ТЕХНИКАЛЫҚ СИПАТТАМА

1266701 , «Бағдарламалардың әрекетін автономды талдау және зиянды бағдарламаны анықтау жүйесі функционалдылық (SCADA/EMS үшін "Anti-APT" бағдарламалық-аппараттық кешені)» сатып алу бойынша Ашық тендер тәсілімен

Лот № 1 (9135-3 Т, 4569469) Бағдарламалық-аппараттық кешен

Тапсырыс беруші: "Электр желілерін басқару жөніндегі Қазақстан компаниясы" (Kazakhstan Electricity Grid Operating Company)"KEGOC" акционерлік қоғамы

Ұйымдастырушы: "Электр желілерін басқару жөніндегі Қазақстан компаниясы" (Kazakhstan Electricity Grid Operating Company)"KEGOC" акционерлік қоғамы

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	9135-3 Т
Атауы және қысқаша сипаттамасы	Бағдарламалық-аппараттық кешен, желілік инфрақұрылымның қауіпсіздігі және қауіпсіздік оқиғалары, оқиғаларды талдау процесін автоматтандыру туралы ақпаратты басқару үшін
ТЖҚЖС санаттың атауы	Бағдарламалық қамтамасыз ету лицензиялары
Қосымша сипаттама	Аталуы: Система автономного анализа поведения программ и идентификации вредоносной функциональности (Программно-аппаратный комплекс "Anti-APT" для SCADA/EMS)
Саны	2.000
Өлшем бірлігі	Дана
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., проспект Тәуелсіздік, 59
Жеткізу шарттары	DDP
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап (қоса алғанда) 12.2026 дейін.
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

1. Сатып алудың мәні мен негізі

Тапсырыс берушінің инфрақұрылымында tlab Anti-APT (бұдан әрі — орнатылған БҚ) лицензиялық бағдарламалық қамтамасыз ету орнатылған және пайдаланылуда. Осы сатып алу "қорғалған пошта шлюзі" (Email Security Gateway, бұдан әрі — жүйе) класындағы электрондық поштаны қорғаудың функционалдық модулі бойынша белгіленген қосымша жинақтау үшін жүзеге асырылады.

1.2. Жалпы талаптар

Бағдарламалық қамтамасыз етуді жеткізу кезінде өнім берушіде Қазақстан Республикасының Ұлттық аккредиттеу жүйесінде аккредиттелген сәйкестікті

растау жөніндегі орган берген, жеткізуге ұсынылатын нұсқаға қолданылатын, сенімнің бағалау деңгейі 4 (төртінші) төмен емес қолданыстағы сәйкестік сертификаты болуға тиіс.

1.3. Жеткізушіге қойылатын талаптар.

1.3.1. Жүйені техникалық қолдау-Қабылдау-тапсыру актісіне қол қойылған күннен бастап 12 (он екі) ай: өтініштерді орыс және қазақ тілдерінде қабылдау, келесі жұмыс күнінен кешіктірмей ден қою, аптасына 5 (бес) күн тәулігіне 8 (сегіз) сағат режимінде кеңес беру, дүйсенбіден жұмаға дейін жаңартуларды қосымша төлемсіз ұсыну. шығарылған күнінен бастап 10 (он) жұмыс күнінен аспайтын мерзім.

1.3.2. Жеткізуші жеткізілім кезінде Тапсырыс берушіге өндірушінің лицензиялық келісімін ұсынады.

1.3.3. Тапсырыс берушінің мамандарын енгізу, баптау және оқыту жөніндегі жұмыстарды "сарапшы"деңгейіндегі бағдарламалық қамтамасыз етуді өндірушінің қолданыстағы сертификаты бар маман орындайды. Сертификаттардың көшірмелері жұмыс басталғанға дейін шартты орындау кезеңінде ұсынылады.

2. Функционалдық талаптар

2.1. Кіріс және шығыс пошта трафигі үшін SMTP қауіпсіздік шлюзі режимінде жұмыс істеу: кемінде 100 Домен, кемінде 4000 пошта жәшігі.

