Тендерлік құжаттамаға
9-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы	"Ұлттық геологиялық қызмет" акционерлік қоғамы
Ұйымдастырушының атауы	"Ұлттық геологиялық қызмет" акционерлік қоғамы
Тендердің №	№ 17944131-1
Тендердің атауы	Деректердің бұзылуын болдырмау жүйесін (DLP)пайдалану құқығына лицензия беру жөніндегі қызметтер
Лоттың №	№ 83859126-ОТ1
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
Бірлік бағасы, қосылған құн салығын қоспағанда*	13760440
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома*	13760440
Қызмет көрсету мерзімі*	согласно технической спецификации
Аванстық төлем мөлшері*	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Техникалық ерекшелік Бағдарламалық қамтамасыз етуді (DLP) пайдалану құқығына лицензиялар беру жөніндегі қызметтер Жалпы талаптар Осы техникалық ерекшелікте DLP жүйесін ілеспе қызметтермен бірге сатып алуға қойылатын жалпы талаптар (бұдан әрі – Қызмет) баяндалған. Техникалық қолдау 12 ай ішінде көрсетіледі. Жеткізу мекенжайы: Астана қаласы, Қонаев көшесі, 12/2. Ұсынылатын барлық сипаттамалар техникалық ерекшелікте көрсетілген техникалық сипаттамаларға сәйкес келуі немесе олардан асып түсуі тиіс. Қызмет көмінде 100 жұмыс станциясында пайдалануды қамтамасыз етуі тиіс. Анықтамалар мен қысқартулар: БҚ – бағдарламалық қамтамасыз ету; КА – конфиденциалды ақпарат; ТҚ – техникалық қолдау. Жеткізу мерзімі: Шартқа қол қойылған күннен бастап ілеспе қызметтерді ескере отырып, 16 (он алты) жұмыс күні ішінде. Әлеуетті өнім берушіге қойылатын талаптар: Өтінімнің құрамына қойылатын талаптар / Әлеуетті өнім берушіге қойылатын талаптар: 1. Әлеуетті өнім берушілердің өтінімдерін салыстыру және олардың техникалық ерекшелік талаптарына сәйкестігін анықтау үшін Әлеуетті өнім беруші өзінің өтінімі құрамында өндірушінің атауын (және/немесе зауыт-өндірушіні) және лицензияның парт-нөмірін көрсетуге тиіс. Ұсынылатын шешім туралы ақпарат ашық дереккөздерде қолжетімді болуға тиіс. 2. Контрафактілік өнімді жеткізуге жол бермеу мақсатында Әлеуетті өнім беруші өтінім құрамында жабдық өндірушісінен немесе оның Қазақстан Республикасы аумағындағы ресми өкілінен жүйені жеткізу құқығына берілген авторизациялық хатты ұсынуға тиіс. Ұсынылған хаттарда мынадай деректемелер көрсетілуге тиіс: Тапсырыс беруші, Өнім беруші және сатып алу нөмірі. Ілеспе қызметтер: Өнім беруші жүйені орнатуды және баптауды жүзеге асыруға тиіс. Сертификатталмаған мамандардың жұмыстарды орындауына жол берілмейді. Енгізу бойынша мамандар жеткізілетін жүйені өндірушіден алынған сертификаттарға ие болуға тиіс. Жұмыстарды қашықтан жүргізуге жол беріледі. Ілеспе қызметтер шеңберінде Өнім беруші Тапсырыс берушінің мамандарына жүйемен жұмыс істеу бойынша нұсқама өткізуге тиіс. 1. Функционалдық талаптар 1.1. Бағдарламалық қамтамасыз ету (БҚ) корпоративтік деңгейдегі жүйе (Enterprise DLP) болуға және соңғы нүктелерде орнатылған агенттің көмегімен құпия деректердің жылыстауынан соңғы нүктелерді қорғау функционалдығына (EndPoint DLP), сондай-ақ желілік арналар бойынша құпия деректердің жылыстауын бақылау функционалдығына (Network DLP) ие болуға тиіс. 1.2. Бағдарламалық қамтамасыз ету жұмыс станцияларында және файлдық серверлерде орналасқан құпия ақпаратты іздеу мүмкіндігін қамтамасыз етуге тиіс (табылған файлдарды карантинге ауыстыру және олардың орнына осындай ауыстырудың себептерін түсіндіретін ақпараттық/мәтіндік файлдарды қалдыру мүмкіндігімен). 