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

24.10.2024 № НИ/5494/24

На № _____ от _____

решение по результатам рассмотрения жалобы

Заказчики согласно извещению
№ 0335200014924002948

Уполномоченное учреждение:
Государственное казенное учреждение Калининградской области «Центр обеспечения организации и проведения торгов»
gkuct@gov39.ru

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

Заявитель:
ИП Попов Алексей Николаевич
popov_aleksei_n@mail.ru

РЕШЕНИЕ № 039/06/33-938/2024

Резолютивная часть объявлена 21.10.2024 г. Калининград
Изготовлено в полном объеме 24.10.2024

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

председатель Комиссии:

Н.С. Иванова – 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;

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

при участии представителей: заявителя – ИП Попова А.Н. (лично), Е.А. Поповой (по доверенности); ответственного заказчика — государственного бюджетного учреждения здравоохранения Калининградской области «Полесская центральная районная больница»: Ю.П. Интайте (по доверенности), А.И. Бабиновича (по доверенности); уполномоченного учреждения – государственного казенного учреждения Калининградской области Центр обеспечения организации и проведения торгов»: А.В. Лигостаева (по доверенности), В.И. Белоговой (по доверенности); заинтересованного лица — ООО «РеСтарт»: Д.С. Максимова (по доверенности),

рассмотрев в режиме видеоконференцсвязи посредством плагина «TrueConf» жалобу ИП Попова А.Н. (вх. № 8032/24 от 14.10.2024) (далее — Заявитель) на действия заказчиков (далее — Заказчики) при осуществлении совместного электронного аукциона, предметом которого является поставка автоматизированных рабочих мест (далее — АРМ) (извещение № 0335200014924002948) (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 14.10.2024 поступила жалоба Заявителя на действия Заказчиков при формировании извещения об осуществлении закупки.

В обоснование своей жалобы Заявитель привел следующие доводы

По мнению Заявителя, в описании объекта закупки установлены избыточные требования к средствам защиты информации в отсутствие специфики использования такого товара, а именно: «СЗИ, реализуют следующие меры: АВЗ.1 усиление 6, АВЗ.1 усиление 8», что соответствует только одному товару ПК ЭЗ «Витязь» производителя «Крафтвэй».

Кроме того, описание объекта закупки содержит некорректные требования к типу оперативной памяти и количеству накопителей SSD.

Заказчиком даны следующие пояснения по сути жалобы Заявителя

Заказчики не согласны с доводами жалобы Заявителя, полагают, что описание объекта закупки составлено в соответствии с требованиями Закона о контрактной системе и потребностью.

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

04.10.2024 Заказчиком на официальном сайте единой информационной системы в сфере закупок (далее – официальный сайт, ЕИС) размещено извещение об осуществлении закупки № 0335200014924002948 с приложениями. Начальная (максимальная) цена контракта – 22 357 200,00 рублей.

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 пункте 41 «Основной части извещения» перечислен перечень документов (электронных документов), содержащихся в извещении, в том числе «Описание объекта закупки (техническое задание)» (далее — Техническое задание).

В Техническом задании установлено, что «Автоматизированное рабочее место» должно обладать, в том числе следующими характеристиками:

Характеристики товара, работы, услуги			
Наименование характеристики	Значение характеристики	Единица измерения характеристики	Инструкция по заполнению характеристик в заявке
Тип оперативной памяти	DDR4		Участник закупки указывает в заявке только одно значение характеристики
Тип оперативной памяти	DDR5		Участник закупки указывает в заявке только одно значение характеристики
Интерфейс накопителя SSD:	SATA		Участник закупки указывает в заявке

			только одно значение характеристики
Интерфейс накопителя SSD:	PCIe		Участник закупки указывает в заявке только одно значение характеристики
Количество накопителей типа SSD	≥ 1	ШТ	Участник закупки указывает в заявке конкретное значение характеристики
СЗИ, реализуют следующие меры: ИАФ.1 - ИАФ.6; УПД.1 - УПД.2; УПД.4 - УПД.6; УПД.9 - УПД.11; УПД.17; ЗНИ.1; ЗНИ.5; ЗНИ.8; РСБ.1 - РСБ.7; ОЦЛ.1; ОЦЛ.3; ЗИС.1; ЗИС.15; ЗИС.21; АВЗ.1; АВЗ.1 усиление 6, АВЗ.1 усиление 8; АВЗ.2.	Наличие		Значение характеристики не может изменяться участником закупки

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

1. В отношении довода об установлении избыточных требований АВЗ.1 усиление 6, усиление 8, соответствующих только одному товару.

