шифрования резервных копий с возможностью использования внешнего менеджера ключей шифрования; • для защиты от киберугроз и обеспечения неизменности хранимых резервных копий система должна иметь функцию защиты данных от удаления или изменения в течение указанного периода времени. Дополнительно система должна предоставлять механизмы защиты от выполнения деструктивных действий, которые могут привести к потере данных и деструктивных действий лица или группы лиц с привилегиями администратора системы и/или офицера информационной безопасности. В случае отсутствия вышеуказанных функций защиты резервных копий следует предусмотреть сохранение дополнительных копий данных на отдельной системе с идентичными к основной системе техническими характеристиками, лицензиями и сроком сервисной поддержки. • возможность включения автоматической защиты данных от удаления или внесения изменений; • возможность использования системы для построения полностью изолированного (air-gapped) хранилища резервных копий;
	Производительность системы	• система должна обеспечивать скорость операций резервного копирования на уровне 15 ТВ/час для протоколов NFS, CIFS, VTL и не менее 32 ТВ/час при использовании протокола распределенной дедупликации; • поддержка многопоточного резервного копирования и восстановления. Система должна поддерживать не менее 400 одновременных потоков операций резервного копирования;

		• технология дедупликации должна обеспечивать масштабирование функционала путем переноса части нагрузки на сервера системы резервного копирования с использованием протоколов оптимизации передачи данных;
	Надежность и целостность информации	• в режиме штатного функционирования система должна круглосуточно обеспечивать возможность выполнения операций резервного копирования, архивации, восстановления и репликации данных. Выполнение различных задач одновременно (например, репликация и копирование данных) не должно оказывать существенного влияния на доступность системы, ее производительность и заявленные возможности; • функция постоянного контроля состояния системы. Система должна обеспечивать постоянную проверку целостности данных и автоматическое устранение\корректировку выявленных ошибок; • система должна поддерживать процедуры расширения дискового пространства без остановки работы; • в целях защиты инвестиций, архитектура системы должна предусматривать возможность процедуры модернизации до более производительной или новой аппаратной версии, а также обеспечивать сохранность всех данных, хранящихся в системе при выполнении такой процедуры. В случае отсутствия такой возможности необходимо предоставить гарантийное письмо производителя системы относительно продолжительности жизненного цикла системы, которое должно составлять не менее 7 лет с момента приобретения системы;
	Аналитическая подсистема	• обеспечение автоматического сбора и анализа данных, мониторинг и формирование отчетности; • наличие функций прогнозирования и планирования использования емкости; • анализ показателей работы системы в реальном времени.
	Гарантия и техническая поддержка	• Не менее 36 месяцев (от производителя оборудования). • Обслуживание в режиме NBD (на следующий рабочий день). • Возможность регистрации обращений к технической поддержке по схеме: 24x7x365. • Гарантийное восстановление работоспособности оборудования или устранение технических неисправностей в работе оборудования должно быть обеспечено по месту эксплуатации оборудования (on-site).

		• Наличие единого колл-центра и/или web-портала производителя оборудования для приема сервисных обращений.		
3.	**Ленточная библиотека**		шт	**1**
	Технические характеристики и требования к оборудованию:			
	Тип устройства	• Роботизированная ленточная библиотека LTO9 Ultrium		
	Архитектура	• Управляющий модуль для монтажа в шкаф 19” размером не более 3U, с возможностью наращивания модулями расширения каждый из которых не превышает 3U. • Поддержка не менее 6 модулей расширения на библиотеку		
	Тип носителей	• Не ниже LTO-9		
	Количество ленточных приводов	• Не менее 6шт. типа LTO9, с возможностью расширения до не менее чем 21		
	Количество слотов для картриджей	• Не менее чем 70, со штрихкодами		
	Емкость	• Емкость картриджа: не менее 18 ТБ (стандартно), не менее 45 ТБ (компрессия не хуже 2.5:1). • Емкость системы в целом: не менее 720 ТБ (стандартно), не менее 1800 ТБ (компрессия не хуже 2.5:1).		
	Внешний интерфейс приводов	• Не менее одного FC порта на один ленточный привод, не хуже 8Гб/с		
	Система управления	• Возможность локального управления с помощью ЖК-дисплея. • Система удаленного управления системой через Web-браузер		
	Другие функции	• Наличие функции управления электропотреблением. • Наличие функции контроля скорости передачи данных. • Наличие функции считывания штрихкода (Bare Code Reader).		
	Совместимость с операционными системами	• SuSE Linux, Red Hat Enterprise Linux, • Windows		
	Электропитание	• Не менее 2 блоков питания на корпус (основной и резервный). • Возможность "горячей" замены блоков питания. • Мощность каждого блока питания достаточно для работы системы в максимальной комплектации в		