1.3. БҚ құпия ақпараттың ықтимал жылыстауының мынадай арналарына бақылау жүргізуге тиіс: - шығыс SMTP-қосылымдары; - шығыс HTTP-қосылымдары; - шығыс HTTPS-қосылымдары; - шығыс IM-қосылымдары; - ақпаратты сыртқы тасымалдағыштарға және ақпараттық ресурстарға көшіру; - ақпаратты жергілікті/желілік принтерде басып шығару. 1.4. БҚ мынадай функционалдық мүмкіндіктерді қамтамасыз етуге тиіс: - корпоративтік электрондық пошта жүйесі арқылы құпия ақпараттың жария етілуіне жол бермеу; - құпия ақпаратты қамтитын шығыс электрондық хаттарды бұғаттау мүмкіндігі; - Интернетке корпоративтік қол жеткізу жүйесі арқылы құпия ақпараттың жария етілуіне жол бермеу; - HTTP/HTTPS-трафиктен құпия ақпаратты алу мүмкіндігі; - HTTP/HTTPS-трафикті бұғаттау мүмкіндігі; - құпия ақпараттың жария етілуіне жол бермеу және жылыстау арналарын мониторингтеу, атап айтқанда: желілік қалтадан құпия ақпаратты жергілікті қатты дискілерге көшіру, құпия ақпаратты алынбалы тасымалдағыштарға көшіру, құпия ақпаратты жергілікті және желілік принтерлерге, сондай-ақ факс арқылы жіберу және көшіру/қою операциялары кезінде алмасу буферінің мазмұнын қорғау; - құпия ақпараттың болуына жергілікті қатты дискілерді, оның ішінде белгіленген кесте бойынша, сканерлеу және табылған файлдарды ауыстыру мүмкіндігі; - графикалық объектілердің (PDF файлдары, кескіндер және т.б.) ішіндегі мәтіндік ақпаратты, сондай-ақ осындай объектілердегі графикалық бейнелерді (жауапты тұлғалардың қолтаңбалары, мөрлер, логотиптер және т.б.) тану мүмкіндігі; - құпия деректерді сканерлеу және олардың «цифрлық ізтаңбаларын» жасау мүмкіндігі, бұл ретте қорғалатын деректерді сәйкестендірудің түйіршіктілігі немесе ең төменгі шекті мөлшері (хэш-сома) қауіпсіздік оқиғасын іске қосатын мән ретінде 64 байттан басталуға, ал шекті мәні 128 байттан басталуға тиіс; - ұсынылған құпия құжаттар негізінде өзін-өзі оқыту және кейіннен ұқсас құжаттарды бұғаттау мүмкіндігі; - соңғы нүкте корпоративтік желіден ажыратылған немесе желілік қосылым жоғалған жағдайда клиенттер мен бағдарламалық модульдердің (анықтау серверлерінің) автономды жұмыс істеу мүмкіндігі; - қауіпсіздік саясаттарын орталықтандырылған басқару мүмкіндігі; - БҚ қауіпсіздік саясатына нақты уақыт режимінде жедел өзгерістер енгізу, сондай-ақ қолданыстағы қағидалар мен баптауларды өзгерту және жаңаларын қосу мүмкіндігі; - БҚ саясатының бұзылғаны туралы автоматты хабарламаларды баптау; - қауіпсіздік саясатының бұзылуына әрекет етудің әртүрлі нұсқаларын баптау; - қауіпсіздік саясатының бұзылған күні және фактілері бойынша есептерді баптау және қалыптастыру; - басқару консолімен орыс, ағылшын және қазақ тілдерінде жұмыс істеу мүмкіндігі; - басқару консолінде аутентификациялау үшін қолданыстағы Active Directory есептік жазбаларын пайдалану мүмкіндігі; - AD есептік жазбасының атрибуттарын (аты, телефоны, бөлімі, лауазымы және т.б.) тікелей консолінен қарау мүмкіндігі. 2. Функционалдық мүмкіндіктер 2.1. Операцияларды бақылау мүмкіндігі: - құпия ақпаратты алынбалы тасымалдағыштарға (USB, CompactFlash, SD) жазу; - қосымша модульдерді орналастыруды (орнатуды) талап етпейтін кіріктірілген «Құрылғыларды басқару» функционалы; - КИ-ді басып шығару (желілік және жергілікті принтерлер); - КИ-ді алмасу буферіне көшіру; - КИ-ді жергілікті дискілерге жазу; - КИ-ді CD/DVD дискілеріне жазу; - қосымшалардың КИ-ге қол жеткізуін бақылау (оның ішінде КИ бар файлдарды Skype және Teams арқылы жіберу); - КИ деректерін HTTP хаттамасы бойынша жіберу; - КИ деректерін HTTPS хаттамасы бойынша жіберу; - пошта клиенті деңгейінде SMTP бақылауы; - КИ файлдарын желілік ресурстарға, оның