Конкурстық құжаттама жобасын алдын ала талқылау хаттамасы
№14690767

Конкурстың № 14364382-1
Конкурстың атауы Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Конкурстық құжаттама жобасына ескертулерді, сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салуларды қабылдау мерзімі бастап 2025-03-27 22:09:13 дейін 2025-04-01 09:00:00
Ұйымдастырушының атауы "Қарағанды қаласының мемлекеттік активтер және сатып алу бөлімі" ММ

Конкурстық құжаттама жобасына ескерту(лер), сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салу(лар) мынадай шешім(дер) қабылданған өнім беруші(лер)ге жіберілген:

№	Әлеуетті өнім берушінің БСН (БСН)/ БСН/УНП	Өтініш түрпаты (түсіндіру туралы ескерту, сұрау салу)	Түсіндіру туралы ескертуді, сұрау салуды жіберу күні мен уақыты	Өтініш мәтіні (ескерту, түсіндіру туралы сұрау)	Шешім қабылданды	Ауытқу себебі, түсіндіру мәтіні
1	210440011371	КК жобасына ескерту	Оперативный центр информационной безопасности не является аппаратно-программным комплексом(Товар), а наоборот поставляется в виде оказания услуги. Для оказания услуги ОЦИБ, требуется программное обеспечение SIEM. Программное обеспечение SIEM рамках оказания услуг может размещаться на мощностях заказчика внутри его инфраструктуры и на мощностях поставщика. Согласно пункту 1 в техническом задании: "Целями закупаемой услуги по обеспечению информационной безопасности являются: 1.1 Мониторинг событий информационной безопасности объектов информатизации Заказчика; 1.2 Выявление, реагирование и предотвращение инцидентов информационной безопасности на объектах информатизации Заказчика; 1.3 Повышение уровня информационной безопасности Заказчика; 1.4 Исполнение требований Закона «Об информатизации» ст.17 п2-1 пп1. «о приобретении услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан». " нет четких требований размещать программное обеспечение SIEM в ЦОДе или поставлять как аппаратно-программный комплекс. В связи с этим наличие ЦОД считается завышенным требованием, данное нарушение создает препятствия для добросовестных участников закупок и может привести к ограничению конкуренции.	2025-03-31 10:44:31	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает что требование к ЦОД соответствовать стандарту Tier-2 обеспечивает высокую надежность и непрерывность работы инфраструктуры. Это крайне важно для оперативного центра информационной безопасности, поскольку он должен функционировать круглосуточно для мониторинга и реагирования на инциденты информационной безопасности. Соответствие требованиям информационной безопасности: Требования ГТС для успешного прохождения аттестации по информационной безопасности являются обязательными для критически важных информационных систем. Это гарантирует, что инфраструктура соответствует необходимым стандартам безопасности и может защитить конфиденциальную информацию. Требования к ЦОД и соответствию стандартам безопасности не ограничивают конкуренцию, а скорее создают равные условия для всех участников закупок. Это гарантирует, что все поставщики услуг ОЦИБ будут соответствовать одинаковым стандартам качества и безопасности. Законодательные требования: Закон «Об информатизации» и другие нормативные акты Казахстана обязывают организации обеспечивать информационную безопасность на высоком уровне. Требования к ЦОД и SIEM-системе являются частью этих обязательств и направлены на повышение общего уровня информационной безопасности в стране.