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.6; УПД.1 - УПД.2; УПД.4 - УПД.6; УПД.9 - УПД.11; УПД.17; ЗНИ.1; ЗНИ.5; ЗНИ.8; РСБ.1 - РСБ.7; ОЦЛ.1; ОЦЛ.3; ЗИС.1; ЗИС.15; ЗИС.21; АВЗ.1; АВЗ.2.

Кроме того, Комиссией также установлено, что в Техническом задании Заказчиками были установлены помимо базовых мер защиты информации, такие меры защиты информации как: 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.

Согласно пояснениям Заказчиков АРМ, являющееся предметом закупки, приобретаются в рамках развития цифрового контура здравоохранения Российской Федерации на территории Калининградской области, с целью подключения медицинских работников к ИС и оказания медицинской помощи. При разработке технического задания закупки оно проходило согласование с Оператором информационной системы - ГКУЗ «Медицинский информационно-аналитический центр Калининградской области». В соответствии с требованиями действующего законодательства Оператор ИС 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. Меры защиты информации, указанные к реализации на закупаемых АРМ, были выбраны с учетом актуальных угроз информационной безопасности и мер не ниже установленных согласно Аттестату соответствия №2384.00008.2021 от 21.12.2021. В целях недопущения загрузки вредоносного программного обеспечения на этапе инициализации операционной системы Заказчиком было заявлено требование, подтвержденное Оператором информационной системы, о наличии средств антивирусной защиты уровня осуществляющих контроль целостности файлов ОС на этапе загрузки АРМ (АВ3.1 усиление 6) и контроль микропрограммного кода загрузочного сектора базовой системы ввода вывода (АВ3.1 усиление 8), что является актуальной угрозой в связи с возросшим количеством вредоносного ПО типа «руткит» и «буткит». Необходимость установления указанных требований, подтвержденная Оператором информационной системы, основывалась, в том числе на информации о новых угрозах и уязвимостях в Банке данных, размещенном на официальном сайте ФСТЭК России. Заказчиками при формировании требований технического задания приняты во внимание пояснения оператора информационной системы, несущего персональную ответственность за обеспечение информационной безопасности и защиту данных в государственной информационной системе и который установил, как базовые меры в отношении государственной информационной системы класса защищенности К1, так и дополнительные меры с учетом актуальных угроз. При формировании НМЦК Заказчиками проводился запрос цен, который был размещен в ЕИС, у неограниченного числа поставщиков. По результатам указанного запроса в адрес ответственного Заказчика поступили предложения от различных поставщиков, предложивших оборудование, соответствующее требованиям технического задания и удовлетворяющих потребности Заказчиков, не менее двух различных производителей (в том числе в отношении средств защиты информации).

В соответствии с представленными материалами для расчета НМЦК при формировании закупки Заказчиками использовались коммерческие предложения от следующих субъектов:

- ООО «КИТ» (ИНН 9717101930) (исх. № 96 от 02.08.2024), в соответствии с которым к поставке предложено: Автоматизированное рабочее место Крафтвэй IC 210 КРПЕ.466216.050, реестровый номер 10468452 от 21.12.2023. В составе: Персональная Электронная Вычислительная Машина Крафтвэй IC 210 КРПЕ.466219.119. Процессор Intel Core i3-12100 3.30 GHz, 12M Cache, 60W, LGA1700, CM8071504651012, Tray, Материнская плата Kraftway KWH610 Intel H610, LGA1700, 2 DIMM DDR4, 1x PCIex16, 1x PCIex1, 2x M.2, 3x SATA, USB 3.2/2.0, HDMI, DP, D-SUB (VGA), RJ45, micro ATX, KWH610, КРПЕ.469535.185, Корпус MiniTower, Блок питания 450 Вт, 256 Gb SSD M.2 2280 PCIe, Модуль памяти Kraftway DIMM 8GB DDR4-3200 КРПЕ.467526.003-01. Антивирус Kaspersky UEFI – лицензия Kaspersky Antivirus for UEFI 1год, KSS, Лицензия Dr.Web Enterprise Security Suite ЭЗ «Витязь» ЭЗ «Витязь версия 2.2 2019 до 2024 — Формуляр, документация на CD, Лицензия на Программный Комплекс Электпронный Замок «Витязь», Электронный USB-токен JaCarta 2 PKI/ГОСТ (в корусе nano), сертификат ФСТЭК № 4446 от 19.09.2021, Простая (неисключительная) лицензия на право использования операционной системы РЕД ОС без ограничения срока действия, стандартная редакция. Конфигурация: «Рабочая станция». Включает 1 год гарантии стандартного уровня (REDOS-DSP-STD-STD-1YE-0224), СЗИ от несанкционированного доступа Dallas Lock Linux Монитор 23,8», ИБП 600 ВА, Клавиатура USB, Мышь. Страна происхождения: Россия, производитель: АО «Крафтвэй

корпорэйшн ПЛС». Сведения содержащиеся в записи о программном обеспечении, включенном в реестр российского программного обеспечения: Предустановленное ПО: 1) Kraftway BIOS — реестровая запись № 8590 от 31.12.2020; 2) RED OS — Реестровая запись № 3751 от 23.07.2017. Предустановленные СЗИ: СЗИ СДЗ Электронный замок Витязь — Сертификат ФСТЭК № 3597 от 11.07.2016, реестровая запись № 2896 от 14.03.2017; 4) СЗИ НДС «Dallas Lock Linux» - Сертификат ФСТЭК № 3594 от 04.07.2016, реестровая запись № 1285 от 05.09.2016; 5) САВЗ Dr.Web Enterprise Security Suite – Сертификат ФСТЭК № 3509 от 27.01.2016, реестровая запись № 48 от 20.02.2016.

- ООО «ТЕМП» (исх. № 74 от 02.08.2024), в соответствии с которым к поставке предложено: автоматизированное рабочее место (АРМ), Реестровый номер № 10451613. В составе: ПЭВМ ICL BasicRay модели B102 G3R: i3-12100/8GB/256Gb SSD M.2/Монитор 23,8 «/ИБП 600 ВА/К/М. Предустановленное ПО: Numa BIOS — реестровая запись № 5467 от 24.06.2019, Альт Рабочая станция 10.1- реестровая запись № 1292 от 05.09.2016. Предустановленные СЗИ: VipNet SafeBoot — Сертификат ФСТЭК № 3823 от 14.11.2017, реестровая запись № 3442 от 03.05.2017, Dallas Lock Linux — Сертификат ФСТЭК № 3594 от 04.07.2016, реестровая запись № 1285 от 05.09.2016, Kaspersky Endpoint Security — Сертификат ФСТЭК № 2534 от 27.12.2011, реестровая запись № 205 от 18.03.2016. Страна происхождения: Россия, производитель ООО «АЙСИЭЛ ТЕХНО».

