

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Digital Silk Road Company" жауапкершілігі шектеулі серіктестігі
Ұйымдастырушының атауы:	"Digital Silk Road Company" жауапкершілігі шектеулі серіктестігі
Конкурстың №:	№ 17778722-1
Конкурстың атауы:	Об организации и проведении электронных государственных закупок услуг по предоставлению лицензий на право использования программного обеспечения способом открытого конкурса
Лоттың нөмірі:	№ 88115828-OK1
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:	14199493.97
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	14199493.97
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	

Қызмет көрсету мерзімі	шарт жасасқан күннен бастап 15 күнтізбелік күн өткеннен кейін 2026 жылғы 31 желтоқсанға дейін
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	ТЕХНИКАЛЫҚ ТАПСЫРМА ақпараттық жүйелерге артықшылықты қолжетімділікті басқаруға және артықшылықты пайдаланушылардың әрекеттерін бақылауға арналған бағдарламалық қамтамасыз етуді пайдалану лицензиясын беру бойынша қызметтер көрсетуге 1. Жалпы талаптар 1.1 Жеткізуші артықшылықты қолжетімділікті басқаруға, артықшылықты пайдаланушылардың әрекеттерін бақылауға және аудиттеуге арналған бағдарламалық қамтамасыз етуді (бұдан әрі — Жүйе) пайдалану лицензиясын беру бойынша қызметтер көрсетуге тиіс. 1.2 Жүйе кемінде 25 пайдаланушыны және мақсатты жүйелердің шектеусіз санын қолдауға тиіс. 1.3 Жүйе бір өндірушінің мынадай бағдарламалық компоненттерінен / модульдерінен тұруға тиіс: □ орталықтандырылған басқару — Жүйені әкімшілендіру, пайдаланушыларды, рөлдерді, қолжетімділік құқықтарын және қауіпсіздік саясаттарын бірыңғай веб-интерфейс арқылы басқару; □ артықшылықты тіркелгі деректерінің қорғалған қоймасы — тіркелгі деректерін қолжетімділікті ажырату және аудиттеу арқылы шифрланған түрде орталықтандырылған сақтау; □ артықшылықты сессияларды басқару (PAM Core) — Жүйенің прокси-компоненттері арқылы мақсатты жүйелерге қолжетімділік беру, сессияларды мониторингтеу және жазу, орындалатын командаларды бақылау және пайдаланушылар әрекеттерін аудиттеу; □ құрылғылар мен тіркелгілерді анықтау — инфрақұрылымды автоматтандырылған сканерлеу, мақсатты жүйелерді, артықшылықты тіркелгілерді және SSH-кілттерді анықтау, анықталған объектілерді Жүйеге импорттау мүмкіндігімен; □ артықшылықты тапсырмаларды автоматтандыру — әкімшілік командалар мен сценарийлерді сұрау бойынша немесе кесте бойынша артықшылықты парольдерді пайдаланушыларға ашпай орындау, құқықтарды ажырату, іске қосуды келісу және нәтижелерді журналға тіркеу арқылы; □ жеке және ортақ қорғалған қойма — парольдерді, файлдарды, жазбаларды және API-құпияларды сақтау, парольдерді генерациялау және ортақ қолжетімділікті бақыланатын түрде беру. 1.4 Жүйе лицензия белсендірілген күннен бастап жазылымның бүкіл әрекет ету мерзіміне өндірушінің техникалық қолдауымен 12 ай мерзімге жазылым түрінде ұсынылуға тиіс. 1.5 Жүйе екі түйіннен тұратын істен шығуға төзімді конфигурацияда орнату үшін ұсынылуға тиіс. Істен шығуға төзімділікті қамтамасыз етуге арналған екінші түйіннің лицензиясы жазылымның бүкіл әрекет ету мерзіміне қызметтер көрсету құнына енгізілуге тиіс. 1.6 Жүйе Тапсырыс берушінің IT-инфрақұрылымында ол ұсынған серверлік ресурстарда жергілікті түрде орнатылуға тиіс. 1.7 Жүйе өндірушісінің талаптарына сәйкес келетін серверлік ресурстар мен виртуалдандыру платформасын Тапсырыс беруші ұсынады. 1.8 Жүйені ұсыну бойынша қызметтер көрсету мерзімі, орнату және баптау жұмыстарын қоса алғанда, Шартқа қол қойылған күннен бастап 70 күнтізбелік күннен аспауға тиіс. 1.9 Жүйе Тапсырыс берушінің ib@nzhkeden.kz электрондық мекенжайына ұсынылуға тиіс. 2. Техникалық талаптар 2.1 Архитектураға және істен шығуға төзімділікке қойылатын талаптар 2.1.1 Жүйе Тапсырыс берушінің IT-инфрақұрылымында алдын ала орнатылған операциялық жүйені,
--	---

	кіріктірілген дерекқорды басқару жүйесін, веб-серверді және Жүйенің қолданбалы компоненттерін қамтитын дайын виртуалды бағдарламалық кешен (All-in-One Virtual Appliance) түрінде жергілікті түрде өрістетілуге тиіс. 2.1.2 Жүйе өндіруші ұсынатын үйлесімді форматтағы виртуалды бағдарламалық кешен бейнесін пайдалана отырып, VMware ESXi және Microsoft Hyper-V виртуалдандыру платформаларында өрістетуді қолдауға тиіс. 2.1.3 Жүйе дерекқорды репликациялау және түйіндер арасында файлдарды синхрондау арқылы екі түйіннен тұратын кластерлік өрістетуді, сондай-ақ істен шыққан түйін жұмысқа қайтарылғаннан кейін синхрондауды қалпына келтіруді қолдауға тиіс. 2.1.4 Жүйе кворумды және екі түйіннің біреуі істен шыққан кезде автоматты түрде ауыстырып қосуды қамтамасыз ету үшін арбитрді пайдалануды, сондай-ақ пайдаланушылық қосылымдарды бөлу үшін кіріктірілген немесе сыртқы жүктеме теңгергішін пайдалануды қолдауға тиіс. 2.1.5 Жүйе әрбір мақсатты жүйеге қосымша лицензиялар сатып алмай, мақсатты жүйелердің шектеусіз санын қосуды қамтамасыз етуге тиіс. Өнімділік пен бір мезгілде өңделетін сессиялар саны есептеу ресурстарын ұлғайту және өндіруші қолдайтын архитектураға сәйкес түйіндер қосу арқылы масштабталуға тиіс. 2.1.6 Жүйе мақсатты жүйелерге жергілікті агенттерді орнатпай немесе жекелеген функциялар үшін оларды барынша аз пайдалана отырып қосылуды қамтамасыз етуге тиіс. 2.1.7 Жүйе пайдаланушылардың жұмыс станцияларының мақсатты жүйелерге тікелей желілік қолжетімділігі қажеттілігін болдырмауға мүмкіндік беретін артықшылықты қосылымдарды проксилеуді қамтамасыз етуге тиіс. 2.1.8 Жүйеде конфигурацияның, тіркелгі деректерінің және сессия жазбаларының сақтық көшірмесін жасаудың кіріктірілген құралдары болуға тиіс. Сақтық көшірмелер шифрланған түрде сақталуға тиіс. 2.1.9 Жүйе артықшылықты тіркелгі деректерінің қорғалған сақтық көшірмесін жасауды және Жүйе қолжетімсіз болған кезде сақталған парольдерге қолжетімділікті авторизацияланған түрде қалпына келтіру мүмкіндігін қамтамасыз етуге тиіс. 2.1.10 Жүйе парольдерді, SSH-кілттерді және өзге де аутентификациялық деректерді AES-256 алгоритмін немесе салыстырмалы не одан жоғары криптографиялық беріктігі бар алгоритмді пайдалана отырып, шифрланған түрде сақтауды қамтамасыз етуге тиіс. 2.2 Функционалдық талаптар 2.2.1 Жүйе артықшылықты тіркелгілерге қолжетімділікті орталықтандырылған басқаруды, мақсатты жүйелерге қосылу кезінде пайдаланушылардың әрекеттерін аудиттеуді және белсенділігін мониторингтеуді қамтамасыз етуге тиіс. 2.2.2 Жүйеде қолжетімділік саясаттары негізінде пайдаланушылар мен топтар үшін жекелеген объектілерге қолжетімділікті ажырата отырып, тіркелгі деректері мен құпиялардың қорғалған қоймасы болуға тиіс. 2.2.3 Жүйе мақсатты жүйелерге SSH (SSH-кілттер көмегімен аутентификацияны қоса алғанда), RDP, HTTP/HTTPS және SFTP хаттамалары бойынша қосылуды, сондай-ақ Microsoft RemoteApp арқылы жарияланған қолданбаларға қолжетімділікті қамтамасыз етуге тиіс. 2.2.4 Жүйе сақталған парольдер мен SSH-кілттерді пайдаланушыларға
--	--