2	210440011371	КК жобасына ескерту	Пункт "4.11.8. Любой активный инфраструктурный компонент или элемент канала распределения должен иметь возможность вывода из эксплуатации для планового обслуживания без воздействия на ИТ-нагрузку. ЦОД должен соответствовать стандарту Tier-2 и требованиям ГТС для успешного прохождения аттестации по информационной безопасности." Это требование является завышенным, поскольку, согласно Техническому заданию на приобретение услуги по обеспечению информационной безопасности, ЦОД необходим для размещения SIEM-системы и хранения событий безопасности (логов). Исходя из этого, стандарт Tier-2 и требования ГТС для успешного прохождения аттестации по информационной безопасности будут относиться к SIEM-системе, а не к информационной системе. Система "Региональный шлюз электронного правительства" и Информационно-коммуникационная инфраструктура здания государственного учреждения "Аппарат акима Карагандинской области" в государственного учреждения "Аппарат акима Карагандинской области" является КВОИКИ, и при прохождении испытаний от ГТС будет испытываться инфраструктура государственного учреждения "Аппарат акима Карагандинской области" и "Региональный шлюз электронного правительства". Поскольку критические является инфраструктурой и системой, требование по соответствию стандарту Tier-2 и требованиям ГТС для успешного прохождения аттестации по информационной безопасности является завышенным. SIEM-система не проходит испытания от ГТС, а является ОДНИМ из требований для прохождения испытаний. Данное нарушение создает препятствия для добросовестных участников закупок и может привести к ограничению конкуренции.	2025-03-31 10:43:59	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает следующее. Требование соответствия ЦОД стандарту Tier-2 и требованиям ГТС для аттестации информационной безопасности не является завышенным, Стандарт Tier-2 обеспечивает базовую избыточность инфраструктуры, что критично для непрерывной работы SIEM-системы, которая требует стабильного хранения и анализа логов безопасности[2][6]. Даже для вспомогательных систем (как SIEM) надежность ЦОД влияет на общую защищенность инфраструктуры. Требования ГТС распространяются на всю информационную систему, включая компоненты, взаимодействующие с КВОИКИ. SIEM-система, как часть инфраструктуры, подпадает под эти нормы, так как её данные используются для мониторинга безопасности всей ИС. Критичность инфраструктуры (КВОИКИ) требует соответствия всех связанных компонентов единым стандартам безопасности. Несоответствие ЦОД требованиям ГТС может привести к отказу в аттестации всей системы, что подтверждается практикой применения стандартов вроде СТБ 2227-2018.Требование обосновано необходимостью обеспечения целостности защиты всей ИС, включая вспомогательные компоненты .Роль SIEM в обеспечении безопасности КВОИКИ SIEM-система, хотя и не является частью критически важной информационно-коммуникационной инфраструктуры (КВОИКИ), выполняет ключевую функцию в защите объектов КВОИКИ, таких как «Региональный шлюз электронного правительства»: - Непрерывный сбор и анализ логов: Прерывание работы SIEM из-за отсутствия резервирования (Tier-2) может привести к потере данных о событиях безопасности, что нарушит требования к мониторингу и аудиту (п. 4.1.3 ГОСТ Р 57580 или аналогичные стандарты РК). - Оперативное реагирование на инциденты: Доступность SIEM напрямую влияет на скорость выявления и устранения угроз для КВОИКИ. Простой системы из-за планового обслуживания ЦОД может создать окно уязвимости. Таким образом, требование к отказоустойчивости ЦОД (Tier-2) обусловлено необходимостью обеспечения непрерывности работы SIEM как инструмента защиты КВОИКИ. Соответствие стандарту Tier-2 Стандарт Tier-2 (Uptime Institute) предусматривает: - Резервирование компонентов (N+1), что позволяет выводить оборудование на обслуживание без остановки работы. - Минимизацию риска потери данных при плановых работах, что критично для SIEM, которая должна гарантировать целостность и доступность логов. Если SIEM размещается в ЦОД без Tier-2: - Обслуживание инфраструктуры (например, замена серверов) потребует остановки системы, что нарушит непрерывность сбора логов. - Это противоречит требованиям п. 5.3.2 ГОСТ Р 56939 («Обеспечение доступности информации»), где указана необходимость резервирования для систем, связанных с безопасностью. SIEM обеспечивает безопасность КВОИКИ, и её недоступность создает риски для защищаемых систем. 2. Соответствие Tier-2 и ГТС — обязательное условие для аттестации инфраструктуры в рамках законодательства РК. 3. Требования согласуются с международными и национальными стандартами информационной безопасности.