2.2. Тапсырыс берушінің пошта серверлерімен (Microsoft Exchange, Postfix немесе баламалы SMTP-үйлесімді) және бұлтты пошта қызметтерімен (Microsoft 365 немесе баламалы) интеграциялау.

2.3. Көп деңгейлі сүзу: спамға қарсы талдау, антивирустық тексеру, жіберушілердің, домендердің, IP мекенжайларының және URL мекенжайларының беделін талдау, мазмұнды сүзу. Беделдің сыртқы көздерінің тізбесін Тапсырыс беруші айқындайды; олар болмаған кезде — беделдің ішкі базасында жұмыс істеу.

2.4. Фишингтік хаттарды анықтау және бұғаттау, жіберушіні ауыстыру, гомоглифтік домендер және файл атауының екі немесе одан да көп кеңейтімдері бар тіркемелер.

2.5. Тіркемелерді бейтараптандыру (CDR): макростарды, сценарийлерді, орындалатын кодты және енгізілген нысандарды құжаттың қолдануға

жарамды нұсқасын құрумен жою. Пішімдер: doc, docx, xls, xlsx, docm, xlsm, ppt, pptx, pptm, pdf. Көлемі 5 (бес) МБ аспайтын салымды өңдеу уақыты — 1 (бір) секундтан аспайды.

2.6. Алушыға хабарлау арқылы Карантин. Әкімшінің қатысуынсыз: себебін көрсете отырып, карантинге орналастырылған хабарламаларды қарауды; әкімшіге дербес шығаруды не шығаруға сұрау салуды; рұқсат етілген және тыйым салынған жөнелтушілердің дербес тізімдерін; реттелетін кезеңділікпен карантин бойынша мерзімді қорытындыны; өз хабарламалары бойынша іздеуді қамтамасыз ететін түпкілікті пайдаланушының өзіне-өзі қызмет көрсету порталының болуы міндетті. Кіру-корпоративтік каталогтың есептік жазбасы бойынша.

2.7. Реттелетін шаблондар мен кілт сөздер бойынша шығыс пошта трафигін (DLP) бақылау; DKIM, SPF, DMARC, ARC механизмдері бойынша Шығыс поштаға қол қою және тексеру.

2.8. Https (соның ішінде Telegram немесе баламалы) хаттамасы бойынша кіру кілті бойынша авторизациясы және хабарламаларды жіберуі бар бағдарламалық агенттер (боттар) үшін құжатталған бағдарламалық интерфейсті ұсынатын мессенджерге хабарландырудың штаттық бағдарламалық модулі. Конфигурация бағдарламалық кодты жазбай басқару консолі арқылы жүзеге асырылады.

2.9. Ақаулыққа төзімділік: жүктемені бөлу (Active-Active) немесе ыстық резерв (Active-Standby) режиміндегі кемінде екі түйіннен тұратын кластер, виртуалды IP-адрес, кіріктірілген пошта трафигін теңестіруші.

2.10. Есептілік және визуализация панельдері, есептерді PDF, CSV, HTML форматтарында экспорттау; оқиғаларды Siem класының сыртқы жүйесіне syslog арқылы CEF немесе LEEF форматтарында беру.

2.11. Аутентификация және қол жетімділікті шектеу: жергілікті тіркелгілер, LDAP (Active Directory немесе баламасы) LDAPS, бірыңғай кіру (SSO), екі факторлы аутентификация, рөлдік модель, әкімші әрекеттерін тексеру журналы.

2.12. Тапсырыс берушінің инфрақұрылымындағы деректерді өңдеуге: пошта хабарламаларын, салымдарды және оларды талдау нәтижелерін өндірушінің бұлтты сервистеріне және үшінші тұлғалардың желісіне беруге жол

берілмейді. Сыртқы көздерден бағдарламалық қамтамасыз етуді, антивирустық және спамға қарсы базаларды және беделді мәліметтерді алуға жол беріледі.