ішінде Office 365 ресурстары мен сервистеріне көшіру; - соңғы нүктелер деңгейінде Print Screen функциясын орталықтандырылған бұғаттау мүмкіндігімен бақылау; - соңғы нүктелердегі агентке саясаттар мен конфигурацияларды оның орналасқан жеріне байланысты: корпоративтік желі ішінде немесе корпоративтік желіден тыс жерде баптау және қолдану мүмкіндігі; - құжаттарды сыртқы тасымалдағыштарға жаппай көшіруді бақылау мүмкіндігі. Жүйе пайдаланушының белгілі бір уақыт аралығында сыртқы дискіге көшіре алатын файлдарының санын бақылауға тиіс; - сыртқы тасымалдағыштарға көшіру кезінде құжаттары шифрлау мүмкіндігі. Құпиясөзді пайдаланушылардың да, БҚ әкімшісінің де белгілеу мүмкіндігі; - MTP хаттамасын бұғаттау мүмкіндігі; бақылау КИ-ді анықтауды да, белгіленген саясаттарға сәйкес КИ-ді беруді бұғаттауды (болдырмауды) да қамтамасыз етуге тиіс. 2.2. Агентті Windows және Linux операциялық жүйелерінде орналастыру мүмкіндігі. 2.3. Оқиғаларға әрекет ету мүмкіндігі: жауапты тұлғаға немесе ақпарат иесіне автоматты түрде хабарлау. 2.4. Оқиғаны эскалациялау және қосымша әрекеттерді (мысалы, КИ-ді шифрлау, КИ-ді ауыстыру және т.б.) бастамашылық ету мүмкіндігі. 2.5. Тануды (OCR – таңбаларды оптикалық тану) қосымша үшінші тарап бағдарламалық қамтамасыз етуін пайдаланбай, кіріктірілген меншікті технология/механизм қамтамасыз етуге тиіс; тану агент деңгейінде жүзеге асырылуға тиіс. - мәтінді тану латын және кириллица әліпбилерін әртүрлі тілдерді қолдай отырып қамтамасыз етуге тиіс; - мынадай форматтардағы сканерленген кескіндерді тану: PDF, BMP, JPEG, PNG, TIFF; - OCR жұмысының бағыттары: - жергілікті сканерлеу; - КИ-ді сыртқы тасымалдағышқа көшіру; - КИ-ді файлдық серверге көшіру; - КИ-ді HTTP/HTTPS арқылы жіберу; - КИ-ді Webmail хаттамасы бойынша жіберу; - SMTP хаттамасы бойынша жіберу. 2.6. Пайдаланушылардың USB-ге қол жеткізу деңгейлерін реттеу мүмкіндігі. 2.7. Ubuntu және CentOS жүйелерінде соңғы нүкте модулін мынадай мүмкіндіктермен орналастыру мүмкіндігі: - тыныштық күйіндегі КИ-ді анықтау; - КИ-дің алынбалы тасымалдағыштарға жылыстауын бақылау, оның ішінде осындай ақпаратты бұғаттау және тіркеу; - HTTP/HTTPS арналары арқылы КИ-дің жылыстауын бақылау; - Webmail хаттамасы арқылы КИ-дің жылыстауын бақылау. 2.8. Бағдарламалық қамтамасыз ету пайдаланушының компьютерге сенімсіз USB-накопительді қосқаны туралы әкімшіге алдын ала хабарлау мүмкіндігін қолдауға тиіс. 3. Интерфейске қойылатын талаптар 3.1. Бағдарламалық қамтамасыз ету интерфейстің мынадай тілдерін қолдауға тиіс: ағылшын, орыс, қазақ тілдері. 3.2. Бағдарламалық қамтамасыз етуді және оқиғаларды басқаруға арналған бірыңғай веб-интерфейс болуы тиіс. 3.3. Шешім интерфейсі арқылы соңғы нүктелердегі агенттерді жою мүмкіндігі болуы тиіс. 3.4. Шешім интерфейсі арқылы соңғы нүктелердегі агенттерді жаңарту мүмкіндігі болуы тиіс. 4. Жіктеуге қойылатын талаптар 4.1. Бағдарламалық қамтамасыз ету Microsoft Office, Microsoft Outlook және Web Outlook 365 файлдарын кіріктірілген жіктеуді қолдауға тиіс. 4.2. Жіктеу файл жабылған кезде емес, файл сақталған кезде орындалуға тиіс. 4.3. Бағдарламалық қамтамасыз ету нақты уақыт режимінде және күту режимінде деректерді іздеу кезінде мәтіндік құжаттар мен кескіндерді жіктеуді қолдауға тиіс. 4.4. Бағдарламалық қамтамасыз ету Outlook шақыруларын жіктеуді қолдауға тиіс. 4.5. Бағдарламалық қамтамасыз ету деректерді жіктеу кезінде құжатқа сутаңбасын (watermark) қою мүмкіндігін қолдауға тиіс. 4.6. Бағдарламалық қамтамасыз ету басып шығару кезінде құжаттарды жіктеу