ПРИЛОЖЕНИЕ 1 К ТЕХНИЧЕСКОМУ ЗАДАНИЮ
ЗАПРОСА ТКП

ЭСКИЗНОЕ ПРОЕКТИРОВАНИЕ КАТАСТРОФОУСТОЙЧИВОЙ ИТ - ИНФРАСТРУКТУРЫ БАНКА «ЗЕНИТ» (ПАО)

ТРЕБОВАНИЕ К ВЫПОЛНЕНИЮ РАБОТ

Оглавление

1. Общие сведения

Настоящее Техническое задание (далее – ТЗ) определяет назначение и общие требования к построению катастрофоустойчивой ИТ - инфраструктуры на базе территориально-распределенных центров обработки данных (далее – Решение) БАНКА «ЗЕНИТ» (ПАО) (далее – Банк или Заказчик), а также требования к технологиям, средствам и механизмам обеспечения восстановления работоспособности ИТ-инфраструктуры и критичных информационных систем (далее – ИС) на случай возникновения чрезвычайной ситуации (далее – ЧС).

В качестве основных сценариев ЧС рассматриваются:

- Веерное отключение электроснабжения;
- Региональное отсутствие коммуникаций и связи;
- Стихийные бедствия;
- Пожар.

Перечисленные выше сценарии ЧС несут следующие угрозы:

- Недоступность работников;
- Недоступность технологий, в том числе информационных и коммуникационных технологий (неработоспособность ИТ-инфраструктуры, информационных систем, потеря коммуникаций и связи);
- Недоступность снабжения (воды, электричества);
- Недоступность помещений;
- Отсутствие доступа к зданиям (помещениям);
- Недоступность ключевых поставщиков, контрагентов;
- Недоступность ключевой информации;
- Недоступность финансовых ресурсов.

В качестве сценариев отказа, для которых необходимо предусмотреть катастрофоустойчивые решения, рассматриваются следующие:

1. Отказоустойчивое решение в рамках одного региона (недоступность ОЦОД);
2. Отказоустойчивое решение при полной недоступности региона (недоступность ОЦОД).

2. Назначение, цели и основные задачи комплексного решения

2.1. Назначение решения

Решение должно предусматривать набор технологий, аппаратно-программных комплексов и организационных процедур, минимизирующих риски потери информации и остановки бизнес-деятельности Банка в случае возникновения природной или техногенной чрезвычайной ситуации (ЧС), повлекшей полную или частичную недоступность основного центра обработки данных (ОЦОД).

Назначение решения:

- Обеспечение сохранности данных и информации.
- Обеспечение доступности критичных бизнес-процессов в случае возникновения ЧС.

2.2. Цель создания решения

Целью данного решения является обеспечение восстановления критичных информационных систем (ИС) Заказчика в случае ЧС в рамках заданных параметров RPO и RTO.

Целью работ по созданию РЦОД:

- Обеспечение резервной площадки для размещения ресурсов (вычислительных, хранения, сетевых), необходимых для функционирования вычислительных контуров ОЦОД в случае катастрофы;
- Обеспечение возможности восстановления работоспособности вычислительных контуров ОЦОД в случае невозможности продления функционирования ОЦОД;
- Резервирование каналов информационного обмена и телекоммуникации, по которым передается информация;
- Обеспечение соответствия требованиям Центробанка России к доступности ключевых деловых процессов Банка (Положение №787-П от 12.01.2022).

2.3. Основные решаемые задачи

Для достижения указанной цели необходимо решить следующие задачи:

- Зарезервировать критичные ИС и системы ИТ-инфраструктуры, обеспечивающие функционирование бизнес-процессов с задействованием географически удалённых площадок для размещения резервных компонентов.
- Обеспечить гарантированную целостность данных в резервном ЦОД в соответствии с заданными параметрами «целевой точки восстановления» (Recovery Point Objective, RPO).
- Обеспечить восстановление ИТ-инфраструктуры и критичных ИС в резервном ЦОД после ЧС или НС в ОЦОД с заданными параметрами «целевого времени восстановления» (Recovery Time Objective, RTO).

