Решение

по делу № 21-05/28-18Ж

«04» сентября 2018 года г. Петропавловск-Камчатский

Комиссия Камчатского УФАС России по рассмотрению жалоб в порядке, предусмотренном статьей 18.1 Федерального закона №135-ФЗ от 26.07.2006 «О защите конкуренции» (далее – Комиссия) в составе:

Председатель Комиссии Кодерле И.В. – временно исполняющая обязанности руководителя УФАС России по Камчатскому краю,

Члены Комиссии:

Муравкина Ю.А. – главный специалист – эксперт отдела правового обеспечения и рекламы УФАС России по Камчатскому краю**;**

Ермолова О.В. – главный специалист – эксперт отдела антимонопольного контроля и закупок УФАС России по Камчатскому краю.

В присутствии заявителя ООО «Тендер»: представитель по доверенности Копылова С.И. (доверенность от 03.09.2018);

Организатора торгов: директор Шарипов Н.Е. (приказ №45-п от 10.10.2017), представитель по доверенности Тарасенко И.А. (доверенность от 03.09.2018), представитель по доверенности Стусенко С.Ю. (доверенность от 03.09.2018)

рассмотрев жалобу ООО «Тендер» на действия КГАУ «Информационно – технологический центр Камчатского края» по проведению открытого конкурса на право оказание услуг по модернизации системы защиты информации, включающих создание рабочего места мониторинга информационной безопасности с последующей аттестацией «ЦОД КГАУ ИТЦ» (извещение №31806746090), в соответствии с порядком рассмотрения антимонопольным органом жалоб на нарушение процедуры торгов и

порядка заключения договоров, установленным статьей 18.1 Федерального закона от 26.07.2006 № 135 – ФЗ «О защите конкуренции» (далее – Закон о защите конкуренции),

УСТАНОВИЛА:

27.08.2018 в УФАС России по Камчатскому краю поступила жалоба ООО «Тендер» на действия КГАУ «Информационно – технологический центр Камчатского края» по проведению открытого конкурса на право оказание услуг по модернизации системы защиты информации, включающих создание рабочего места мониторинга информационной безопасности с последующей аттестацией «ЦОД КГАУ ИТЦ» (извещение №31806746090).

Основные доводы жалобы.
1. Отсутствие в документации требований по сертификации товаров в описании объекта закупки.
2. Нарушение правил описания объекта закупки: неоднозначность при формировании требований к товару.
3. Нарушение принципов и основных положений закупки товаров, работ, услуг, определенных статьей 3 Федерального закона от 18.07.2011 №223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – Закон о закупках).
4. Формирование излишних требований к оказанию услуг.

В ходе поступления жалобы от Общества, Камчатское УФАС назначило рассмотрение дела №21-05/28-18ж на 04.09.2018 в 15 часов 00 минут, предварительно уведомив по факсимильной связи ООО «Тендер» и КГАУ «Информационно – технологический центр Камчатского края».

04.09.2018 года состоялось рассмотрение дела №21-05/28-18ж.

В ходе рассмотрения дела установлено.
24 июля 2018 года Учреждением в Единой информационной системе размещено извещение №31806746090 о проведении закупки в форме открытого конкурса - на право оказания услуг по модернизации системы защиты информации, включающих создание рабочего места мониторинга информационной безопасности с последующей аттестацией «ЦОД КГАУ ИТЦ» (далее - конкурс, Закупка). Начальная максимальная цена договора 9 324 030 рублей 00 коп.
Срок приема заявок на участие в конкурсе был установлен с

25.07.2018 по 14.08.2018. В период приема заявок от потенциальных участников закупки было принято 3 запроса разъяснений положений документации:

- 09.08.2018 от генерального директора ООО «ТДИ» Антонова И.Д. о документах, входящих в состав заявки;
- 09.08.2018 от индивидуального предпринимателя Деревяхиной А.В. о

разъяснении пункта 3 Технического задания;

- 09.08.2018 от индивидуального предпринимателя Головина Д.В. о сроке оказания услуг.

10 августа 2018 года в извещение и документацию были внесены изменения (уточнен срок оказания услуг) в связи с чем срок приема заявок на участие в конкурсе был продлен. Срок окончания подачи заявок - 28 августа 2018 года.
14.08.2018 на участие в конкурсе была подана заявка от ООО «Информационный центр».
Других заявок на участие в конкурсе не поступало.

На основании подпункта 7.13.1. пункта 7.13. Положения о закупке конкурс признан несостоявшимся так как по окончании срока подачи конкурсных заявок, установленного конкурсной документацией, получена только одна заявка.