мүмкіндігіне ие болуға тиіс. 4.7. Бағдарламалық қамтамасыз ету пайдаланушының экранына сутаңбасын қою мүмкіндігіне ие болуға тиіс, бұл ретте оның орналасуын, көрінуін таңдауға, сондай-ақ сутаңбаны бүкіл экранға қоюға мүмкіндік болуы тиіс. 4.8. Бағдарламалық қамтамасыз ету нақты уақыт режимінде файлдарды ғана емес, қалталарды да жіктеуге тиіс. 4.9. Бағдарламалық қамтамасыз ету файлдарды алмасу буфері деңгейінде көшіруді бақылауға және файлдың жіктеу деңгейіне байланысты осындай операцияны бұғаттау мүмкіндігіне ие болуға тиіс. 4.10. Бағдарламалық қамтамасыз ету Microsoft Office файлдарының скриншоттарын бақылауға және жіктелген файлдар үшін скриншот жасау әрекеттерін бұғаттауға тиіс. 4.11. Әрбір жіктеу деңгейіне бірегей түс беру мүмкіндігі. 4.12. Жіктеуді орындаған автордан басқа тұлғалардың файлдарды қайта жіктеуіне тыйым салу мүмкіндігі. 4.13. Құпия электрондық хаттың тақырыбын өзгерту мүмкіндігі. 4.14. Office 365 веб-хаттарын жіктеу мүмкіндігі. 4.15. Үшінші тараптардың жіктеу жүйелерімен интеграциялану мүмкіндігі. 5. Қосымша талаптар 5.1. БҚ мамандандырылған стандартты хаттамаларды (MTA) пайдалана отырып, үшінші тараптардың пошта сервистерімен интеграцияны қолдауға тиіс. 5.2. БҚ мамандандырылған стандартты хаттамаларды (ICAP) пайдалана отырып, үшінші тараптардың веб-сервистерімен (шлюздермен) интеграцияны қолдауға тиіс. 5.3. БҚ Office 365 бұлтты ортасымен интеграциялауды қолдауға тиіс, бұл осы ортадағы КИ-ге байланысты оқиғаларды БҚ орталықтандырылған консолінде қарау мүмкіндігін қамтамасыз етеді. Бұл OneDrive және OneDrive for Business жүйелеріндегі файлдармен жұмыс істеу мүмкіндігін қамтиды. 5.4. Қатысушы техникалық қолдау (ТҚ) шеңберінде Тапсырыс берушінің аумағында жүйені толық іске асыруды және баптауды, сондай-ақ жүйені және оның компоненттерін пайдалану мен әкімшілендіру бойынша консультациялық қолдауды қамтамасыз етуге қабілетті болуға тиіс. Жүйенің ТҚ-ға қойылатын талаптар: - Тапсырыс берушінің аумағында жүйені толық іске асыру және баптау, жүйені және оның компоненттерін пайдалану мен әкімшілендіру бойынша Тапсырыс берушінің кемінде үш маманына консультациялық қолдау көрсету; - Тапсырыс берушінің персоналына (кемінде 3 адам) құпия ақпараттың жылыстауын болдырмау жүйесін орнату және баптау бойынша техникалық консультациялар өткізу. 5.5. «Off-Premise DLP» функциясының болуы, бұл ретте агент орталықтандырылған консольге қосылған кезде қорғау саясаттарының бір жиынтығын, ал автономды режимде басқа саясаттар жиынтығын қолдануға тиіс. 5.6. Агенттің трафикті ұстап қалуы пайдаланушы браузеріне плагин орнатылмай жүзеге асырылуға тиіс. 5.7. Жүйеде әрбір функция үшін файлдарды сканерлеудің ең жоғары уақытын жеке белгілеу мүмкіндігі болуы тиіс. 5.8. Active Directory-ге байланыстырмай пайдаланушы топтарын құру мүмкіндігі болуы тиіс. 5.9. БҚ белгілі бір веб-сайттар үшін пакеттерді шифрдан шығармай тексеруді толық айналып өту мүмкіндігіне ие болуға тиіс. 5.10. Алынбалы тасымалдағыштардан файлдарды жою мүмкіндігін бұғаттау функционалы болуы тиіс. 5.11. Агенттер үшін жергілікті деңгейде рұқсат етілген IP-мекенжайларды көрсету мүмкіндігі. 5.12. Жүйемен өзара әрекеттесуді неғұрлым ыңғайлы ету үшін AI-көмекшісінің болуы. 5.13. БҚ желілік қойманы, SharePoint, OneDrive жүйелерін аудиттеу мүмкіндігін қолдауға тиіс; файлдардың ашылуын, өзгертілуін, жойылуын және атауының өзгертілуін мониторингтеу жүзеге асырылуға тиіс. 5.14. БҚ агенті жасырын режимде жұмыс істеуді қолдауға тиіс; барлық процестер соңғы пайдаланушыдан жасырылуға тиіс. 5.15. БҚ агенті мәтіндік хабарламалар мен файлдар үшін Telegram-ды онлайн және жергілікті тексеруді қолдауға 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)	

