Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті" коммерциялық емес акционерлік қоғамы
Ұйымдастырушының атауы:	"Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті" коммерциялық емес акционерлік қоғамы
Конкурстың №:	№ 17721006-1
Конкурстың атауы:	Ақпараттық қауіпсіздік аудиті бойынша қызметтерді (440)
Лоттың нөмірі:	№ 81645047-ОК1
Лоттың атауы	Ақпараттық технологиялар тексеруін жүргізу бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	749020.000.000072
Қызметтің атауы:	Ақпараттық технологиялар тексеруін жүргізу бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	11607140
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	11607140
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	Шарт жасалған сәттен бастап 01.12.2026 жылға дейін
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық ерекшелік 1. Жұмыстардың мақсаттары «Академик Е. А. Бөкетов атындағы Қарағанды университеті» КЕАҚ ақпараттық қауіпсіздік саласындағы проблемаларды анықтау және жою. 2. Жұмыстардың кезеңдері 1. Ақпараттық қауіпсіздікті алдын ала бағалау және ақпараттық қауіпсіздікті бағалау бойынша қысқаша есеп қалыптастыру. 2. Автоматты сканерлеу және енуге тестілеу (ішкі және сыртқы) рәсімдерін жүргізу. 3. Ақпараттық қауіпсіздіктің бұзылу тәуекелдерін бағалауды жүргізу. 4. Компанияның ақпараттық қауіпсіздігіне кешенді аудит жүргізу, оның ішінде ақпараттық қауіпсіздік саласындағы құжаттаманың аудиті (ақпараттық қауіпсіздік аудиті бойынша егжей-тегжейлі есеп, Компанияның ақпараттық қауіпсіздік деңгейін арттыруға/сақтауға арналған ұсынымдар, оның ішінде техникалық құралдар мен ұйымдастырушылық іс-шаралар, сондай-ақ IT бөлімінен басқа Компанияның өзге қызметтерімен өзара іс-қимыл регламенттері). 5. Желілік инфрақұрылымның оқшаулану деңгейін бағалау. 6. Анықталған объектілердің функционалын талдау (реверс-инжиниринг) — объектінің қауіптілік дәрежесін және қосымша зиянды объектілердің болуы мүмкіндігін анықтау мақсатында. 7. Аудит барысында күдікті мінез-құлық белгілері анықталған серверлер мен жұмыс станцияларының компьютерлік криминалистикасын (форензикасын) жүргізу. 3. Ақпараттық қауіпсіздікке қатысты IT-инфрақұрылым аудиті Аппараттық-бағдарламалық бөліктің санын, бастапқы код көлемін, желілер мен ішкі желілердің санын көрсете отырып, сауалнаманы толтыру арқылы ақпараттық инфрақұрылым объектілері мен элементтеріне тексеру жүргізіледі. Сонымен қатар ақпараттық инфрақұрылым объектілерінің (бұдан әрі — АИО) деңгейлері (қолданбалы бағдарламалық қамтамасыз ету, дерекқор, операциялық жүйе, виртуализация ортасы), сондай-ақ ақпаратты қорғау құралдары мен істен шығуға төзімділік жүйелерінің болуы зерделенеді. 1. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың, виртуализация ортасының және серверлік жабдықтың операциялық жүйесінің функционалы қауіпсіздігін талдау, ақпараттық қауіпсіздік талаптарына сәйкессіздіктерді анықтау (Орындаушының сәйкессіздіктерді жою жөніндегі ұсынымдарды беруі, АИО әзірлеушілерінің ескертулерді жоюын бақылау). Жұмыстардың осы түрі ақпараттық қауіпсіздік функцияларын (бұдан әрі — АҚФ) сынау шеңберінде жүзеге асырылады. 