ашпай, қашықтан қол жеткізу мен әкімшілендірудің стандартты клиенттік қолданбаларын, оның ішінде пайдаланушылардың жұмыс станцияларында жергілікті түрде орнатылғандарын пайдалануды қолдауға тиіс. 2.2.5 Жүйе сақталған парольдерді пайдаланушыларға ашпай, әкімшілендіруге және әзірлеуге арналған мамандандырылған клиенттік қолданбаларды пайдалана отырып дерекқорларға қосылуды қолдауға тиіс. 2.2.6 Жүйе веб-браузерді немесе графикалық ортаны пайдалану қажеттілігінсіз пайдаланушы терминалынан SSH-прокси арқылы мақсатты жүйелерге қолжетімділікті қамтамасыз етуге тиіс. 2.2.7 Жүйе пайдаланушының жұмыс станциясында орнатылған жеке клиенттік қолданбаларды пайдалану қажеттілігінсіз SSH, RDP, RemoteApp және HTTP/HTTPS сессияларын веб-браузер терезесінде (арқылы) іске қосуды қамтамасыз етуге тиіс. 2.2.8 Жүйе артықшылықты сессияларда алмасу буферін пайдалануды және файлдарды беруді басқаруды, оның ішінде қолжетімділік саясаттары, қосылым түрі, пайдаланушы, пайдаланушылар тобы, мақсатты жүйе және қосылым көзінің ішкі желісі негізінде тиісті мүмкіндіктерді қосуды, ажыратуды және шектеуді қамтамасыз етуге тиіс. 2.2.9 Жүйе артықшылықты сессиялардың веб-интерфейсі арқылы файлдарды беруді, оның ішінде файлдарды сүйреп апару арқылы беруді қолдауға тиіс. 2.2.10 Веб-клиент арқылы RDP-сессиялар үшін пайдаланушының жұмыс станциясынан файлдарды жүктеу және оларға қашықтағы сессияда қосылатын виртуалды немесе желілік диск арқылы кейіннен қол жеткізу қолдау көрсетілуге тиіс. 2.2.11 Веб-клиент арқылы SSH/SFTP-сессиялар үшін пайдаланушының жұмыс станциясы мен мақсатты жүйе арасында файлдарды жүктеу және түсіру қолдау көрсетілуге тиіс. 2.2.12 Веб-клиент арқылы HTTP/HTTPS-сессиялар үшін тиісті рұқсаттар болған кезде файлдарды жүктеу және жүктеп алу қолдау көрсетілуге тиіс. 2.2.13 Жүйе артықшылықты сессияны іске қосу кезінде және парольді қарау кезінде аутентификацияның екінші факторын сұрау мүмкіндігін қамтамасыз етуге тиіс. 2.2.14 Жүйе қосылым орнату кезінде қолмен енгізілетін пайдаланушының жеке тіркелгі деректерін қоймада алдын ала сақтау қажеттілігінсіз пайдалана отырып, сессияны бақылауды және жазуды қамтамасыз ете отырып, прокси арқылы мақсатты жүйелерге қосылуды қолдауға тиіс. 2.2.15 Жүйе сессия шеңберінде sudo арқылы артықшылықтарды арттыру кезінде артықшылықты тіркелгі паролін автоматты түрде қоюды қамтамасыз етуге тиіс. 2.2.16 Жүйе орындалатын командаларды бақылауды және тыйым салынған әрекеттерге ден қоюды, оның ішінде сессияны немесе пайдаланушыны бұғаттауды қамтамасыз етуге тиіс. 2.2.17 Жүйе мақсатты құрылғыны тіркеу кезінде оның желілік қолжетімділігін тексеруді және тексеру нәтижесін интерфейсте көрсетуді қамтамасыз етуге тиіс. 2.2.18 Жүйе сертификаттарды мақсатты жүйелерге қосылу үшін пайдаланылатын тіркелгі деректерімен байланыстыруды, сондай-ақ SSL/TLS-сертификаттарды және тиісті жабық кілттерді қорғалған түрде сақтауды қамтамасыз етуге тиіс. 2.2.19 Жүйе SSL/TLS-сертификаттарды пайдалана отырып дерекқорларға қорғалған қосылуды қолдауға тиіс. 2.2.20 Жүйе желілік