* мәліметтер сатып алу жоспарынан алынады (автоматты түрде көрсетіледі).

Ескерту:

1. Әрбір талап етілетін сипаттамалар, параметрлер, бастапқы деректер және қосымша шарттар бөлек жолда көрсетіледі.

2. Техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.

3. Өзге құжаттарда техникалық ерекшеліктің талаптарын белгілеуге жол берілмейді.

Приложение 9
к тендерной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Национальная геологическая служба"
Наименование организатора	Акционерное общество "Национальная геологическая служба"
№ тендера	№ 17944131-1
Наименование тендера	Услуги по предоставлению лицензий на право использования системы предотвращения утечки данных (DLP)
Номер лота	№ 83859126-ОТ1
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*	13760440
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*	13760440
Срок оказания услуги*	согласно технической спецификации
Размер авансового платежа*	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Техническая спецификация Услуги по предоставлению лицензий на право использования программного обеспечения(DLP) Общие требования В настоящей технической спецификации изложены общие требования по приобретению DLP системы с сопутствующими услугами (далее - Услуга). Техническая поддержка оказывается в течение 12 месяцев. Адрес поставки: г Астана, ул Кунаева 12/2. Все предложенные характеристики должны соответствовать или превосходить технические характеристики, указанные в технической спецификации. Услуга должна обеспечивать возможность использования не менее чем для 100 рабочих станции. Определения и сокращения: ПО – программное обеспечение; КИ – конфиденциальная информация; ТП – техническая поддержка. Срок поставки: в течение 16 дней со дня подписания Договора с учетом сопутствующих услуг. Требования к Потенциальному поставщику: Требования к составу заявки/требования к Потенциальному поставщику: 1. Для сопоставления заявок Потенциальных поставщиков и определения их соответствия требованиям технической спецификации, Потенциальный поставщик должен в составе своей заявки указать наименование производителя (и/или завод-изготовитель) и партномера лицензии. Информация о предлагаемом решении должна быть доступна в открытых источниках. 2. Во избежание поставки контрафактной продукции Потенциальный поставщик в составе заявки должен предоставить авторизационное письмо на право поставки системы от производителя оборудования либо его официального представителя на территории Республики Казахстан. В предоставленных письмах должны быть указаны следующие реквизиты: Заказчик, Поставщик и номер закупки. Сопутствующие услуги: Поставщик должен осуществить инсталляцию, настройку системы. Несертифицированные специалисты не будут допущены к работам. Специалисты по внедрению должны иметь сертификаты от производителя поставляемой системы. Допускается проведение работ удаленно. В рамках сопутствующих услуг Поставщик должен провести инструктаж специалистов Заказчика по работе с системой. 1. Функциональные требования 1.1. Программное обеспечение (ПО) должно быть системой корпоративного класса (Enterprise DLP) и обладать как функциональностью защиты конечных точек от утечки конфиденциальных данных с помощью агента, установленного на конечных точках (EndPoint DLP), так и функциональностью контроля утечки конфиденциальных данных по сетевым каналам (Network DLP). 