3	991140000634	КК жобасына ескерту	Уважаемый заказчик! Вами опубликован тендер методом открытого конкурса на предоставление «Услуги по обеспечению информационной безопасности». Согласно пункта 2. Статьи 7-2 Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК: «2. Оперативный центр информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий». Так, согласно Приложения 1 к Закону Республики Казахстан «О разрешениях и уведомлениях» от 16 мая 2014 года № 202-V ЗРК «Лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий» относится к перечню разрешений первой категории. На основании вышеизложенного, руководствуясь пунктом 72 Правил осуществления государственных закупок (Приказ Министра финансов Республики Казахстан от 9 октября 2024 года № 687 ГЗ), требуем исключить установленные вами квалификационные требования согласно приложения 8 и установить требование о наличии разрешения первой категории (лицензии) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.	2025-03-28 11:41:40	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает что наличие трудовых ресурсов обусловлено необходимостью интеграции с различными внутренними службами Заказчика и наличие соответствующих компетенций должно быть подтверждено сертификатами. Соответствующие компетенции у Заказчика отсутствуют, данные требования по наличию трудовых ресурсов должны обеспечить правильную настройку интеграционных модулей в критически важную инфраструктуру Заказчика. Любой активный инфраструктурный компонент или элемент канала распределения должен иметь возможность вывода из эксплуатации для планового обслуживания, никак не затрагивая ИТ-нагрузку. ЦОД должен соответствовать стандарту Tier-2 и соответствовать требованиям ГТС для успешного прохождения аттестации по информационной безопасности

Осы конкурсқа қатысуға өтінімдер осы хаттама және бекітілген конкурстық құжаттаманың мәтіні мемлекеттік сатып алу веб-порталында орналастырылған сәттен бастап бес жұмыс күнінен кешіктірілмей қабылданады.

руководитель ГУ «Отдел государственных активов и закупок города Караганды» Калиакпаров Бауыржан Климович

Аббревиатураларды таратып жазу:
БСН – бизнес-сәйкестендіру нөмірі;
ЖСН – жеке сәйкестендіру нөмірі;
ССН – салық төлеушінің сәйкестендіру нөмірі;
ТЕН – төлеушіні есепке алу нөмірі;
Т.А.Ә. – тегі аты әкесінің аты (ол бар болса).

Протокол предварительного обсуждения проекта конкурсной документации №14690767

№ конкурса 14364382-1
Название конкурса Услуги по обеспечению информационной безопасности
Срок приема замечаний к проекту конкурсной документации, а также запросов о разъяснении положений конкурсной документации с 2025-03-27 22:09:13 по 2025-04-01 09:00:00
Наименование организатора ГУ "Отдел государственных активов и закупок города Караганды"

Замечание (я) к проекту конкурсной документации, а также запрос(ы) о разъяснении положений конкурсной документации направлены следующим(и) потенциальным поставщиком (ами), по которому (ым) принято(ы) следующее (ие) решение(я):

№	БИН (ИИН)/ ИНН/УНП потенциального поставщика	Тип обращения (замечание, запрос о разъяснении)	Текст обращения	Дата и время направления замечания, запроса о разъяснении	Принято решение	Причина отклонения, текст разъяснения
1	210440011371	Замечание к КД	Оперативный центр информационной безопасности не является аппаратно-программным комплексом(Товар), а наоборот поставляется в виде оказания услуги. Для оказания услуги ОЦИБ, требуется программное обеспечение SIEM. Программное обеспечение SIEM рамках оказания услуг может размещаться на мощностях заказчика внутри его инфраструктуры и на мощностях поставщика. Согласно пункту 1 в техническом задании: "Целями закупаемой услуги по обеспечению информационной безопасности являются: 1.1 Мониторинг событий информационной безопасности объектов информатизации Заказчика; 1.2 Выявление, реагирование и предотвращение инцидентов информационной безопасности на объектах информатизации Заказчика; 1.3 Повышение уровня информационной безопасности Заказчика; 1.4 Исполнение требований Закона «Об информатизации» ст.17 п2-1 пп1. «о приобретении услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан». " нет четких требований размещать программное обеспечение SIEM в ЦОДе или поставлять как аппаратно-программный комплекс. В связи с этим наличие ЦОД считается завышенным требованием, данное нарушение создает препятствия для добросовестных участников закупок и может привести к ограничению конкуренции.	2025-03-31 10:44:31	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает что требование к ЦОД соответствовать стандарту Tier-2 обеспечивает высокую надежность и непрерывность работы инфраструктуры. Это крайне важно для оперативного центра информационной безопасности, поскольку он должен функционировать круглосуточно для мониторинга и реагирования на инциденты информационной безопасности. Соответствие требованиям информационной безопасности: Требования ГТС для успешного прохождения аттестации по информационной безопасности являются обязательными для критически важных информационных систем. Это гарантирует, что инфраструктура соответствует необходимым стандартам безопасности и может защитить конфиденциальную информацию. Требования к ЦОД и соответствию стандартам безопасности не ограничивают конкуренцию, а скорее создают равные условия для всех участников закупок. Это гарантирует, что все поставщики услуг ОЦИБ будут соответствовать одинаковым стандартам качества и безопасности. Законодательные требования: Закон «Об информатизации» и другие нормативные акты Казахстана обязывают организации обеспечивать информационную безопасность на высоком уровне. Требования к ЦОД и SIEM-системе являются частью этих обязательств и направлены на повышение общего уровня информационной безопасности в стране.

