Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Ұлттық ұлан Бас қолбасшылығы" республикалық мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Ұлттық ұлан Бас қолбасшылығы" республикалық мемлекеттік мекемесі
Конкурстың №:	№ 17985497-1
Конкурстың атауы:	2027 жылға арналған Ұлттық ұлан үшін бағдарламалық қамтамасыз пайдалану құқығына лицензиялар беру жөніндегі қызметтер
Лоттың нөмірі:	№ 88569484-ОК1
Лоттың атауы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582950.000.000001
Қызметтің атауы:	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	48095689.65
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	48095689.65
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	2027 жылдың 31 желтоқсанды қоса алғанда

Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Бағдарламалық қамтымды пайдалану құқығына лицензиялар беру жөніндегі қызметтерге ТЕХНИКАЛЫҚ СИПАТТАМА 1. ЖАЛПЫ МӘЛІМЕТТЕР 1.1. Жүйенің мақсаты Жүйе SIEM-жүйеден түсетін хабарламаларды талдау мен тергеуді автоматтандыру, жасанды интеллект технологияларын қолдану, инциденттер карточкаларын автоматтандырылған түрде жүргізу және уәкілетті қызметкерлерге жедел хабардар ету есебінен Тапсырыс берушінің киберқауіпсіздік мамандарының жұмыс тиімділігін арттыруға арналған. 1.2. Жүйені пайдалану мақсаттары: ақпараттық қауіпсіздік хабарламаларын бастапқы талдау уақытын қысқарту; типикалық және жалған оң (ложноположительный) іске қосылуларды автоматтандырылған түрде өңдеу арқылы талдаушыларға түсетін жүктемені азайту; Тапсырыс берушінің ақпараттық жүйелерінен қосымша контекст алу және Threat Intelligence (Қатерлер туралы мәліметтер) қолдану арқылы тергеу сапасын арттыру; автоматтандырылған талдау және тергеу нәтижелерін орталықтандырылған түрде ұсыну; инциденттер карточкаларын автоматтандырылған түрде жасау, өзектендіру және синхрондау; тапсырыс берушінің уәкілетті мамандарын жедел хабардар ету; ақпараттық қауіпсіздік оқиғаларын талдау мен тергеуді автоматтандыру үшін жасанды интеллект технологияларын қолдану. 1.3. Нормативтік база: Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V «Киберқауіпсіздік туралы» Заңы; Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Цифрландыру және киберқауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар. 2. САТЫП АЛУ ПӘНІ Сатып алу пәні Тапсырыс берушінің цифрлық инфрақұрылымында жергілікті орналастыру (On-Premise) арқылы жасанды интеллект технологияларын қолдана отырып, біріктірілген бірыңғай платформа болып табылатын «SOC Portal SIEM» бағдарламалық кешенін пайдалану құқығына лицензияларды беруді қамтитын Тапсырыс берушінің қызметін алу болып табылады. Бұл ретте оның құрамына оқиғаларды орталықтандырылған жинау қосалқы жүйесі (SIEM), соңғы нүктелердің қатерлерін анықтау және оларға әрекет ету (EPP), әрекет етуді оркестрлеу және автоматтандыру (IPR), қатерлер туралы деректермен алмасу платформасы (TIP) және желілік трафикті талдау (NTA) кіреді. Бұл лицензияланған бағдарламалық қамтамасыз етілу кешені 2026 жылы сатып алынды, 2026 жыл ішінде Тапсырыс берушінің орталық аппаратының цифрлық инфрақұрылымында орнатылып, енгізілді және Тапсырыс берушінің киберқауіпсіздік қызметімен қолданылады. Қолданыстағы (орнатылған) лицензияның қолданылу мерзімі 2026 жылдың 31 желтоқсанына дейін. Фирмалық атауды көрсетуді негіздеу: Қазақстан Республикасының «Мемлекеттік сатып алу туралы» Заңының 12-бабының 4-тармағы 2-тармақшасының екінші бөлігіне сәйкес, мемлекеттік сатып алу рәсімдерін жүргізу кезінде тауар белгілеріне, қызмет көрсету белгілеріне, фирмалық атауларға, патенттерге, пайдалы моделдерге, өнеркәсіптік үлгілерге, тауардың шыққан жерінің атауына және өндірушінің атауына, сондай-ақ сатып алынатын қызметтің жекелеген әлеуетті өнім берушіге тиесілігін айқындайтын өзге

	де сипаттамаларға сілтемелерді көрсету негізгі (орнатылған) жабдықты, сондай-ақ орнатылған бағдарламалық қамтамасыз етілуді (лицензияланған бағдарламалық қамтамасыз етілуді) қосымша жинақтау, жаңғырту және қайта жарақтандыру кезінде көрсетіледі. Қосымша мынаны атап өткен жөн: мұндай бағдарламалық қамтамасыз етілуді енгізу циклі, әсіресе үлкен ауқымда, әдетте 3 айдан 12 айға дейінгі уақытты алады. Егер бағдарламалық қамтамасыз етілуді енгізу 3 айдан 12 айға дейін уақыт алса, ал оны Ұлттық ұланның инфрақұрылымына баптау және бейімдеу циклі жаңа ғана басталған болса, келесі жылы платформаны басқа бағдарламалық қамтамасыз етілуге ауыстыру айтарлықтай уақытша және қаржылық шығындарға әкеп соқтыруы мүмкін. Мұндай күрделі жүйелерді енгізу тек техникалық интеграцияны ғана емес, сонымен қатар персоналды оқытуды, процестерді ретке келтіруді және нақты жағдайларда жұмыс тәжірибесін жинақтауды талап етеді, бұл қолданыстағы шешімді пайдалануды жалғастыруды анағұрлым тиімді етеді. Қаржыландыру киберқауіпсіздікті қамтамасыз ету орталығы үшін ақпаратты қорғау құралдарына жылдық жазылымдарды беру жөніндегі бір қызметке бөлінген. КТЖС (КТРУ) – 582950.000.000001 – Бағдарламалық қамтамасыз етілуді пайдалану құқығына лицензиялар беру жөніндегі қызметтер. Платформаның барлық компоненттері Тапсырыс берушінің есептеу инфрақұрылымында Жергілікті орналастыру моделі (On-Premise) бойынша Жеткізушімен таратылады, орнатылады және бапталады. Серверлік жабдық, деректерді сақтау жүйелері және желілік инфрақұрылым Тапсырыс берушімен ұсынылады. Қызмет көрсету Бірлескен басқару моделі (Co-Managed) бойынша жүзеге асырылады, бұл ретте Жеткізуші таратуды, баптауды және кепілдік қолдауды қамтамасыз етеді, ал деректер мен инфрақұрылым Тапсырыс берушінің бақылауында қалады. 