	қолжетімділік және үйлесімді қосылу механизмдері болған жағдайда, бұлттық және гибриді инфрақұрылымдардағы, оның ішінде Microsoft Azure, Amazon Web Services және Oracle Cloud Infrastructure ортасындағы басқарылатын PostgreSQL дерекқорларына қосылуды қолдауға тиіс. 2.2.21 Жүйе генерацияланатын парольдерге қойылатын талаптарды Тапсырыс берушінің парольдік саясатына сәйкес баптауды қамтамасыз етуге тиіс. 2.2.22 Жүйе операциялық жүйелердің, дерекқорлардың және желілік жабдықтың артықшылықты тіркелгілерінің парольдерін автоматты түрде ауыстыруды қолдау көрсетілетін мақсатты жүйелер тізбесін кеңейту мүмкіндігімен қамтамасыз етуге тиіс. 2.2.23 Жүйе HTTP/HTTPS пайдалана отырып, мақсатты жүйелердің веб-интерфейстері арқылы парольдерді автоматты түрде ауыстыруды қолдауға тиіс. 2.2.24 Жүйе парольдерді кесте бойынша және пайдаланушы парольді қарағаннан кейін бапталатын аралық өткен соң автоматты түрде ауыстыруды қамтамасыз етуге тиіс. 2.2.25 Жүйе әкімшілердің стандартты хаттамалар мен интерфейстерді пайдалана отырып, оның ішінде тиісті орындаушыны немесе қосылым түрін таңдай отырып, парольдерді ауыстырудың пайдаланушылық үлгілерін жасауын және өңдеуін қолдауға тиіс. 2.2.26 Жүйе сақталған парольдердің өзектілігін автоматты түрде тексеруді және тиісті өкілеттіктері бар пайдаланушының сұрауы бойынша парольді генерациялауды қамтамасыз етуге тиіс. 2.2.27 Жүйе SSH-кілттерді басқаруды, оның ішінде оларды ротациялауды және жаңа кілттің ашық бөлігін мақсатты құрылғыларда жариялауды қамтамасыз етуге тиіс. 2.2.28 Жүйе артықшылықты қолжетімділікті уақытша беруді, оның ішінде Just-in-Time тетіктерін немесе функционалдық жағынан ұқсас тетіктерді, белгіленген мерзім өткеннен кейін берілген құқықтарды автоматты түрде кері қайтарып алу арқылы қолдауға тиіс. 2.2.29 Жүйе аса сезімтал тіркелгі деректеріне қол жеткізу кезінде бір пайдаланушының толық парольді алу мүмкін еместігін көздейтін өкілеттіктерді бөлуді қолдауға тиіс. 2.2.30 Жүйе жергілікті агенттерді орнатпай немесе оларды барынша аз пайдалана отырып, штаттық желілік хаттамаларды пайдалану арқылы құрылғыларды және олармен байланысты тіркелгі деректерін автоматтандырылған түрде анықтауды қамтамасыз етуге тиіс. 2.2.31 Анықтау кезінде пайдаланушылар, артықшылықты және домендік тіркелгілер, SSH-кілттер, сертификаттар және тіркелгі деректерімен байланысты Windows қызметтері анықталуға тиіс. 2.2.32 Жүйе Linux/Unix және Windows серверлерін, дерекқорларды, жұмыс станцияларын және желілік құрылғыларды, оның ішінде желіаралық экрандарды, маршрутизаторларды, коммутаторларды және жүктеме теңгергіштерін анықтауды қамтамасыз етуге тиіс. 2.2.33 Жүйе мақсатты жүйеде тиісті деректер қолжетімді болған жағдайда, анықталған объектілер туралы мәліметтерді, оның ішінде түйін атауын, IP-мекенжайды, тіркелгі деректерінің тізбесін, артықшылықтар түрін, соңғы қол жеткізу күнін және парольдің өзгергені туралы мәліметтерді жинауды қамтамасыз етуге тиіс. 2.2.34 Жүйе алдын ала бапталған ережелер, сөздіктер немесе жіктеу үлгілері негізінде
--	--

	анықталған объектілерді қорғалған қоймаға автоматты түрде импорттауды қамтамасыз етуге тиіс. 2.2.35 Жүйеде пайдаланушылық рөлдерді жасау және қажетті өкілеттіктерді тағайындау мүмкіндігі бар кіріктірілген рөлдік қолжетімділік моделі болуға тиіс. 2.2.36 Жүйе мақсатты жүйелер, мақсатты жүйелер топтары және артықшылықты тіркелгілер бойынша қолжетімділікті ажыратуды қамтамасыз етуге тиіс. 2.2.37 Жүйе артықшылықты тіркелгіні қосылу үшін пайдалану құқықтарын және оның паролін қарау құқықтарын бөлек тағайындауды қамтамасыз етуге тиіс. 2.2.38 Жүйе кіріктірілген екі факторлы аутентификацияны және көп факторлы аутентификацияның сыртқы провайдерлерін пайдалану мүмкіндігін қолдауға тиіс. 2.2.39 Жүйе қолжетімділікті шектеулі уақыт кезеңіне, апта күндері және тәулік уақыты бойынша, сондай-ақ уәкілетті пайдаланушы немесе келісушілер тобы келіскеннен кейін беруді қамтамасыз етуге тиіс. 2.2.40 Жүйе күдікті белсенділік немесе аутентификацияның бірнеше рет сәтсіз әрекеттері анықталған кезде қосылым көздерін автоматты түрде бұғаттауды қамтамасыз етуге тиіс. 2.2.41 Жүйе әкімшінің IP-мекенжайларды немесе хосттарды қолмен бұғаттауын және бұғаттан шығаруын қамтамасыз етуге тиіс. 2.2.42 Жүйе артықшылықты сессияларды автоматты түрде жазуды, қолдау көрсетілетін сессия түрлерінде әрекеттерді мәтіндік хаттамалауды және аяқталған сессиялардың журналдары бойынша аяқталған барлық сессиялардың журналдары бойынша мәтінді іздеуді қамтамасыз етуге тиіс. 2.2.43 Жүйе белсенді сессияларды нақты уақыт режимінде қарауды, сондай-ақ уәкілетті пайдаланушылардың оларды тоқтата тұруын және мәжбүрлі түрде аяқтауын қамтамасыз етуге тиіс. 2.2.44 Жүйе әкімші-пайдаланушылар, артықшылықты тіркелгілер және мақсатты жүйелер бөлінісінде белсенділіктің статистикалық модельдерін құруды қамтамасыз етуге тиіс. 2.2.45 Жүйе шекті мәндерді және ден қою әрекеттерін, оның ішінде пайдаланушыны бұғаттауды, сессияны бұғаттауды немесе сессияны аудитке жіберуді баптай отырып, статистикалық модельдерден ауытқулар негізінде аномалияларды анықтауды қамтамасыз етуге тиіс. 2.2.46 Жүйе аудитордың түсініктемелер қосу және тексерудің аяқталғаны туралы белгі қою мүмкіндігімен сессияларды аудитке автоматты және қолмен жіберуді қамтамасыз етуге тиіс. 2.2.47 Жүйе сессия жазбаларын сақтау мерзімдерін баптауды және таңдалған жазбаларды сақтау мерзімі өткеннен кейін автоматты түрде жоюдан алып тастауды қамтамасыз етуге тиіс. 2.2.48 Жүйе пайдаланушыға артықшылықты тіркелгі деректеріне тікелей қолжетімділік бермей, мақсатты жүйелерде әкімшілік командалар мен сценарийлерді орталықтандырылған түрде орындауды қамтамасыз етуге тиіс. 2.2.49 Жүйе тапсырмаларды орындау құқықтарын ажыратуды, сұрау немесе кесте бойынша іске қосуды, іске қосуды жауапты қызметкердің келісуін, мәртебені қадағалауды және орындау нәтижесін алуды қамтамасыз етуге тиіс. 2.2.50 Жүйе парольдерді, файлдарды, жазбаларды және API-құпияларды жеке және ортақ қорғалған түрде сақтауды, парольдерді генерациялауды және тағайындалған рұқсаттар негізінде объектілерге басқа
--	--

