Конкурстық құжаттама жобасын алдын ала талқылау хаттамасы
№18695921

Конкурстың № 17721006-1
Конкурстың атауы Ақпараттық қауіпсіздік аудиті бойынша қызметтерді (440)
Конкурстық құжаттама жобасына ескертулерді, сондай-ақ конкурстық құжаттама ережелерін түсіндіру туралы сұрау салуларды қабылдау мерзімі бастап 2026-10-02 17:15:09 дейін 2026-10-06 17:15:09
Ұйымдастырушының атауы "Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті" коммерциялық емес акционерлік қоғамы

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	161240004496	ҚҚ ережелерін түсіндіру туралы сұрау салу	Вопрос по пункту 6 технической спецификации: В пункте 6 предусмотрено: «Анализ функционала обнаруженных объектов (реверс-инжиниринг) — для определения степени опасности объекта и возможного наличия дополнительных вредоносных объектов». Просим уточнить, что именно Заказчик понимает под «обнаруженными объектами» и «реверс-инжинирингом» в рамках настоящего аудита. В частности, просим уточнить: - какие объекты предполагается подвергать анализу (вредоносное программное обеспечение, исполняемые файлы, скрипты, приложения, библиотеки и иные объекты); - предусматривается ли проведение статического и/или динамического анализа программного кода; - предполагается ли исследование исходного кода либо анализ только скомпилированных/исполняемых файлов; - в каком объеме и при каких условиях указанные	2026-10-06 16:41:48	Представить разъяснение положений конкурсной документации	1) По пункту 6 «Анализ функционала обнаруженных объектов (реверс-инжиниринг)» сообщаем, что под обнаруженными объектами понимаются выявленные в ходе проведения аудита подозрительные и потенциально вредоносные объекты информационной инфраструктуры, включая исполняемые файлы, скрипты, библиотеки, программные компоненты и иные объекты, имеющие признаки компрометации. Анализ проводится в объеме, необходимом для определения степени опасности объекта, выявления возможных вредоносных функций и дополнительных связанных объектов. При необходимости применяется статический и/или динамический анализ. 2) По пункту 7: Форенсика проводится в отношении серверов и рабочих станций, на которых в ходе аудита выявлены признаки подозрительной активности или компрометации. Включает анализ цифровых артефактов, при необходимости создание

			работы должны выполняться. Вопрос по пункту 7 технической спецификации: В пункте 7 предусмотрено: «Компьютерная криминалистика (форенсика) серверов и рабочих станций, имеющих признаки подозрительного поведения, выявленных в ходе аудита». Просим уточнить объем и порядок выполнения указанных работ. В частности, просим уточнить: - что именно понимается под «компьютерной криминалистикой (форенсикой)» в рамках настоящего аудита; - предусматривается ли проведение полного криминалистического исследования серверов и рабочих станций либо только анализ журналов событий, файлов, процессов, сетевой активности и иных артефактов информационной безопасности; - предусматривается ли изъятие и создание криминалистических копий (образов) дисков и иных носителей информации; - требуется ли			криминалистических образов, восстановление хронологии инцидента, определение способа проникновения и действий нарушителя. Количество объектов определяется по результатам аудита.
			восстановление хронологии событий, установление способа проникновения, источника компрометации и действий нарушителя; - каким образом определяется количество серверов и рабочих станций, подлежащих форенсике, поскольку в технической спецификации их количество не указано. Просим предоставить соответствующие разъяснения для однозначного определения состава, объема и трудоемкости работ, предусмотренных пунктами 6 и 7 технической спецификации.			

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

И.о. Председателя Правления-Ректора Умуркулова Мадина Максимовна

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
№18695921

№ конкурса 17721006-1
Название конкурса Услуги по аудиту информационной безопасности (440)
Срок приема замечаний к проекту конкурсной документации, а также запросов о разъяснении положений конкурсной документации с 2026-10-02 17:15:09 по 2026-10-06 17:15:09
Наименование организатора Некоммерческое акционерное общество "Карагандинский национальный исследовательский университет имени академика Е.А.Букетова"

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	161240004496	Запрос о разъяснении КД	Вопрос по пункту 6 технической спецификации: В пункте 6 предусмотрено: «Анализ функционала обнаруженных объектов (реверс-инжиниринг) — для определения степени опасности объекта и возможного наличия дополнительных вредоносных объектов». Просим уточнить, что именно Заказчик понимает под «обнаруженными объектами» и «реверс-инжинирингом» в рамках настоящего аудита. В частности, просим уточнить: - какие объекты предполагается подвергать анализу (вредоносное программное обеспечение, исполняемые файлы, скрипты, приложения, библиотеки и иные объекты); - предусматривается ли проведение статического и/или динамического анализа программного кода; - предполагается ли исследование исходного кода либо анализ только скомпилированных/исполняемых файлов; - в каком объеме и при каких условиях указанные	2026-10-06 16:41:48	Представить разъяснение положений конкурсной документации	1) По пункту 6 «Анализ функционала обнаруженных объектов (реверс-инжиниринг)» сообщаем, что под обнаруженными объектами понимаются выявленные в ходе проведения аудита подозрительные и потенциально вредоносные объекты информационной инфраструктуры, включая исполняемые файлы, скрипты, библиотеки, программные компоненты и иные объекты, имеющие признаки компрометации. Анализ проводится в объеме, необходимом для определения степени опасности объекта, выявления возможных вредоносных функций и дополнительных связанных объектов. При необходимости применяется статический и/или динамический анализ. 2) По пункту 7: Форенсика проводится в отношении серверов и рабочих станций, на которых в ходе аудита выявлены признаки подозрительной активности или компрометации. Включает анализ цифровых артефактов, при необходимости создание

			работы должны выполняться. Вопрос по пункту 7 технической спецификации: В пункте 7 предусмотрено: «Компьютерная криминалистика (форенсика) серверов и рабочих станций, имеющих признаки подозрительного поведения, выявленных в ходе аудита». Просим уточнить объем и порядок выполнения указанных работ. В частности, просим уточнить: - что именно понимается под «компьютерной криминалистикой (форенсикой)» в рамках настоящего аудита; - предусматривается ли проведение полного криминалистического исследования серверов и рабочих станций либо только анализ журналов событий, файлов, процессов, сетевой активности и иных артефактов информационной безопасности; - предусматривается ли изъятие и создание криминалистических копий (образов) дисков и иных носителей информации; - требуется ли			криминалистических образов, восстановление хронологии инцидента, определение способа проникновения и действий нарушителя. Количество объектов определяется по результатам аудита.
			восстановление хронологии событий, установление способа проникновения, источника компрометации и действий нарушителя; - каким образом определяется количество серверов и рабочих станций, подлежащих форенсике, поскольку в технической спецификации их количество не указано. Просим предоставить соответствующие разъяснения для однозначного определения состава, объема и трудоемкости работ, предусмотренных пунктами 6 и 7 технической спецификации.			

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

И.о. Председателя Правления-Ректора Умуркулова Мадина Максимовна

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).