3. ЖЕТКІЗУ ЖӘНЕ КЕПІЛДІК ҚОЛДАУ ҚҰРАМЫ № Жеткізу компоненті Қысқаша сипаттамасы 1. 1 Киберқауіпсіздік оқиғалары мен инциденттерін басқару қосалқы жүйесі (SOC Portal SIEM) Оқиғаларды орталықтандырылған жинау, толық мәтінді іздеу, қалыпқа келтіру және корреляциялау үшін корпоративтік деңгейдегі кластер (кемінде 10 000 EPS). 2. 2 Инциденттерге ден қою және оркестрлеу қосалқы жүйесі (IRP) Инциденттерді басқаруды (кейс-менеджмент), жергілікті байыту қозғалтқышымен интеграцияны және плейбуктер арқылы ден қою сценарийлерін автоматтандыруды қамтамасыз етеді (компрометацияланған хостты автоматты түрде желілік оқшаулауды қоса алғанда). 3. 3 Қатерлер туралы деректермен алмасу қосалқы жүйесі (TIP) Компрометация индикаторларын (IoC) орталықтандырылған сақтауды, қатер фидтерін қосуды, STIX/TAXII стандарттарын қолдауды және тергеу үшін IoC-ті инцидент карточкаларына автоматты түрде беруді қамтамасыз етеді. 4. 4 Соңғы нүктелердің қатерлерін анықтау және оларға ден қою қосалқы жүйесі (EPP) Кеңейтілген телеметрияны жинауды, файлсыз шабуылдарды анықтауды, белсенді әрекет етуді және хосттарды желіден қашықтан оқшаулауды қамтамасыз етеді. 5. 5 NTA (Network Traffic Analysis) Желілік трафикті мониторинг жасауға, жинауға және терең

	талдауға арналған қосалқы жүйе. 6. 6 Бағдарламалық платформаны пайдалану құқығы Белгіленген мерзім ішінде Тапсырыс берушінің инфрақұрылымында серверлік компоненттер мен Жүйенің веб-интерфейсін орнату және пайдалану құқығы. 7. 7 Орналастыру және баптау Бағдарламалық компоненттерді орнату, жергілікті орналастыруды және ақпараттық жүйелермен келісілген өзара іс-қимылды баптау. 8. 8 Автоматтандырылған талдау Хабарламаларды талдау, жіктеу және бағалау үшін ЖИ технологияларын пайдалану. 9. 9 Автоматтандырылған тергеу Қосымша контекстті алу және талдау, тергеу нәтижелері мен ден қою бойынша ұсынымдарды қалыптастыру. 10. 10 Инциденттер карточкаларын басқару Тапсырыс берушінің біріктірілген қосалқы жүйесінде инциденттер карточкаларын автоматты түрде жасау және өзектендіру, сондай-ақ Жүйенің веб-порталымен синхрондау. 11. 11 Threat Intelligence Талдау және тергеу нәтижелерін байыту үшін қатерлер туралы деректер мен IOC қолдану. 12. 12 Data Masking Сыртқы жасанды интеллект модельдерін пайдалану кезінде сезімтал ақпаратты бүркемелеу және жасырын еті көрсету. 13. 13 Хабарламалар Баптатылған ережелерге сәйкес келісілген арналар арқылы Тапсырыс берушінің уәкілетті қызметкерлерін хабардар ету. 14. 14 Автоматты дауыстық хабарлау Баптатылған эскалация шарттары туындаған кезде Тапсырыс берушінің қызметкерлеріне автоматты телефон қоңырауларын шалу. 15. 15 Жаңартулар және кепілдік қолдау Жаңартуларды ұсыну, ақауларды диагностикалау және жою, Жүйе жұмысы мен интеграциялар бойынша кеңес беру. 4. ҚАБЫЛДАУ ТӘРТІБІ ЖӘНЕ КЕПІЛДІК МІНДЕТТЕМЕЛЕРІ Осы техникалық спецификация 2027 жылғы 31 желтоқсанға дейін кепілдік қолдауы бар бағдарламалық қамтамасыз етілуге лицензия алуды көздейді. Жеткізу мерзімі 2027 жылғы 15 наурызға дейін, жеткізу орны – Қазақстан Республикасы Ұлттық ұланының «6636 әскери бөлімі» РММ. Кепілдік мерзімі ішінде – 2027 жылғы 31 желтоқсанға дейін – Жеткізуші сарапшылық техникалық қолдауды қамтамасыз етеді, оның ішінде: Тапсырыс берушінің сұрауы бойынша платформаны баптаудың анықталған кемшіліктерін жою; анықталған архитектуралық кемшіліктерді, интеграция сәтсіздіктерін және ережелер логикасындағы қателерді өтеусіз жою. Қабылдау Жүйені пайдалану құқығын ұсыну, оны жергілікті орналастыру, келісілген интеграциялардың жұмысқа қабілеттілігі және функционалдық тексерулердің нәтижелері негізінде жүзеге асырылады: Жүйе компоненттері мен деректерін жергілікті орналастыру, уәкілетті пайдаланушылар үшін веб-порталдың қолжетімділігі; SIEM жүйесі арқылы NTA және EPP үйлесімді компоненттерінен сынақ хабарламасы мен оқиғаларды алу; негізделген нәтиже мен пайдаланылған деректерді көрсете отырып, автоматтандырылған талдауды орындау; негізгі мәліметтерді синхрондай отырып, инциденттер карточкаларын жасау және өзектендіру; хабарлама алу және автоматты дауыстық сынақ қоңырауын орындау. Қабылдау кезіндегі функционалдық тексерулер: № Тексеру Әрекет Сәттілік критерийі 1 Жергілікті орналастыру Бағдарламалық компоненттер мен Жүйенің негізгі деректерінің орналасуы тексеріледі.