		режиме максимальной нагрузки без ограничения во времени.
	Комплект поставки	• Не менее 20 (двадцать) картриджей RW емкостью 18 ТБ (без компрессии) каждый. • Не менее 2 картриджей для чистки механизма считывания/записи. • Комплект рельсов для установки в шкаф. • Кабели питания 2M Rack Power Cord C13/C14 12A – 4 шт. • стандарт OM4 Fibre Cable LC-LC длиной 5 метров – не менее 10 шт
	Гарантия и техническая поддержка	• Не менее 36 месяцев (от производителя оборудования). • Обслуживание в режиме NBD (на следующий рабочий день). • Возможность регистрации обращений к технической поддержке по схеме: 24x7x365. • Гарантийное восстановление работоспособности оборудования или устранение технических неисправностей в работе оборудования должно быть обеспечено по месту эксплуатации оборудования (on-site). • Наличие единого колл-центра и/или web-портала производителя оборудования для приема сервисных обращений.
4.	**Требования к программному обеспечению для резервного копирования, репликации и восстановления.**	
	Общие требования	Лицензии ПО для резервного копирования должны покрывать все 24 хоста поставляемой гиперконвергентной инфраструктуры
	Поддержка виртуальных инфраструктур	• Поддержка резервного копирования виртуальной инфраструктуры на базе платформы VMware vSphere 6.0 и выше, включая VMware vSphere 8.0, иметь сертификацию VMware Ready for vSAN; • Поддержка копирования виртуальной инфраструктуры на базе платформы Microsoft Hyper-V начиная с версии Windows Server 2012 и выше, включая Microsoft Hyper-V 2022 и поддержку 64 TB VHDX; • Поддержка резервного копирования виртуальной инфраструктуры на базе платформы Nutanix AHV, начиная с версии AHV 5.5.x и выше; • Поддержка резервного копирования виртуальной инфраструктуры на базе платформы Red Hat Virtualization, начиная с версии RHV 4.4 SP1. Версия Red Hat Virtualization manager 4.5.0 и выше; • Поддержка резервного копирования контейнеров vApp, ВМ и их метаданных, а также их