	пайдаланушыларға қолжетімділік беруді қамтамасыз етуге тиіс. 2.2.51 Жүйе сессияларды ашу, парольдерді қарау және ауыстыру, тыйым салынған командаларды орындауға жасалған әрекеттер, конфигурация объектілерін жасау, өзгерту және жою, қолжетімділік саясаттарын және интеграция параметрлерін өзгерту оқиғаларын тіркеуді қамтамасыз етуге тиіс. 2.2.52 Жүйе пайдалану оқиғаларын, оның ішінде мақсатты түйіндермен байланыстың жоғалуы мен қалпына келуін, сақтық көшірме жасау нәтижелерін және парольдерді ауыстыру операцияларын орындау қателерін тіркеуді қамтамасыз етуге тиіс. 2.2.53 Жүйе уәкілетті келісушілерді тағайындай отырып, парольдерді қарауға және артықшылықты сессияларды іске қосуға қолжетімділікті келісудің бапталатын рәсімдерін қамтамасыз етуге тиіс. 2.2.54 Жүйе белгіленген келісушілер иерархиясына сәйкес сұрауларды көп деңгейлі дәйекті келісуді қолдауға тиіс. 2.2.55 Жүйе бапталған саясатқа сәйкес негіздеме мен сұралатын қолжетімділік кезеңін міндетті түрде көрсетуді қамтамасыз етуге тиіс. 2.2.56 Жүйе әкімшілік веб-интерфейс арқылы электрондық хабарламалардың тақырыбы мен мәтінін өзгертуді, деректерді автоматты түрде қою үшін үлгі айнымалыларын, оның ішінде сұраудың нөмірі мен мәртебесін, бастамашы мен келісушіні, мақсатты жүйенің атауы мен IP-мекенжайын, тіркелгі атауын, негіздеме мен сұралатын қолжетімділік кезеңін, сондай-ақ сұрауды келісуге немесе қабылдамауға арналған сілтемелерді қолдай отырып қамтамасыз етуге тиіс. 2.3 Есептілікке қойылатын талаптар 2.3.1 Жүйе берілген үлгілер негізінде есептер қалыптастыруды қамтамасыз етуге және Жүйенің жай-күйі мен пайдаланылуын мониторингтеу панельдерін ұсынуға тиіс. 2.3.2 Жүйе ақпараттық қауіпсіздік оқиғалары, пайдаланушылар мен әкімшілердің әрекеттері, қолжетімділік саясаттары мен интеграция баптауларының өзгерістері бойынша есептілік қалыптастыруды қамтамасыз етуге тиіс. 2.3.3 Жүйе артықшылықты тіркелгілерді пайдалану бойынша, оның ішінде парольдерді қарау, беру, ауыстыру, тексеру және қалпына келтіру бойынша есептілік қалыптастыруды қамтамасыз етуге тиіс. 2.3.4 Жүйе мақсатты жүйелердің өзекті парольдерін қараған пайдаланушылар туралы есепті, сондай-ақ таңдалған кезеңдегі пайдаланушылардың парольдерге қол жеткізу тарихын ұсынуға тиіс. 2.3.5 Жүйе пайдаланушыны, мақсатты жүйені, тіркелгіні, басталу және аяқталу уақытын, ұзақтығын және қосылым көзін көрсете отырып, артықшылықты сессиялар бойынша есептер қалыптастыруды қамтамасыз етуге тиіс. 2.3.6 Жүйе басқарылатын тіркелгілер, парольдердің қолданылу мерзімдері, парольдердің соңғы ауыстырылған күндері, парольдердің ұзақ уақыт ауыстырылмауы және алдағы ротация операциялары бойынша есептілікті қамтамасыз етуге тиіс. 2.3.7 Жүйе күні мен уақытын, мақсатты жүйені, тіркелгіні, нәтижені және қате болған жағдайда оның сипаттамасын көрсете отырып, парольдерді ауыстырудың сәтті және сәтсіз операциялары бойынша есептілікті қамтамасыз етуге тиіс. 2.3.8 Жүйе сақтық көшірме жасау, операцияларды орындау қателері, компоненттердің қолжетімділігі және мақсатты түйіндермен
--	---

	байланыс жай-күйі бойынша есептілікті қамтамасыз етуге тиіс. 2.3.9 Жүйе оқиға түрін, оқиғаның маңыздылық деңгейін, алушыны және жіберу мәртебесін көрсете отырып, хабарламалар мен ескертулер бойынша есептілікті қамтамасыз етуге тиіс. 2.3.10 Жүйе тыйым салынған командаларды орындау әрекеттері» лучше заменить на «тыйым салынған командаларды орындауға жасалған әрекеттер және оларға байланысты ден қою әрекеттері бойынша есептілікті қамтамасыз етуге тиіс. 2.3.11 Жүйе тіркелген пайдаланушылар, олардың рөлдері, топтары, қолжетімділік профильдері және тағайындалған өкілеттіктері бойынша есептілікті қамтамасыз етуге тиіс. 2.3.12 Жүйе артықшылықты сессиялардың бейнежазбаларын уәкілетті үшінші тұлғаларға беру және Жүйеден тыс қарау үшін экспорттауды қамтамасыз етуге тиіс. 2.3.13 Жүйе есептерде көрсетілетін деректер құрамын баптауды және есептерді көрсетілген алушыларға кесте бойынша автоматты түрде жіберуді қамтамасыз етуге тиіс. 2.3.14 Жүйе есептелген тәуекел бағасын және әдеттегі мінез-құлықтан ауытқу белгілерін көрсете отырып, артықшылықты сессиялардың және тіркелгі деректерін қарау операцияларының анықталған аномалиялары бойынша есептер ұсынуға тиіс. 2.4 Интерфейске қойылатын талаптар 2.4.1 Жүйе орталықтандырылған әкімшілендіруге, пайдаланушыларды, рөлдерді, қолжетімділік саясаттарын, мақсатты жүйелерді және тіркелгі деректерін басқаруға арналған бірыңғай веб-интерфейсті ұсынуға тиіс. Веб-интерфейс орыс, ағылшын, неміс, испан, француз, поляк және португал тілдерін қолдауға тиіс. Пайдаланушы интерфейсі тағайындалған құқықтарға сәйкес пайдаланушыға қолжетімді мақсатты жүйелерді, тіркелгі деректерін және функцияларды көрсетуге тиіс. 2.4.2 Веб-интерфейс рұқсат етілген артықшылықты сессияларды іске қосуды, қолжетімділікке сұраулар беруді, сұрауларды келісуді және оларды өңдеу мәртебесін қарауды қамтамасыз етуге тиіс. 2.4.3 Интерфейс пайдаланушының өкілеттіктеріне сәйкес белсенді және аяқталған сессияларды қарауды, журналдар бойынша іздеуді, аудитордың сессия жазбаларымен жұмысын және есептерге қолжетімділікті қамтамасыз етуге тиіс. 2.4.4 Интерфейс артықшылықты тапсырмаларды баптауды және іске қосуды, орындау мәртебесін және операциялар нәтижелерін қарауды қамтамасыз етуге тиіс. 2.4.5 Жүйеде пайдаланушы құқықтарына сәйкес жеке және ортақ қойманың рұқсат етілген объектілеріне қорғалған қолжетімділік үшін Google Play арқылы қолжетімді Android 10 және одан жоғары нұсқасына арналған мобильді қолданба болуға тиіс. 2.5 Үшінші тарап жүйелерімен интеграцияларға қойылатын талаптар 2.5.1 Жүйе Microsoft Active Directory тіркелгілері бар пайдаланушыларды LDAP/LDAPS арқылы аутентификациялауды қолдауға тиіс. 2.5.2 Жүйе Microsoft Active Directory топтарын синхрондауды және пайдаланушыларға олардың топтарға тиесілілігіне сәйкес рөлдер мен ресурстарға қолжетімділікті тағайындауды қолдауға тиіс. 2.5.3 Жүйе RADIUS хаттамасы бойынша көп факторлы аутентификацияның сыртқы провайдерлерімен интеграцияны, сондай-ақ IdP жағында көп факторлы аутентификацияны орындай отырып, бірыңғай
--	---