3. Орнатылған бағдарламалық жасақтамамен үйлесімділікке қойылатын талаптар

3.1. Сатып алынатын бағдарламалық қамтамасыз ету tlab Anti-APT бағдарламалық кешенінің электрондық поштасын қорғаудың функционалдық модулі болуы тиіс, оның әзірлеушісі және құқық иесі белгіленген БҚ-ның құқық иесі болып табылады және бірыңғай бағдарламалық платформаның құрамына орнатылған БҚ-мен енгізілуі тиіс.

3.2. Жүйенің белгіленген бағдарламалық жасақтамамен өзара әрекеттесуі штаттық құралдармен қамтамасыз етіледі және лицензияны орнатқаннан және іске қосқаннан кейін — әзірлеусіз, пысықтаусыз, бағдарламалаусыз және интеграциялық жұмыстарсыз жұмыс істей алады.

3.3. Жүйені басқару және орнатылған бағдарламалық жасақтамамен орындалған тіркемелерді талдау нәтижелерін қарау бірыңғай басқару консолінен жүзеге асырылады.

3.4. Тіркелгілердің, рөлдердің және қауіпсіздік саясатының бірыңғай базасы; жүйенің функциялары мен орнатылған бағдарламалық жасақтама арасында ауысу кезінде тіркелгі деректерін қайта енгізу қажет емес.

3.5. Пошта хабарламасының карточкасынан тиісті салым бойынша белгіленген БҚ-ның толық есебіне тікелей көшу қамтамасыз етіледі.

3.6. Орнатылған бағдарламалық жасақтаманың оны ауыстырусыз жұмыс істейтін нұсқасымен үйлесімділік; жаңартуларды бір авторлық құқық иесі келісілген циклде шығарады.

3.7. Орнатылған БҚ қолжетімсіз болған кезде жүйе объектілерді талдауға кезекке қоя отырып және қолжетімділік қалпына келтірілгеннен кейін автоматты түрде қайта жібере отырып, салымдарды сүзу және залалсыздандырудың қалған құралдарымен пошта трафигін өңдеуді жалғастырады.

3.8. Белгіленген БҚ-ның екі торабы (данасы) арасындағы талдауға объектілерді беру кезінде жүктемені теңгерімдеу жүйенің штаттық құралдарымен қамтамасыз етіледі және лицензияны орнатқаннан және іске қосқаннан кейін тікелей қол жетімді: теңшелетін алгоритмі бар

сұраныстарды бөлу, қол жетімсіз торапты автоматты түрде алып тастау және оны қалпына келтіргеннен кейін жұмысқа қайтару, ауысу кезінде объектілерді жоғалтпау. Жеке лицензия, сыртқы теңгерімші және пысықтау жұмыстары қажет емес.

4. Кешен құрамындағы серверлік жабдық

4.1. Әрбір кешеннің құрамына мынадай сипаттамалары бар серверлік жабдық кіреді: форма-фактор — 2U артық емес; процессор — кемінде 1 дана, кемінде 16 (Он алты) ядро, базалық тактілік жиілігі кемінде 2,9 ГГц; жедел жады көлемі — кемінде 48 ГБ; сыйымдылығы кемінде 2 ТБ HDD үлгісіндегі диск, жылдамдығы 7200 айн/мин кем емес, өткізу қабілеті 12 Гбит/с кем емес SAS интерфейсі, ыстық ауыстыру қолдауымен — 2 (екі) данадан кем емес; RAID-контроллер — аппараттық; қуаты 750 Вт — тан аспайтын қуат блогы-2 (екі) данадан кем емес. Жабдық 19 дюймдік тірекке орнатуға мүмкіндік беруі керек.

4.2. Кешен құрамындағы серверлік жабдық — жаңа, пайдалануда болмаған, Шығарылған жылы шарт жасалған күнге дейін кемінде 3 (үш) жыл бұрын. Бағдарламалық жасақтама жеткізу күні жаңартылған нұсқада жеткізіледі.

4.3. Бағдарламалық жасақтама серверлік жабдыққа алдын-ала орнатылған және іске қосылған; кешен пайдалануға дайын Тапсырыс берушіге беріледі.