№ п.п	Задача
1.	Получить информацию от Заказчика, необходимую для проведения работ в рамках выполнения данного ТЗ.
2.	Разработать ФТТ для всех подсистем ИТ-инфраструктуры в охвате проекта, включая требования:

№ п.п	Задача
	• Требования к целевым импортозамещающим решениям, включая требования по взаимодействию с существующими используемыми решениями, требования ИБ. • Требования к целевой катастрофоустойчивой инфраструктуре
3.	Предоставить long-list решений, доступных на рынке РФ, в разрезе используемых компонентов ИТ-инфраструктуры, подлежащих замене в рамках импортозамещения ИТ-инфраструктуры.
4.	Провести скоринг решений, входящих в long-list.
5.	Сформировать проект целевого технологического решения ИТ-инфраструктуры Заказчика, обеспечивающий непрерывность предоставления ИТ-сервисов в случае воздействия катастроф, включая требования: ▪ Зарезервировать критичные ИС и ситемы ИТ-инфраструктуры, обеспечивающие функционирование бизнес-процессов уровня Mission critical и Business critical. ▪ Обеспечить гарантированную целостность данных в резервном ЦОД в соответствии с заданными параметрами «целевой точки восстановления» (Recovery Point Objective, RPO). ▪ Обеспечить восстановление ИТ-инфраструктуры и критичных ИС в резервном ЦОД после ЧС или НС в ОЦОД с заданными параметрами «целевого времени восстановления» (Recovery Time Objective, RTO).
6.	Сформировать матрицу совместимости из решений, входящих в short-list.

2.4. Ограничения решения

Комплексное решение имеет следующие ограничения, исключения и особые условия:

- Временные параметры восстановления RTO/RPO учитывают исключительно техническое время восстановления и допустимой потери данных (время на принятия управленческих решений и реализацию организационных мероприятий не принимается в расчет);
- Показатели RTO/RPO не применимы к случаю логического искажения данных, например, вследствие ошибок в ПО, и не учитывают время восстановления из резервной копии.

3. Общие сведения и характеристики объекта автоматизации

Объектами, для которых создается РЦОД, являются вычислительные контуры, функционирующие в рамках ОЦОД:

- Вычислительный контур для размещения основного объёма вычислительных ресурсов. Условное обозначение – ВК;
- Вычислительный контур для размещения ИС относящихся к ОКИИ. Условное обозначение – ЗОКИИ;
- Вычислительный контур для организации Процессинга;
- Вычислительный контур для ИС Автоматизированная банковская система (АБС).

Размещение площадки РЦОД определяется по итогам эскизного проектирования с учётом технических ограничений и требований, предъявляемых к ИТ-инфраструктуре со стороны ИС и деловых процессов.

Перечень ИС вычислительных контуров, для размещения в РЦОД, уточняются в техническом проекте и ТЗ на создание РЦОД по результатам эскизного проектирования.

В настоящий момент для критичных ИС Заказчика применяется резервирование «на площадке» с размещением «полукомплектов» оборудования в рамках одного здания.

Защита данных реализована как на уровне синхронной репликации средствами СХД, так и за счёт встроенных средств СУБД и приложений.

В составе ОЦОД Заказчика в настоящий момент имеются серверные ресурсы, используемые для размещения продуктивных экземпляров БД на платформах СУБД MS SQL, Oracle, PostgreSQL.

Основная часть серверных ресурсов используется для размещения системы виртуализации на базе ПО VMware vSphere.

ИТ-инфраструктура РКЦОД предназначена для хранения исторических резервных копий критичных ИС в соответствии с требованиями регулятора и обладает ограниченным набором вычислительных ресурсов для временного восстановления данных в ходе расследования инцидентов.

Пользователи ИС размещаются в 70 региональных отделениях, подключаемых средствами выделенных каналов L2/L3 VPN с задействованием шифрования по алгоритмам IPSEC/ГОСТ.

Также имеется своя интернет сеть, необходимая для организации доступа из вне к ресурсам банка. В текущей инфраструктуре организована возможность удаленного доступа для сотрудников.

4. Требования к комплексному решению в целом

4.1. Требования к архитектуре решения

Архитектура целевой катастрофоустойчивой ИТ-инфраструктуры должна быть реализована в трех датацентрах – ОЦОД (существующий), РЦОД (проектируемый), РКЦОД (существующий). Необходимо предусмотреть наличие узла(ов)/систем(ы) мониторинга для помощи в принятии решения о переключении между основным и резервным ЦОДами.

Совокупность инфраструктурных систем, сервисов и служб ОЦОД и РЦОД должна образовывать единую инфраструктуру, в которой часть компонентов может функционировать в различных ЦОД.

Выбор режима работы РЦОД (Активный/Активный, Активный/Пассивный) осуществляется по итогам эскизного проектирования.

Оптимальные режимы функционирования инфраструктурных систем, сервисов и служб должны быть определены в ходе эскизного проектирования.

