ФЕДЕРАЛЬНАЯ
АНТИМОНОПОЛЬНАЯ СЛУЖБА

УПРАВЛЕНИЕ
Федеральной антимонопольной службы
по Калининградской области

ул. Барнаульская 4, г. Калининград, 236006
бокс № 5033
тел. (4012) 53-72-01, факс (4012) 53-72-00
e-mail: to39@fas.gov.ru

14.03.2024 № ИБ/1190/24

На № _____ от _____

решение по результатам рассмотрения жалобы

Заявитель:
ИП Попов Алексей Николаевич
popov_aleksei_n@mail.ru

Оператор электронной площадки:
ООО «РТС-тендер»
ko@rts-tender.ru; info@rts-tender.ru

Заказчик:
Государственное казенное учреждение здравоохранения «Медицинский информационно-аналитический центр Калининградской области»
i.rusina@infomed39.ru;n.safiullina@infomed39.ru;miac@infomed39

РЕШЕНИЕ № 039/06/33-147/2024

Резолютивная часть объявлена 11.03.2024 г. Калининград
Изготовлено в полном объеме 14.03.2024

Комиссия Управления Федеральной антимонопольной службы по Калининградской области по контролю в сфере закупок (далее - Комиссия) в составе:

председатель Комиссии:

И.С. Болтенко – заместитель руководителя — начальник отдела контроля органов власти, закупок и рекламы Калининградского УФАС России;

члены Комиссии:

О.И. Филатов – ведущий специалист – эксперт отдела контроля органов власти, закупок и рекламы Калининградского УФАС России;

И.Ю. Затолюк – специалист-эксперт отдела контроля органов власти, закупок и рекламы Калининградского УФАС России,

при участии представителей: заявителя – ИП Попова Алексея Николаевича (лично); Е.А. Поповой (по доверенности); заказчика - государственного казенного учреждения здравоохранения «Медицинский информационно-аналитический центр Калининградской области»: Д.В. Куделки (по доверенности); А.И. Бабиновича (по доверенности); И.Б. Русиной (по доверенности),

рассмотрев в режиме видеоконференцсвязи посредством плагина «TrueConf» жалобу ИП Попова Алексея Николаевича (вх. № 1633/24 от 04.03.2024) на действия заказчика - Государственного казенного учреждения здравоохранения «Медицинский информационно-аналитический центр Калининградской области» при проведении запроса котировок в электронной форме, предметом которого является поставка автоматизированных рабочих мест (извещение № 0335200007524000009) (далее – Аукцион), и в результате внеплановой проверки, проведенной в соответствии с частью 15 статьи 99 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон о контрактной системе),

УСТАНОВИЛА:

В Управление Федеральной антимонопольной службы по Калининградской области 04.03.2024 поступила жалоба Заявителя на действия Заказчика при формировании извещения об осуществлении закупки.

В обоснование своей жалобы Заявитель привел следующие доводы

По мнению Заявителя, установленные в описании объекта закупки меры защиты информации являются избыточными, более того, в настоящее время в Российской Федерации не существует ни одного сертифицированного средства защиты информации, которое одновременно отвечало бы всем требованиям, заявленным в Техническом задании.

Заказчиком даны следующие пояснения по сути жалобы Заявителя

Заказчик не согласен с доводами жалобы Заявителя, полагает, что описание объекта закупки составлено в соответствии с требованиями Закона о контрактной системе и его потребностью.

В результате рассмотрения жалобы и проведения в соответствии с частью 15 статьи 99 Закона о контрактной системе внеплановой проверки, Комиссия установила следующее

26.02.2024 Заказчиком на официальном сайте единой информационной системы в сфере закупок (далее – официальный сайт, ЕИС) размещено извещение об осуществлении закупки № 0335200007524000009 с приложениями. Начальная (максимальная) цена контракта – 8 730 843,00 рублей.

В силу статьи 6 Закона о контрактной системе контрактная система в сфере закупок основывается на принципах открытости, прозрачности информации о контрактной системе в сфере закупок, обеспечения конкуренции, профессионализма заказчиков, стимулирования инноваций, единства контрактной системы в сфере закупок, ответственности за результативность обеспечения государственных и муниципальных нужд, эффективности осуществления закупок.