		восстановления непосредственно в инфраструктуру vCloud Director. • Поддержка автоматизации задачи и обеспечение возможности работы через портал самообслуживания для VMware vCloud Director
	Поддержка ОС	• Резервное копирование пользовательских систем с установленной ОС Microsoft Windows 7 SP1 и выше; • Резервное копирование серверных систем с установленной ОС Microsoft Windows Server 2008 R2 SP1 и выше; • Резервное копирование систем с установленной ОС Linux на основе Debian 10.13 и выше, Ubuntu 16.04 и выше, CentOS 7.0 и выше, RHEL 6.0 выше, Oracle Linux 6 и выше, Fedora 36 и выше, openSUSE 15.3, SLES 12 SP4 и выше; • Резервное копирование систем с установленной ОС IBM AIX 6.1 и выше, Oracle Solaris 10-11.4 SPARC и Oracle Solaris 10-11.4 x86; • Резервное копирование систем с установленной ОС macOS следующих версий: Big Sur 11.X.X, Catalina 10.15.X, Mojave 10.14.X и High Sierra 10.13.6, Monterey 12, Ventura 13;
	Поддержка корпоративных приложений и баз данных	• Поддержка резервного копирования отдельных баз данных при помощи интеграции с интерфейсов backint SAP HANA для SAP HANA 2.0: SPS 02, SPS 03, SPS 04, SPS 05, SPS 06 (только через Backint версии 1.0), SAP HANA 1.0: SPS 12 и далее; • Поддержка резервного копирования отдельных баз данных при помощи интеграции с BR*Tools для SAP на Oracle с поддержкой BR*Tools 7.20 Patch 42 и далее, Oracle Database 11gR2, 12c, 18c, 19c: редакций Standard и Enterprise. С поддержкой платформ: SUSE Linux Enterprise Server 11, 12, 15 (x86_64), Red Hat Enterprise Linux для SAP Applications 6, 7 (x86_64), Oracle Linux 6, 7; • Поддержка резервного копирования отдельных баз данных при помощи интеграции с Oracle RMAN для Oracle Database 11gR2, 12c, 18c, 19c, 21c: редакций Standard и Enterprise; • Поддержка резервного копирования отдельных баз данных Microsoft SQL Server при помощи интеграции с Microsoft SQL Server Management Studio для Microsoft SQL Server 2014 SP3 – 2022;
	Общие функциональные возможности платформы резервного копирования:	• Платформа резервного копирования должна иметь распределенную и горизонтально масштабируемую архитектуру резервного копирования; • Платформа резервного копирования должна иметь возможность встроенного резервного копирования самой себя для восстановления настроек; • Предоставлять Rest API для удаленного конфигурирования и управления;

		• Обеспечивать использование центрального сервера управления в качестве сервера распределения лицензий; • Основные компоненты платформы резервного копирования, за исключением управляющего сервера, должны иметь возможность развертывания, как на операционных системах Microsoft Windows, так и на семейство операционных систем Linux; • Платформа резервного копирования должна обеспечивать возможность выбора используемой базы данных для хранения конфигурации между Microsoft SQL Server версии 2012 и выше, а также PostgreSQL сервер версии 14.x и выше; • Платформа резервного копирования должна реализовывать поддержку протокола версии IPv6 для всех компонентов архитектуры; • Решение должно поддерживать возможность двухфакторной аутентификации с использованием специализированных приложений при доступе к консоли управления, как при наличии доступа к сети интернет, так и при его отсутствии; • Решение должно поддерживать учётные записи Microsoft gMSA, а также протокол Kerberos для выполнения операций аутентификации на гостевых операционных системах;
	Резервное копирование виртуальных машин	• Платформа резервного копирования должна обеспечивать возможность резервного копирования ВМ на уровне образов, с возможностью копирования только изменившихся блоков и с сохранением состояния приложений, а также без установки специализированных приложений внутрь ВМ; • Платформа резервного копирования должна поддерживать передачу резервных копий, как по сети передачи, так и по сети хранения данных, включая резервное копирования ВМ напрямую с NFS хранилищ; • Платформа резервного копирования должна поддерживать механизм автоматического изменения скорости процесса резервного копирования при увеличении времени отклика на чтение на всех системах хранения с возможностью определения порогов времени отклика; • Платформа резервного копирования должна иметь механизм дедупликации и сжатия резервных копий “на лету”, возможность исключать блоки служебных файлов ОС, а также папки и файлы, указанные пользователем, для ускорения процесса резервного копирования, а также для уменьшения объема хранимых данных; • Платформа резервного копирования должна уметь использовать аппаратные снимки СХД для резервного копирования, с возможностью обеспечения целостности приложений внутри