При выборе целевой архитектуры и технологий РЦОД, Исполнитель должен руководствоваться целевыми параметрами доступности ИС и деловых процессов с учётом ограничений проекта, предъявляемых Заказчиком: бюджетные ограничения, требования к размещению площадки РЦОД.

4.2. Требования по составу резервируемых информационных и инфраструктурных систем

В рамках проекта Исполнителем должны быть спроектированы и реализованы решения по обеспечению резервирования информационных систем Заказчика

Резервированию в рамках проекта РЦОД подлежат только производственные экземпляры ИС и ИТ-инфраструктуры. Резервирование сред тестирования и разработки не требуется.

4.3. Требования к целостности данных и времени восстановления

Параметры RTO/RPO для ИС определяются на этапе обследования в рамках эскизного проектирования целевой ИТ-Инфраструктуры.

Для инфраструктурных систем, сервисов и служб параметры RTO/RPO определяются в соответствии с зависимостью доступности информационных систем от отдельно взятой инфраструктурной системы, сервиса или службы.

4.4. Требования к надежности

Надежность функционирования ЦОД должна обеспечиваться общей архитектурой, не имеющей единой точки отказа для основных аппаратных компонентов (серверы, СХД, сетевое оборудование и оборудование сети хранения данных).

Аппаратные возможности единиц серверного и телекоммуникационного оборудования, устанавливаемого в ЦОД, должны предусматривать замену или добавление блоков питания, модулей охлаждения и дисков в «горячем» режиме.

Подключения оборудования в ЦОД к сетевой инфраструктуре и сети хранения данных, а также подключения внешних каналов связи должны быть задублированы. Подключения должны

быть распределены по независимым единицам коммутационного оборудования. В случае выхода из строя одного из сетевых интерфейсов или одной единицы сетевого оборудования, должна быть обеспечена бесперебойная работа сетевого подключения с сохранением конфигурации TCP/IP для данного подключения.

4.5. Требования к защите информации от несанкционированного доступа

Используемые при разработке решения системы и средства защиты информации должны иметь действующий сертификат соответствия. В случае передачи защищаемой информации (требующей защиты по требованиям законодательства и подзаконных актов) защита каналов связи должна осуществляться с использованием сертифицированных средств защиты информации не ниже КС2 (КС3), с учетом действующей модели угроз, находящихся в зоне ответственности Банка (исключающих доступ к администрированию третьих лиц).

В целях выполнения лицензионных требований ФСБ Банком форма договора с РЦОД должна обеспечить закрепление за Банком «права собственности или иного законного основания на владение и использование помещений, сооружений, технологического, испытательного, контрольно-измерительного оборудования и иных объектов, необходимых для осуществления лицензируемой деятельности» на используемые помещения.

РЦОД должен иметь ежегодно подтверждаемый сертификат PCI DSS с целью контроля применимых требований в части физической защищенности и контроля доступа.

Для зоны оборудования, обрабатывающих данные PIN (карты), должны выполняться применимые требования PCI PIN Security в части организации контроля физического доступа (требования к укрепленности, системы контроля доступа, сигнализации, видеонаблюдения, сроков хранения журналов и записей итп).

Физические линии каналов передачи данных должны исключать возможность физического доступа к ним третьих лиц, иначе такие каналы (в том числе беспроводные каналы передачи информации) должны обеспечивать защиту с использованием средств криптографической защиты информации (шифрования и имитовставки).

Под термином «шифрование» здесь и далее подразумевается использование решений для комплексной защиты, как конфиденциальности, так и целостности передаваемой информации (шифрование и имитовставка).

Потоки информации, передаваемые по недоверенным каналам сети Интернет, должны шифроваться средствами активного сетевого оборудования.

Потоки информации между клиентскими устройствами самообслуживания пластиковых карт и процессинговым центром, передаваемые по недоверенным каналам Интернет и WAN, должны шифроваться средствами активного сетевого оборудования.

Каналы связи между ОЦОД и РЦОД должны обеспечивать защиту с использованием средств криптографической защиты информации (шифрования и имитовставки).

Доступ к управлению оборудованием и специализированным ПО должен быть технически ограничен определенным кругом лиц, имеющих права доступа к администрированию соответствующего оборудования.

Подключения администраторов к интерфейсам управления серверным или телекоммуникационным оборудованием должны осуществляться с использованием средств и протоколов, поддерживающих шифрование передаваемых/получаемых данных. Для управления должны использоваться протоколы SSH v2, SNMP v3, HTTPS.