В силу пункта 1 части 2 статьи 42 Закона о контрактной системе извещение об осуществлении закупки, если иное не предусмотрено настоящим Федеральным законом, должно содержать электронный документ, отражающий описание объекта закупки в соответствии со статьей 33 Закона о контрактной системе.

В соответствии с пунктом 1 части 1 статьи 33 Закона о контрактной системе заказчик в случаях, предусмотренных настоящим Федеральным законом, при описании объекта закупки должен руководствоваться следующими правилами:

1) в описании объекта закупки указываются функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки (при необходимости). В описание объекта закупки не должны включаться требования или указания в отношении товарных знаков, знаков обслуживания, фирменных наименований, патентов, полезных моделей, промышленных образцов, наименование страны происхождения товара, требования к товарам, информации, работам, услугам при условии, что такие требования или указания влекут за собой ограничение количества участников закупки. Допускается использование в описании объекта закупки указания на товарный знак в следующих случаях:

а) сопровождение такого указания словами «или эквивалент»;

б) несовместимость товаров, на которых размещаются другие товарные знаки, и необходимость обеспечения взаимодействия таких товаров с товарами, используемыми заказчиком;

в) осуществление закупки запасных частей и расходных материалов к машинам и оборудованию, используемым заказчиком, в соответствии с технической документацией на указанные машины и оборудование;

г) осуществление закупки медицинских изделий, специализированных продуктов лечебного питания, необходимых для назначения пациенту по медицинским показаниям (индивидуальная

непереносимость, по жизненным показаниям) по решению врачебной комиссии, которое фиксируется в медицинской документации пациента и журнале врачебной комиссии. Перечень указанных медицинских изделий, специализированных продуктов лечебного питания и порядок его формирования утверждаются Правительством Российской Федерации.

В пункте 39 «Основной части извещения о проведении запроса котировок», являющейся неотъемлемой частью извещения указан перечень документов (электронных документов), содержащихся в извещении, в том числе «Описание объекта закупки (техническое задание)» (далее — Техническое задание).

В пункте 1 Технического задания, размещенного в составе извещения об осуществлении закупки указано, в том числе следующее: *«СЗИ, реализуют следующие меры: ИАФ.1-ИАФ.5; УПД.1-УПД.6; УПД.9-УПД.11; УПД.13-УПД.17; ОПС.1-ОПС.3; РСБ.1-РСБ.8; ЗНИ1-ЗНИ3; ЗНИ5; ЗНИ8; АВЗ.1; АВЗ.1 усиление 6, АВЗ.1 усиление 8; АВЗ.2».*

Также в Техническом задании указано, что СЗИ должные соответствовать:

«-Требованиям о защите информации, не составляющей государственную тайну, содержащейся в ГИС, утвержденных приказом ФСТЭК России №17 от 11февраля 2013 г.,

-Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены приказом ФСТЭК России от 18.03.2013 №21».

Как полагает, Заявитель установленные меры защиты информации, а именно: ИАФ.2, УПД.3, УПД.13, УПД.14, УПД.15 ,УПД.16, ОПС.1, ОПС.2, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.3, ЗНИ.5, ЗНИ.8, РСБ.2, РСБ.6, РСБ.8, АВЗ.1 (усиление 6 и 8), АВЗ.2 являются избыточными, также Заявитель в своих дополнениях к жалобе указывает, что программный комплекс «Электронный замок «ВИТЯЗЬ», версии 2.2 является единственным СЗИ, сертифицированным ФСТЭК России по профилю СДЗ подходящим под требования меры АВЗ.1 усиления 6 и 8, АВЗ.2 Технического задания. Меры АВЗ.1 (усиление 6 и 8) и РСБ.8 могут быть включены только в уточняющий адаптированный базовый набор мер и требуют обоснования утвержденной оператором Единой государственной информационной системы в сфере здравоохранения и согласованной с ФСТЭК и ФСБ модели угроз. Такая модель угроз у Заказчика отсутствует.

Комиссия, проанализировав представленные материалы и сведения, принимая во внимание пояснения сторон, приходит к следующим выводам.

