Конкурстық құжаттама жобасын алдын ала талқылау хаттамасы
№15602045

Конкурстың № 15198498-1
Конкурстың атауы Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Конкурстық құжаттама жобасына ескертулерді, сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салуларды қабылдау мерзімі бастап 2025-08-08 09:08:15 дейін 2025-08-12 09:08:15
Ұйымдастырушының атауы "Қарағанды облысының қаржы және мемлекеттік активтер басқармасы" 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 тұрпаты (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	221040017755	ҚҚ жобасына ескерту	П. 8.5.1 и 8.5.2 закрепляют, что все компоненты должны быть частью единой системы, управляться через единый веб-интерфейс и развёртываться с единого образа ПО с активацией лицензией без установки дополнительного ПО. Это исключает международно признанные SIEM-системы с модульной архитектурой (Elastic, IBM QRadar, Splunk без указанных модулей и др.), которые широко применяются в госсекторе и полностью соответствуют требованиям ИБ. Предлагаем: Исключить требование обязательного развёртывания всех модулей с единого образа ПО, допустив модульную архитектуру при условии интеграции и хранения данных в соответствии с законодательством РК.	2025-08-11 15:46:27	Представить разъяснение положений конкурсной документации	Данные требования обусловлены необходимостью минимизации точек уязвимости, обеспечения централизованного управления компонентами и гарантии их совместимости. Это является ключевым условием для поддержания целостности, безопасности и управляемости информационных систем государственного уровня в соответствии с параграфом 8 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (редакция 2024–2025 гг.), где регламентируется необходимость интеграции компонентов в единую сертифицированную платформу с централизованным управлением и контролем: https://adilet.zan.kz/rus/docs/P1600000832 При этом допускается применение модульной архитектуры с условием, что все модули полностью интегрированы в единую платформу, исключается необходимость ручной доустановки дополнительного программного обеспечения, а управление всеми компонентами осуществляется через единый веб-интерфейс. Такое требование обеспечивает соответствие системы нормам информационной безопасности и свидетельствует о наличии централизованного контроля, что предотвращает появление несанкционированных изменений, повышает уровень защищённости и совместимости системы. Закон Республики Казахстан «О государственных закупках» от 1 июля 2024 года № 106-VIII (вступает в силу с 1 января 2025 года) позволяет заказчику устанавливать технические требования с целью обеспечения безопасности и соответствия нормативным актам, при этом требования должны быть объективными, функциональными и не создавать необоснованных преимуществ отдельных производителей. https://adilet.zan.kz/rus/docs/Z2400000106 Исключение требования о развёртывании всех модулей с единого образа программного обеспечения без возможности модульной архитектуры может привести к снижению уровня контроля безопасности и управления системой, что противоречит задачам информационной безопасности государственных информационных систем.

2	221040017755	ҚҚ жобасына ескерту	П. 8.4.13 предусматривает, что функции сканирования уязвимостей (запуск сканирования, настройка сценариев, изменение глубины сканирования) должны выполняться исключительно через единый интерфейс SIEM-системы. Это исключает использование SIEM-систем, которые интегрируются с внешними сканерами уязвимостей (Tenable Nessus, Qualys, MaxPatrol и др.), что является мировой практикой и не снижает уровень безопасности. Данное требование искусственно сужает круг участников и создаёт преимущества решениям, в которых сканер встроен непосредственно в SIEM (например, Splunk с определёнными модулями). Предлагаем: Допустить использование SIEM-систем, взаимодействующих с внешними сканерами уязвимостей, при условии обеспечения интеграции и передачи данных в единый интерфейс для анализа.	2025-08-11 15:45:18	Представить разъяснение положений конкурсной документации	Требование централизованного управления функциями сканирования уязвимостей направлено на обеспечение целостности, безопасности и управляемости системы безопасности, что исключает риски фрагментации данных, несанкционированного доступа и появления дополнительных уязвимостей. В соответствии с Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (редакция 2024–2025 гг.), в параграфе 8 (начиная с пункта 141) установлены требования по централизованному управлению средствами защиты, включая интеграцию внешних компонентов при условии управления ими через единый интерфейс SIEM: https://adilet.zan.kz/rus/docs/P1600000832 Также, согласно Закону Республики Казахстан «О государственных закупках» от 1 июля 2024 года № 106-VIII, вступающему в силу с 1 января 2025 года, заказчик вправе устанавливать технические требования, направленные на обеспечение безопасности закупок, при условии, что такие требования являются объективными, функциональными и не создают необоснованных преимуществ для отдельных поставщиков: https://adilet.zan.kz/rus/docs/Z2400000106 Использование SIEM-систем с интеграцией внешних сканеров уязвимостей (например, Tenable Nessus, Qualys, MaxPatrol и др.) допускается при условии, что весь функционал управления сканированием — запуск, настройка сценариев, изменение параметров — осуществляется через единый интерфейс SIEM-платформы. Это соответствует принципам обеспечения безопасности и управления системой в целом.