Для задач администрирования и управления не допускается использование средств и протоколов, передающих учетные данные пользователя в открытом виде (например, telnet, rlogin).

В рамках проекта должна быть сохранена сегментация сети в соответствии с существующими принятыми принципами и правилами прохождения трафика между сегментами. Проектировщик может предложить оптимизации существующей схемы для достижения целей проекта в рамках эскизного проектирования.

5. Требования к составу и этапам работ

5.1. Этапность работ

В рамках эскизного проектирования выделяются следующие этапы работ:

1. Обследование ИТ-инфраструктуры и ИС
2. Разработка вариантов эскизной архитектуры РЦОД
3. Разработка бюджетной оценки согласованных вариантов реализации
4. Защита решений на Технологическом комитете
5. Разработка Технического задания на реализацию РЦОД
6. Разработка закупочных спецификаций и требований к поставке оборудования и ПО для реализации РЦОД

5.2. Обследование ИТ-инфраструктуры и ИС

Работы по обследованию ИТ-инфраструктуры проводятся специалистами Исполнителя удаленно и должны включать в себя следующие мероприятия:

- Анализ документации по ИТ-инфраструктуре в составе:
  - Архитектурные схемы;
  - Описание архитектуры систем;
  - Технический проект (при наличии).
- Сбор данных о средствах защиты информации, используемых в существующих ЦОД;
- Сбор и анализ технических отчётов, выгрузок и результатов выполнения команд из инфраструктурных систем Заказчика (при необходимости);
- Интервью со специалистами Заказчика, отвечающими за эксплуатацию и развитие ИТ-инфраструктуры в существующих ЦОД.

Работы по обследованию ИС проводятся специалистами Исполнителя удаленно и должны включать в себя следующие мероприятия:

- Анализ документации по ИС в составе:
  - Инсталляционная карта ИС/Архитектурное описание решений;
  - DR-планы и/или инструкции по переключению ИС в случае катастрофы;
  - Схема интеграционного взаимодействия;
- Интервью со специалистами Заказчика, отвечающими за развитие и эксплуатацию ИС;
- Сбор и анализ технических отчётов, выгрузок и результатов выполнения команд из ОС, СУБД и других компонентов, входящих в состав ИС (при необходимости).

Предоставление информации по ИС и компонентам ИТ-инфраструктуры, документации, отчётов, выгрузок, выводов команд и доступа на существующие площадки, находится в зоне ответственности Заказчика.

Результатом работ на данном этапе является отчёт об обследовании ИТ-инфраструктуры и ИС (по форме Исполнителя), содержащий систематизированную информацию, полученную в ходе проведённого обследования.

5.3. Разработка вариантов эскизной архитектуры РЦОД

Варианты эскизной архитектуры решений должны быть проработаны с учётом информации о составе и конфигурации ИТ-инфраструктуры и ИС, полученной в рамках этапа обследования (см. раздел 5.2).

Эскизная архитектура решения должна быть проработана для следующих вариантов реализации (при размещении основного ЦОД в г. Москва):

- Размещение РЦОД в арендуемом коммерческом ЦОД в пределах Республики Татарстан.
- Размещение РЦОД в арендуемом коммерческом ЦОД в пределах г. Москва.

Эскизная архитектура решений должна рассматривать следующие аспекты:

- Возможные варианты реализации каналов связи ОЦОД-РЦОД;
- Возможные технологии защиты информации от сбоев (типы репликации и технические средства для реализации);
- Существенные аспекты реализации подсистем ИТ-инфраструктуры (такие как: сеть передачи данных, дисковые массивы, СУБД, СРК);
- Реально достижимые показатели RTO/RPO для предлагаемых вариантов;
- Экспертную оценку Исполнителя по вопросу возможности/невозможности импортозамещения подсистем ИТ-инфраструктуры РЦОД в рамках реализации последующего проекта построения РЦОД;
- Возможность задействования существующего оборудования и ПО и их резервов для реализации решений РЦОД.

Результатом работ на данном этапе является эскизный проект (по форме Исполнителя), содержащий структурные схемы решений РЦОД и описание аспектов технической архитектуры предлагаемых решений, являющихся существенными для реализации проекта.

5.4. Разработка бюджетной оценки согласованных вариантов реализации

Бюджетная оценка реализации вариантов построения РЦОД производится для согласованных с Заказчиком решений в рамках эскизного проектирования (см. п. 5.3) – не более 3 вариантов.