Согласно представленным материалам Государственная информационная система в сфере здравоохранения Калининградской области (далее — ИС) в соответствии с Аттестатом соответствия №2384.00008.2021 от 21.12.2021, выданным 000 «БАЛТ-информ» (далее - Аттестат соответствия №2384.00008.2021 от 21.12.2021) соответствует следующим требованиям по защите информации: *«класс защищенности К1, 2 уровень защищенности персональных данных, 3 категория значимости, оператор ИС - МИАЦ, соответствует Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК России от I 1.02.2013 № 17, Составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждены приказом ФСТЭК России от 18.02.2013 №21, Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждены Приказом ФСТЭК России от 25.12.2017 №239».*

Согласно пункту 20 Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - Приказ ФСТЭК России от 11.02.2013 № 17) организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;
защиту машинных носителей информации;
регистрацию событий безопасности;
антивирусную защиту;
обнаружение (предотвращение) вторжений;
контроль (анализ) защищенности информации;
целостность информационной системы и информации;
доступность информации;
защиту среды виртуализации;
защиту технических средств;
защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении № 2 к настоящим Требованиям.

В соответствии с пунктом 21 Приказа ФСТЭК России от 11.02.2013 № 17 выбор мер защиты информации для их реализации в информационной системе в рамках ее системы защиты информации включает:

определение базового набора мер защиты информации для установленного класса защищенности информационной системы в соответствии с базовыми наборами мер защиты информации, приведенными в приложении № 2 к настоящим Требованиям;

адаптацию базового набора мер защиты информации применительно к структурно-функциональным характеристикам информационной системы, информационным технологиям, особенностям функционирования информационной системы (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении № 2 к настоящим Требованиям, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включенных в модель угроз безопасности информации;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Для выбора мер защиты информации для соответствующего класса защищенности информационной системы применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 года № 1085.

В силу пункта 22 Приказа ФСТЭК России от 11.02.2013 № 17 в информационной системе соответствующего класса защищенности в рамках ее системы защиты информации должны быть реализованы меры защиты информации, выбранные в соответствии с пунктом 21 настоящих Требований и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации.

ФСТЭК России 11.02.2014 года утвержден «Методический документ. Меры защиты информации в государственных информационных системах» разработанный и утвержденный в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.08.2004 года № 1085 (далее — Методический документ).

Методический документ детализирует организационные и технические меры защиты информации (далее - меры защиты информации), принимаемые в государственных информационных системах (далее - информационные системы) в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах,

утвержденными приказом ФСТЭК России от 11.02.2013 года № 17, а также определяет содержание мер защиты информации и правила их реализации.

Методический документ предназначен для обладателей информации, заказчиков, заключивших государственный контракт на создание информационной системы (далее - заказчики), операторов информационных систем (далее - операторы), лиц, обрабатывающих информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющих им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее - уполномоченные лица), а также лиц, привлекаемых в соответствии с законодательством Российской Федерации для проведения работ по созданию (проектированию) информационных систем в защищенном исполнении и (или) их систем защиты информации (далее - разработчики (проектировщики)).

Методический документ применяется для выбора и реализации в соответствии с пунктом 21 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 года № 17, мер защиты информации в информационных системах, направленных на обеспечение:

конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

целостности информации (исключение неправомерного уничтожения или модифицирования информации);

доступности информации (исключение неправомерного блокирования информации).

Согласно абзацу 2 пункта 2 Методического документа выбор мер защиты информации осуществляется исходя из класса защищенности информационной системы, определяющего требуемый уровень защищенности содержащейся в ней информации, и угроз безопасности информации, включенных в модель угроз безопасности информационной системы, а также с учетом структурно-функциональных характеристик информационной системы, к которым относятся структура и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, взаимосвязи с иными информационными системами и информационно- телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

В соответствии с абзацами 2, 3 подпункта «а» пункта 2.3 Методического документа определение базового набора мер защиты информации основывается на классе защищенности информационной системы, установленном в соответствии с пунктом 2.1 настоящего методического документа. В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 г. № 17, и приложением № 2 к настоящему методическому документу в качестве начального выбирается один из четырех базовых наборов мер защиты информации, соответствующий установленному классу защищенности информационной системы. Меры защиты информации, обозначенные знаком «+» в приложении № 2 включены в базовый набор мер защиты информации для соответствующего класса защищенности информационной системы. Меры защиты информации, не обозначенные знаком «+», к базовому набору мер не относятся, и могут применяться при последующих действиях по адаптации, уточнению, дополнению мер защиты информации, а также разработке компенсирующих мер защиты информации.