2	210440011371	Замечание к КД	Пункт "4.11.8. Любой активный инфраструктурный компонент или элемент канала распределения должен иметь возможность вывода из эксплуатации для планового обслуживания без воздействия на ИТ-нагрузку. ЦОД должен соответствовать стандарту Tier-2 и требованиям ГТС для успешного прохождения аттестации по информационной безопасности." Это требование является завышенным, поскольку, согласно Техническому заданию на приобретение услуги по обеспечению информационной безопасности, ЦОД необходим для размещения SIEM-системы и хранения событий безопасности (логов). Исходя из этого, стандарт Tier-2 и требования ГТС для успешного прохождения аттестации по информационной безопасности будут относиться к SIEM-системе, а не к информационной системе. Система "Региональный шлюз электронного правительства" и Информационно-коммуникационная инфраструктура здания государственного учреждения "Аппарат акима Карагандинской области" в государственного учреждения "Аппарат акима Карагандинской области" является КВОИКИ, и при прохождении испытаний от ГТС будет испытываться инфраструктура государственного учреждения "Аппарат акима Карагандинской области" и "Региональный шлюз электронного правительства". Поскольку критические является инфраструктурой и системой, требование по соответствию стандарту Tier-2 и требованиям ГТС для успешного прохождения аттестации по информационной безопасности является завышенным. SIEM-система не проходит испытания от ГТС, а является ОДНИМ из требований для прохождения испытаний. Данное нарушение создает препятствия для добросовестных участников закупок и может привести к ограничению конкуренции.	2025-03-31 10:43:59	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает следующее. Требование соответствия ЦОД стандарту Tier-2 и требованиям ГТС для аттестации информационной безопасности не является завышенным, Стандарт Tier-2 обеспечивает базовую избыточность инфраструктуры, что критично для непрерывной работы SIEM-системы, которая требует стабильного хранения и анализа логов безопасности[2][6]. Даже для вспомогательных систем (как SIEM) надежность ЦОД влияет на общую защищенность инфраструктуры. Требования ГТС распространяются на всю информационную систему, включая компоненты, взаимодействующие с КВОИКИ. SIEM-система, как часть инфраструктуры, подпадает под эти нормы, так как её данные используются для мониторинга безопасности всей ИС. Критичность инфраструктуры (КВОИКИ) требует соответствия всех связанных компонентов единым стандартам безопасности. Несоответствие ЦОД требованиям ГТС может привести к отказу в аттестации всей системы, что подтверждается практикой применения стандартов вроде СТБ 2227-2018.Требование обосновано необходимостью обеспечения целостности защиты всей ИС, включая вспомогательные компоненты .Роль SIEM в обеспечении безопасности КВОИКИ SIEM-система, хотя и не является частью критически важной информационно-коммуникационной инфраструктуры (КВОИКИ), выполняет ключевую функцию в защите объектов КВОИКИ, таких как «Региональный шлюз электронного правительства»: - Непрерывный сбор и анализ логов: Прерывание работы SIEM из-за отсутствия резервирования (Tier-2) может привести к потере данных о событиях безопасности, что нарушит требования к мониторингу и аудиту (п. 4.1.3 ГОСТ Р 57580 или аналогичные стандарты РК). - Оперативное реагирование на инциденты: Доступность SIEM напрямую влияет на скорость выявления и устранения угроз для КВОИКИ. Простой системы из-за планового обслуживания ЦОД может создать окно уязвимости. Таким образом, требование к отказоустойчивости ЦОД (Tier-2) обусловлено необходимостью обеспечения непрерывности работы SIEM как инструмента защиты КВОИКИ. Соответствие стандарту Tier-2 Стандарт Tier-2 (Uptime Institute) предусматривает: - Резервирование компонентов (N+1), что позволяет выводить оборудование на обслуживание без остановки работы. - Минимизацию риска потери данных при плановых работах, что критично для SIEM, которая должна гарантировать целостность и доступность логов. Если SIEM размещается в ЦОД без Tier-2: - Обслуживание инфраструктуры (например, замена серверов) потребует остановки системы, что нарушит непрерывность сбора логов. - Это противоречит требованиям п. 5.3.2 ГОСТ Р 56939 («Обеспечение доступности информации»), где указана необходимость резервирования для систем, связанных с безопасностью. SIEM обеспечивает безопасность КВОИКИ, и её недоступность создает риски для защищаемых систем. 2. Соответствие Tier-2 и ГТС — обязательное условие для аттестации инфраструктуры в рамках законодательства РК. 3. Требования согласуются с международными и национальными стандартами информационной безопасности.