	Компоненттер мен деректер Тапсырыс берушінің инфрақұрылымында орналасқан. 2 Авторизация және құқықтар Пайдаланушылар жергілікті атаулы тіркелгі жазбаларымен кіреді; рөлдердің шектеулері тексеріледі. Рұқсат етілген функциялар қолжетімді, өкілеттіктен тыс қолжетімділік шектелген. 4 NTA және EPP оқиғалары SIEM арқылы келісілген NTA және EPP сынақ оқиғалары беріледі. Оқиғалар SIEM арқылы алынды және талдау үшін қолжетімді. 5 Хабарламаны талдау Сынақ хабарламасы мен жеткіліксіз контекст сценарийі талданады. Қорытынды негізделген; пайдаланылған деректер көрсетілген; контексттің жеткіліксіздігі белгіленген. 6 Карточка және синхрондау Карточка жасалады немесе өзектендіріледі; біріктірілген қосалқы жүйедегі және веб-порталдағы мәліметтердің үйлесімділігі тексеріледі. Карточка жасалды немесе жаңартылды; негізгі мәліметтер келісілген. 7 Threat Intelligence Келісілген көздегі сынақ индикаторы тексеріледі. Байыту нәтижесі Жүйеде көрсетіледі. 8 Бүркемелеу және прокси Сыртқы модельді пайдалану кезінде сынақ сезімтал деректерімен сұрау орындалады. Бапталған деректер санаттары жіберілмес бұрын бүркемеленеді; сұрау прокси арқылы рұқсат етілген ресурсқа өтеді. 9 Интеграцияның тұрақтылығы Байланысты кейіннен қалпына келтіре отырып, SIEM-тің уақытша қолжетімсіздігі имитацияланады. Қате тіркелді; байланыс қалпына келтірілгеннен кейін өңдеу жалғасады. 10 Сақтық көшірме жасау Сынақ сақтық көшірмесінен деректер мен конфигурацияны қалпына келтіру тексеріледі. Қалпына келтіру берілген құжаттама бойынша орындалады. 11 Хабарлама арнасы Келісілген алушыға сынақ хабарламасы жіберіледі. Хабарлама алынды. 12 Дауыстық хабарлау Келісілген нөмірге сынақ автоматты қоңырауы орындалады. Қоңырау тіркелді немесе алынды. 13 Қолдау және құжаттама Өтініштерді тіркеу арнасы мен берілетін құжаттама жиынтығы тексеріледі. Арна қолжетімді; құжаттама мен әкімшілік тіркелгі деректері белгіленген тәртіппен берілді. 5. ФУНКЦИОНАЛДЫҚ ТАЛАПТАР 5.1. Ақпараттық қауіпсіздік хабарламаларын автоматтандырылған талдау жасанды интеллект технологияларын қолдана отырып, түсетін хабарламаларды автоматтандырылған талдау; хабарламаларды жіктеу және талдаудың негізделген нәтижесін қалыптастыру; жалған оң (ложноположительный) немесе шынайы оң іске қосылу ықтималдығын бағалау; сыни деңгейін және қорғалатын ақпараттық ресурстарға ықтимал әсерін анықтау; Тапсырыс берушінің маманы үшін қысқаша аналитикалық түйіндеме қалыптастыру; кейіннен қарау және аудит үшін талдау нәтижесін сақтау. 5.2. Инциденттерді автоматтандырылған түрде тергеу берілген құқықтар шегінде Тапсырыс берушінің біріктірілген жүйелерінен қосымша контекст алу; байланысты оқиғаларды, хабарламаларды, объектілерді және бұрын тіркелген инциденттерді талдау; ақпаратты Threat Intelligence деректерімен байыту; негіздемесі және пайдаланылған деректер туралы мәліметтері бар қорытынды аналитикалық тұжырымды қалыптастыру; пайдаланылған деректердің толықтығы мен үйлесімділігін ескере отырып, тергеу нәтижесіне сенімділік дәрежесінің бағасын дайындау; Тапсырыс

	берушінің уәкілетті маманы үшін ұсынымдар дайындау. 5.3. Талдау нәтижелерін жіктеу және бағалау Жүйе өңдеу нәтижелерін кем дегенде False Positive (жалған оң) және True Positive (шынайы оң) санаттары бойынша жіктеуді, сондай-ақ ақпараттық ресурстарға немесе бизнес-процестерге елеулі әсері бар расталған оқиғаларды бөліп көрсету мүмкіндігін қолдауға тиіс. Деректер жеткіліксіз болған жағдайда, Жүйе хабарламаны міндетті түрде False Positive немесе True Positive санатына жатқызбай, маманның қосымша тексеруі қажет екенін айқын көрсетуі тиіс. Автоматтандырылған бағыттау, эскалация және ұсынымдарды қалыптастыру үшін пайдаланылатын сенімділік шекті мәндері бапталатын болуы тиіс және осы Техникалық спецификациямен бекітілмейді. 5.4. Инциденттер карточкаларын басқару және деректерді синхрондау Тапсырыс берушінің біріктірілген қосалқы жүйесінде инциденттер карточкаларын автоматты түрде жасау және өзектендіру; Жүйенің веб-порталында байланысты карточкалар мен талдау нәтижелерін көрсету; негізгі атрибуттарды, мәртебелерді және өңдеу нәтижелерін синхрондау; Тапсырыс беруші маманының тергеудің байланысты объектілеріне өту мүмкіндігі; өңдеу тарихы мен талдаушы шешімдерін сақтау. 5.5. Threat Intelligence қолдану IP-адрестерді, домендік атауларды, URL, хэш-сомаларды және өзге де IOC тексеру; талдау нәтижелеріне беделдік және контекстік ақпаратты қосу; тұжырымдар мен ұсынымдарды қалыптастыру кезінде қатерлер туралы деректерді пайдалану. 5.6. Сценарийлер мен ұсынымдар Жүйе әр түрлі хабарлама түрлері, активтер мен ақпараттық жүйелер үшін Тапсырыс берушімен келісілген сценарийлерді, нұсқаулықтарды және ұсынымдарды қолдануды қолдауға тиіс. Сценарийлерді қолданудың нақты ішкі іске асырылуы Жүйенің бағдарламалық логикасының бөлігі болып табылады және осы Техникалық спецификацияда жария етуге жатпайды. 5.7. Жүйенің веб-интерфейсі пайдаланушыларды аутентификациялау және авторизациялау; түскен хабарламалар мен инциденттер карточкаларын қарау; автоматтандырылған талдау және тергеу нәтижелерін қарау; сенімділік бағасын және қалыптастырылған ұсынымдарды қарау; берілген өкілеттіктер шегінде инциденттер бойынша мәртебелермен және шешімдермен жұмыс істеу; ақпаратты іздеу және сүзгілеу; әрекеттер тарихы мен хабарламаларды қарау. 5.8. Хабарламалар Жүйе Тапсырыс берушінің уәкілетті мамандарын жедел хабардар ету үшін келісілген байланыс арналарымен интеграцияны қамтамасыз етуге тиіс. Хабарламалардың құрамы, алушылар және жіберу шарттары өзара іс-қимылдың келісілген регламентіне сәйкес бапталуы тиіс. Берілетін ақпараттың құрамы Тапсырыс берушінің деректерді қорғаудың келісілген саясатына сәйкес келуі тиіс. 5.9. Автоматты дауыстық хабарлау Тапсырыс берушінің уәкілетті қызметкерлерінің байланыс телефондарының бапталатын тізбесін жүргізу; белгіленген эскалация шарттары туындаған кезде автоматты телефон қоңырауларын бастамашылық ету; баптауларға сәйкес тізбекті немесе топтық хабарлауды қолдау; байланыс сервисінің техникалық мүмкіндігі болған кезде қоңырауды орындау фактісін