1. Решением Межведомственной комиссии полномочного представителя Президента Российской Федерации в Дальневосточном федеральном округе по информационной безопасности от 17.11.2017 №67 (далее - Решение МВК) поставлена задача организовать постоянный контроль и координацию выполнения работ по защите информации, обрабатываемой в государственных информационных системах. Для реализации данной задачи, пунктом 3.6 Решения МВК рекомендовано особое внимание уделить принятию следующих мер:

- мониторинг информационной безопасности;
- выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов.

Вышеуказанным Решением МВК предполагается постоянное выполнение данных мер.
В ходе заседания Совета по информационной безопасности при

Губернаторе Камчатского края 23.05.2018 принято решение, в соответствии с которым органам государственной власти и местного самоуправления Камчатского края необходимо продолжить работу по постоянному контролю (мониторингу) защищенности государственных и муниципальных информационных систем, с представлением отчетных материалов по проводимому мониторингу. Особое внимание также поручено обратить на мониторинг информационной безопасности и выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри

разрешенных сетевых протоколов (пункты 1.2.1, 1.2.2 протокола от 23.05.2018 №1).
Срок внедрения указанных мер и отчета о проделанной работе для государственных органов и органов местного самоуправления Камчатского края установлен до 01 ноября 2018 года.
Обеспечить реализацию вышеуказанных мер на постоянной основе штатными силами существующих подразделений по информационной безопасности не представляется возможным, ввиду того, что постоянный мониторинг предполагает изучение всех событий на обслуживаемых компонентах информационной инфраструктуры, их анализ и выявление среди них аномалий. Для выполнения данных работ необходима автоматизация с использованием технического средства или набор таких средств, реализующих следующие функциональные возможности:

- сбор информации из различных источников с целью поиска критических событий безопасности.
- поиск взаимосвязи событий информационной безопасности для превращения исходных данных, поступающих с различных источников, в значащую информацию.
- применение долговременного хранилища данных в историческом порядке для корреляции данных по времени и для обеспечения их обработки.

На настоящий момент, подобный функционал реализован в программном обеспечении, представляющим собой автоматизированную систему сбора и анализа журналов событий и лог-файлов (хранилищ, содержащий информацию о событиях, происходящих в системе в хронологическом порядке).
С учетом вышеизложенного принято решение о необходимости внедрения в существующую информационную инфраструктуру указанного программного обеспечения (ПО).
Пунктом 3.4 Технического задания (ТЗ) описаны требования к характеристикам программного обеспечения, реализующего

функции системы сбора и анализа журналов событий и лог-файлов (хранилищ, содержащих информацию о событиях, происходящих в системе в хронологическом порядке) средств обработки, передачи и хранения информации с компонентом аналитики для установки на один сервер с максимальной производительностью обработки до 20 ООО событий в секунду (EPS) включительно.

В пункте 4.1 жалобы приведены ссылки на нормативные документы, в соответствии с которыми в государственных информационных системах должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации.

Программное обеспечение, описанное в пункте 3.4 ТЗ, не является средством защиты информации и используется для комплексного сбора журналов событий с различных источников (рабочие компьютеры, серверное и телекоммуникационное оборудование) с целью их последующего аудита и анализа.

Порядок сертификации средств защиты информации по требованиям безопасности информации на момент публикации конкурсной документации определялся документом «Положение о сертификации средств защиты информации по требованиям безопасности информации» (утверждено Приказом председателя Гостехкомиссии России от 27.10.1995 №199). Приложением №1 к указанному положению утвержден «Перечень средств защиты информации, подлежащих сертификации в системе сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России (№ РОСС RU.OOOI.OIBHOO)».

В указанном перечне отсутствует программное средство сбора и анализа событий информационной безопасности, таким образом программное обеспечение, предполагаемое к развертыванию в рамках пункта 3.4 ТЗ, не является средством защиты информации и к нему не предъявляются требования по оценке соответствия в форме обязательной сертификации.

Инструментами данного программного обеспечения планируется осуществлять сбор информации о техническом состоянии элементов ИТ-инфраструктуры с целью мониторинга работоспособности аппаратного и программного обеспечения.

П О ViPNet TIAS, как и описанное выше программное обеспечение, предназначено для автоматического выявления инцидентов на основе анализа событий информационной безопасности. Данный тип решений так же не содержит функций средств защиты информации и требования по оценке соответствия в форме обязательной сертификации к указанному ПО неприменимы.