	кіру (SSO) үшін SAML 2.0 және OpenID Connect хаттамалары бойынша сыртқы сәйкестендіру провайдерлерімен (IdP) интеграцияны қолдауға тиіс. 2.5.4 Жүйе үйлесімді аутентификатор-қолданбалар қалыптастыратын TOTP бір реттік парольдерін пайдалануды, сондай-ақ RSA Authenticator, Duo Security және AuthID провайдерлерімен мамандандырылған интеграцияларды қолдауға тиіс. 2.5.5 Жүйе X.509 сертификаттарын пайдалана отырып пайдаланушыларды аутентификациялауды қолдауға тиіс. 2.5.6 Жүйе көп факторлы аутентификацияның сыртқы провайдерлерімен интеграцияны қолдауға тиіс. 2.5.7 Жүйе қауіпсіздік оқиғалары мен пайдалану оқиғаларын сыртқы мониторинг жүйелеріне және SIEM-ге беруді қамтамасыз етуге тиіс. 2.5.8 Берілетін оқиғалар құрылымдалған форматта болуға және сәйкестендіргішті, түрін, оқиғаның маңыздылық деңгейін, оқиға сипаттамасын, процесс сәйкестендіргішін және оқиға контекстісі бар қосымша өрістерді қамтуға тиіс. 2.5.9 Жүйе рұқсат етілген операцияларды іске қосу және олардың орындалу мәртебесі мен нәтижелерін алу үшін автоматтандыру және оркестрлеу жүйелерімен интеграцияның API-ін немесе өзге де қолдау көрсетілетін тетіктерін ұсынуға тиіс. 2.5.10 Жүйе артықшылықты қолжетімділік берер алдында өтінім сәйкестендіргішін міндетті түрде көрсетуді және тексеруді, сондай-ақ кейінгі аудит үшін өтінім мен берілген қолжетімділік арасындағы байланысты сақтауды қамтамасыз ете отырып, IT-қызметтерді басқару (ITSM) жүйелерімен интеграцияны қолдауға тиіс. 2.6 Өндірушінің техникалық қолдауына қойылатын талаптар 2.6.1 Техникалық қолдау ақауларды диагностикалауды, Жүйенің жұмысы бойынша кеңес беруді және қолжетімді түзетулерді ұсынуды қамтуға тиіс. Шұғыл инциденттер 24/7 режимінде, қалған өтініштер жұмыс уақытында қызмет көрсетіледі. Жүгіну тәртібі мен ден қою мерзімдері жеткізілетін қолдау пакеті үшін өндірушінің регламентімен айқындалады. Өтініштер порталына, білім базасына қолжетімділік ұсынылуға тиіс. 3. Жеткізушіге қойылатын талаптар 4.1 Жеткізуші Жүйені ұсынумен бірге оны Тапсырыс берушінің инфрақұрылымында орнату және баптау жұмыстарын жүргізуге тиіс, бұл тараптардың Көрсетілген қызметтер актісімен расталады; 4.2 Жүйені орнату және баптау жұмыстары қашықтан қосылу әдісімен орындалуға тиіс; 4.3 Жүйе өндірушісінің техникалық қолдауының әрекет ету мерзімі ішінде Жеткізуші жұмыс күндері сағат 9.00-ден 18.00-ге дейін орыс және/немесе қазақ тілдерінде бірінші деңгейдегі жергілікті техникалық қолдау көрсетуге тиіс; 4.4 Жергілікті техникалық қолдау мыналарды қамтуға тиіс: сатып алынған лицензияларды белсендіруге көмектесу, орнату, баптау және әкімшілендіру мәселелері бойынша кеңес беру, Жүйе жұмысындағы ақаулар мен іркілістерді жою, Жүйенің жай-күйі мен баптауларының өндіруші ұсынымдарына сәйкестігін диагностикалау, жүйелік конфигурацияларды, ережелер мен саясаттарды баптау және түзету, жүйені өтінім бойынша және Тапсырыс берушімен келісілген жұмыс жоспары мен кестесі бойынша соңғы тұрақты нұсқаға дейін тұрақты әрі уақтылы жаңарту;
--	---