Бюджетная оценка должна включать стоимость комплекса работ по проектированию и реализации РЦОД, включая планирование и миграцию конфигурации ИС и оборудования в целевое состояние, а также оценку стоимости оборудования и ПО, необходимых для реализации решений.

Результатом работ на данном этапе является сводный расчёт (по форме Исполнителя) стоимости реализации вариантов построения РЦОД по оценке Исполнителя.

5.5. Защита решений на проектном комитете

На этапе защиты решений Исполнитель готовит разделы отчётной презентации по форме, предоставляемой Заказчиком для руководства Банка и лиц, принимающих решение о старте реализации РЦОД.

В основе презентации должно лежать сравнение вариантов реализации и их стоимость (на основании бюджетной оценки), в том числе возможные риски реализации.

В случае необходимости, представители Исполнителя могут быть привлечены к участию в защите решений перед руководством Банка.

Результатом работ на данном этапе являются согласованные Заказчиком разделы отчётной презентации.

5.6. Разработка Технического задания на реализацию РЦОД

Техническое задание на реализацию проекта РЦОД должно быть разработано для варианта РЦОД, согласованного Заказчиком с руководством Банка по результатам этапа 5.5.

Техническое задание должно описывать требования к РЦОД в целом, ключевым параметрам назначения ИС, архитектуре, технические требования к подсистемам ИТ-инфраструктуры, составу и порядку проведения работ по реализации проекта.

Результатом работ на данном этапе являются согласованное Заказчиком ТЗ на реализацию проекта РЦОД.

5.7. Разработка закупочных спецификаций и требований к поставке оборудования и ПО для реализации РЦОД

По итогам разработки и согласования Технического задания на реализацию РЦОД, исполнитель готовит спецификации и/или технические требования на закупку оборудования и ПО, необходимых для реализации проекта в соответствии с согласованным ТЗ.

В случае невозможности подготовки спецификаций для оборудования и ПО, связанными с санкционными ограничениями, Исполнитель ограничивается подготовкой технических требований. Исполнитель не может нести ответственность за доступность оборудования и ПО на территории РФ, необходимого для реализации проекта РЦОД, однако должен оказывать необходимые консультации Заказчику в отношении доступности необходимых компонентов.

Результатом работ на данном этапе являются согласованный Заказчиком комплект спецификаций и технических требований на реализацию проекта РЦОД (по форме, согласованной представителями Заказчика и Исполнителя на старте выполнения работ).

6. Требования к работам, выполняемым Исполнителем

Для достижения поставленных целей в рамках реализации настоящих технических требований необходимо выполнить следующие работы, разбитые на этапы:

1. Подготовка к выполнению работ по выбору целевых инфраструктурных программных и аппаратных решений ИТ-инфраструктуры:
   - Получение информации об используемом в ИТ-инфраструктуре Заказчика ПО и оборудовании, включая:
     - Аппаратные платформы (серверное оборудование, СХД, СРК)
     - Серверное и клиентское ПО, используемое в рамках всех направлений, перечисленных в п. **Ошибка! Источник ссылки не найден.**;
     - Клиентские ОС, прикладное и системное ПО.
   - Получение информации о производителях периферийных устройств, преимущественно используемых в ИТ-инфраструктуре Заказчика, используемых пользователями со своих АРМ;
   - Получение информации о текущей архитектуре и конфигурации компонентов ИТ-инфраструктуры Заказчика в функциональных границах проекта, обозначенных в п. 2.2;
   - Получение информации о направлениях деятельности и зоне ответственности подразделений ИТ, включая регламенты взаимодействия входящих в его состав подразделений;
   - Согласование с Заказчиком методологии проведения анализа соответствия инфраструктурных программных и аппаратных решений ИТ-инфраструктуры техническим и функциональным требованиям (заполнение скоринговых таблиц и матрицы совместимости);
   - Разработка функциональных и нефункциональных технических требований к целевым инфраструктурным программным и аппаратным решениям ИТ-инфраструктуры (включая требования ИБ), выбор и согласование веса каждого требования, формирование скоринговых таблиц;
   - Актуализация требований к производителям целевых инфраструктурных программных и аппаратных решений ИТ-инфраструктуры;
   - Анализ аппаратного и программного обеспечения российских производителей или продуктов альтернативных поставщиков на предмет наличия ПО, подходящего для реализации задач Заказчика;
   - Актуализация перечня (long-list) производителей целевых инфраструктурных программных и аппаратных решений ИТ-инфраструктуры, потенциально подходящих для реализации задач Заказчика.
2. Проведение анализа соответствия целевых инфраструктурных программных и аппаратных решений ИТ-инфраструктуры и их производителей предъявляемым требованиям и формирование шорт-листа решений (не более 2-х) по каждому из направлений работ по выбору импортозамещающих решений (см. п. **Ошибка! Источник ссылки не найден.**):
   - Анализ совместимости текущих решений и целевых инфраструктурных программных и аппаратных решений ИТ-инфраструктуры (в рамках заполнения скоринговых таблиц) для обеспечения поэтапного внедрения и их совместной