	және оның нәтижесін тіркеу; Тапсырыс берушінің сұрауы бойынша кезекші қызметкерлердің құрамын өзгерту. 6. ЖАСАНДЫ ИНТЕЛЛЕКТ ТЕХНОЛОГИЯЛАРЫН ҚОЛДАНУ 6.1. Жалпы талаптар Жүйе құрамындағы жасанды интеллект технологиялары талдауды, жіктеуді, тергеуді, деректерді байытуды және ұсынымдарды дайындауды автоматтандыру үшін пайдаланылуы тиіс. ЖИ жұмысының нәтижелері Тапсырыс берушінің мамандарының шешім қабылдауын қолдау құралы ретінде қарастырылуы тиіс. 6.2. Сыртқы және жергілікті модельдерді пайдалану Жүйе сыртқы және/немесе жергілікті түрде орналастырылған жасанды интеллект модельдерін пайдалана алады. Нақты модельді таңдау және сұрауларды бағыттаудың ішкі тетігі Жүйені жүзеге асырудың бөлігі болып табылады. Сыртқы модельдерді пайдалануға Тапсырыс берушімен келісім бойынша жол беріледі. Сыртқы модельдерге ақпаратты беру корпоративті прокси-сервер арқылы тек аналитикалық міндетті орындау үшін қажетті көлемде, деректерді қорғау талаптарын сақтай отырып жүзеге асырылады. Жүйені жергілікті орналастыру рұқсат етілген сыртқы модельдерді пайдалануды жоққа шығармайды. 6.3. Data Masking Сыртқы жасанды интеллект модельдерін пайдалану кезінде Жүйе сыртқы сервистерге деректер берілгенге дейін Тапсырыс берушінің инфрақұрылымында Data Masking тетіктерін қолдануды қамтамасыз етуге тиіс. Бүркемеленуге жататындар: Тапсырыс беруші мен Орындаушы сезімтал деп анықтаған деректер санаттары, оның ішінде дербес деректер, тіркелгі жазбалары, электрондық пошта мекенжайлары, телефон нөмірлері, ішкі желілік идентификаторлар, түйін атаулары және өзге де шектеулі қолжетімділік мәліметтері. Келісілген саясаттарға сәйкес бүркемелеуі тиіс деректерді Data Masking орындамай сыртқы модельдерге беруге жол берілмейді. 6.4. Жасанды интеллект модельдеріне өтініштерді бақылау сыртқы модельге жүгіну фактісін тіркеу; жүгінген күні мен уақыты; сұрау немесе операция идентификаторы; Data Masking қолданылуы туралы мәліметтер; сұрауды орындау нәтижесі немесе мәртебесі; инцидент карточкасының тұтастығын бұзбай сыртқы сервис қателерін өңдеу. 6.5. ЖИ нәтижелерінің сапасын бақылау жіктеу және тергеу сапасын талдау; жалған оң нәтижелерді анықтау және есепке алу; сапаның нашарлауын бақылау; баптаулар мен пайдаланылатын модельдерді түзету мүмкіндігі; автоматтандырылған өңдеудің маңызды нәтижелерін журналға түсіру. 6.6. Human-in-the-Loop Жүйе адамның шешімін талап ететін нәтижелерді Тапсырыс беруші маманының міндетті түрде қарау мүмкіндігін қамтамасыз етуге тиіс. Инцидентті растау, жабу, эскалациялау және ден қою іс-шараларын орындау туралы түпкілікті шешімді Тапсырыс берушінің уәкілетті маманы қабылдайды. 7. АҚПАРАТТЫ ҚОРҒАУҒА ҚОЙЫЛАТЫН ТАЛАПТАР 7.1. Берілетін деректерді қорғау Жүйе компоненттері, біріктірілетін ақпараттық жүйелер арасында және қашықтан сүйемелдеу кезінде қорғалған байланыс арналарын пайдалану; жалпы пайдалану желілері бойынша деректерді беру кезінде криптографиялық қорғауды қолдану; берілетін деректердің тұтастығын бақылау; біріктірілетін компоненттерді

	аутентификациялау. 7.2. Қолжетімділікті басқару пайдаланушылардың жеке жергілікті тіркелгі жазбалары; қолжетімділіктің рөлдік моделі (RBAC); барынша аз қажетті артықшылықтар қағидаты; қолжетімділікті бұғаттау және кері қайтарып алу мүмкіндігі; тиісті конфигурация болған кезде көп факторлы аутентификацияны қолдау. 7.3. Журналға түсіру Жүйе аудит пен тергеу үшін қажетті көлемде пайдаланушылардың әрекеттерін, инцидент мәртебелерінің өзгеруін, интеграциялық алмасу операцияларын және басқа да маңызды қауіпсіздік оқиғаларын журналға түсіруді қамтамасыз етуге тиіс. 7.4. Деректерді сақтау және жою Бастапқы оқиға журналдары мен SIEM деректерінің негізгі массиві Тапсырыс берушінің инфрақұрылымында қалады. Хабарламалар, инциденттер карточкалары, автоматтандырылған талдау нәтижелері және Жүйенің техникалық журналдары Тапсырыс берушінің инфрақұрылымында жергілікті түрде сақталуға тиіс. Оларды Орындаушының инфрақұрылымында тұрақты сақтау көзделмейді. Шектелген деректер құрамын сыртқы модельдер мен хабарлау сервистеріне беруге келісілген саясаттарға және осы Техникалық спецификацияның талаптарына сәйкес жол беріледі. Деректерді сақтау мерзімдері Тапсырыс берушінің киберқауіпсіздік саясатымен айқындалады. Жүйені пайдалану мерзімі аяқталғаннан кейін деректер Тапсырыс берушінің бақылауында қалады. Оларды экспорттау және әрі қарай сақтау, жою немесе жасырын еті көрсету тәртібін Тапсырыс беруші айқындайды. 7.5. Деректерді оқшаулау және сақтық көшірме жасау Жергілікті орналастыру Тапсырыс берушінің деректерін оқшаулап сақтауды және оларға тек уәкілетті тұлғалардың ғана қолжетімділігін қамтамасыз етуге тиіс. Тараптар келіскен құралдармен Жүйенің деректері мен конфигурациясының сақтық көшірмесін жасау және қалпына келтіру мүмкіндігі қамтамасыз етілуі тиіс. Сақтық көшірмелер Тапсырыс берушінің инфрақұрылымында орналастырылады. 