3	991140000634	Замечание к КД	Уважаемый заказчик! Вами опубликован тендер методом открытого конкурса на предоставление «Услуги по обеспечению информационной безопасности». Согласно пункта 2. Статьи 7-2 Закона Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК: «2. Оперативный центр информационной безопасности осуществляет свою деятельность на основании лицензии на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для оперативно-розыскных мероприятий». Так, согласно Приложения 1 к Закону Республики Казахстан «О разрешениях и уведомлениях» от 16 мая 2014 года № 202-V ЗРК «Лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий» относится к перечню разрешений первой категории. На основании вышеизложенного, руководствуясь пунктом 72 Правил осуществления государственных закупок (Приказ Министра финансов Республики Казахстан от 9 октября 2024 года № 687 ГЗ), требуем исключить установленные вами квалификационные требования согласно приложения 8 и установить требование о наличии разрешения первой категории (лицензии) на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий.	2025-03-28 11:41:40	Представить разъяснение положений конкурсной документации	ГУ "Аппарат акима города Караганды" в ответ на Ваше замечание к КД сообщает что наличие трудовых ресурсов обусловлено необходимостью интеграции с различными внутренними службами Заказчика и наличие соответствующих компетенций должно быть подтверждено сертификатами. Соответствующие компетенции у Заказчика отсутствуют, данные требования по наличию трудовых ресурсов должны обеспечить правильную настройку интеграционных модулей в критически важную инфраструктуру Заказчика. Любой активный инфраструктурный компонент или элемент канала распределения должен иметь возможность вывода из эксплуатации для планового обслуживания, никак не затрагивая ИТ-нагрузку. ЦОД должен соответствовать стандарту Tier-2 и соответствовать требованиям ГТС для успешного прохождения аттестации по информационной безопасности

Заявки на участие в данном конкурсе принимаются не позднее пяти рабочих дней с момента размещения данного протокола и текста утвержденной конкурсной документации на веб-портале государственных закупок

руководитель ГУ «Отдел государственных активов и закупок города Караганды» Калиакпаров Бауыржан Климович

Расшифровка аббревиатур:
БИН – бизнес-идентификационный номер;
ИИН – индивидуальный идентификационный номер;
ИНН – идентификационный номер налогоплательщика;
УНП – учетный номер плательщика;
Ф.И.О. – фамилия имя отчество (при его наличии).