работы с текущими решениями. При анализе совместимости, в числе прочего, необходимо ориентироваться на список Mission critical и Business critical систем Компании;

- Сравнение (скоринг) производителей и их импортозамещающих решений путем заполнения скоринговых таблиц;
- Выбор по результатам скоринга не менее двух решений (short-list) для каждого компонента ИТ-инфраструктуры;

3. Формирование эскизного проекта целевой инфраструктуры РЦОД, обеспечивающего непрерывность предоставления ИТ-сервисов в случае воздействия катастроф, включая:
   - Описание вариантов реализации для каждой подсистем ИТ-инфраструктуры РЦОД (не менее 3-х вариантов)
   - Преимущества и недостатки вариантов реализации
   - Эскизный проект архитектуры целевого варианта реализации и обоснование выбора целевого варианта
   - Описание механизмов и ключевых технологий резервирования данных и приложений ИС в РЦОД
   - Краткая фиксация типов данных для каждой ИС и предлагаемых технологий резервирования
4. Разработка подхода к переводу ИТ-инфраструктуры на целевые импортозамещающие и катастрофоустойчивые решения:
   - Разработка дорожной карты перевода ИТ-инфраструктуры на согласованные целевые импортозамещающие и катастрофоустойчивые решения;
   - Разработка подхода к реализации дорожной карты с учетом организационного объема, волн/этапов, необходимых ресурсов).

7. Требования к плану работ и содержанию этапов.

Требования к плану работ и содержанию этапов приведены в таблице 1

№ этапа	Название этапа	Содержание работ	Результат
1.	Подготовка к выполнению работ по выбору целевых импортозамещающих решений	По каждому из направлений работ по выбору импортозамещающих решений: 1. Обследование ИТ-инфраструктуры Компании в части используемого оборудования и/или ПО, архитектуры и конфигурации компонентов ИТ-инфраструктуры. 2. Разработка ФТТ для целевых импортозамещающих решений, включая требования по взаимодействию с используемыми решениями, требования по совместимости с целевыми решениями смежных инициатив, требования ИБ. 3. Актуализация требований к целевым импортозамещающим решениям и производителям, формирование скоринговых таблиц. 4. Формирование long-list производителей и продуктов целевых импортозамещающих решений. 5. Формирование требований как по восстановлению информационных/прикладных систем (RTO/RPO), так и требований к обеспечивающим подсистемам инфраструктуры РЦОД	1. Проведено обследование ИТ-инфраструктуры, сформирован отчетный документ «**Отчет об обследовании**» 2. Сформированы и согласованы технические требования в формате скоринговых таблиц и отчетного документа «**Требования к импортозамещающим решениям**». 3. Сформированы и согласованы long-list производителей целевых импортозамещающих решений. 4. Сформированы и согласованы технические требования к катастрофоустойчивости решений между ЦОД и целевым РЦОД в разрезе подсистем ИТ-инфраструктуры и отчетного документа «**Требования к целевой катастрофоустойчивой инфраструктуре**»
2.	Анализ соответствия целевых импортозамещающих решений предъявляемым требованиям	1. Анализ целевых импортозамещающих решений из long-list на соответствие предъявляемым требованиям (заполнение скоринговых таблиц). 2. Анализ целевых импортозамещающих решений на соответствие требованиям ИБ. 3. Анализ совместимости текущего ПО с целевых импортозамещающих решений из long-list. 4. Формирование short-list целевых импортозамещающих решений.	1. Заполнены и согласованы скоринговые таблицы сравнения целевых импортозамещающих решений. 2. Сформирован и согласован short-list, сформирован отчетный документ «**Выбор целевых решений**»
3.	Концепция целевой инфраструктуры РЦОД	1. Описание вариантов реализации геораспределенной инфраструктуры для каждой подсистем ИТ-инфраструктуры (не менее 2-х вариантов) и обоснование выбора целевого варианта 2. Описание механизмов и ключевых технологий резервирования данных и приложений ИС в РЦОД 3. Краткая фиксация типов данных для каждой ИС и	Сформирован и согласован Отчетный документ «**Эскизный проект целевой катастрофоустойчивой инфраструктуры (РЦОД)**»