		виртуальных машин. Взаимодействие должно реализовываться при помощи специализированных API на уровне хранилища и без установки дополнительного программного обеспечения на них;
	Тестирование целостности и возможности восстановления резервных копий виртуальных машин	• Платформа резервного копирования должна иметь возможность создать изолированную среду на продуктивной инфраструктуре Заказчика, с возможностью использовать ее для автоматического тестирования резервных копий или для создания тестовых зон; • Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности резервных копий ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из резервных копий и/или аппаратных снимков СХД в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри резервируемой ВМ. Должна быть возможность использовать, как встроенные скрипты проверки, так и возможность использовать собственные скрипты; • Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности резервных копий ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из резервных копий в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри резервируемой ВМ. Должна быть возможность использовать, как встроенные скрипты проверки, так и возможность использовать собственные скрипты;
	Резервное копирование физических машин	• Платформа резервного копирования должна обеспечивать возможность резервного копирования ОС на уровне образов, на уровне томов, а также на уровне отдельных файлов, с сохранением состояния приложений; • Платформа резервного копирования должна поддерживать возможность использования аппаратных снимков СХД в качестве источника для резервного копирования томов с машин под управлением ОС MS Windows Server. Взаимодействие должно реализовываться при помощи специализированных API на уровне хранилища; • Платформа резервного копирования должна обеспечивать возможность копирования только изменившихся блоков, для уменьшения передаваемых данных; • Обладать возможностью резервного копирования в локальный кэш, в случае недоступности целевого устройства для резервного копирования, с

		последующей автоматической передачей данных из кэша на целевое устройство, при восстановлении доступа к данному целевому устройству; • Реализовывать механизм интеграции с приложениями, работающими на сервере с возможностью взаимодействия с транзакционными логами таких систем, как Microsoft Exchange, Microsoft SQL Server, Oracle database и PostgreSQL; • Осуществлять поддержку резервного копирования службы Microsoft Clustering; • Поддерживать возможность создания периодических синтетических полных резервных копий • Поддерживать возможность создания периодических активных полных резервных копий в рамках существующего задания резервного копирования; • Обеспечивать резервное копирование системы с учётом состояния таких приложений, как PostgreSQL и MySQL и обеспечения их консистентности; • Поддерживать управление, в том числе централизованное развёртывание и обновление, агентского программного обеспечения через единую консоль; • Реализовывать поддержку токена восстановления "Recovery Token" при восстановлении на новую аппаратную платформу; • Реализовывать поддержку аутентификации типа Oauth / Modern; • Платформа резервного копирования должна поддерживать возможность выбора метода создания снимков тома при бэкапе файловых систем семейства ОС Linux между собственной технологией и снимками LVM;
	Резервное копирование сетевых ресурсов	• Обеспечивать возможность создания резервных копий сетевых ресурсов, общий доступ к которым предоставляется по протоколам SMB (включая SMB v3) или NFS (включая NFS v4.1); • Поддерживать возможность создания VSS снимков при резервном копировании данных по протоколу SMB v3, для обеспечения консистентности; • Обладать функционалом хранения исторических версий файлов, с возможностью выгрузки наиболее старых версий на второстепенное хранилище резервных копий; • Поддерживать возможность использования аппаратных снимков СХД в качестве источника для резервного копирования файловых ресурсов, позволяющих избежать ограничений, связанных с блокировками файлов. Взаимодействие должно реализовываться при помощи специализированных

		API на уровне хранилища и без установки дополнительного программного обеспечения на них; • Поддерживать возможность сохранения резервных копий напрямую на объектное хранилище • Реализовывать возможность копирования всех точек восстановления на архивное хранилище и в случае недоступности основного хранилища автоматический переключаться на архивное во время восстановления данных; • Реализовывать поддержку установки опции неизменности данных на поддерживаемых хранилищах, а также иметь возможность проведения регулярной проверки состояния данных, хранимых на хранилище; • Платформа резервного копирования должна иметь возможность шифровать резервные копии файловых ресурсов; • Платформа резервного копирования должна обеспечивать возможность восстановления зашифрованных резервных копий даже в случае потери ключа шифрования
	Функциональные возможности репликации и аварийного восстановления виртуальных машин	• Платформа должна регулировать доступ к ресурсам резервной площадки с помощью делегирования контроля доступа; • Платформа резервного копирования должна поддерживать, как прямую репликацию виртуальных машин для платформ Microsoft Hyper-V и VMware vSphere, так и репликацию из существующих резервных копий, с возможностью обеспечения создания множества точек восстановления и передачей только изменившихся блоков; • Платформа должна обеспечивать целостность приложений внутри ВМ при репликации, без установки специализированных приложений внутрь ВМ; • При репликации ВМ между хранилищами, платформа резервного копирования должна иметь возможность возобновляемой передачи реплик между площадками с использованием механизмов сжатия и глобальной дедупликации трафика, и кэширования информации на обеих площадках на специализированных серверах; • Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину с возможностью автоматической смены сетевого интерфейса и IP адреса; • Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину даже при потере сервера резервного копирования;