- ООО «АКСИОМА» (ИНН 3906377795) (исх. № 167 от 02.08.2024), в соответствии с которым к поставке предложено: Автоматизированное рабочее место Крафтвэй IC 210 КРПЕ.466216.050, реестровый номер 10468452 от 21.12.2023. В составе: Персональная Электронная Вычислительная Машина Крафтвэй IC 210 КРПЕ.466219.119. Процессор Intel Core i3-12100 3.30 GHz, 12M Cache, 60W, LGA1700, CM8071504651012, Tray, Материнская плата Kraftway KWH610 Intel H610, LGA1700, 2 DIMM DDR4, 1x PCIex16, 1x PCIex1, 2x M.2, 3x SATA, USB 3.2/2.0, HDMI, DP, D-SUB (VGA), RJ45, micro ATX, KWH610, КРПЕ.469535.185, Корпус MiniTower, Блок питания 450 Вт, 256 Gb SSD M.2 2280 PCIe, Модуль памяти Kraftway DIMM 8GB DDR4-3200 КРПЕ.467526.003-01. Антивирус Kaspersky UEFI – Лицензия Kaspersky Antivirus for UEFI 1год, KSS, Лицензия Dr.Web Enterprise Security Suite ЭЗ «Витязь» ЭЗ «Витязь версия 2.2 2019 до 2024 — Формуляр, документация на CD, Лицензия на Программный Комплекс Электронный Замок «Витязь», Электронный USB-токен JaCarta 2 PKI/ГОСТ (в корпусе nano), сертификат ФСТЭК № 4446 от 19.09.2021, Простая (неисключительная) лицензия на право использования операционной системы РЕД ОС без ограничения срока действия, стандартная редакция. Конфигурация: «Рабочая станция». Включает 1 год гарантии стандартного уровня (REDOS-DSP-STD-STD-1YE-0224), СЗИ от несанкционированного доступа Dallas Lock Linux Монитор 23,8», ИБП 600 ВА, Клавиатура USB, Мышь. Страна происхождения: Россия, производитель: АО «Крафтвэй корпорэйшн ПЛС». Сведения содержащиеся в записи о программном обеспечении, включенном в реестр российского программного обеспечения: Предустановленное ПО: 1) Kraftway BIOS — реестровая запись № 8590 от 31.12.2020; 2) RED OS — Реестровая запись № 3751 от 23.07.2017. Предустановленные СЗИ: СЗИ СДЗ Электронный замок Витязь — Сертификат ФСТЭК № 3597 от 11.07.2016, реестровая запись № 2896 от 14.03.2017; 4) СЗИ НДС «Dallas Lock Linux» - Сертификат ФСТЭК № 3594 от 04.07.2016, реестровая запись № 1285 от 05.09.2016; 5) САВЗ Dr.Web Enterprise Security Suite – Сертификат ФСТЭК № 3509 от 27.01.2016, реестровая запись № 48 от 20.02.2016.

Таким образом, в коммерческих предложениях, которые использовались при формировании НМЦК были предложены к поставке АРМы разных производителей: ПЭВМ ICL BasicRay (ООО «АЙСИЭЛ ТЕХНО») и Крафтвэй IC 210 КРПЕ.466216.050 (АО «Крафтвэй корпорэйшен ПЛС») с разными наборами СЗИ: (VipNet SafeBoot, Dallas Lock Linux, Kaspersky Endpoint Security) и (СЗИ СДЗ Электронный замок Витязь, СЗИ НДС «Dallas Lock Linux», САВЗ Dr.Web Enterprise Security Suite).

В целях подтверждения соответствия АРМов с указанными в коммерческих предложениях характеристиками ответственным Заказчиком были направлены запросы производителям: ООО «АйСиЭл Техно» (исх. № 98 от 25.09.2024) и АО «Крафтвэй корпорэйшен ПЛС» (исх. № 97 от 25.09.2024).

В своих ответах ООО «АйСиЭл Техно» (исх. № 1636 от 25.09.2024) и АО «Крафтвэй корпорэйшен ПЛС» (исх. № 754 от 26.09.2024), представленных по запросам ответственного Заказчика, подтвердили соответствие характеристик АРМов, представленных в коммерческих предложениях.

Вместе с тем, Заявителем, в свою очередь, в материалы рассмотрения жалобы была представлена, в том числе следующая информация.