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)	
--	--

**Техническая спецификация
закупаемых услуг
(заполняется заказчиком)**

Наименование заказчика	Товарищество с ограниченной ответственностью "Digital Silk Road Company"
Наименование организатора	Товарищество с ограниченной ответственностью "Digital Silk Road Company"
№ конкурса:	№ 17778722-1
Наименование конкурса:	Ашық конкурс тәсілімен бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулерді электрондық мемлекеттік сатып алуды ұйымдастыру және өткізу туралы
Номер лота:	№ 88115828-OK1
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:	14199493.97
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	14199493.97
Срок оказания услуги:	по истечении 15 календарных дней с даты заключения договора по 31 декабря 2026 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	ТЕХНИЧЕСКОЕ ЗАДАНИЕ на оказание услуг по предоставлению лицензии на использование программного обеспечения для управления привилегированным доступом к информационным систем и контроля действий привилегированных пользователей 1. Общие требования 1.1 Поставщик должен оказать услуги по предоставлению лицензии на использование программного обеспечения для управления привилегированным доступом, контроля и аудита действий привилегированных пользователей (далее — Система). 1.2 Система должна поддерживать не менее 25 пользователей и неограниченное количество целевых систем. 1.3 Система должна состоять из следующих программных компонентов / модулей от одного производителя: □ централизованное управление — администрирование Системы, управление пользователями, ролями, правами доступа и политиками безопасности через единый веб-интерфейс; □ защищённое хранилище привилегированных учётных данных — централизованное хранение учётных данных в зашифрованном виде с разграничением и аудитом доступа; □ управление привилегированными сессиями (PAM Core) — предоставление доступа к целевым системам через прокси-компоненты Системы, мониторинг и запись сессий, контроль выполняемых команд и аудит действий пользователей; □ обнаружение устройств и учётных записей — автоматизированное сканирование инфраструктуры, выявление целевых систем, привилегированных учётных записей и SSH-ключей с возможностью импорта обнаруженных объектов в Систему; □ автоматизация привилегированных задач — выполнение административных команд и сценариев по запросу или расписанию без раскрытия привилегированных паролей пользователям, с разграничением прав, согласованием запуска и журналированием результатов; □ персональное и совместное защищённое хранилище — хранение паролей, файлов, заметок и API-секретов, генерация паролей и контролируемое предоставление совместного доступа. 1.4 Система должна быть предоставлена в виде подписки сроком на 12 месяцев с технической поддержкой от производителя на весь срок действия подписки с даты активации лицензии. 1.5 Система должна быть предоставлена для установки в отказоустойчивой конфигурации из двух узлов. Лицензия на второй узел для обеспечения отказоустойчивости должна быть включена в стоимость предоставления услуг на весь срок действия подписки. 1.6 Система должна устанавливаться локально в ИТ-инфраструктуре Заказчика на предоставленных им серверных ресурсах. 1.7 Серверные ресурсы и платформа виртуализации, соответствующие требованиям производителя Системы, предоставляются Заказчиком. 1.8 Срок оказания услуг по предоставлению Системы, включая работы по установке и настройке, должен составлять не более 70 календарных дней с даты подписания Договора. 1.9 Система должна быть предоставлена на электронный адрес Заказчика ib@nzhkeden.kz. 2. Технические требования 2.1 Требования к архитектуре и отказоустойчивости 2.1.1 Система должна развёртываться локально в ИТ-инфраструктуре Заказчика в виде готового виртуального программного комплекса (All-in-One Virtual
---	---

	Appliance), включающего предустановленную операционную систему, встроенную систему управления базами данных, веб-сервер и прикладные компоненты Системы. 2.1.2 Система должна поддерживать развёртывание на платформах виртуализации VMware ESXi и Microsoft Hyper-V с использованием предоставляемого производителем образа виртуального программного комплекса в совместимом формате. 2.1.3 Система должна поддерживать кластерное развёртывание из двух узлов с репликацией базы данных и синхронизацией файлов между узлами, а также восстановлением синхронизации после возвращения отказавшего узла в работу. 2.1.4 Система должна поддерживать использование арбитра для обеспечения кворума и автоматического переключения при отказе одного из двух узлов, а также использование встроенного или внешнего балансировщика нагрузки для распределения пользовательских подключений. 2.1.5 Система должна обеспечивать подключение неограниченного количества целевых систем без приобретения дополнительных лицензий на каждую целевую систему. Производительность и количество одновременно обрабатываемых сессий должны масштабироваться посредством увеличения вычислительных ресурсов и добавления узлов в соответствии с поддерживаемой производителем архитектурой. 2.1.6 Система должна обеспечивать подключение к целевым системам без установки локальных агентов либо с минимальным их использованием для отдельных функций. 2.1.7 Система должна обеспечивать проксирование привилегированных подключений, позволяющее исключить необходимость прямого сетевого доступа рабочих станций пользователей к целевым системам. 2.1.8 Система должна иметь встроенные средства резервного копирования конфигурации, учётных данных и записей сессий. Резервные копии должны храниться в зашифрованном виде. 2.1.9 Система должна обеспечивать защищённое резервное копирование привилегированных учётных данных и возможность авторизованного восстановления доступа к сохранённым паролям при недоступности Системы. 2.1.10 Система должна обеспечивать хранение паролей, SSH-ключей и иных аутентификационных данных в зашифрованном виде с использованием алгоритма AES-256 либо алгоритма с сопоставимой или более высокой криптографической стойкостью. 2.2 Функциональные требования 2.2.1 Система должна обеспечивать централизованное управление доступом к привилегированным учётным записям, аудит действий и мониторинг активности пользователей при подключении к целевым системам. 2.2.2 Система должна иметь защищённое хранилище учётных данных и секретов с разграничением доступа к отдельным объектам для пользователей и групп на основании политик доступа. 2.2.3 Система должна обеспечивать подключение к целевым системам по протоколам SSH, включая аутентификацию с помощью SSH-ключей, RDP, HTTP/HTTPS и SFTP, а также доступ к приложениям, опубликованным посредством Microsoft RemoteApp. 2.2.4 Система должна поддерживать использование стандартных клиентских приложений удалённого доступа и администрирования, в том числе установленных локально на рабочих станциях
--	--

	пользователей, без раскрытия пользователям сохранённых паролей и SSH-ключей. 2.2.5 Система должна поддерживать подключение к базам данных с использованием специализированных клиентских приложений для администрирования и разработки без раскрытия сохранённых паролей пользователям. 2.2.6 Система должна обеспечивать доступ к целевым системам через SSH-прокси из терминала пользователя без необходимости использования веб-браузера или графической среды. 2.2.7 Система должна обеспечивать запуск SSH, RDP, RemoteApp и HTTP/HTTPS сессий в окне (посредством) веб-браузера без необходимости использования отдельных клиентских приложений, установленных на рабочей станции пользователя. 2.2.8 Система должна обеспечивать управление использованием буфера обмена и передачей файлов в привилегированных сессиях, включая включение, отключение и ограничение соответствующих возможностей на основании политик доступа, типа подключения, пользователя, группы пользователей, целевой системы и подсети источника подключения. 2.2.9 Система должна поддерживать передачу файлов через веб-интерфейс привилегированных сессий, в том числе посредством перетаскивания файлов. 2.2.10 Для RDP-сессий через веб-клиент должна поддерживаться загрузка файлов с рабочей станции пользователя с последующим доступом к ним в удалённой сессии через подключаемый виртуальный или сетевой диск. 2.2.11 Для SSH/SFTP-сессий через веб-клиент должна поддерживаться загрузка и выгрузка файлов между рабочей станцией пользователя и целевой системой. 2.2.12 Для HTTP/HTTPS-сессий через веб-клиент должна поддерживаться загрузка и скачивание файлов при наличии соответствующих разрешений. 2.2.13 Система должна обеспечивать возможность запроса второго фактора аутентификации при запуске привилегированной сессии и при просмотре пароля. 2.2.14 Система должна поддерживать подключение к целевым системам через прокси с использованием персональных учётных данных пользователя, вводимых вручную при установлении соединения, без необходимости их предварительного сохранения в хранилище, с обеспечением контроля и записи сессии. 2.2.15 Система должна обеспечивать автоматическую подстановку пароля привилегированной учётной записи при повышении привилегий посредством sudo в рамках сессии. 2.2.16 Система должна обеспечивать контроль выполняемых команд и реагирование на запрещённые действия, включая блокировку сессии или пользователя. 2.2.17 Система должна обеспечивать проверку сетевой доступности целевого устройства при его регистрации с отображением результата проверки в интерфейсе. 2.2.18 Система должна обеспечивать привязку сертификатов к учётным данным, используемым для подключения к целевым системам, а также защищённое хранение SSL/TLS-сертификатов и соответствующих закрытых ключей. 2.2.19 Система должна поддерживать защищённое подключение к базам данных с использованием SSL/TLS-сертификатов. 2.2.20 Система должна поддерживать подключение к управляемым базам данных PostgreSQL в облачных и гибридных инфраструктурах, включая Microsoft
--	--