8. ҚОЛЖЕТІМДІЛІК ЖӘНЕ МАСШТАБТАУ ТАЛАПТАРЫ жүйенің серверлік компоненттері келісіettien технологиялық терезелерді қоспағанда, 24x7 режимінде жұмыс істеуге тиіс; жүйе архитектурасы қажетті есептеу ресурстары ұсынылған және пайдалану құқықтары шегінде пайдаланушылар санын және өңделетін хабарламалар көлемін ұлғайту мүмкіндігін қамтамасыз етуге тиіс; біріктірілетін ақпараттық жүйелердің құрамын кеңейту техникалық мүмкіндік болған кезде Тапсырыс берушінің өтінім бойынша жүзеге асырылады; жүйенің қолжетімділігіне әсер ететін жоспарлы жұмыстар авариялық жұмыстарды қоспағанда, Тапсырыс берушіге алдын ала хабарлай отырып орындалуы 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)	Қазақстан Республикасының «Рұқсаттар және хабарламалар туралы» Заңына сәйкес қызметтерді көрсетудің және кепілдік қолдаудың бүкіл мерзіміне қолданыстағы лицензияның болуы қажеттігі туралы талап енгізіледі: лицензияның атауы және лицензияның болуы талап етілетін қызмет түрі– Ақпаратты таратудың техникалық арналарын және жедел-іздестіру іс-шараларын жүргізуге арналған арнайы техникалық құралдарды анықтау жөніндегі, сондай-ақ ақпараттық қауіпсіздіктің жедел орталығы қызметі және ақпараттық қауіпсіздік инциденттеріне ден қою қызметі шеңберіндегі қызметтерді көрсетуге арналған лицензия; лицензияның болуы талап етілетін қызмет кіші түрінің атауы – Ақпараттық қауіпсіздіктің жедел орталығы қызметі аясында ақпаратты таратудың техникалық арналарын және жедел-іздестіру іс-шараларын жүргізуге арналған арнайы техникалық құралдарды анықтау; санаты – бірінші; коды – Q78. Әлеуетті Орындаушының шарттың қолданылу мерзімі ішінде Тапсырыс берушіге ұсынылатын бағдарламалық қамтамасыз етілуді жергілікті орналастырумен пайдалану құқығын беру, оны орнату, баптау, жаңарту, сүйемелдеу және техникалық қолдау үшін жеткілікті заңды құқықтары болуы тиіс. Егер әлеуетті Орындаушы ұсынылатын бағдарламалық қамтамасыз етілудің құқық иеленушісі (әзірлеушісі) болып табылмаса, ол осы сатып алу шеңберінде бағдарламалық қамтамасыз етілуді пайдалану құқығын беру, оны енгізу, сүйемелдеу және техникалық қолдау құқығын растайтын құқық иеленушінің (әзірлеушінің) немесе ол уәкілеттік берген өзге де тұлғаның авторлану хатын ұсынуға тиіс. Егер әлеуетті Орындаушы ұсынылатын бағдарламалық қамтамасыз етілудің құқық иеленушісі болып табымалса, оның авторлықты және/немесе бағдарламалық қамтамасыз етілуге айрықша мүліктік құқықтардың тиесілігін растайтын құжаттары болуы тиіс. Әлеуетті Орындаушы Жүйені Тапсырыс берушіге ұсыну кезінде үшінші тұлғалардың құқықтарының бұзылмауына және өзі пайдаланатын бағдарламалық компоненттерге қажетті құқықтардың болуына кепілдік беруге тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Республиканское государственное учреждение "Главное командование Национальной гвардии Республики Казахстан"
Наименование организатора	Республиканское государственное учреждение "Главное командование Национальной гвардии Республики Казахстан"
№ конкурса:	№ 17985497-1
Наименование конкурса:	Услуги по предоставлению лицензии на право использования программного обеспечения для Национальной гвардии на 2027 год
Номер лота:	№ 88569484-ОК1
Наименование лота:	Услуги по предоставлению лицензий на право использования программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582950.000.000001
Наименование услуги:	Услуги по предоставлению лицензий на право использования программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	48095689.65
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	48095689.65
Срок оказания услуги:	по 31 декабря 2027 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на услуги по предоставлению лицензий на право использования программного обеспечения 1. ОБЩИЕ СВЕДЕНИЯ 1.1. Назначение Системы Система предназначена для повышения эффективности работы специалистов кибербезопасности Заказчика за счет автоматизации анализа и расследования оповещений, поступающих из SIEM-системы, применения технологий искусственного интеллекта, автоматизированного ведения карточек инцидентов и оперативного уведомления уполномоченных сотрудников. 1.2. Цели использования Системы сокращение времени первичного анализа оповещений информационной безопасности; снижение нагрузки на аналитиков за счет автоматизированной обработки типовых и ложноположительных срабатываний; повышение качества расследования за счет получения дополнительного контекста из информационных систем Заказчика и использования Threat Intelligence; централизованное представление результатов автоматизированного анализа и расследования; автоматизированное создание, актуализация и синхронизация карточек инцидентов; оперативное уведомление уполномоченных специалистов Заказчика; применение технологий искусственного интеллекта для автоматизации анализа и расследования событий информационной безопасности. 1.3. Нормативная база - Закон Республики Казахстан «О кибербезопасности» от 24 ноября 2015 года № 418-V; - Единые требования в области цифровизации и обеспечения кибербезопасности, утвержденной постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832. 2. ПРЕДМЕТ ЗАКУПКИ Предметом закупки является получение Заказчиком услуги, включающей предоставление лицензий на установленное в цифровой инфраструктуре Заказчика программный комплекс «SOC Portal SIEM», представляющий собой единую интегрированную платформу, с использованием технологий искусственного интеллекта с локальным размещением (On-Premise), включающую в себя подсистемы централизованного сбора событий (SIEM), обнаружения и реагирования на угрозы конечных точек, оркестрации и автоматизации реагирования (IPR), платформу обмена данными об угрозах (TIP) и анализ сетевого трафика (NTA). Данный комплекс лицензионного программного обеспечения приобретен в 2026 году, установлен и внедрен в течении 2026 года в цифровой инфраструктуре центрального аппарата Заказчика и применяется службой кибербезопасности Заказчика. Срок действия действующей (установленной) лицензии до 31 декабря 2026 года. Обоснование указания фирменного наименования: В соответствии с частью второй подпункта 2 пункта 4 статьи 12 Закона Республики Казахстан «О государственных закупках» при проведении процедур государственных закупок содержание указаний на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара и наименование производителя, а также иные характеристики, определяющие принадлежность приобретаемой услуги отдельному потенциальному поставщику отражается при доукомплектовании, модернизации и дооснащения основного