- Письмо АО «Крафтвэй корпорэйшен ПЛС» (исх. № 1605/3 от 16.05.2023), в котором сообщается следующее: *«Решение компании Kraftway ПК ЭЗ «Витязь» 2.2, является средством доверенной загрузки и средством антивирусной защиты второго класса, которое может применятся для защиты не только конфиденциальной информации (АС 1Г, ГИС К1, ИСПДн У31), а также сведений составляющих государственную тайну до уровня совершенно секретно включительно.*

ПК ЭЗ «Витязь» 2.2 реализует меры защиты, в том числе:

- *ИАФ.1 - усиление 1а, 2а, 3, 4;*
- *УПД.17 - усиление 1, 2;*
- *АВЗ.1 - усиление 6, 8;*
- *ОЦЛ.1 - усиление 1, 2;*
- *и другие*

ПК ЭЗ «Витязь» 2.2 поставляется исключительно в предустановленном виде и реализован на основе программно-аппаратного решения российского производства в составе материнских плат компании, внесенных в Реестр промышленной продукции, произведенной на территории Российской Федерации»;

- Ответ АО «ИнфоТеКС», представленный по запросу Арбитражного суда Калининградской области в рамках дела № А21-3284/2024, в котором сообщается какие меры защиты выполняются ПМДЗ ViPNet SafeBoot в соответствии с приказом ФСТЭК России № 17 от 11.02.2013, так меры защиты, такие как: АВЗ.1 усиление 6, усиление 8, указанные Заказчиками в Техническом задании, у ПМДЗ ViPNet SafeBoot отсутствуют;

- Письмо ООО «Конфидент» (исх. № 174-3/24 от 07.08.2024), в котором сообщается какие меры защиты выполняются СЗИ Dallas Lock for Linux, Комиссией установлено, что такие меры защиты как: АВЗ.1 усиление 6, усиление 8, указанные Заказчиками в Техническом задании, у СЗИ Dallas Lock for Linux отсутствуют.

Таким образом, согласно информации, представленной Заявителем, следует, что СЗИ ViPNet SafeBoot и Dallas Lock for Linux не выполняют меры защиты АВЗ.1 усиление 6, усиление 8, указанные Заказчиками в Техническом задании

В соответствии с протоколом подачи ценовых предложений от 14.10.2024 №ЦПА1, протоколом подведения итогов определения поставщика (подрядчика, исполнителя) от 16.10.2024 №ИЭА1 на участие в закупке поступило две заявки с идентификационными номерами: 117450170, 117444795. Снижение на торгах составило — 5,50%. Заявка с идентификационным номером 117450170 отклонена по основанию, предусмотренному пунктом 8 части 12 статьи 48 Закона о контрактной системе, заявка с идентификационным номером 117444795, занявшая второе место по торгам, признана соответствующей.

В качестве обоснования отклонения заявки с идентификационным номером 117450170 комиссией по осуществлению закупок Уполномоченного учреждения указано следующее:

«пункт 8 части 12 статьи 48 Закона № 44-ФЗ, пункт 41 документа «Основная часть извещения о проведении электронного аукциона» извещения о закупке, подпункт 1 пункта 2 Раздела 1 «Требования к содержанию, составу заявки на участие в закупке» и Раздела 2 «Инструкция по заполнению заявки» документа «Требования к содержанию, составу заявки на участие в закупке и инструкция по ее заполнению», а именно: ***выявление недостоверной информации****, содержащейся в заявке на участие в закупке.*

В структурированной части Заявки участник закупки предлагает к поставке товар «Автоматизированное рабочее место» с значениями характеристик:

- ***СЗИ****, реализуют следующие меры: ИАФ.1 - ИАФ.6; УПД.1 - УПД.2; УПД.4 - УПД.6; УПД.9 - УПД.11; УПД.17; ЗНИ.1; ЗНИ.5; ЗНИ.8; РСБ.1 - РСБ.7; ОЦЛ.1; ОЦЛ.3; ЗИС.1; ЗИС.15; ЗИС.21; АВЗ.1;* ***АВЗ.1 усиление 6, АВЗ.1 усиление 8;*** *АВЗ.2.:* ***Наличие.***

Вместе с тем в составе своей заявки участник закупки согласно требованиям пункта 2 постановления Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления

закупок для обеспечения государственных и муниципальных нужд», в отношении характеристики «Средства защиты информации (СЗИ)), указал порядковый номер реестровой записи № 407 (Dallas Lock 8.0-К) в реестре российского программного обеспечения.