	Тестирование целостности и возможности восстановления реплицированных виртуальных машин:	• Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности реплик ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из реплик в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри ВМ. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты; • Платформа должная обеспечивать автоматическое тестирование планов послеаварийного восстановления по требованию или по расписанию, и проверять их готовность без дополнительных ручных процедур; • Платформа должна обеспечивать возможность автоматической группировки виртуальных машин на основе подготовленных категорий, или тэгов; • Платформа резервного копирования должна обеспечивать возможность проверки резервных копий на наличие вирусов в составе процедуры автоматического тестирования. Проверка должна выполнятся при помощи антивирусного решения, используемого в инфраструктуре предприятия;
	Функциональные возможности непрерывной репликации и аварийного восстановления для виртуальных машин VMware vSphere	• Платформа резервного копирования должна поддерживать непрерывную репликацию виртуальных машин VMware vSphere, без использования снимков виртуализации, обеспечивающую минимальную потерю данных в пределах 2 секунд; • Платформа должна поддерживать возможность непрерывной репликации для VMware vSphere, VMware vCloud, а также репликацию в vCloud сервисного провайдера, предоставляющего данные услуги на территории страны; • Платформа должна непрерывно реплицировать операции ввода/вывода виртуальных машин и хранить их в специальном журнале на целевом хранилище данных в течении нескольких часов, указанных в краткосрочной политике хранения, в целях обеспечения возможности восстановления ВМ на определенный момент времени с заданным шагом; • Платформа должна обеспечивать возможность создания дополнительных точек восстановления ВМ, выходящих за пределы краткосрочной политики репликации, с учетом состояния работающих внутри приложении и обеспечения их консистентности, без установки специализированных приложений внутрь ВМ.
	Хранение резервных копий виртуальных машин	• Платформа резервного копирования должна интегрироваться со специализированными

		решениями для хранения резервных копий (дедуплицирующие устройства дискового хранения): EMC Data Domain по протоколу DDBoost, HPE StoreOnce по протоколу Catalyst, а также Quantum DXi и Fujitsu; • Платформа резервного копирования должна реализовывать интеграцию со специализированным решением для хранения резервных копий ExaGrid; • Платформа резервного копирования должна иметь возможность шифровать резервные копии виртуальных машин; • Платформа резервного копирования должна обеспечивать возможность восстановления зашифрованных резервных копий даже в случае потери ключа шифрования • Платформа резервного копирования должна иметь возможность интегрироваться с машинами на базе ОС Linux для использования их в качестве защищенных хранилищ резервных копий, позволяющих установить настройку неизменности данных, обеспечивающую возможность защиты от удаления и изменения блоков данных резервных копий на указанный промежуток времени; • Обеспечить возможность добавления и использования защищённых хранилищ на базе ОС Linux без необходимости сохранения учётной записи и пароля суперпользователя операционной системы в консоли управления; • Платформа резервного копирования должна иметь возможность объединения различных физических СХД в логически единый масштабируемый пул хранения резервных копий, для объединения доступного пространства отдельных СХД.; • Платформа резервного копирования должна иметь возможность сохранения данных резервных копий напрямую на объектные хранилища AWS S3/S3-совместимый/Azure Blob/Google Cloud Storage API, без необходимости использования промежуточного хранения данных; • Платформа резервного копирования должна иметь возможность перемещения резервных копий на устройства или сервисы объектного хранения на основе протокола AWS S3/S3-совместимый/Azure Blob/Google Cloud Storage API. Перемещение данных должно производиться, как по достижению определённого времени хранения, так и дублированием данных; • Платформа резервного копирования должна иметь возможность перемещения резервных копий из объектных хранилищ AWS/Azure в рамках единого логического масштабируемого пула на дополнительный архивный уровень на базе Amazon S3 Glacier/Azure Archival Storage. Перемещение