Базовый набор мер защиты информации, выбранный в соответствии с классом защищенности информационной системы, подлежит адаптации применительно к структурно-функциональным характеристикам и особенностям функционирования информационной системы, уточнению в зависимости от угроз безопасности информации и при необходимости дополнению мерами защиты информации, включенными в иные нормативные правовые акты, нормативные и методические документы по защите информации.

Комиссией установлено, что в соответствии с Приложением № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах, утвержденным приказом ФСТЭК России № 17 от 11.02.2013 к классу защищенности информационной системы К1, которому согласно Аттестату соответствия № 2384.00008.2021 от 21.12.2021 соответствует ИС Заказчика, применяются следующие базовые меры защиты информации, выбранные Заказчиком: ИАФ.1-ИАФ.5; УПД.1-УПД.6; УПД.9-УПД.11; УПД.13-УПД.17; ОПС.1-ОПС.3; РСБ.1-РСБ.7; ЗНИ1-ЗНИ2; ЗНИ5; ЗНИ8; АВЗ.1; АВЗ.2.

Таким образом, Комиссия приходит к выводу, что позиция Заявителя о том, что установленные базовые меры защиты информации, которые по мнению Заявителя также являются избыточными, а именно: ИАФ.2, УПД.3, УПД.13, УПД.14, УПД.15 ,УПД.16, ОПС.1, ОПС.2, ОПС.3, ЗНИ.1, ЗНИ.2, ЗНИ.5, ЗНИ.8, РСБ.2, РСБ.6, АВЗ.2 является несостоятельной.

Комиссией также установлено, что в Техническом задании по позиции 1 Заказчиком были установлены помимо базовых мер защиты информации, меры защиты информации, применяющиеся при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности, а именно: РСБ.8, ЗНИ.3, АВЗ.1 (усиление 6 и 8).

Согласно абзацам 2, 3 подпункта «в» пункта 2.3 Методического документа уточнение адаптированного базового набора мер защиты информации проводится с учетом результатов оценки возможности адаптированного базового набора мер защиты информации адекватно блокировать (нейтрализовать) все угрозы безопасности информации, включенные в модель угроз безопасности информации, или снизить вероятность их реализации исходя из условий функционирования информационной системы.

Исходными данными при уточнении адаптированного базового набора мер защиты информации являются перечень угроз безопасности информации и их характеристики (потенциал, оснащенность, мотивация), включенные в модель угроз безопасности информации.

В соответствии с абзацами 6, 7, 8, 10 подпункта «в» пункта 2.3 Методического документа уточненный адаптированный базовый набор мер защиты информации подлежит реализации в информационной системе в соответствии с разделом 3 настоящего методического документа.

В подразделах «требования к реализации меры защиты информации» для каждой меры, приведенной в разделе 3 настоящего методического документа, указано требование к тому, каким образом и в каком объеме должна быть реализована каждая мера защиты информации. Требования к реализации мер защиты информации являются минимальными требованиями, выполнение которых должно быть обеспечено в информационной системе соответствующего класса защищенности, в случае если эта мера выбрана для реализации в качестве уточненной адаптированной базовой меры защиты информации.

В зависимости от класса защищенности информационной системы минимальные требования к реализации уточненной адаптированной базовой меры защиты информации подлежат усилению для повышения уровня защищенности информации. Все возможные усиления мер защиты информации приведены в подразделах «требования к усилению меры защиты информации», приведенных в разделе 3 настоящего методического документа для каждой меры защиты информации. Усиления мер защиты информации применяются дополнительно к требованиям по реализации мер защиты информации, приведенным в подразделах «требования к реализации меры защиты информации».

Усиления мер защиты информации, приведенные в подразделе «требования к усилению меры защиты информации» и не включенные в таблицу с содержанием базовой меры защиты информации в подразделе «содержание базовой меры защиты информации», применяется по решению обладателя информации, заказчика и (или) оператора для повышения уровня защищенности информации, содержащейся в информационной системе, или при адаптации, уточнении, дополнении мер защиты информации, а также при разработке компенсирующих мер защиты информации.