Камералдық бақылау хабарлама (лар) беру негізінде келесі лоттарға конкурстық құжаттарды өзгерту туралы шешім қабылданды:

Лот нөмірі	**Лот сомасы**	**Хабарлама №**	**Хабарламаны жеткізу күні**
74083816-ОК5	26371428.57	346797	2025-08-08 17:50:38

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

Заместитель руководителя	Рустембекова Айслу Болатовна

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 №15602045

№ конкурса 15198498-1
Название конкурса Услуги по обеспечению информационной безопасности
Срок приема замечаний к проекту конкурсной документации, а также запросов о разъяснении положений конкурсной документации с 2025-08-08 09:08:15 по 2025-08-12 09:08:15
Наименование организатора ГУ "Управление финансов и государственных активов Карагандинской области"

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	221040017755	Замечание к КД	П. 8.5.1 и 8.5.2 закрепляют, что все компоненты должны быть частью единой системы, управляться через единый веб-интерфейс и развёртываться с единого образа ПО с активацией лицензией без установки дополнительного ПО. Это исключает международно признанные SIEM-системы с модульной архитектурой (Elastic, IBM QRadar, Splunk без указанных модулей и др.), которые широко применяются в госсекторе и полностью соответствуют требованиям ИБ. Предлагаем: Исключить требование обязательного развёртывания всех модулей с единого образа ПО, допустив модульную архитектуру при условии интеграции и хранения данных в соответствии с законодательством РК.	2025-08-11 15:46:27	Представить разъяснение положений конкурсной документации	Данные требования обусловлены необходимостью минимизации точек уязвимости, обеспечения централизованного управления компонентами и гарантии их совместимости. Это является ключевым условием для поддержания целостности, безопасности и управляемости информационных систем государственного уровня в соответствии с параграфом 8 Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (редакция 2024–2025 гг.), где регламентируется необходимость интеграции компонентов в единую сертифицированную платформу с централизованным управлением и контролем: https://adilet.zan.kz/rus/docs/P1600000832 При этом допускается применение модульной архитектуры с условием, что все модули полностью интегрированы в единую платформу, исключается необходимость ручной доустановки дополнительного программного обеспечения, а управление всеми компонентами осуществляется через единый веб-интерфейс. Такое требование обеспечивает соответствие системы нормам информационной безопасности и свидетельствует о наличии централизованного контроля, что предотвращает появление несанкционированных изменений, повышает уровень защищённости и совместимости системы. Закон Республики Казахстан «О государственных закупках» от 1 июля 2024 года № 106-VIII (вступает в силу с 1 января 2025 года) позволяет заказчику устанавливать технические требования с целью обеспечения безопасности и соответствия нормативным актам, при этом требования должны быть объективными, функциональными и не создавать необоснованных преимуществ отдельных производителей. https://adilet.zan.kz/rus/docs/Z2400000106 Исключение требования о развёртывании всех модулей с единого образа программного обеспечения без возможности модульной архитектуры может привести к снижению уровня контроля безопасности и управления системой, что противоречит задачам информационной безопасности государственных информационных систем.

2	221040017755	Замечание к КД	П. 8.4.13 предусматривает, что функции сканирования уязвимостей (запуск сканирования, настройка сценариев, изменение глубины сканирования) должны выполняться исключительно через единый интерфейс SIEM-системы. Это исключает использование SIEM-систем, которые интегрируются с внешними сканерами уязвимостей (Tenable Nessus, Qualys, MaxPatrol и др.), что является мировой практикой и не снижает уровень безопасности. Данное требование искусственно сужает круг участников и создаёт преимущества решениям, в которых сканер встроен непосредственно в SIEM (например, Splunk с определёнными модулями). Предлагаем: Допустить использование SIEM-систем, взаимодействующих с внешними сканерами уязвимостей, при условии обеспечения интеграции и передачи данных в единый интерфейс для анализа.	2025-08-11 15:45:18	Представить разъяснение положений конкурсной документации	Требование централизованного управления функциями сканирования уязвимостей направлено на обеспечение целостности, безопасности и управляемости системы безопасности, что исключает риски фрагментации данных, несанкционированного доступа и появления дополнительных уязвимостей. В соответствии с Постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (редакция 2024–2025 гг.), в параграфе 8 (начиная с пункта 141) установлены требования по централизованному управлению средствами защиты, включая интеграцию внешних компонентов при условии управления ими через единый интерфейс SIEM: https://adilet.zan.kz/rus/docs/P1600000832 Также, согласно Закону Республики Казахстан «О государственных закупках» от 1 июля 2024 года № 106-VIII, вступающему в силу с 1 января 2025 года, заказчик вправе устанавливать технические требования, направленные на обеспечение безопасности закупок, при условии, что такие требования являются объективными, функциональными и не создают необоснованных преимуществ для отдельных поставщиков: https://adilet.zan.kz/rus/docs/Z2400000106 Использование SIEM-систем с интеграцией внешних сканеров уязвимостей (например, Tenable Nessus, Qualys, MaxPatrol и др.) допускается при условии, что весь функционал управления сканированием — запуск, настройка сценариев, изменение параметров — осуществляется через единый интерфейс SIEM-платформы. Это соответствует принципам обеспечения безопасности и управления системой в целом.

Принято решение о внесении изменения в конкурсную документацию на основании отправленного (ых) уведомления (й) Камеральным контролем по лоту (ам):

№ лота	**Сумма лота**	**№ уведомления**	**Дата доставки уведомления**
74083816-ОК5	26371428.57	346797	2025-08-08 17:50:38

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

Заместитель руководителя	Рустембекова Айслу Болатовна

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).