Согласно письму ООО «Конфидент» меры защиты АВ3.1 — усиление 6, 8 не обеспечивается средствами Dallas Lock 8.0-К, что не соответствует характеристикам, указанным участником закупки в структурированной части заявки на закупку: «СЗИ, реализуют следующие меры: ИАФ.1 - ИАФ.6; УПД.1 - УПД.2; УПД.4 - УПД.6; УПД.9 - УПД.11; УПД.17; ЗНИ.1; ЗНИ.5; ЗНИ.8; РСБ.1 - РСБ.7; ОЦЛ.1; ОЦЛ.3; ЗИС.1; ЗИС.15; ЗИС.21; АВ3.1; ***АВ3.1 усиление 6, АВ3.1 усиление 8****; АВ3.2.:* ***Наличие.****».*

Иных номеров в отношении характеристики (СЗИ)) участником закупки в в составе заявки не указано.

Таким образом, заявка участника содержит недостоверную информацию в отношении предлагаемого к поставке товара».

Комиссией установлено, что в заявках, поданных на участие в закупке, содержится следующая информация о предлагаемом к поставке товаре:

- в заявке с идентификационным номером 117450170 предложено к поставке: АРМ с товарным знаком «Бештау», страна происхождения: Российская Федерация. АРМ/ПЭВМ БЕШТАУ РС1167/Q670-01, БЕРТ.466219.005-008, Реестровый номер № 10431144 (Исторический реестровый номер № 1972\2\2023); ОПЕРАЦИОННАЯ СИСТЕМА АЛЬТ 8 СП, Реестровый номер №4305 от 29.03.2018; Базовая система ввода-вывода для системной платы BESHTAU-BIOS I-10-13, Реестровая запись №23946 от 06.09.2024; Dallas Lock 8.0-К, Реестровый номер № 407; Kaspersky Endpoint Security для бизнеса, Реестровый номер №207 от 18.03.2016;

- в заявке с идентификационным номером 117444795 предложено к поставке: АРМ ПЭВМ ICL BasicRay модели B102 G3R КШДС.466219.004-05, страна происхождения товара: Российская Федерация, также приложены следующие выписки: на товар реестровый номер № 10451613 Исторический реестровый номер № 2908\1\2023 (Машины вычислительные электронные персональные ПЭВМ ICL BasicRay модели B102 G3R КШДС.466219.004-05, ООО «АЙСИЭЛ ТЕХНО»), на программное обеспечение: реестровый номер 48 от 20.02.2016 (средство антивирусной защиты Dr.Web Enterprise Security Suite, правообладатель ООО «ДОКТОР ВЕБ»), реестровый номер 1285 от 05.09.2016 (средства защиты от несанкционированного доступа к информации - Система защиты информации от несанкционированного доступа «Dallas Lock Linux», правообладатель ООО «КОНФИДЕНТ»), реестровый номер 2896 от 14.07.2017 (Программный комплекс «Электронный замок Витязь», правообладатель ЗАО «Крафтвэй корпорэйшн ПЛС»), реестровый номер 3751 от 23.07.2017 (операционная система РЕД ОС, правообладатель ООО «РЕД СОФТ»), реестровый номер 8590 от 31.12.2020 (встроенное программное обеспечение Kraftway BIOS, правообладатель АО «КРАФТВЭЙ КОРПОРЭЙШН ПЛС»).

Таким образом, в заявке с идентификационным номером 117450170 к поставке было предложено СЗИ компании ООО «Конфидент» - Dallas Lock 8.0-К.

В целях принятия решения о соответствии либо об отклонении заявки с идентификационным номером 117450170 Уполномоченным учреждением был направлен запрос в ООО «Конфидент» (вх. № 612-РН от 16.10.2024).