4.4. Серверлік жабдыққа кепілдік-қабылдау — тапсыру актісіне қол қойылған күннен бастап кемінде 12 (он екі) ай; істен шыққан компоненттерді-жеткізуші 10 (он) жұмыс күнінен аспайтын мерзімде жөндейді не ауыстырады.

5. Лицензиялау және тіл

5.1. 2 (екі) кешен жеткізілуге жатады. Әрбір кешен құрамындағы Лицензия — кемінде 4000 (төрт мың) белсенді пошта жәшігіне мерзімсіз. Жалпы Қызмет көрсетілетін сыйымдылық-кемінде 4000 пошта жәшігі; екінші кешен сыйымдылықтың ұлғаюын емес, ақауларға төзімділікті қамтамасыз етеді. Екі кешен екі түйіннен тұратын ақауларға төзімді кластердің жұмысын қамтамасыз етеді; кластерлеуге, жоғары қолжетімділікке және жүктемені

теңестіруге жеке лицензия талап етілмейді. Лицензия қосымша модульдерді сатып алмай және үшінші тарап бағдарламалық жасақтамасын лицензиялау шығындарынсыз осы техникалық ерекшеліктің барлық талаптарын қамтиды.

5.2. Мемлекеттік (қазақ) тілді қолдау міндетті. Басқару интерфейсі, есептер, түпкі пайдаланушыларға хабарламалар және өзіне-өзі қызмет көрсету порталы жүйе құралдарымен тілді ауыстыра отырып, мемлекеттік (қазақ), орыс және ағылшын тілдерінде қолжетімді болуы тиіс. Мемлекеттік тілге Локализация интерфейстің барлық бөлімдерін, соның ішінде саясатты орнатуды, карантинді басқаруды, журналдар мен есептерді қамтиды. Пайдалану құжаттамасы-мемлекеттік және орыс тілдерінде.

Қол қойған	Жумабаева Алия Нурланкызы
Қол қойылған күні	03.11.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

**по закупке 1266701 , «Система автономного анализа поведения программ и идентификации вредоносной функциональности (Программно-аппаратный комплекс «Anti-APT» для SCADA/EMS)»
способом Открытый тендер**

Лот № 1 (9135-3 Т, 4569469) Комплекс программно-аппаратный

Заказчик: Акционерное общество "Казахстанская компания по управлению электрическими сетями" (Kazakhstan Electricity Grid Operating Company) "KEGOC"

Организатор: Акционерное общество "Казахстанская компания по управлению электрическими сетями" (Kazakhstan Electricity Grid Operating Company) "KEGOC"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	9135-3 Т
Наименование и краткая характеристика	Комплекс программно-аппаратный, для управления информацией о безопасности и событиях безопасности, автоматизации процесса анализа событий сетевой инфраструктуры
Наименование категории ОКТРУ	Лицензии для программного обеспечения
Дополнительная характеристика	Наименование: Система автономного анализа поведения программ и идентификации вредоносной функциональности (Программно-аппаратный комплекс "Anti-APT" для SCADA/EMS)
Количество	2.000
Единица измерения	Штука
Место поставки	КАЗАХСТАН, г.Астана, проспект Тәуелсіздік, 59
Условия поставки	DDP
Срок поставки	С даты подписания договора по (включительно) 12.2026
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

1. Предмет и основание закупки

В инфраструктуре Заказчика установлено и эксплуатируется лицензионное программное обеспечение tLab Anti-APT (далее — установленное ПО). Настоящая закупка осуществляется для доукомплектования, установленного ПО функциональным модулем защиты электронной почты класса «Защищённый почтовый шлюз» (Email Security Gateway, далее — Система).

1.2. Общие требования

Поставщик при поставке программного обеспечения должен иметь действующий сертификат соответствия указанному стандарту с оценочным уровнем доверия не ниже 4 (четвёртого), выданный органом по

подтверждению соответствия, аккредитованным в национальной системе аккредитации Республики Казахстан, распространяющийся на предлагаемую к поставке версию.

1.3. Требования к Поставщику.