		данных должно производиться по достижению определённого времени хранения данных; • Платформа резервного копирования должна уметь передавать резервные копии между различными хранилищами с возможностью указания новой глубины хранения для резервной копии; • При передаче резервных копий между хранилищами, платформа резервного копирования должна иметь возможность возобновляемой передачи резервных копий между площадками с использованием механизмов сжатия и глобальной дедупликации трафика, и кэширования информации на обеих площадках на специализированных серверах; • Платформа резервного копирования должна поддерживать возможность перемещения резервных копий между разными хранилищами, а также поддерживать перемещение отдельных виртуальных машин между разными заданиями включая уже созданные для неё резервные копии; • Платформа резервного копирования должна иметь возможность передачи резервных копий между удаленными площадками без установления дополнительного VPN соединения; • Платформа резервного копирования должна поддерживать резервное копирование на ленточные библиотеки, включая многопоточную запись, возможность объединять ленточные накопители в пул с разных ленточных библиотек; • Платформа резервного копирования должна иметь возможность формирования синтетической полной резервной копии при записи на ленту из имеющихся в дисковом хранилище резервных копий полной резервной копии и цепочки инкрементальных без создания временной синтетической полной копии на диске;
	Хранение резервных копий физических машин	• Поддерживать политики хранения резервных копий на основе дней работы защищаемой физической машины; • Реализовывать возможность сохранения резервных копий в облачное хранилище Microsoft OneDrive Business и Personal с возможностью производить Bare-Metal восстановление непосредственно с точки хранения; • Платформа резервного копирования должна иметь возможность сохранения данных резервных копий напрямую на объектные хранилища AWS S3/S3-совместимый/Azure Blob/Google Cloud Storage API, без необходимости использования промежуточного хранения; • Поддерживать следующие целевые устройства для хранения резервных копий: локальные диски, съемные USB-носители, общие сетевые папки;

		• Предоставлять возможность архивировать резервные копий физических машин на ленточные носители данных, с возможностью последующего восстановления; • Платформа резервного копирования должна иметь возможность шифровать резервные копии; • Платформа резервного копирования должна обеспечивать возможность восстановления зашифрованных резервных копий даже в случае потери ключа шифрования
	Восстановление данных из резервных копий виртуальных машин	• Платформа резервного копирования должна поддерживать возможность восстановления из резервных копий даже в случае полной потери сервера резервного копирования; • Платформа резервного копирования должна поддерживать восстановление виртуальных машин как целиком, так и отдельных виртуальных дисков, и файлов конфигураций. Восстановление должно идти как по сети передачи, так и по сети хранения данных; • Платформа резервного копирования должна обеспечивать моментальный запуск виртуальных машин непосредственно из хранилища резервных копий, как для платформы VMware vSphere, Microsoft Hyper-V так и для платформы Nutanix AHV. Данная технология должна иметь возможность последующего переноса виртуальной машины на выбранное хранилище данных без прерывания работы, а также поддерживаться на специализированных дедуплицирующих системах хранения; • Позволять осуществлять восстановление из резервной копии напрямую в Microsoft Azure/Amazon EC/Google Cloud в виде виртуальной машины; • Платформа резервного копирования должна обеспечивать возможность предварительного антивирусного сканирования и проверки резервных копий при восстановлении; • Платформа резервного копирования должна обеспечивать возможность до восстановления ВМ в рабочую инфраструктуру удалить данные из этой ВМ, не удаляя эти данные из резервной копии; • Платформа резервного копирования должна реализовывать гранулярное восстановление данных приложений из резервных копий, в промежуточное и/или исходное месторасположение без установки специализированного агента; • Платформа резервного копирования должна реализовывать гранулярное восстановление баз данных Oracle на Windows и Linux (с поддержкой технологии ASM), включая возможность восстановления данных до конкретной транзакции, в