Согласно подпункту «г» пункта 2.3 Методического документа дополнение уточненного адаптированного базового набора мер защиты информации осуществляется с целью выполнения требований о защите информации, установленных иными нормативными правовыми актами в области защиты информации, в том числе в области защиты персональных данных.

Дополнение уточненного адаптированного базового набора мер защиты информации может потребоваться, в том числе в случае:

а) если федеральным законом, указом Президента Российской Федерации, постановлением Правительства Российской Федерации, нормативными актами органа государственной власти, органа местного самоуправления или организации, определяющими порядок создания и эксплуатации информационной системы, устанавливаются дополнительные требования к защите информации, выполнение которых не предусмотрено Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 года № 17.

В соответствии с пунктом 4 статьи 16 Федерального закона от 27.07.2006г. № 149 ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

На заседании Комиссии представители Заказчика пояснили, что АРМ, являющееся предметом закупки, приобретаются с целью реализации новой информационной системы «Электронная регистратура», реализуемой в рамках развития цифрового контура здравоохранения Российской Федерации и оператором которой является Заказчик. Оператор информационной системы самостоятельно определяет состав мер информационной безопасности (как организационных, так и технических) с учетом законодательства Российской Федерации в области защиты информации, достаточный для противодействия угрозам безопасности. В целях недопущения загрузки вредоносного программного обеспечения на этапе инициализации операционной системы Заказчиком было заявлено требование о наличие средств антивирусной защиты уровня осуществляющих контроль целостности файлов ОС на этапе загрузки АРМ (АВЗ.1 усиление 6) и контроль микропрограммного кода загрузочного сектора базовой системы ввода вывода (АВЗ.1 усиление 8), что является актуальной угрозой в связи с возросшим количеством вредоносного ПО типа «руткит» и «буткит». Меры СЗИ, указанные в описании объекта закупки распространены не на единое средство защиты информации, а на составную подсистему защиты информации из нескольких решений, сертифицированных в соответствии с требованиями регуляторов в области обеспечения информационной безопасности (ФСТЭК России и ФСБ России).

Также, согласно пояснениям Заказчика на постоянной основе обновляется информация о новых угрозах и уязвимостях в Банке данных, размещенном на официальном сайте ФСТЭК России. Последнее обновление Банка угроз осуществлено ФСТЭК России 06.03.2024 года и по состоянию на указанную дату в нем содержалась информация о 222 выявленных угрозах и 55242 уязвимостях. Заказчик как оператор, несущий персональную ответственность за обеспечение информационной безопасности и защиту данных в государственной информационной системе, в ходе доработки подсистемы защиты информации учел, как базовые меры в отношении государственной информационной системы класса защищенности К1, так и дополнительные меры с учетом актуальных угроз.

Комиссия отмечает, что Заявителем в ходе рассмотрения жалобы не было представлено каких-либо сведений, позволяющих сделать вывод, что выбранные Заказчиком меры защиты не соответствуют его фактической потребности, кроме того, Заказчик является оператором ИС, что

накладывает на него ответственность за не соблюдение законодательства Российской Федерации в области защиты информации.

В части доводов жалобы Заявителя о том, что программный комплекс «Электронный замок «ВИТЯЗЬ», версии 2.2 является единственным СЗИ, сертифицированным ФСТЭК России по профилю СДЗ подходящим под требования меры АВЗ.1 усиления 6 и 8, АВЗ.2 и, что в настоящий момент нет ни одного сертифицированного средства защиты информации, которое одновременно отвечало бы всем требованиям, заявленным в Техническом задании, Комиссия отмечает следующее.

При расчете НМЦК по настоящей закупке Заказчиком использовались коммерческие предложения, представленные:

- ООО «Центр защиты информации» (исх. № 151 от 09.02.2024), согласно которому к поставке предложено (АРМ, тип 1, страна происхождения: Россия, реестровая запись № 3279\1\2023 в составе: ПЭВМ ICL BasicRay модели B102 G2R: i3-12100/8GB/256GB SSD M.2/Монитор 23,8» /ИБП 600 ВА/К/М Предустановленное ПО: Numa BIOS, Альт Рабочая станция 10.1 Предустановленные СЗИ: ViPNet SafeBoot, Dallas Lock Linux, Kaspersky Endpoint Security);
- АО «Крафтвэй корпорэйшн ПЛС» (исх. № ДП/0902 от 09.02.2024), согласно которому к поставке предложено (АРМ Крафтвэй IC210 КРПЕ.466216.050 Персональная ЭВМ Крафтвэй IC210 КРПЕ.466216.119);
- ООО «Комплексные инновационные технологии» (исх. № 6 от 12.02.2024), согласно которому к поставке предложено (АРМ Крафтвэй IC210 КРПЕ.466216.050 Персональная ЭВМ Крафтвэй IC210 КРПЕ.466216.119);

Таким образом, в коммерческих предложениях в соответствии с Техническим заданием к поставке были предложены разные АРМ.