		предлагаемых технологий резервирования	
4.	Оформление результатов	4. Подготовка презентационных материалов для руководства.	Презентация в составе (Приложение 13): - согласованный long-list (Приложение 2); - согласованный short-list; - покрытие требований и обоснование выбора целевых импортозамещающих решений - решения, используемые в рамках построения РЦОД
5.	Разработка подхода построению РЦОД	1. Разработка дорожной карты к построению РЦОД. 2. Разработка подхода к реализации дорожной карты	Разработана и согласована «**Дорожная карта проекта построения резервного ЦОД**», отражающая подход построению РЦОД со следующей детализацией: - дорожная карта миграции; - подход к реализации дорожной карты миграции.

8. Требования к документированию

Текстовая часть документов готовится в формате Microsoft Word, табличная часть - в формате Microsoft Excel, графическая часть - в формате Microsoft Visio.

При разработке документации рекомендуется придерживаться стандартной ИТ-методологии.

Шаблоны и формат типовых форм документирования должны быть согласованы с Заказчиком

Разработанная Исполнителем документация сохраняет свою актуальность для выполнения работ по внедрению решений в течение 1 года с даты подписания Сторонами Акта выполненных работ при условии отсутствия изменений ИТ-инфраструктуры и ИС, влияющих на технические решения. Спецификации оборудования, услуг и ПО действительны для закупки в течение 1 месяца при условии их согласования Заказчиком и подписания Сторонами Акта выполненных Работ. Актуализация разработанной Исполнителем документации и внесение изменений, необходимость в которых возникла не по вине Исполнителя по истечении срока, указанного в настоящем абзаце ТЗ, может быть выполнена Исполнителем на основании дополнительного соглашения к Договору, подписанному Сторонами, в сроки и на условиях, согласованных Сторонами в таком дополнительном соглашении.

9. Требования к проектной команде

Исполнитель обязуется сформировать проектную команду, возглавляемую Руководителем проекта со стороны Исполнителя с привлечением профильных технических специалистов.

Исполнитель должен предусмотреть в составе рабочей группы не менее одного проектного менеджера, одного администратора проекта, одного архитектора, двух аналитиков по направлению ИТ, необходимое количество технических экспертов по функциональным областям проекта, одного квалифицированного аналитика по направлению ИБ.

Исполнитель должен отвечать следующим требованиям и компетенциям в областях информационных технологий:

1. Наличие необходимого количества сертифицированных технических специалистов и компетенций, позволяющих квалифицированно выполнять работы, включая специалистов по продуктам и технологиям:
    - Windows Server – не менее 2;
    - Microsoft Active Directory – не менее 2;
    - MS SQL Server - не менее 2;
    - MS System Center - не менее 2;
    - MS RDS – не менее 1;
    - MS SharePoint Server – не менее 1.
2. Наличие необходимого количества сертифицированных технических специалистов и компетенций, позволяющих квалифицированно выполнять работы по внедрению информационных систем на базе продуктов, включенных в реестр отечественного ПО, включая, но не ограничиваясь:
    - Операционные системы – не менее 2 специалистов.
    - Системы управления электронной почты не менее 2 специалистов.
    - Система серверной виртуализации не менее 2 специалистов.
    - Система видеоконференцсвязи не менее 2 специалистов.
    - Офисные системы не менее 2 специалистов.
3. Наличие опыта реализации не менее 2 проектов по обследованию решений на базе продуктов компании Microsoft, включая, но не ограничиваясь, следующие продукты и технологии:
    - MS Active Directory;
    - Windows Server;
    - MS SQL Server;
    - MS System Center;
    - MS Windows Server Hyper-V;
    - MS SharePoint Server;
    - MS Windows Server RDP;
    - Oracle,
    - PostgreSQL,
    - SAN,
    - СХД
4. Среди членов команды должны быть представлены специалисты, обладающие компетенциями в области аудитов, стандартов и методологий BCI, ITSM подтвержденными сертификатами:
    a. аудитор информационных систем (CISA);
    b. аудитора по системе управления (ISO 22301 BCMS);
5. Наличие у исполнителя действующих статусов авторизованного партнера производителей программных продуктов, включенных в реестр отечественного ПО.

10. Порядок контроля и приемки результатов работ

Содержание отчетных материалов должно быть отдельно согласовано на уровне специалистов Исполнителя и рабочей группы Заказчика на основе данного ТЗ.