Указанное программное обеспечение является средством автоматизации процесса анализа и аудита лог-файлов и событий с определенных источников событий (продуктовая линейка ViPNet разработки отечественного производителя ОАО «Инфотекс»), для

которых сертификация в качестве средства защиты информации по профилю «Система обнаружения вторжений» обязательна.
Данное сертифицированное СЗИ СОВ ViPNet IDS 1000 2.x, уже имеется в КГАУ ИТЦ, а также в связи с нехваткой производительности имеющихся мощностей дополнительно поставляется в соответствии с пунктом 4 раздела 2 «Объем оказываемых услуг» Технического задания.
ViPNet IDS 1000 2.x непосредственно выполняет функции средства защиты информации и обладает соответствующим набором сертификатов.
Таким образом, ПО ViPNet TIAS, не является средством защиты информации и требования по оценке соответствия в форме обязательной сертификации к указанному ПО неприменимы, в связи с чем нарушения Федерального законодательства о защите персональных данных и документов, утвержденных ФСТЭК России, в закупочной документации отсутствуют.
В своей закупочной деятельности заказчик руководствуется Положением о закупке в редакции от 15.06.2017. В жалобе ООО «Тендер» ссылается на нарушение заказчиком Положения о закупке в редакциях «от 19.12.2012 №4, от 29.03.2013 №1, от 25.12.2013 №4» которые в настоящее время признаны утратившими силу, в связи с чем положения указанного документа нарушены быть не могут.
2 . Порядок сертификации средств защиты информации по требованиям безопасности информации на момент публикации конкурсной документации определялся документом «Положение о сертификации средств защиты информации по требованиям безопасности информации» (утверждено Приказом председателя Гостехкомиссии России от 27.10.1995 №199). Приложением №1 к указанному положению утвержден «Перечень средств защиты информации, подлежащих сертификации в системе сертификации средств защиты информации по требованиям безопасности информации Гостехкомиссии России (№ РОСС 1Ш.0001.01БИ00)».
ПО, реализующее функции клиентского модуля системы защиты от НСД, предназначенного для защиты серверного компонента от НСД на базе ОС Linux, по своей функциональности является как минимум:

- Программой, обеспечивающей разграничение доступа к информации;
- Программой идентификации и аутентификации терминалов и пользователей;
- Программой контроля целостности информационных массивов;
- Программой уничтожения остаточной информации в запоминающих устройствах.

Это соответствует пунктам 2.3, 2.4, 2.5 и 2.7 указанного выше перечня.
Соответственно, к данному продукту предъявляется требование оценки соответствия в форме обязательной сертификации в отличие от ПО, реализующего функции системы сбора и анализа событий информационной безопасности и ПО ViPNet TIAS-VA 3.x.
В связи с изложенным, требования к предмету закупки изложены однозначно и нарушений требований к описанию предмета закупки, предусмотренных Законом о закупках нет.
3 . На момент публикации конкурсной документации и по сей день существует всего два сертифицированных решения ПАК, реализующего функции высокопроизводительного TLS-криптошлюза с числом внешних клиентов не менее 5000 и предельной пропускной способностью не менее 680 Мбит/с. Это ViPNet TLS Gateway (ОАО «Инфотекс») и «Континент TLS VPN Сервер» (ООО «Код Безопасности»).
ОАО «ИнфоТеКС» в соответствии с Условиями предоставления услуги «Техническая поддержка» (SLA) , опубликованного по адресу https://infotecs.ru/support/sla/ осуществляет техническую поддержку уровня «Совместная расширенная» с 9-00 до 18-00 по Московскому времени для инцидентов всех уровней критичности. ООО «Код Безопасности» в свою очередь в соответствии с SLA, опубликованного по адресу https://www.securitvcode.ru/services/tech-support/, осуществляет техническую поддержку уровня «Расширенная» с 10-00 до 18-00 по Московскому времени для инцидентов уровней «Существенный» и «Некритичиный», а для уровня «Критичный» в круглосуточном режиме.
Чтобы не допустить ограничений по выбору поставляемого ПАК, было принято решение выставить минимальные требования к оказанию технической поддержки с 9-00 до 18-00 по Московскому времени.
Время оказания услуг совместной технической поддержки для установлено в соответствии с Условия предоставления услуги «Техническая поддержка» (SLA) производителя программно-аппаратных комплексов и программного обеспечения (ОАО «ИнфоТеКС»), опубликованного по адресу https://infotecs.ru/support/sla/. Потенциальный поставщик передает Заказчику только ключ активации сервиса совместной технической поддержки. Техническую поддержку оказывает непосредственно производитель на условиях, описанных в SLA.
Таким образом, требования заказчика к часовому поясу не могут считаться противоречием требованиям статьи 3 Закона №223-Ф, так как заказчиком выбраны наиболее оптимальные требования для закупки услуг по минимальной цене и привлечения наибольшего числа участников закупки. Считаем, что нарушения принципа закупки «целевое и экономически эффективное расходование денежных

