Приложение №1а
к Поручению на
проведение закупочных
процедур

ТЕХНИЧЕСКОЕ ЗАДАНИЕ 16-4964

на открытый запрос предложений по выбору исполнителя работ (услуг)
Разграничение доступа пользователей к виртуализированным вычислительным ресурсам VMware филиала "Невский"

(номер закупки по ГКПЗ: 1090/7.46-1069)
ПСДТУ и ИТ филиала «Невский» ОАО «ТГК-1».
(наименование структурного подразделения) *(наименование филиала)*

ОКВЭД	62.09
ОКДП	62.09.20.190

I. Общие требования.
Требования к месту выполнения работ:
Центр обработки данных ОАО «ТГК-1»
(адрес нахождения объекта)
Должность, ФИО, контактный телефон ответственного лица, составившего техническое задание: Директор ПСДТУиИТ Алексей Викторович Малафеев, 901-36-48

Период выполнения работ (услуг):
Начало: с даты заключения договора
Окончание: декабрь 2016 г.

Объем работ: Разграничение доступа пользователей к виртуализированным вычислительным ресурсам VMware филиала "Невский" – 1440 час.

Обобщенные характеристики выполняемых работ (услуг):
В рамках проведенной в 2015 г. модернизации Корпоративной мультисервисной сети связи (КМСС) Невского филиала ОАО «ТГК-1» топология последней претерпела значительные изменения. Модернизации предшествовал длительный процесс постепенного развития ИТ-инфраструктуры ОАО «ТГК-1», внедрения новых информационных систем и изменения потребностей отдельных абонентов[1] и целых сегментов КМСС в наличии связи с другими ее сегментами.
В результате принятые принципы категоризации и группировки абонентов КМСС, порядка разграничения доступа между ними оказались устаревшими; накопилось большое число исключений из правил обмена трафиком (как актуальных, так и устаревших), требующих ручного администрирования. Результатом этого является высокая нагрузка и низкая продуктивность работы специалистов отдела сетевых технологий ПСДТУиИТ, увеличение времени исполнения заявок на обеспечение сетевой связности и высокая частота перерывов связи вследствие сбоев и ошибок администрирования. Другим результатом является наличие сетевой связности между многими абонентами КМСС сверх необходимой для работы последних, создающее предпосылки для нарушения

[1] Под абонентами КМСС понимаются все виды физических и виртуальных конечных устройств: IP-телефоны, проводные и беспроводные рабочие станции, физические сервера, виртуальные машины VMware (в том числе виртуальные рабочие столы), интерфейсы управления активного сетевого оборудования.

принципа минимальных необходимых прав доступа и привилегий, предписываемого Политикой информационной безопасности ОАО «ТГК-1».
Необходимо обновление политики группировки абонентов КМСС и разграничения доступа (обеспечения выборочной сетевой связности), для чего требуется:

- обследовать и документировать состав существующих групп абонентов КМСС ОАО «ТГК-1» (функциональных сетей), а также существующие взаимные и односторонние связи между ними;
- провести анализ целесообразности распределения пользователей, физических и виртуальных серверов и прочих абонентов КМСС ОАО «ТГК-1» по функциональным сетям; выполнить целесообразное перераспределение абонентов между функциональными сетями;
- разработать новую политику разграничения доступа между функциональными сетями, исключить доступ пользователей к технологическим и бизнес-приложениям ОАО «ТГК-1», а равно исключить прочие виды связи между функциональными сетями КМСС ОАО «ТГК-1», кроме требующихся для функционирования приложений и исполнения пользователями своих должностных обязанностей.

Расчетная (максимальная) цена закупки – 5 000 тыс. руб. без НДС.
Ценовая характеристика стоимости работ должна определяться в соответствии с требованиями системы ценообразования, принятой в ОАО «ТГК-1».

II. Требования к выполнению услуг.

1. Цель выполнения услуг:

Упрощение процедур администрирования КМСС, снижения вероятности сбоев КМСС и приведение КМСС в согласие с Политикой ИБ ОАО «ТГК-1» путем разработки новой единой политики разграничения доступа в КМСС и минимизации числа исключений из нее.