	Azure, Amazon Web Services и Oracle Cloud Infrastructure, при наличии сетевой доступности и совместимых механизмов подключения. 2.2.21 Система должна обеспечивать настройку требований к генерируемым паролям в соответствии с парольной политикой Заказчика. 2.2.22 Система должна обеспечивать автоматическую смену паролей привилегированных учётных записей операционных систем, баз данных и сетевого оборудования с возможностью расширения перечня поддерживаемых целевых систем. 2.2.23 Система должна поддерживать автоматическую смену паролей через веб-интерфейсы целевых систем с использованием HTTP/HTTPS. 2.2.24 Система должна обеспечивать автоматическую смену паролей по расписанию и через настраиваемый интервал после просмотра пароля пользователем. 2.2.25 Система должна поддерживать создание и редактирование администраторами пользовательских шаблонов смены паролей с использованием стандартных протоколов и интерфейсов, включая выбор соответствующего исполнителя или типа подключения. 2.2.26 Система должна обеспечивать автоматическую проверку актуальности сохранённых паролей и генерацию пароля по запросу пользователя с соответствующими полномочиями. 2.2.27 Система должна обеспечивать управление SSH-ключами, включая их ротацию и публикацию открытой части нового ключа на целевых устройствах. 2.2.28 Система должна поддерживать временное предоставление привилегированного доступа, в том числе механизмы Just-in-Time либо функционально аналогичные механизмы, с автоматическим отзывом предоставленных прав по истечении установленного срока. 2.2.29 Система должна поддерживать разделение полномочий при доступе к особо чувствительным учётным данным, предусматривающее невозможность получения полного пароля одним пользователем. 2.2.30 Система должна обеспечивать автоматизированное обнаружение устройств и связанных с ними учётных данных с использованием штатных сетевых протоколов без установки локальных агентов либо с минимальным их использованием. 2.2.31 При обнаружении должны выявляться пользователи, привилегированные и доменные учётные записи, SSH-ключи, сертификаты и службы Windows, связанные с учётными данными. 2.2.32 Система должна обеспечивать обнаружение серверов Linux/Unix и Windows, баз данных, рабочих станций и сетевых устройств, включая межсетевые экраны, маршрутизаторы, коммутаторы и балансировщики нагрузки. 2.2.33 Система должна обеспечивать сбор сведений об обнаруженных объектах, включая имя узла, IP-адрес, перечень учётных данных, тип привилегий, дату последнего доступа и сведения об изменении пароля, при доступности соответствующих данных на целевой системе. 2.2.34 Система должна обеспечивать автоматический импорт обнаруженных объектов в защищённое хранилище на основании заранее настроенных правил, словарей или шаблонов классификации. 2.2.35 Система должна иметь встроенную ролевую модель доступа с возможностью создания пользовательских ролей и назначения необходимых полномочий. 2.2.36 Система должна обеспечивать разграничение доступа по целевым системам,
--	--

	группам целевых систем и привилегированным учётным записям. 2.2.37 Система должна обеспечивать раздельное назначение прав на использование привилегированной учётной записи для подключения и на просмотр её пароля. 2.2.38 Система должна поддерживать встроенную двухфакторную аутентификацию и возможность использования внешних провайдеров многофакторной аутентификации. 2.2.39 Система должна обеспечивать предоставление доступа на ограниченный период времени, по дням недели и времени суток, а также после согласования уполномоченным пользователем или группой согласующих. 2.2.40 Система должна обеспечивать автоматическую блокировку источников подключения при выявлении подозрительной активности или многократных неуспешных попыток аутентификации. 2.2.41 Система должна обеспечивать ручную блокировку и разблокировку IP-адресов или хостов администратором. 2.2.42 Система должна обеспечивать автоматическую запись привилегированных сессий, текстовое протоколирование действий в поддерживаемых типах сессий и сквозной поиск текста по журналам завершённых сессий. 2.2.43 Система должна обеспечивать просмотр активных сессий в реальном времени, а также их приостановку и принудительное завершение уполномоченными пользователями. 2.2.44 Система должна обеспечивать построение статистических моделей активности в разрезе пользователей-администраторов, привилегированных учётных записей и целевых систем. 2.2.45 Система должна обеспечивать выявление аномалий на основании отклонений от статистических моделей с настройкой порогов и действий реагирования, включая блокировку пользователя, блокировку сессии или направление сессии на аудит. 2.2.46 Система должна обеспечивать автоматическое и ручное направление сессий на аудит с возможностью добавления комментариев аудитором и отметки о завершении проверки. 2.2.47 Система должна обеспечивать настройку сроков хранения записей сессий и исключение выбранных записей из автоматического удаления по истечении срока хранения. 2.2.48 Система должна обеспечивать централизованное выполнение административных команд и сценариев на целевых системах без предоставления пользователю прямого доступа к привилегированным учётным данным. 2.2.49 Система должна обеспечивать разграничение прав на выполнение задач, запуск по запросу или расписанию, согласование запуска ответственным сотрудником, отслеживание статуса и получение результата выполнения. 2.2.50 Система должна обеспечивать персональное и совместное защищённое хранение паролей, файлов, заметок и API-секретов, генерацию паролей и предоставление доступа к объектам другим пользователям на основании назначенных разрешений. 2.2.51 Система должна обеспечивать регистрацию событий открытия сессий, просмотра и смены паролей, попыток выполнения запрещённых команд, создания, изменения и удаления объектов конфигурации, изменения политик доступа и параметров интеграции. 2.2.52 Система должна обеспечивать регистрацию эксплуатационных событий, включая потерю и восстановление связности с целевыми узлами, результаты
--	---