	(установленного) оборудования, а также установленного программного обеспечения (лицензионного программного обеспечения). Дополнительно подчеркивается, что цикл внедрения подобного программного обеспечения, особенно в больших масштабах, как правило, занимает от 3 до 12 месяцев. Если внедрение программного обеспечения занимает от 3 до 12 месяцев, а цикл его настройки и адаптации к инфраструктуре Национальной гвардии только начался, смена платформы на другое программное обеспечение в следующем году может привести к значительным временным и финансовым затратам. Внедрение подобных сложных систем, требует не только технической интеграции, но и обучения персонала, отладки процессов и накопления опыта работы в реальных условиях, что делает более рациональным продолжение использования существующего решения. Финансирование выделено на одну услугу по предоставлению годовых подписок на средства защиты информации для центра обеспечения кибербезопасности. КТРУ - 582950.000.000001 - Услуги по предоставлению лицензий на право использования программного обеспечения. Все компоненты платформы, развёртываются, устанавливаются и настраиваются Поставщиком по модели локального размещения (On-Premise) на вычислительной инфраструктуре Заказчика. Серверное оборудование, системы хранения данных и сетевая инфраструктура предоставляются Заказчиком. Оказание услуг осуществляется по модели совместного управления (Co-Managed), при которой Поставщик обеспечивает развёртывание, настройку и гарантийную поддержку, а данные и инфраструктура остаются под контролем Заказчика. 3. СОСТАВ ПОСТАВКИ И ГАРАНТИЙНОЙ ПОДДЕРЖКИ № Компонент поставки Краткое описание 1. Подсистема управления событиями и инцидентами кибербезопасности (SOC Portal SIEM) Кластер корпоративного уровня (не менее 10 000 EPS) для централизованного сбора, полнотекстового поиска, нормализации и корреляции событий. 2. Подсистема реагирования на инциденты и оркестрации (IRP) Обеспечивает управление инцидентами (кейс-менеджмент), интеграцию с локальным движком обогащения и автоматизацию сценариев реагирования через плейбуки (включая автоматическую сетевую изоляцию скомпрометированного хоста). 3. Подсистема обмена данными об угрозах (TIP) Обеспечивает централизованное хранение индикаторов компрометации (IoC), подключение фидов угроз, поддержку стандартов STIX/TAXII и автоматическую передачу IoC в карточки инцидентов для расследования. 4. Подсистема обнаружения и реагирования на угрозы конечных точек Обеспечивает сбор расширенной телеметрии, обнаружение бесфайловых атак, активное реагирование и удаленную изоляцию хостов от сети 5. NTA (Network Traffic Analysis) Подсистема предназначенная для мониторинга, сбора и глубокого анализа сетевого трафика 6. Право использования программной платформы Право установки и использования серверных компонентов и веб-интерфейса Системы в инфраструктуре Заказчика в течение установленного срока. 7. Развертывание и настройка Установка программных компонентов, настройка локального

	размещения и согласованного взаимодействия с информационными системами. 8. Автоматизированный анализ Использование технологий ИИ для анализа, классификации и оценки оповещений. 9. Автоматизированное расследование Получение и анализ дополнительного контекста, формирование результатов расследования и рекомендаций по реагированию. 10. Управление карточками инцидентов Автоматическое создание и актуализация карточек инцидентов в интегрированной подсистеме Заказчика, а также синхронизация с веб-порталом Системы. 11. Threat Intelligence Использование данных об угрозах и IOC для обогащения результатов анализа и расследования. 12. Data Masking Маскирование и обезличивание чувствительной информации при использовании внешних моделей искусственного интеллекта. 13. Уведомления Уведомление уполномоченных сотрудников Заказчика через согласованные каналы в соответствии с настроенными правилами. 14. Автоматическое голосовое оповещение Автоматическое выполнение телефонных вызовов сотрудникам Заказчика при наступлении настроенных условий эскалации. 15. Обновления и гарантийная поддержка Предоставление обновлений, диагностика и устранение неисправностей, консультации по работе Системы и интеграций. 4. ПОРЯДОК ПРИЁМКИ И ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА Настоящей технической спецификацией предусматривается получение лицензии на программное обеспечение до 31 декабря 2027 года с гарантийной поддержкой. Срок поставки по 15 марта 2027 года, место поставки – РГУ «Воинская часть 6636 Национальной гвардии Республики Казахстан». В течение гарантийного срока - до 31 декабря 2027 года - Поставщик обеспечивает экспертную техническую поддержку, в том числе: - устранение выявленных недостатков настройки платформы по запросу Заказчика; - безвозмездное устранение выявленных архитектурных недостатков, сбоев интеграции и ошибок в логике правил. Приемка осуществляется на основании предоставления права использования Системы, ее локального развертывания, работоспособности согласованных интеграций и результатов функциональных проверок: локальное размещение компонентов и данных Системы, доступность веб-портала для уполномоченных пользователей; получение через SIEM-систему тестового оповещения и событий от совместимых компонентов NTA и EPP; выполнение автоматизированного анализа с отображением обоснованного результата и использованных данных; создание и актуализация карточек инцидентов с синхронизацией ключевых сведений; получение уведомления и выполнение тестового автоматического голосового вызова. Функциональные проверки при приемке: № Проверка Действие Критерий успешности 1 Локальное размещение Проверяется размещение программных компонентов и основных данных Системы. Компоненты и данные размещены в инфраструктуре Заказчика. 2 Авторизация и права Пользователи входят с локальными именными учетными записями; проверяются ограничения ролей. Разрешенные функции доступны, доступ вне полномочий ограничен. 4 События NTA и EPP Через SIEM передаются согласованные тестовые события NTA и EPP.