Из информации, представленной ООО «Конфидент» (вх. № 592-РН от 16.10.2024) по запросу Уполномоченного учреждения, следует, что в продуктовой линейке Dallas Lock, включая СЗИ НСД Dallas Lock 8.0 и СЗИ НСД Dallas Lock Linux, не реализован функционал, обеспечивающий антивирусную защиту (АВЗ), в том числе и меры защиты АВ3.1 - усиление 6, 8.

Таким образом, из анализа выше изложенного, а именно: ответа АО «ИнфоТеКС», представленного по запросу Арбитражного суда Калининградской области в рамках дела № А21-3284/2024, письма ООО «Конфидент» (исх. № 174-3/24 от 07.08.2024), информации, представленной ООО «Конфидент» (вх. № 592-РН от 16.10.2024) по запросу Уполномоченного учреждения, Комиссия приходит к выводу, что СЗИ: VipNet SafeBoot и Dallas Lock, не обеспечивают меры защиты информации, такие как: АВ3.1 усиление 6, усиление 8, указанные Заказчиками в Техническом задании.

Из этого обстоятельства следует, что в коммерческом предложении ООО «ТЕМП» (исх. № 74 от

02.08.2024), использовавшемся при формировании НМЦК по рассматриваемой закупке предложен к поставке товар, не соответствующий характеристикам, указанным Заказчиками в Техническом задании.

В свою очередь, в коммерческих предложениях: ООО «КИТ» (исх. № 96 от 02.08.2024) и ООО «АКСИОМА» (ИНН 3906377795) (исх. № 167 от 02.08.2024), заявке с идентификационным номером 117444795, признанной соответствующей, предложено к поставке, в том числе СЗИ СДЗ Электронный замок Витязь, которое согласно письму АО «Крафтвэй корпорэйшен ПЛС» (исх. № 1605/3 от 16.05.2023) и пояснениям сторон реализует меры защиты АВ3.1 - усиление 6, 8.

Комиссия обращает внимание, что ответственный Заказчик в ходе рассмотрения жалобы не смог пояснить и представить вопреки доводам и доказательствам Заявителя информацию о том, какие ещё СЗИ, помимо СДЗ Электронный замок Витязь правообладателя АО «Крафтвэй корпорэйшен ПЛС», реализуют меры защиты АВ3.1 - усиление 6, 8.

Согласно статье 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.

Статьей 8 Закона о контрактной системе установлено, что контрактная система в сфере закупок направлена на создание равных условий для обеспечения конкуренции между участниками закупок. Любое заинтересованное лицо имеет возможность в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами о контрактной системе в сфере закупок стать поставщиком (подрядчиком, исполнителем).

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:

- 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.

Исполнением требований статьи 33 Закона о контрактной системе должно являться наличие на рынке как минимум двух производителей, товар которых соответствует всем требованиям, обозначенным в извещение об осуществлении закупки.

При этом Комиссия отмечает, что включение в извещение об осуществлении закупки требований к закупаемому товару, которые свидетельствуют о его конкретном производителе является нарушением положений статьи 33 Закона о контрактной системе. Данная позиция находит свое отражение также в пункте 2 Обзора судебной практики применения законодательства Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, утвержденного Президиумом Верховного Суда Российской Федерации 28.06.2017.

Таким образом, с учетом представленных материалов, пояснений сторон, поданных заявок на участие в закупке, в отсутствие представленных со стороны Заказчиков доказательств, подтверждающих потребность в мерах защиты информации: АВ3.1 усиления 6, 8, а также соответствие данным мерам иных СЗИ, помимо СДЗ Электронный замок Витязь правообладателя АО «Крафтвэй корпорэйшен ПЛС», Комиссия приходит к выводу, что указанным требованиям Технического задания соответствует только СДЗ Электронный замок Витязь правообладателя АО «Крафтвэй корпорэйшен ПЛС».

При изложенных обстоятельствах, Комиссия приходит к выводу, что действия Заказчиков при формировании Технического задания в данной части нарушают требования пункта 1 части 1 статьи 33 Закона о контрактной системе. Довод жалобы Заявителя является обоснованным.