Результаты работ по каждому этапу в электронном виде предоставляются Исполнителем Заказчику не позднее 3 рабочих дней после завершения этапа.

В течение 5 рабочих дней Заказчик рассматривает предоставляемые Исполнителем документы и, при необходимости, представляет Исполнителю список замечаний. В течение 5 рабочих дней Исполнитель обязан устранить замечания и провести защиту документов перед Заказчиком.

Устранение выявленных несоответствий технических решений проекта Исполнитель производит за свой счёт без изменения сроков реализации Проекта.

На всех этапах работ Заказчик может проводить контроль качества выполнения работ, о чём ставит в известность Исполнителя.

Контроль качества выполненных работ может выполняться как собственными силами Заказчика, так и с привлечением сторонних подрядчиков, включая системных интеграторов и/или производителей оборудования/решений.

Результаты работ будут считаться принятыми Заказчиком при условии подписания акта выполненных работ, соответствующего требованиям настоящего ТЗ, и устранения всех выявленных замечаний.

11. Порядок внесения изменений

Настоящий документ может быть изменен и дополнен в ходе разработки решения и реализации проекта в установленном порядке по взаимному соглашению Заказчика и Исполнителя.

Согласование и утверждение изменений производится теми же должностными лицами, что и согласование (утверждение) настоящего ТЗ.

Изменения ТЗ могут повлечь за собой изменение стоимости и сроков выполнения проекта. При этом дополнительная стоимость фиксируется итогом математического расчета затраченных ч/часов и стоимости ч/часов каждого вовлеченного в проект специалиста Исполнителя.

12. Перечень условных обозначений, сокращений и терминов

ACI	Application Centric Infrastructure
CRM	Система работы с корпоративными клиентами
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone — демилитаризованная зона
DNS	Domain Name System
Downtime	Время простоя сервиса
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ESXI	Гипервизор, входящий в ПО VMware vSphere
FC	Fibre Channel
HA	High Availability - Высокая доступность
HTTPS	HyperText Transfer Protocol Secure — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
LAN	Local Area Network
MS	Microsoft
NAS	Network Attached Storage
NAT	Network Address Translation
NTP	Network Time Protocol
RPO	Recovery Point Objective, объем возможных потерь данных в случае сбоя
RTO	Recovery Time Objective, допустимое время простоя сервиса в случае сбоя
SAN	Storage Area Network
SSH	Secure Shell — «безопасная оболочка»- сетевой протокол прикладного уровня
SNMP	Simple Network Management Protocol — простой протокол сетевого управления
VLAN	Virtual Local Area Network
VM (ВМ)	Виртуальная машина
vSphere	Платформа виртуализации
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
ПАО	Публичное акционерное общество
АРМ	Автоматизированное рабочее место
Банк	БАНК «ЗЕНИТ» (ПАО)
БД	База данных
БП	Блок питания
ВМ	Виртуальная машина
ВОЛС	Волоконно-оптическая линия связи
ГОСТ	Государственный стандарт
ИТ	Информационные технологии
КПД	Каналы передачи данных
КСПД	Корпоративная сеть передачи данных
КХД (ЛХД)	Корпоративное хранилище данных (локальное хранилище данных)
МСЭ	Межсетевой экран
НС	Нештатная ситуация - сочетание условий и обстоятельств при эксплуатации технических систем, отли

	чающихся от предусмотренных проектами, нормами и регламентами и ведущих к возникновению опасных состояний в технических системах
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
РФ	Российская федерация
РЦОД	Резервный центр обработки данных
СПД	Сеть передачи данных
СРК	Система резервного копирования
СУБД	Система управления базами данных
СХД	Система хранения данных
УЦ	Удостоверяющий центр
ЧС	Чрезвычайная ситуация - это обстановка на определённой территории, сложившаяся в результате аварии, опасного природного явления, катастрофы, распространения заболевания, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей
ЭП	Эскизный проект
АС	Автоматизированная система
ВМ	Виртуальная машина
ЦОД	Центр обработки данных
ОЦОД	Основной центр обработки данных
РЦОД	Резервный центр обработки данных
ЗОКИИ	Значимые объекты критической информационной инфраструктуры
ИБ	Информационная безопасность
ИС	Информационная система
ОКИИ	Объекты критической информационной инфраструктуры
ПНР	Пуско-наладочные работы
ПОИБ	Подсистема информационной безопасности
РД	Рабочая документация
ТЗ	Техническое задание