	События получены через SIEM и доступны для анализа. 5 Анализ оповещения Выполняется анализ тестового оповещения и сценария с недостаточным контекстом. Вывод обоснован; использованные данные отображены; недостаточность контекста обозначена. 6 Карточка и синхронизация Создается или актуализируется карточка; проверяется согласованность сведений в интегрированной подсистеме и веб-портале. Карточка создана или обновлена; ключевые сведения согласованы. 7 Threat Intelligence Выполняется проверка тестового индикатора в согласованном источнике. Результат обогащения отображается в Системе. 8 Маскирование и прокси При использовании внешней модели выполняется запрос с тестовыми чувствительными данными. Настроенные категории данных замаскированы до отправки; запрос проходит через прокси к разрешенному ресурсу. 9 Устойчивость интеграции Имитируется временная недоступность SIEM с последующим восстановлением связи. Ошибка зарегистрирована; после восстановления связи обработка возобновляется. 10 Резервное копирование Проверяется восстановление данных и конфигурации из тестовой резервной копии. Восстановление выполняется по переданной документации. 11 Канал уведомления Отправляется тестовое уведомление согласованному получателю. Уведомление получено. 12 Голосовое оповещение Выполняется тестовый автоматический звонок на согласованный номер. Вызов зарегистрирован или получен. 13 Поддержка и документация Проверяются канал регистрации обращений и комплект передаваемой документации. Канал доступен; документация и административные учетные данные переданы установленным порядком. 5. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ 5.1. Автоматизированный анализ оповещений информационной безопасности автоматизированный анализ поступающих оповещений с использованием технологий искусственного интеллекта; классификация оповещений и формирование обоснованного результата анализа; оценка вероятности ложноположительного или истинноположительного срабатывания; определение уровня критичности и возможного влияния на защищаемые информационные ресурсы; формирование краткого аналитического резюме для специалиста Заказчика; сохранение результата анализа для последующего просмотра и аудита. 5.2. Автоматизированное расследование инцидентов получение дополнительного контекста из интегрированных систем Заказчика в пределах предоставленных прав; анализ связанных событий, оповещений, объектов и ранее зарегистрированных инцидентов; обогащение информации данными Threat Intelligence; формирование итогового аналитического заключения с обоснованием и сведениями об использованных данных; формирование оценки степени уверенности в результате расследования с учетом полноты и согласованности использованных данных; подготовка рекомендаций для уполномоченного специалиста Заказчика. 5.3. Классификация и оценка результатов анализа Система должна поддерживать классификацию результатов обработки не менее чем по категориям False Positive и True Positive, а также возможность выделения подтвержденных событий с существенным

	влиянием на информационные ресурсы или бизнес-процессы Заказчика. При недостаточности данных Система должна явно указывать на необходимость дополнительной проверки специалистом, без обязательного отнесения оповещения к категории False Positive или True Positive. Пороговые значения уверенности, используемые для автоматизированной маршрутизации, эскалации и формирования рекомендаций, должны быть настраиваемыми и не фиксируются настоящей Технической спецификацией. 5.4. Управление карточками инцидентов и синхронизация данных автоматическое создание и актуализация карточек инцидентов в интегрированной подсистеме Заказчика; отображение связанных карточек и результатов анализа в веб-портале Системы; синхронизация ключевых атрибутов, статусов и результатов обработки; возможность перехода специалиста Заказчика к связанным объектам расследования; сохранение истории обработки и решений аналитика. 5.5. Использование Threat Intelligence проверка IP-адресов, доменных имен, URL, хэш-сумм и иных IOC; добавление репутационной и контекстной информации к результатам анализа; использование данных об угрозах при формировании заключений и рекомендаций. 5.6. Сценарии и рекомендации Система должна поддерживать применение согласованных с Заказчиком сценариев, инструкций и рекомендаций для различных типов оповещений, активов и информационных систем. Конкретная внутренняя реализация применения сценариев является частью программной логики Системы и не подлежит раскрытию в настоящей Технической спецификации. 5.7. Веб-интерфейс Системы аутентификация и авторизация пользователей; просмотр поступивших оповещений и карточек инцидентов; просмотр результатов автоматизированного анализа и расследования; просмотр оценки уверенности и сформированных рекомендаций; работа со статусами и решениями по инцидентам в пределах предоставленных полномочий; поиск и фильтрация информации; просмотр истории действий и уведомлений. 5.8. Уведомления Система должна обеспечивать интеграцию с согласованными каналами связи для оперативного уведомления уполномоченных специалистов Заказчика. Состав уведомлений, получатели и условия отправки должны настраиваться в соответствии с согласованным регламентом взаимодействия. Состав передаваемой информации должен соответствовать согласованной политике защиты данных Заказчика. 5.9. Автоматическое голосовое оповещение ведение настраиваемого перечня контактных телефонов уполномоченных сотрудников Заказчика; инициирование автоматических телефонных вызовов при наступлении заданных условий эскалации; поддержка последовательного или группового оповещения в соответствии с настройками; регистрация факта выполнения вызова и его результата при наличии технической возможности сервиса связи; изменение состава дежурных сотрудников по запросу Заказчика. 6. ПРИМЕНЕНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА 6.1. Общие требования Технологии искусственного интеллекта в составе Системы должны использоваться для автоматизации анализа, классификации, расследования,