1.3.1. Техническая поддержка Системы — 12 (двенадцать) месяцев с даты подписания акта приёма-передачи: приём обращений на русском и казахском языках, реагирование не позднее следующего рабочего дня, консультирование в режиме 8 (восемь) часов в сутки 5 (пять) дней в неделю, с понедельника по пятницу предоставление обновлений без дополнительной оплаты в срок не более 10 (десяти) рабочих дней с даты выпуска.

1.3.2. Поставщик при поставке предоставляет Заказчику лицензионное соглашение производителя.

1.3.3. Работы по внедрению, настройке и обучению специалистов Заказчика выполняются специалистом, имеющим действующий сертификат производителя программного обеспечения уровня «Эксперт». Копии сертификатов представляются на этапе исполнения договора до начала работ.

2. Функциональные требования

2.1. Работа в режиме SMTP-шлюза безопасности для входящего и исходящего почтового трафика: не менее 100 доменов, не менее 4000 почтовых ящиков.

2.2. Интеграция с почтовыми серверами Заказчика (Microsoft Exchange, Postfix или эквивалентные SMTP-совместимые) и с облачными почтовыми сервисами (Microsoft 365 или эквивалентные).

2.3. Многоуровневая фильтрация: антиспам-анализ, антивирусная проверка, репутационный анализ отправителей, доменов, IP-адресов и URL, контентная фильтрация. Перечень внешних источников репутации определяется Заказчиком; при их отсутствии — работа на внутренней базе репутации.

2.4. Обнаружение и блокирование фишинговых писем, подмены отправителя, гомоглифных доменов и вложений с двумя и более расширениями имени файла.

2.5. Обезвреживание вложений (CDR): удаление макросов, скриптов, исполняемого кода и внедрённых объектов с формированием пригодной для использования версии документа. Форматы: doc, docx, xls, xlsx, docm, xlsm, p

pt, pptx, pptm, pdf. Время обработки вложения размером не более 5 (пяти) МБ — не более 1 (одной) секунды.

2.6. Карантин с уведомлением получателя. Обязательно наличие портала самообслуживания конечного пользователя, обеспечивающего без участия администратора: просмотр помещённых в карантин сообщений с указанием причины; самостоятельный выпуск либо запрос на выпуск администратору; персональные списки разрешённых и запрещённых отправителей; периодическую сводку по карантину с настраиваемой периодичностью; поиск по собственным сообщениям. Вход — по учётной записи корпоративного каталога.

2.7. Контроль исходящего почтового трафика (DLP) по настраиваемым шаблонам и ключевым словам; подпись и верификация исходящей почты по механизмам DKIM, SPF, DMARC, ARC.

2.8. Штатный программный модуль уведомлений в мессенджер, предоставляющий документированный программный интерфейс для программных агентов (ботов) с авторизацией по ключу доступа и передачей сообщений по протоколу HTTPS (в том числе Telegram или эквивалентный). Настройка выполняется средствами консоли управления без написания программного кода.

2.9. Отказоустойчивость: кластер не менее чем из двух узлов в режиме распределения нагрузки (Active-Active) либо горячего резерва (Active-Standby), виртуальный IP-адрес, встроенный балансировщик почтового трафика.

2.10. Отчётность и панели визуализации, экспорт отчётов в форматах PDF, CSV , HTML; передача событий во внешнюю систему класса SIEM по syslog в форматах CEF либо LEEF.

2.11. Аутентификация и разграничение доступа: локальные учётные записи, L DAP (Active Directory или эквивалент) с LDAPS, единый вход (SSO), двухфакторная аутентификация, ролевая модель, журнал аудита действий администраторов.

2.12. Обработка данных в инфраструктуре Заказчика: передача почтовых сообщений, вложений и результатов их анализа на облачные сервисы производителя и в сети третьих лиц не допускается. Получение обновлений программного обеспечения, антивирусных и антиспам-баз и репутационных сведений из внешних источников допускается.

3. Требования к совместимости с установленным программным обеспечением

3.1. Приобретаемое программное обеспечение должно являться функциональным модулем защиты электронной почты программного комплекса tLab Anti-APT, разработчиком и правообладателем которого является правообладатель установленного ПО, и входить с установленным ПО в состав единой программной платформы.