		промежуточное и/или исходное месторасположение без установки специализированного агента. Решение должно быть сертифицировано по программе Oracle Backup Solutions Program (BSP) http://www.oracle.com/technetwork/database/availability/bsp-088814.html; • Платформа резервного копирования должна обеспечивать возможность моментального запуска и последующего восстановления баз данных MS SQL и Oracle из резервной копии на определенный момент времени на сервер или кластер баз данных. Запуск должен производиться без предварительного извлечения данных из резервной копии. Также должна быть реализована возможность параллельного фонового копирования файлов баз данных в целевое местоположение, синхронизации изменений и последующего переключения; • Платформа резервного копирования должна обеспечивать возможность позволять делегировать пользователям самостоятельно восстанавливать из резервной копии объекты приложений через Web-портал;
	Восстановление данных из резервных копий физических машин	• Поддерживать восстановление данных на уровне образа ОС, уровне томов, уровне отдельных объектов файловой системы; • Обеспечивать возможность восстановления для физических машин всей системы целиком в режиме bare-metal, а также на целевую систему с отличающейся аппаратной конфигурацией; • Обеспечивать возможность восстановления резервных копий на физический компьютер с дисками большего или меньшего размера; • Обеспечивать создание универсального аварийного загрузочного носителя для физических машин используемого для целей восстановления; • Обеспечивать возможность конвертации и экспорта резервных копии физических компьютеров в виде дисков виртуальных машин платформ виртуализации Microsoft Hyper-V и VMware vSphere; • Обеспечивать возможность моментального запуска виртуальной машины из резервной копии, созданной с физической системы под управлением MS Windows или Linux в средах виртуализации Microsoft Hyper-V, VMware vSphere. Запуск должен производиться без извлечения данных из резервной копии. Также должна быть реализована возможность переноса работающей виртуальной машины в режиме моментального запуска на производственные системы хранения данных без прерывания работы; • Позволять осуществлять восстановление из резервной копии физической машины или сервера напрямую в Microsoft Azure/Amazon EC/Google

		Cloud в виде виртуальной машины, при помощи, как самостоятельного решения, так и средствами централизованной консоли управления; • Платформа резервного копирования должна обеспечивать целостность приложений и реализовывать гранулярное восстановление данных приложений из резервных копий, в промежуточное и/или исходное месторасположение; • Обеспечивать возможность моментального запуска и последующего восстановления баз данных MS SQL и Oracle из резервной копии, созданной с физической системы на определенный момент времени на физический/виртуальный сервер или кластер баз данных. Запуск должен производиться без предварительного извлечения данных из резервной копии. Также должна быть реализована возможность параллельного фонового копирования файлов баз данных в целевое местоположение, синхронизации изменений и последующего переключения;
	Восстановление данных из резервных копий сетевых ресурсов	• Иметь несколько режимов восстановления: весь сетевой ресурс целиком, отдельные файлы и папки, только изменённые файлы на определённый момент времени; • Предоставлять возможность выбора исторической версии файла при восстановлении; • Обеспечивать возможность моментального восстановления файловых ресурсов, с помощью их публикации на сервере резервного копирования с доступом по протоколу SMB на определенный момент времени; • Обеспечивать возможность моментального восстановления файловых ресурсов, с помощью их публикации на сервере резервного копирования с доступом по протоколу NFS на определенный момент времени в режиме "только для чтения";
	Восстановление данных из реплик виртуальных машин	• Платформа должна обеспечивать возможность аварийного запланированного переключения на реплицированную виртуальную машину в случае, когда необходимо минимизировать время простоя при переключении, а также при миграции ВМ на новое оборудование; • Платформа должна обеспечивать возможность возврата к исходной виртуальной машине с сохранением, или без, накопленных после включения реплики данных в случае, если это необходимо; • Платформа должна обеспечивать возможность возврата к реплицированной копии виртуальной машины, если возврат в исходное месторасположение завершился неуспешно;