2. Ақпараттық қауіпсіздік мониторингі жүйесінің (бұдан әрі — SIEM) баптауларын тексеру (бар болған жағдайда). SIEM болмаған жағдайда желілік инфрақұрылым деңгейіндегі қорғалу деңгейін тексеру, желілік жабдықтың (желілік экранның) баптауларын ақпараттық қауіпсіздік талаптарына сәйкестігі тұрғысынан тексеру. Бұл жұмыстар желілік инфрақұрылымды қорғау функцияларының техникалық құжаттаманың талаптарына, Қазақстан Республикасының нормативтік құқықтық актілеріне және Қазақстан Республикасының аумағында қолданыстағы ақпараттық қауіпсіздік саласындағы стандарттарға сәйкестігін тексеруді, бағдарламалық қамтамасыз етуде осалдықтардың бар-жоғын сканерлеуді, қажет болған жағдайда бағдарламалық құралдарды пайдалана отырып,

	Тапсырыс берушінің желілік инфрақұрылымын зерттеуді, сондай-ақ анықталған сәйкессіздіктерді жою жөніндегі ұсынымдарды беруді қамтиды. Жұмыстардың осы түрі ақпараттық қауіпсіздік объектілерін сынау шеңберінде жүзеге асырылады. 3. Негізгі және резервтік (егер АИО 1 және 2-сыныпқа жататын болса) серверлік үй-жай периметрінің физикалық қорғалуын тексеру (Орындаушының Тапсырыс берушінің деректерді өңдеу орталығына баруы, бақылау нәтижелері бойынша сәйкессіздіктерді жою жөніндегі ұсынымдарды беру). 4. Қорытынды есеп және ұсынымдар Осы техникалық ерекшелікте көзделген барлық жұмыстар аяқталғаннан кейін Орындаушы міндетті түрде жүргізілген ақпараттық қауіпсіздік аудитінің нәтижелері бойынша Тапсырыс берушіге толық қорытынды есеп ұсынады. Қорытынды есеп мыналарды қамтуы тиіс: 1. жүргізілген іс-шаралар мен зерттелген объектілердің толық тізбесі; 2. анықталған осалдықтар, бұзушылықтар, сәйкессіздіктер және ақпараттық қауіпсіздік тәуекелдері; 3. анықталған әрбір проблеманың сипаттамасы; 4. анықталған бұзушылықтардың маңыздылық деңгейін және ықтимал салдарын бағалау; 5. жүргізілген сканерлеу, енуге тестілеу және өзге де техникалық тексерулердің нәтижелері; 6. ұйымдастырушылық және техникалық қорғау шараларын талдау нәтижелері; 7. нормативтік және ұйымдастырушылық құжаттамада анықталған кемшіліктер; 8. анықталған әрбір бұзушылық пен осалдықты жою бойынша нақты ұсынымдар мен техникалық шаралар; 9. анықталған бұзушылықтардың қайталама туындауының алдын алу жөніндегі ұсынымдар; 10. олардың маңыздылық деңгейін ескере отырып, анықталған кемшіліктерді жою басымдығы; 11. тәуекел деңгейі бойынша сыни, жоғары, орташа және төмен санаттарға жататын бұзушылықтарды жоюдың ұсынылатын мерзімдері. Толық қорытынды есепті және анықталған барлық бұзушылықтарды жою жөніндегі ұсынымдарды ұсыну аудит бойынша жұмыстарды аяқтаудың міндетті шарты болып табылады. Қорытынды есеп, аудит нәтижелері, анықталған осалдықтар, ақпараттық жүйелер, желілік инфрақұрылым және ақпаратты қорғау құралдары туралы мәліметтер Тапсырыс берушінің құпия ақпараты болып табылады. Орындаушы аудит жүргізу барысында алынған ақпараттың құпиялылығын қамтамасыз етуге және Тапсырыс берушінің алдын ала жазбаша келісімінсіз оны жария етуге, беруге немесе үшінші тұлғаларға ұсынуға жол бермеуге міндетті, Қазақстан Республикасының заңнамасында көзделген жағдайларды қоспағанда. Қорытынды есеп құжат түрінде ресімделіп, Тапсырыс берушіге ресми түрде электрондық форматта, кейіннен сақтау және ресми құжат ретінде пайдалану мүмкіндігімен, сондай-ақ Тапсырыс берушінің талабы бойынша қағаз жеткізгіште беріледі. Есепке Орындаушының уәкілетті өкілі қол қоюы және онда аудит жүргізілген күні, жұмыстарды жүргізу кезеңі, зерттелген объектілердің тізбесі, сондай-ақ қорытынды тұжырымдар мен ұсынымдар көрсетілуі тиіс.

Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Некоммерческое акционерное общество "Карагандинский национальный исследовательский университет имени академика Е.А.Букетова"
Наименование организатора	Некоммерческое акционерное общество "Карагандинский национальный исследовательский университет имени академика Е.А.Букетова"
№ конкурса:	№ 17721006-1
Наименование конкурса:	Услуги по аудиту информационной безопасности (440)
Номер лота:	№ 81645047-ОК1
Наименование лота:	Услуги по проведению аудита информационных технологий
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	749020.000.000072
Наименование услуги:	Услуги по проведению аудита информационных технологий
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	11607140
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	11607140
Срок оказания услуги:	с момента заключения Договора по 01.12.2026 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация 1. Цели работ Выявление и устранение проблем в области информационной безопасности НАО «Карагандинский университет имени академика Е. А. Букетова». 2. Этапы работ 1. Предварительная оценка информационной безопасности с формированием краткого отчета об оценке информационной безопасности. 2. Проведение процедуры автоматического сканирования и тестирования на проникновение (внутреннее и внешнее). 3. Проведение оценки рисков нарушения информационной безопасности. 4. Комплексный аудит ИБ Компании, включая аудит документации в области ИБ (детальный отчет об аудите ИБ, рекомендации по повышению/поддержанию уровня ИБ Компании, включая технические средства и организационные мероприятия, а также регламенты взаимодействия с другими службами Компании, помимо IT). 5. Оценка изолированности сетевой инфраструктуры. 6. Анализ функционала обнаруженных объектов (реверс-инжиниринг) - для определения степени опасности объекта и возможного наличия дополнительных вредоносных объектов. 7. Компьютерная криминалистика (форенсика) серверов и рабочих станций, имеющих признаки подозрительного поведения, выявленных в ходе аудита 3. Аудит ИТ инфраструктуры информационной безопасности Проводится обследования ОИ и элементов информационной инфраструктуры путём заполнения опросника с указанием количества аппаратно-программной части, объема исходного кода, количество сетей и подсетей, изучение уровней ОИ (прикладного программного обеспечения, базы данных, операционной системы, среды виртуализации), а также наличие средств защиты информации и систем отказоустойчивости. 1. Анализ безопасности функционала прикладного программного обеспечения, базы данных, среды виртуализации и операционной системы серверного оборудования, выявление несоответствий требованиям по ИБ (выдача исполнителем рекомендаций по устранению несоответствий, контроль за устранением замечаний Разработчиками ОИ), данный вид работ в рамках испытаний функций информационной безопасности (далее - ФИБ); 3. Проверка настроек системы мониторинга ИБ (далее - SIEM) (при наличии), в случае отсутствия SIEM. Проверка защищенности на уровне сетевой инфраструктуры, проверка настроек сетевого оборудования (межсетевого экрана) в соответствии с требованиями по ИБ которое включает в себя проверку соответствия функций защиты сетевой инфраструктуры требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информационной безопасности, сканирование на наличие уязвимостей программного обеспечения, обследование сетевой инфраструктуры заявителя, в том числе с применением программных средств при необходимости, с выдачей рекомендаций по устранению, данный вид работ выполняется в рамках испытания ОСИ; 4. Проверка физической защиты периметра основного и резервного (в случае если ОИ 1 и 2 класса) серверного помещения (выезд исполнителя в Центр обработки данных Заказчика, по результатам наблюдений выдача рекомендаций по

	устранению несоответствий). 4. Итоговый отчет и рекомендации По окончании выполнения всех предусмотренных настоящей технической спецификацией работ Исполнитель в обязательном порядке предоставляет Заказчику полный итоговый отчет по результатам проведенного аудита информационной безопасности. Итоговый отчет должен содержать: 1. полный перечень проведенных мероприятий и обследованных объектов; 2. выявленные уязвимости, нарушения, несоответствия и риски информационной безопасности; 3. описание каждой выявленной проблемы; 4. оценку уровня критичности и потенциальных последствий выявленных нарушений; 5. результаты проведенного сканирования, тестирования на проникновение и иных технических проверок; 6. результаты анализа организационных и технических мер защиты; 7. выявленные недостатки в нормативной и организационной документации; 8. конкретные рекомендации и технические меры по устранению каждого выявленного нарушения и уязвимости; 9. рекомендации по предотвращению повторного возникновения выявленных нарушений; 10. приоритетность устранения выявленных недостатков с учетом уровня их критичности; 11. рекомендуемые сроки устранения критичных, высоких, средних и низких по уровню риска нарушений. Предоставление полного итогового отчета и рекомендаций по устранению всех выявленных нарушений является обязательным условием завершения работ по аудиту. Итоговый отчет, результаты аудита, выявленные уязвимости, сведения об информационных системах, сетевой инфраструктуре и средствах защиты информации являются конфиденциальной информацией Заказчика. Исполнитель обязан обеспечить конфиденциальность полученной в ходе проведения аудита информации и не допускать ее разглашения, передачи или предоставления третьим лицам без предварительного письменного согласия Заказчика, за исключением случаев, предусмотренных законодательством Республики Казахстан. Итоговый отчет оформляется в документальном виде и передается Заказчику официально, в электронном формате с возможностью последующего хранения и использования в качестве официального документа, а также на бумажном носителе — по требованию Заказчика. Отчет должен быть подписан уполномоченным представителем Исполнителя и содержать дату проведения аудита, период проведения работ, перечень обследованных объектов и итоговые выводы и рекомендации.

Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	