	обогащения данных и подготовки рекомендаций. Результаты работы ИИ должны рассматриваться как инструмент поддержки принятия решений специалистами Заказчика. 6.2. Использование внешних и локальных моделей Система может использовать внешние и/или локально развернутые модели искусственного интеллекта. Выбор конкретной модели и внутренний механизм маршрутизации запросов являются частью реализации Системы. Использование внешних моделей допускается по согласованию с Заказчиком. Передача информации во внешние модели осуществляется через корпоративный прокси-сервер только в объеме, необходимом для выполнения аналитической задачи, с соблюдением требований защиты данных. Локальное размещение Системы не исключает использования разрешенных внешних моделей. 6.3. Data Masking При использовании внешних моделей искусственного интеллекта Система должна обеспечивать применение механизмов Data Masking в инфраструктуре Заказчика до передачи данных во внешние сервисы. Маскированию подлежат категории данных, определенные Заказчиком и Исполнителем как чувствительные, включая персональные данные, учетные записи, адреса электронной почты, номера телефонов, внутренние сетевые идентификаторы, имена узлов и иные сведения ограниченного доступа. Передача данных, которые в соответствии с согласованными политиками должны быть замаскированы, во внешние модели без выполнения Data Masking не допускается. 6.4. Контроль обращений к моделям искусственного интеллекта регистрация факта обращения к внешней модели; дата и время обращения; идентификатор запроса или операции; сведения о применении Data Masking; результат или статус выполнения запроса; обработка ошибок внешнего сервиса без нарушения целостности карточки инцидента. 6.5. Контроль качества результатов ИИ анализ качества классификации и расследования; выявление и учет ложноположительных результатов; контроль деградации качества; возможность корректировки настроек и используемых моделей; журналирование значимых результатов автоматизированной обработки. 6.6. Human-in-the-Loop Система должна обеспечивать возможность обязательного рассмотрения специалистом Заказчика результатов, требующих человеческого решения. Окончательное решение о подтверждении, закрытии, эскалации инцидента и выполнении мероприятий реагирования принимает уполномоченный специалист Заказчика. 7. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ 7.1. Защита передаваемых данных использование защищенных каналов связи между компонентами Системы, интегрируемыми информационными системами и при удаленном сопровождении; применение криптографической защиты при передаче данных по сетям общего пользования; контроль целостности передаваемых данных; аутентификация интегрируемых компонентов. 7.2. Управление доступом индивидуальные локальные учетные записи пользователей; ролевая модель доступа (RBAC); принцип минимально необходимых привилегий; возможность блокировки и отзыва доступа; поддержка многофакторной аутентификации при наличии соответствующей конфигурации. 7.3.

	Журналирование Система должна обеспечивать журналирование действий пользователей, изменений статусов инцидентов, операций интеграционного обмена и иных значимых событий безопасности в объеме, необходимом для аудита и расследования. 7.4. Хранение и удаление данных Первичные журналы событий и основной массив данных SIEM остаются в инфраструктуре Заказчика. Оповещения, карточки инцидентов, результаты автоматизированного анализа и технические журналы Системы должны храниться локально в инфраструктуре Заказчика. Их постоянное хранение в инфраструктуре Исполнителя не предусматривается. Передача ограниченного состава данных во внешние модели и сервисы уведомления допускается в соответствии с согласованными политиками и требованиями настоящей Технической спецификации. Сроки хранения данных определяются политиками кибербезопасности Заказчика. После окончания срока использования Системы данные остаются под контролем Заказчика. Порядок их экспорта и дальнейшего хранения, удаления или обезличивания определяется Заказчиком. 7.5. Изоляция данных и резервное копирование Локальное развертывание должно обеспечивать обособленное хранение данных Заказчика и доступ к ним только уполномоченных лиц. Должна обеспечиваться возможность резервного копирования и восстановления данных и конфигурации Системы средствами, согласованными сторонами. Резервные копии размещаются в инфраструктуре Заказчика. 8. ТРЕБОВАНИЯ К ДОСТУПНОСТИ И МАСШТАБИРУЕМОСТИ серверные компоненты Системы должны функционировать в режиме 24x7, за исключением согласованных технологических окон; архитектура Системы должна обеспечивать возможность увеличения количества пользователей и объема обрабатываемых оповещений при предоставлении необходимых вычислительных ресурсов и в пределах предоставленных прав использования; расширение состава интегрируемых информационных систем осуществляется по заявке Заказчика при наличии технической возможности; плановые работы, влияющие на доступность Системы, должны выполняться с предварительным уведомлением Заказчика, за исключением аварийных работ.

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)	В соответствии с Законом Республики Казахстан «О разрешениях и уведомлениях» включается требование о необходимости наличия действующей лицензии на весь срок оказания услуг и гарантийной поддержки.: наименование лицензии и вида деятельности, для осуществления которой требуется наличие лицензии - Лицензия на оказание услуг по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, а также в рамках деятельности оперативного центра информационной безопасности и деятельности службы реагирования на инциденты информационной безопасности; наименование подвида деятельности, для осуществления которой требуется наличие лицензии - Выявление технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, в рамках деятельности оперативного центра информационной безопасности; категория – первая; код – Q78. Потенциальный Исполнитель должен обладать законными правами, достаточными для предоставления Заказчику права использования предлагаемого программного обеспечения с локальным размещением, его установки, настройки, обновления, сопровождения и технической поддержки в течение срока действия договора. Если потенциальный Исполнитель не является правообладателем (разработчиком) предлагаемого программного обеспечения, он должен предоставить авторизационное письмо от правообладателя (разработчика) либо иного уполномоченного им лица, подтверждающее право на предоставление права использования программного обеспечения, его внедрение, сопровождение и техническую поддержку в рамках настоящей закупки. Если потенциальный Исполнитель является правообладателем предлагаемого программного обеспечения, он должен иметь документы, подтверждающие авторство и/или принадлежность исключительных имущественных прав на программное обеспечение. Потенциальный Исполнитель должен гарантировать отсутствие нарушения прав третьих лиц при предоставлении Системы Заказчику и наличие необходимых прав на используемые им программные компоненты.