2. Характеристика существующих средств разграничения доступа:

2.1 По мере развития ИТ-инфраструктуры ОАО «ТГК-1» последняя постоянно пополняется новыми технологическими и бизнес-приложениями, заступающими в строй в дополнение к уже существующим или вместо них, причем в ходе этого процесса наблюдается интеграция приложений с возрастанием числа и сложности связей между ними. Вместе с этим претерпевают изменения роли отдельных пользователей и целых их групп, так что изменяется потребность в наличии связи этих пользователей между собой и их доступа к упомянутым приложениям. Основным способом управления доступом пользователей и приложений к ресурсам ИТ-инфраструктуры ОАО «ТГК-1» были и остаются аутентификация и авторизация средствами приложений и используемых операционных систем. Однако в рамках принятой концепции «многоуровневой защиты» в дополнение к описанной аутентификации в ОАО «ТГК-1» применяется также межсетевое экранирование с помощью специализированных сетевых устройств и программного обеспечения, а также организация выборочной сетевой связности между абонентами КМСС ОАО «ТГК-1». Политика ИБ ОАО «ТГК-1» постулирует принцип минимальных необходимых привилегий и прав доступа. Примененный к сетевой связности, он обеспечивает снижение нагрузки на средства аутентификации, авторизации и межсетевого экранирования, а также на КМСС в целом, повышает стабильность работы и упрощает администрирование КМСС и указанных средств.
Для организации выборочной связности между абонентами КМСС ОАО «ТГК-1» эти абоненты разделяются на группы отдельных абонентов и целых сетей –

функциональные сети, имеющие собственные, отдельные таблицы маршрутов. Эти функциональные сети не взаимодействуют и не обмениваются маршрутной информацией между собой или ограниченно взаимодействуют в рамках политики обмена маршрутами, определяемой сетевыми администраторами ОАО «ТГК-1». Существующее распределение абонентов по функциональным сетям и политика обмена маршрутами между сетями не соответствует настоящим нуждам ОАО «ТГК-1», с одной стороны, обеспечивая избыточную сетевую связность, а с другой, - требуя специальных исключений для функционирования многих информационных систем Общества.

2.2 Корпоративная мультисервисная сеть связи филиала «Невский» ОАО «ТГК-1» предназначена для обеспечения инфраструктурных требований производственных и иных приложений, развернутых в ОАО «ТГК-1». Основным назначением системы является передача данных указанных приложений в виде пакетов IPv4 устройствами-абонентами КМСС в пределах филиала «Невский». Среди прочих на основе КМСС функционируют сети пакетной телефонной и видеоконференцсвязи. Значительную нагрузку на КМСС создает используемая в ОАО «ТГК-1» технология виртуализации рабочих мест персонала Virtual Desktop Infrastructure (VDI).
В состав КМСС входят:

- каналы связи между площадками филиала «Невский», в том числе предоставляемые сторонними операторами связи и принадлежащие ОАО «ТГК-1»;
- локальные вычислительные сети (далее – «ЛВС») объектов филиала «Невский»; среди них выделяются ЛВС Центров обработки данных (далее – ЦОД), расположенных на ТЭЦ-17 и ТЭЦ-15 и содержащих основную массу вычислительных ресурсов и ресурсов хранения данных.

Отдельно можно выделить сетевое оборудование, обеспечивающее связь между площадками Невского филиала ТГК-1, являющееся составными частями соответствующих ЛВС, но совместно образующее логически выделяемый сегмент межобъектовой связи или ядро КМСС.

КМСС имеет иерархическую структуру, составленную несколькими уровнями. КМСС в основном является отказоустойчивой, причем в зависимости от уровня иерархии используются различные технологии резервирования и обеспечения высокой доступности. После проведенной в 2015 году модернизации ядра КМСС последнее имеет топологию «двойная звезда» с центрами в объектах ЦОД Невского филиала ТГК-1 на ТЭЦ-15 и ТЭЦ-17.