3.2. Взаимодействие Системы с установленным ПО обеспечивается штатными средствами и работоспособно непосредственно после установки и активации лицензии — без разработки, доработки, программирования и интеграционных работ.

3.3. Управление Системой и просмотр результатов анализа вложений, выполненного установленным ПО, осуществляются из единой консоли управления.

3.4. Единая база учётных записей, ролей и политик безопасности; повторный ввод учётных данных при переходе между функциями Системы и установленного ПО не требуется.

3.5. Из карточки почтового сообщения обеспечивается прямой переход к полному отчёту установленного ПО по соответствующему вложению.

3.6. Совместимость с эксплуатируемой версией установленного ПО без её замены; обновления выпускаются в согласованном цикле одним правообладателем.

3.7. При недоступности установленного ПО Система продолжает обработку почтового трафика остальными средствами фильтрации и обезвреживания вложений, с постановкой объектов в очередь на анализ и автоматической повторной отправкой после восстановления доступности.

3.8. Балансировка нагрузки при передаче объектов на анализ между двумя узлами (экземплярами) установленного ПО обеспечивается штатными средствами Системы и доступна непосредственно после установки и активации лицензии: распределение запросов с настраиваемым алгоритмом, автоматическое исключение недоступного узла и его возврат в работу после восстановления, отсутствие потери объектов при переключении. Отдельная лицензия, внешний балансировщик и работы по доработке не требуются.

4. Серверное оборудование в составе Комплекса

4.1. В состав каждого Комплекса входит серверное оборудование со следующими характеристиками: форм-фактор — не более 2U; процессор — не менее 1 шт., не менее 16 (шестнадцати) ядер, базовая тактовая частота не менее 2,9 ГГц; объём оперативной памяти — не менее 48 ГБ; накопитель типа HDD ёмкостью не менее 2 ТБ, скорость не менее 7200 об/мин, интерфейс SAS с пропускной способностью не менее 12 Гбит/с, с поддержкой горячей замены — не менее 2 (двух) шт.; RAID-контроллер — аппаратный; блок питания мощностью не более 750 Вт — не менее 2 (двух) шт. Оборудование должно допускать монтаж в стойку 19 дюймов.

4.2. Серверное оборудование в составе комплекса — новое, не бывшее в эксплуатации, год выпуска не ранее чем за 3 (три) года до даты заключения договора. Программное обеспечение поставляется в актуальной на дату поставки версии.

4.3. Программное обеспечение поставляется предустановленным на серверное оборудование и активированным; Комплекс передаётся Заказчику готовым к эксплуатации.

4.4. Гарантия на серверное оборудование — не менее 12 (двенадцати) месяцев с даты подписания акта приёма-передачи; ремонт либо замена вышедших из строя компонентов — Поставщиком в срок не более 10 (десяти) рабочих дней.

5. Лицензирование и язык

5.1. Поставке подлежат 2 (два) Комплекса. Лицензия в составе каждого Комплекса — бессрочная, не менее чем на 4000 (четыре тысячи) активных почтовых ящиков. Суммарная обслуживаемая ёмкость — не менее 4000 почтовых ящиков; второй Комплекс обеспечивает отказоустойчивость, а не увеличение ёмкости. Два Комплекса обеспечивают работу отказоустойчивого кластера из двух узлов; отдельная лицензия на кластеризацию, высокую доступность и балансировку нагрузки не требуется. Лицензия покрывает все требования настоящей технической спецификации без приобретения дополнительных модулей и без затрат на лицензирование стороннего программного обеспечения.

5.2. Обязательна поддержка государственного (казахского) языка. Интерфейс управления, отчёты, уведомления конечным пользователям и портал

самообслуживания должны быть доступны на государственном (казахском), русском и английском языках с переключением языка средствами Системы. Локализация на государственный язык распространяется на все разделы интерфейса, включая настройку политик, управление карантином, журналы и отчёты. Эксплуатационная документация — на государственном и русском языках.

Подписал	Жумабаева Алия Нурланкызы
Дата подписания	03.11.2026