В соответствии с протоколом подведения итогов определения поставщика (подрядчика, исполнителя) от 06.03.2024 №ИЗК1 на участие в запросе котировок подано две заявки с идентификационными номерами № 116011117, 115974635 Заявка № 116011117 отклонена, а заявка № 115974635 признана соответствующей. В заявке № 115974635, признанной соответствующей предложено к поставке АРМ Крафтвэй IC210 КРПЕ.466216.050 реестровая запись № 5987\1\2023 от 21.12.2023 страна происхождения Россия. В заявке № 116011117, отклоненной предложено к поставке АРМ происхождения товара Россия.

Как пояснил представитель Заказчика на заседании Комиссии к поставке требуется комплекс, отвечающий требованиям, установленным в Техническом задании, который поставщик комплектует самостоятельно.

Комиссия обращает внимание, что в материалы рассмотрения жалобы Заявителем не было представлено каких-либо сведений, позволяющих сделать вывод, что единственным СЗИ, сертифицированным ФСТЭК России по профилю средства доверенной загрузки, подходящим под требования меры АВЗ.1 усиления 6 и 8, АВЗ.2 является только программный комплекс «Электронный замок «ВИТЯЗЬ», версии 2.2.

При том, представленные коммерческие предложения, поданные заявки на участие в закупке, вопреки позиции Заявителя об отсутствии на рынке сертифицированного средства защиты информации, которое одновременно отвечало бы всем требованиям, заявленным в Техническом задании, свидетельствуют о том, что на рынке имеются поставщики, готовые осуществить поставку в соответствии с требованиями Технического задания Заказчика.

Таким образом, с учетом представленных материалов, пояснений сторон, поданных заявок на участие в закупке, в отсутствие представленных со стороны Заявителя доказательств: о невозможности поставки АРМ, заявленного Заказчиком в Техническом задании; о соответствие требованиям меры АВЗ.1 усиления 6 и 8, АВЗ.2 только программного комплекса «Электронный замок «ВИТЯЗЬ», версии 2.2, Комиссия приходит к выводу, что в действиях Заказчика при формировании извещения об осуществлении закупки отсутствуют признаки нарушения Закона о контрактной системе. Доводы жалобы Заявителя являются необоснованными.

В заседании Комиссии представители лиц, участвующих в рассмотрении жалобы, на вопрос Председателя Комиссии о достаточности доказательств, представленных в материалы дела, пояснили,

что все доказательства, которые они намеревались представить, имеются в распоряжении Комиссии, иных доказательств, ходатайств, в том числе о представлении или истребовании дополнительных доказательств не имеется.

В связи с изложенным, руководствуясь частями 1, 4, 7 статьи 105, частью 8 статьи 106 Закона о контрактной системе, Комиссия

РЕШИЛА:

Признать жалобу ИП Попова Алексея Николаевича необоснованной.

Председатель комиссии И.С. Болтенко

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота ФАС России

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Болтенко Ирина Сергеевна**
Сертификат № 00E09AD2EBFF2436A93D402924416B6580
Действителен с 06.09.2023 по 29.11.2024

Члены комиссии:

О.И. Филатов

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота ФАС России

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Филатов Олег Игоревич**
Сертификат № 00DAD033B13779F83A47338B44373611A5
Действителен с 10.01.2024 по 04.04.2025

И.Ю. Затолюк

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота ФАС России

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Затолюк Ирина Юрьевна**
Сертификат № 5EF3AA4FE507CCE3B9B5746DE40E2D6C
Действителен с 02.10.2023 по 25.12.2024

В соответствии с частью 9 статьи 106 Закона о контрактной системе, решение может быть обжаловано в судебном порядке в течение трех месяцев со дня его принятия.