Для всех объектов Невского филиала ТГК-1 доминирующим направлением передачи сетевого трафика являются направления в ЦОД и обратно, однако, некоторые информационные системы ТГК-1 требуют непосредственной связности между абонентами КМСС разных объектов и без участия ЦОД.
Вычислительные средства ЦОД ОАО «ТГК-1» в большинстве своем виртуализованы с использованием продукта VMware vSphere, так что информационные приложения ОАО «ТГК-1» размещаются на виртуальных машинах. Аналогично часть рабочих мест сотрудников виртуализована по технологии VDI и размещена в ЦОД, то есть также являет собой виртуальные машины. Все указанные виртуальные ресурсы VMware (виртуальные машины) являются полноправными абонентами КМСС и на общих основаниях входят в соответствующие им функциональные сети.
С учетом упомянутого выше доминирующего направления передачи сетевого трафика от пользователей к виртуальным машинам ЦОД, разграничение доступа пользователей к виртуальным машинам ЦОД является не единственным, но главным положением

политики обмена трафиком между функциональными сетями КМСС.

2.3 Разделение абонентов КМСС ОАО «ТГК-1» на функциональные сети производится на сетевом оборудовании уровня доступа локальных вычислительных сетей объектов ОАО «ТГК-1». Указанное оборудование разнородно и по большинству представлено коммутаторами и маршрутизаторами производства компании Cisco Systems. На этом уровне преобладают устройства серий Catalyst 2950, 2960, 3560, 3750 и 6500. В ЦОДах на уровне доступа используются более современные высокопроизводительные устройства, в частности, серии Catalyst 4500X, а также программно реализованное сетевое оборудование, однако, принципы распределения абонентов (как аппаратных, так и программных) по функциональным сетям при этом остаются неизменными.
Будучи первоначально разделенным, трафик абонентов КМСС, принадлежащих разным функциональным сетям, в рамках единой физической инфраструктуры передается раздельно и не смешивается.
Ограниченный, определяемый администраторами ОАО «ТГК-1» обмен между функциональными сетями производится на оборудовании ядра КМСС. Указанное оборудование составлено высокопроизводительными коммутаторами и маршрутизаторами Cisco Systems старших моделей Catalyst 6500, Cisco 7600 и Cisco ASR, связанными между собой высокоскоростными каналами 1Гбит/с и 10Гбит/с. Обмен между функциональными сетями не централизован и производится распределенно, так что любое из устройств ядра КМСС способно выступить шлюзом между функциональными сетями в рамках, установленных политикой разграничения доступа.
Оптимизация порядка разделения абонентов КМСС по функциональным сетям и политики разграничения доступа между функциональными сетями является основной целью настоящего Задания.

2.4 В настоящее время в КМСС выделено 15 категорий абонентов КМСС, которые с учетом принадлежности к ЛВС различных объектов разделены примерно на 130 функциональных сетей. Точные сведения о существующих правилах разграничения сетевого трафика не относятся к свободно распространяемой информации; существующая матрица доступности должна быть составлена Подрядчиком на основании фактически действующих правил доступа, передача информации о которых должна быть выполнена на основании соглашения о неразглашении конфиденциальной информации.

УКРУПНЕННАЯ ВЕДОМОСТЬ
объёмов услуг

по разграничению доступа пользователей ОАО «ТГК-1» к виртуализированным ресурсам VMware

ПСДТУ и ИТ филиала «Невский» ОАО «ТГК-1».
(наименование структурного подразделения) *(наименование филиала)*

Требования к составу и объему проводимых работ (оказываемых услуг):
Объем работ: Разграничение доступа пользователей к виртуализированным вычислительным ресурсам VMware филиала "Невский" – 1440 час.

1. ***Требования к составу и объему работ***

В рамках разграничения доступа пользователей ОАО «ТГК-1» к виртуализированным ресурсам VMware требуется:

- Провести обследование КМСС ОАО «ТГК-1» и разработать существующую матрицу разграничения доступа между функциональными сетями ОАО «ТГК-1». Матрица должна включать в себя:
  - Перечень категорий абонентов КМСС с указанием их назначения
  - Перечень функциональных сетей КМСС с указанием их назначения
  - Перечни физических и виртуальных абонентов КМСС и их групп, входящих в каждую категорию или функциональную сеть
  - Собственно, матрицу разграничения доступа между функциональными сетями КМСС по форме, разработанной Подрядчиком, согласованной и утвержденной совместно с представителями ОАО «ТГК-1».
- Получить от ответственных представителей ОАО «ТГК-1», оформить и согласовать с ними требования к разграничению доступа для каждой наличной категории или функциональной сети.
- Провести анализ целесообразности существующего распределения абонентов КМСС по категориям и функциональным сетям. Выработать и согласовать с представителями ОАО «ТГК-1» предложения по оптимизации перечня категорий абонентов КМСС, перечня функциональных сетей и распределения абонентов по категориям и функциональным сетям.
- Разработать новую, целевую матрицу разграничения доступа между функциональными сетями, учитывающую только фактически необходимые связи между функциональными сетями. Согласовать целевую матрицу доступа с ответственными представителями ОАО «ТГК-1».
- Провести перенастройку сетевого оборудования ядра КМСС в соответствии с целевой матрицей разграничения доступа между функциональными сетями. Конфигурации всех сетевых устройств ядра КМСС должны быть консистентны и реализовать единую политику разграничения доступа во всех случаях, в том числе и при отказах оборудования и каналов связи, влекущих за собой изменение маршрутов передачи сетевого трафика.
- В период опытно-промышленной эксплуатации оперативно производить корректировку матрицы разграничения доступа и проводить соответствующую перенастройки сетевого оборудования КМСС.
- Разработать и согласовать с ответственными представителями ОАО «ТГК-1» программу приемо-сдаточных испытаний в отношении целевой политики разграничения доступа, в том числе контролирующие отсутствие избыточной связности, не предусмотренной политикой. Выполнить приемо-сдаточные испытания и сдать перенастроенное ядро КМСС в промышленную эксплуатацию.

2. ***Требования к поддержке:***

Весь комплекс проведенных работ и выпущенных документов должен обеспечиваться технической поддержкой, осуществляемой Исполнителем, в течение не менее 1 года.

3. ***Требования к подрядной организации:***

- Наличие положительного опыта по выполнению аналогичных работ;
- Наличие партнерского статуса компании Cisco Systems уровня не ниже Premier В своей заявке участник должен представить сертификат, подтверждающий партнерство с компанией Cisco Systems;

- Наличие в штате компании специалистов, сертифицированных компанией Cisco Systems по программе CCIE или CCDE – не менее 1 человека;
- Предоставление полной информации о составе и объеме предлагаемых услуг;
- Обеспечить соответствие сметной документации требованиям системы ценообразования, принятой в ОАО «ТГК-1»;
- Акты сдачи - приемки могут быть подписаны Заказчиком при условии выполнения подрядчиком указанных выше требований.

4. ***Специальные требования:***

- Возможность поддержки выполняемых работ (оказываемых услуг) оборудования техническим сопровождением (сервисом).

- Заявка участника должна быть действительна в течение срока, указанного Участником в письме о подаче оферты. В любом случае этот срок не должен быть менее 90 календарных дней со дня, следующего за днем окончания приема Заявок. Указание меньшего срока может быть основанием для отклонения Заявки.

- Договор на оказание Услуг должен соответствовать форме, представленной на ЭЗП.

5. ***Требования к защите конфиденциальной информации:***

Исполнитель обязан предоставить сведения:
- перечень нормативных документов по защите информации, составляющей коммерческую тайну, и иной конфиденциальной информации;
- об ограничении доступа к информации, составляющей коммерческую тайну контрагентов, порядке обращения с этой информацией и контроле за его соблюдением;
- о наличии в трудовых договорах с работниками запрета разглашения информации, составляющей коммерческую тайну, обладателями которой являются контрагенты, и использования без их согласия этой информации в личных целях.

Исполнитель обязан заключить с ОАО «ТГК-1» соглашение о конфиденциальности (по форме ОАО «ТГК-1»), данная форма должна быть неотъемлемым приложением договора между Исполнителем и ТГК-1.

Руководитель:
Директор ПСДГУ и ИТ филиала «Невский» ОАО «ТГК-1» Малафеев А.В.

(должность руководителя Подразделения, являющегося Инициатором закупки) (подпись) (ФИО)