средств на приобретение товаров, работ, услуг (с учетом при необходимости стоимости жизненного цикла закупаемой продукции) и реализация мер, направленных на сокращение издержек заказчика» и ограничения круга потенциальных участников закупки в данной закупке не было.
4. КГАУ ИТЦ является подведомственным учреждением Агентства по информатизации и связи Камчатского края (далее - АИС), являющегося органом исполнительной власти Камчатского края. КГАУ ИТЦ в соответствии с приказом АИС от 01.07.2015 №61-п «О защите информации в государственных информационных системах, функционирующих в краевом государственном автономном учреждении «Информационно-технологический центр Камчатского края» назначено ответственными по осуществлению организационных и техническим мер по защите информации в следующих государственных информационных системах:

- ГИС «Региональная система межведомственного электронного взаимодействия Камчатского края»;
- ГИС «Реестр государственных и муниципальных услуг Камчатского края»;
- ГИС «Региональный портал государственных и муниципальных услуг Камчатского края».

Подписаны соглашения о размещении ГИС на базе инфраструктуры ЦОД КГАУ ИТЦ:
Государственная информационная система Камчатского края "Управление автомобильным транспортом, используемым для осуществления регулярных перевозок пассажиров и багажа в Камчатском крае" (Оператор- Министерство транспорта и дорожного строительства Камчатского края);

- ГИС Многофункционального центра предоставления государственных и муниципальных услуг (оператор - подведомственное учреждение Министерства экономического развития и торговли Камчатского края Краевое государственное казенное учреждение "Многофункциональный центр предоставления государственных и муниципальных услуг в Камчатском крае").

Подписаны соглашения о размещении иных информационных систем Агентства по занятости населения и миграционной политике Камчатского края, Инспекции государственного технического надзора Камчатского края, Министерства социального развития и труда Камчатского края и Министерства экономического развития и

торговли Камчатского края.
А также КГАУ ИТЦ является оператором следующих ГИС:

- ГИС «Инфраструктура пространственных данных Камчатского края»;
- ГИС «Удостоверяющий центр».

В ближайшем будущем планируется разместить от 3 до 5 пяти информационных систем (в том числе ГИС) иных органов государственной власти Камчатского края.
В соответствии с пунктом 17.6 Приказа ФСТЭК России от 11.02.2013 №17 «Об утверждении требований к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», в случае, если информационная система создается на базе центра обработки данных уполномоченного лица, такой центр обработки данных должен быть аттестован по классу защищенности не ниже класса защищенности, установленного для создаваемой информационной системы. При аттестации информационной системы должны использоваться результаты аттестации общей инфраструктуры оператора информационной системы. Согласно пункту 3 постановления Правительства Российской Федерации от 06.07.2015 №676 (в редакции постановления Правительства Российской Федерации от 11.05.2017 №555): «Рекомендовать иным государственным органам, помимо федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, а также органам управления государственными внебюджетными фондами, органам местного самоуправления руководствоваться в своей деятельности требованиями, утвержденными настоящим постановлением».
Также согласно информационному сообщению ФСТЭК России от 22.06.2017 №240/22/3031: «Рассмотрению в ФСТЭК России подлежат проекты моделей угроз безопасности информации и технических заданий на создание государственных информационных систем, оформленные в установленном порядке и поступившие от заказчиков или операторов государственных информационных систем».
Таким образом, требование согласования Модели угроз и Технического задания с ФСТЭК России не является излишним.

На основании вышеизложенного, руководствуясь частью 20 статьей 18.1. Федерального закона от 26.07.2006 № 135-ФЗ «О защите конкуренции», Комиссия,

РЕШИЛА:

1. Признать жалобу ООО ООО «Тендер» на действия КГАУ «Информационно – технологический центр Камчатского края» по проведению открытого конкурса на право оказание услуг по модернизации системы защиты информации, включающих создание рабочего места мониторинга информационной безопасности с последующей аттестацией «ЦОД КГАУ ИТЦ» (извещение №31806746090), ***необоснованной.***

Решение может быть обжаловано в арбитражном суде в течение трех месяцев со дня его принятия.

Председатель Комиссии И.В. Кодерле

Члены Комиссия Ю.А. Муравкина

О.В. Ермолова