	резервного копирования и ошибки выполнения операций смены паролей. 2.2.53 Система должна обеспечивать настраиваемые процедуры согласования доступа к просмотру паролей и запуску привилегированных сессий с назначением уполномоченных согласующих. 2.2.54 Система должна поддерживать многоуровневое последовательное согласование запросов в соответствии с установленной иерархией согласующих. 2.2.55 Система должна обеспечивать обязательное указание обоснования и запрашиваемого периода доступа в соответствии с настроенной политикой. 2.2.56 Система должна обеспечивать изменение темы и текста электронных уведомлений через административный веб-интерфейс с поддержкой шаблонных переменных для автоматической подстановки данных, включая номер и статус запроса, инициатора и согласующего, имя и IP-адрес целевой системы, имя учётной записи, обоснование и запрашиваемый период доступа, а также ссылки для согласования или отклонения запроса. 2.3 Требования к отчетности 2.3.1 Система должна обеспечивать формирование отчётов на основании заданных шаблонов и предоставлять панели мониторинга состояния и использования Системы. 2.3.2 Система должна обеспечивать формирование отчётности по событиям информационной безопасности, действиям пользователей и администраторов, изменениям политик доступа и настроек интеграции. 2.3.3 Система должна обеспечивать формирование отчётности по использованию привилегированных учётных записей, включая просмотр, выдачу, смену, проверку и восстановление паролей. 2.3.4 Система должна предоставлять отчёт о пользователях, просматривавших актуальные пароли целевых систем, а также историю доступа пользователей к паролям за выбранный период. 2.3.5 Система должна обеспечивать формирование отчётов по привилегированным сессиям с указанием пользователя, целевой системы, учётной записи, времени начала и окончания, длительности и источника подключения. 2.3.6 Система должна обеспечивать отчётность по управляемым учётным записям, срокам действия паролей, датам последней смены паролей, длительному отсутствию смены паролей и предстоящим операциям ротации. 2.3.7 Система должна обеспечивать отчётность по успешным и неуспешным операциям смены паролей с указанием даты и времени, целевой системы, учётной записи, результата и описания ошибки при её наличии. 2.3.8 Система должна обеспечивать отчётность по резервному копированию, ошибкам выполнения операций, доступности компонентов и состоянию связности с целевыми узлами. 2.3.9 Система должна обеспечивать отчётность по уведомлениям и оповещениям с указанием типа события, уровня критичности, получателя и статуса отправки. 2.3.10 Система должна обеспечивать отчётность по попыткам выполнения запрещённых команд и связанным с ними действиям реагирования. 2.3.11 Система должна обеспечивать отчётность по зарегистрированным пользователям, их ролям, группам, профилям доступа и назначенным полномочиям. 2.3.12 Система должна обеспечивать экспорт видеозаписей привилегированных сессий для передачи уполномоченным третьим лицам и
--	--

	просмотра вне Системы. 2.3.13 Система должна обеспечивать настройку состава отображаемых в отчётах данных и автоматическую отправку отчётов указанным получателям по расписанию. 2.3.14 Система должна предоставлять отчёты по выявленным аномалиям привилегированных сессий и операций просмотра учётных данных с отображением рассчитанной оценки риска и признаков отклонения от типичного поведения. 2.4 Требования к интерфейсу 2.4.1 Система должна предоставлять единый веб-интерфейс для централизованного администрирования, управления пользователями, ролями, политиками доступа, целевыми системами и учётными данными. Веб-интерфейс должен поддерживать русский, английский, немецкий, испанский, французский, польский и португальский языки. Пользовательский интерфейс должен отображать доступные пользователю целевые системы, учётные данные и функции в соответствии с назначенными правами. 2.4.2 Веб-интерфейс должен обеспечивать запуск разрешённых привилегированных сессий, подачу запросов на доступ, согласование запросов и просмотр статуса их обработки. 2.4.3 Интерфейс должен обеспечивать просмотр активных и завершённых сессий, поиск по журналам, работу аудитора с записями сессий и доступ к отчётам в соответствии с полномочиями пользователя. 2.4.4 Интерфейс должен обеспечивать настройку и запуск привилегированных задач, просмотр статуса выполнения и результатов операций. 2.4.5 Система должна иметь мобильное приложение для Android версии 10 и выше, доступное через Google Play, для защищённого доступа к разрешённым объектам персонального и совместного хранилища в соответствии с правами пользователя. 2.5 Требования к интеграциям со сторонними системами 2.5.1 Система должна поддерживать аутентификацию пользователей с учётными записями Microsoft Active Directory посредством LDAP/LDAPS. 2.5.2 Система должна поддерживать синхронизацию групп Microsoft Active Directory с назначением пользователям ролей и доступа к ресурсам в соответствии с их принадлежностью к группам. 2.5.3 Система должна поддерживать интеграцию с внешними провайдерами многофакторной аутентификации по протоколу RADIUS, а также интеграцию с внешними поставщиками удостоверений (IdP) по протоколам SAML 2.0 и OpenID Connect для единого входа (SSO) с выполнением многофакторной аутентификации на стороне IdP. 2.5.4 Система должна поддерживать использование одноразовых паролей TOTP, формируемых совместимыми приложениями-аутентификаторами, а также специализированные интеграции с провайдерами RSA Authenticator, Duo Security и AuthID. 2.5.5 Система должна поддерживать аутентификацию пользователей с использованием сертификатов X.509. 2.5.6 Система должна поддерживать интеграцию с внешними провайдерами многофакторной аутентификации. 2.5.7 Система должна обеспечивать передачу событий безопасности и эксплуатационных событий во внешние системы мониторинга и SIEM. 2.5.8 Передаваемые события должны иметь структурированный формат и содержать идентификатор, тип, уровень критичности, описание события, идентификатор процесса
--	--

	и дополнительные поля с контекстом события. 2.5.9 Система должна предоставлять API либо иные поддерживаемые механизмы интеграции с системами автоматизации и оркестрации для запуска разрешённых операций и получения статуса и результатов их выполнения. 2.5.10 Система должна поддерживать интеграцию с системами управления ИТ-услугами (ITSM), обеспечивая обязательное указание и проверку идентификатора заявки перед предоставлением привилегированного доступа, а также сохранение связи между заявкой и предоставленным доступом для последующего аудита. 2.6 Требования к технической поддержке производителя 2.6.1 Техническая поддержка должна включать диагностику неисправностей, консультации по работе Системы и предоставление доступных исправлений. Срочные инциденты обслуживаются в режиме 24/7, остальные обращения — в рабочие часы. Порядок обращения и сроки реакции определяются регламентом производителя для поставляемого пакета поддержки. Должен предоставляться доступ к portalу обращений, базе знаний. 3. Требования к Поставщику 4.1 Поставщик вместе с предоставлением Системы должен произвести работы по ее установке и настройке в инфраструктуре Заказчика, что подтверждается сторонами Актом оказанных услуг; 4.2 Работы по установке и настройке Системы должны выполняться методом удаленного подключения; 4.3 В течение срока действия технической поддержки от производителя Системы Поставщик должен оказывать локальную техническую поддержку первого уровня на русском и/или казахском языках с 9.00 до 18.00 в рабочие дни; 4.4 Локальная техническая поддержка должна включать: помощь в активации приобретенных лицензий, консультирование по вопросам установки, настройки и администрирования, устранение сбоев и отказов в работе Системы, диагностика состояния Системы и настроек на соответствие рекомендациям производителя, настройка и корректировка системных конфигураций, правил и политик, регулярное своевременное обновление системы до последней стабильной версии по заявке и согласованному плану и графику работ с Заказчиком;
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)	