2. В отношении довода о некорректных требованиях к типу оперативной памяти и количеству накопителей SSD, Комиссия отмечает следующее.

В описании объекта закупки (Техническом задании), сформированном с использованием ЕИС в структурированном виде, содержится по указанным характеристикам следующее:

Характеристики товара, работы, услуги (Автоматизированное рабочее место)			
Наименование характеристики	Значение характеристики	Единица измерения характеристики	Инструкция по заполнению характеристик в заявке
Тип оперативной памяти	DDR4 DDR5	Участник закупки указывает в заявке только одно значение характеристики	
Интерфейс накопителя SSD:	SATA PCIe	Участник закупки указывает в заявке только одно значение характеристики	
Количество накопителей типа SSD	≥ 1	ШТ	Участник закупки указывает в заявке конкретное значение характеристики

Согласно пояснениям ответственного Заказчика и Уполномоченного учреждения структурированное описание объекта закупки (Техническое задание) размещается в ЕИС закупки. При интеграции в ЕИС и на электронную площадку система предлагает выпадающий список, состоящий из двух значений, участнику закупки необходимо выбрать одно из значений характеристики. Заявка заполняется на сайте электронной площадки в электронной форме. При выборе характеристики: «Интерфейс накопителя SSD» система предлагает выпадающий список, состоящий из двух значений «SATA» и «PC1e» как и при выборе характеристики «Тип оперативной памяти» система предлагает выпадающий список, состоящий из двух значений «DDR4» и «DDR5», также количество накопителей типа SSD может быть равно одно, что вписывается в указанные параметры.

Комиссия отмечает, что по данным характеристикам запрос на разъяснение положений извещения об осуществлении закупки не поступал, в коммерческих предложениях, представленных по запросу Заказчика, как и в заявках, поданных на участие в закупке, указаны конкретные значения характеристик в единственном роде.

Запрос о представлении ценовой информации (исх. № 67 от 02.08.2024), в ответ на который хозяйствующими субъектами были представлены коммерческие предложения: исх. №№: 74, 96 167 от 02.08.2024, соответствует Техническому заданию, размещенному в составе извещения об осуществлении закупки № 0335200014924002948 в формате «word» и запросу о предоставлении ценовой информации исх. № 73 от 27.08.2024, размещенному в ЕИС.

При изложенных обстоятельствах, Комиссия приходит к выводу, что действия Заказчиков в данной части при формировании извещения об осуществлении закупки не нарушают требования Закона о контрактной системе. Довод жалобы Заявителя является необоснованным.

Учитывая тот факт, что допущенное нарушение пункта 1 части 1 статьи 33 Закона о контрактной системе при формировании извещения об осуществлении закупки нарушает права и законные интересы неограниченного круга лиц, в том числе Заявителя, Комиссия приходит к выводу о необходимости выдачи обязательного для исполнения предписания об устранении выявленного нарушения Закона о контрактной системе.

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:

1. Признать жалобу ИП Попова А.Н. частично обоснованной.
2. Признать заказчиков по извещению № 0335200014924002948 нарушившими пункт 1 части 1 статьи 33 Закона о контрактной системе.
3. Выдать заказчикам по извещению № 0335200014924002948, комиссии по осуществлению закупок Уполномоченному учреждению, оператору электронной площадки (в части имеющихся полномочий) предписание об устранении выявленного нарушения Закона о контрактной системе.
4. Передать материалы дела должностному лицу Калининградского УФАС России для решения вопроса о привлечении лиц, допустивших нарушение Закона о контрактной системе, к административной ответственности.

Председатель комиссии Н.С. Иванова

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

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Иванова Наталия Сергеевна**
Сертификат № 00CC85071B8D43C07E0B9D1A153C0357AB
Действителен с 09.09.2024 по 03.12.2025

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

О.И. Аркадьева

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

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Кому выдан: **Аркадьева Ольга Ивановна**
Сертификат № 00D1C436CA622B6F8037F1C54D26C4A443
Действителен с 23.04.2024 по 17.07.2025

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.