		• Платформа должна предоставлять возможность восстановления объектов поддерживаемых приложения и файловых системы непосредственно из реплицированных копий виртуальных машин;
	Требования к функциям мониторинга, планирования, отчетности среды виртуализации и платформы резервного копирования	• Поддержка не менее двух платформ виртуализации в области мониторинга и планирования нагрузки; • Сбор статистики по производительности с платформы резервного копирования; • Возможность установки на стандартную ОС, которая покупается отдельно; • Наличие встроенной базы знаний, содержащую исчерпывающие сведения о распространенных проблемах виртуальной инфраструктуры и платформы резервного копирования; • Моделирование оповещений при изменение пороговых значений производительности, без применения данных значений; • Объединение виртуальных машин, хостов или хранилищ в логические группы по любым заданным специализированным критериям: сервис, отдел, город, центр затрат и пр.; • Обеспечивать возможность создания календаря заданий на резервное копирование; • Предоставлять Rest API для удаленного конфигурирования и управления;
	Требования к функциям мониторинга виртуальной инфраструктуры	• Мониторинг операций ввода/вывода (по отдельности и суммарно), к каждому хранилищу, от каждой виртуальной машины или хоста виртуализации; • Мониторинг задержек по чтению и записи, к каждому хранилищу, от каждой виртуальной машины или хоста виртуализации; • Мониторинг состояния оперативной памяти, процессоров и сетевых интерфейсов с учетом специализированных метрик виртуализации;
	Требования к функциям мониторинга инфраструктуры резервного копирования	• Мониторинг производительности компонентов резервного копирования по ЦПУ, ОЗУ, дисковой подсистеме и сети передачи данных; • Отображение состояние всех компонентов платформы резервного копирования. Текущее состояние задач на резервное копирование и репликацию;
	Требования к функциям планирования нагрузки и учета виртуальной инфраструктуры	• Оценка наиболее и наименее загруженных хостов, и виртуальных машин; • Возможность регулярно получать настраиваемые отчеты о производительности хостов и машин в различных форматах; • Прогнозирование загрузки хостов и машин на основе данных за прошлые периоды;

		• Получение отчетов, содержащих информацию об избыточно выделенных виртуальным машинам ресурсах; • Предоставление рекомендаций по планированию и расширению виртуальной инфраструктуре на любой заданный период в будущем времени; • Подготовка отчета об изменениях, произошедших в виртуальной инфраструктуре за любой период времени; • Подготовка отчетов, показывающих изменение нагрузки на серверы в кластере, при выходе из строя одного или нескольких из них. Получение рекомендаций; • Моделирование добавления новых виртуальных машин и просчет изменения нагрузки на кластер виртуальной инфраструктуры; • Создание схемы зависимостей объектов виртуальной инфраструктуры и выгрузка отчета в формате Visio;
	Техническая поддержка ПО	• В поставку должна быть включена техническая поддержка на 36 месяцев • Техническая поддержка должна включать в себя возможность обновления на новые версии ПО той же редакции; • Техническая поддержка должна осуществляться в режиме 24 часа, 7 дней в неделю, 365 дней в году;
	Требования к функциям планирования нагрузки и учета платформы резервного копирования	• Предоставление отчета о системах, которые есть в резервных копиях, но не включенных в задания на резервное копирование; • Возможность отслеживания изменения настроек заданий резервного копирования и репликации; • Прогнозирование роста объема резервных копий на основе данных за прошлые периоды; • Предоставление отчета о ВМ, которые не соответствуют требованиям по минимальному количеству резервных копий; • Возможность отслеживания операций восстановления авторизованными пользователями (пользователь, запустивший восстановление и какие объекты были восстановлены); • Предоставление отчета о системах, которые присутствуют в нескольких заданиях;
	Требования к работам, выполняемым представителями производителя	• Предпроектное обследование инфраструктуры с выработкой рекомендаций по архитектуре и режимам работы системы резервного копирования; • Технический аудит внедренной системы на соответствие требуемым показателям и рекомендациям производителя.
5.	**Перечень работ по серверной инфраструктуре, инфраструктуре хранения и резервного копирования**	**работы** / **1**

	Требования к составу работ:
	• Низкоуровневый дизайн, который включает архитектуру технологии “stretched cluster”, подсистему резервного копирования • План миграции на новое оборудование и последующее сопровождение миграции • Конфигурирование политик резервного копирования и политик хранения резервных копий • Установка гипервизоров, конфигурирование HA, DRS, vSAN, vCenter • Обновление микрокодов всего предложенного оборудования до рекомендуемых версий производителями

в.и.о. директора департамента
информационных технологий **А. Кенжаев**