1.2. Программное обеспечение должно обеспечивать возможность поиска конфиденциальной информации, расположенной на рабочих станциях и файловых серверах (с возможностью перемещения найденных файлов в карантин и оставления на их месте информационных/текстовых файлов с объяснением причин такого перемещения). 1.3. ПО должно контролировать следующие потенциальные каналы утечки конфиденциальной информации: • исходящие SMTP-соединения; • исходящие HTTP-соединения; • исходящие HTTPS-соединения; • исходящие IM-соединения; • копирование информации на внешние носители и информационные ресурсы; • печать информации на локальном/сетевом принтере. 1.4. ПО должно обеспечивать следующие функциональные возможности: • предотвращение разглашения конфиденциальной информации через корпоративную систему электронной почты; • возможность блокирования исходящих электронных писем, содержащих конфиденциальную информацию; • предотвращение разглашения конфиденциальной информации через корпоративную систему доступа в Интернет; • возможность извлечения конфиденциальной информации из HTTP/HTTPS-трафика; • возможность блокирования HTTP/HTTPS-трафика; • предотвращение разглашения конфиденциальной информации и мониторинг каналов утечки, а именно: копирование конфиденциальной информации из сетевой папки на локальные жесткие диски, копирование конфиденциальной информации на съемные носители, отправка конфиденциальной информации на локальные и сетевые принтеры, а также по факсу, и защита содержимого буфера обмена при операциях копирования/вставки; • возможность сканирования (в том числе по заданному расписанию) локальных жестких дисков сетевого конечного устройства на наличие конфиденциальной информации с возможностью перемещения найденных файлов; • возможность распознавания текстовой информации внутри графических объектов (файлы pdf, изображения и т.д.), а также графических изображений в таких объектах (подписи ответственных лиц, штампы, логотипы и т.д.); • возможность сканирования конфиденциальных данных и создания их «цифровых отпечатков», при этом гранулярность, или минимальный пороговый размер для сопоставления защищенных данных (хэш-сумма), который запускает событие безопасности, должен быть от 64 байт, с пороговым значением от 128 байт; • возможность самообучения на основе предоставленных конфиденциальных документов с последующей блокировкой аналогичных документов; • возможность автономной работы клиентов и программных модулей (серверов обнаружения) в случае отключения конечной точки от корпоративной сети или потери сетевого соединения; • возможность централизованного администрирования политик безопасности; • возможность вносить оперативные изменения в политику безопасности ПО в режиме реального времени, а также изменять существующие и добавлять новые правила и настройки; • настройка автоматических уведомлений о нарушениях политики ПО; • настройка различных вариантов реагирования на нарушения политики безопасности; • настройка и генерация отчетов по дате и фактам нарушений политики безопасности; • возможность работы с консолью управления на русском, английском и казахском языках; • возможность использования существующих учетных записей Active Directory для аутентификации в консоли управления; • возможность просмотра атрибутов учетной записи AD (имя, телефон, отдел, должность и т. д.) непосредственно из консоли . 2.1. Возможность контроля операций: • Запись конфиденциальной информации на съемные носители (USB, CompactFlash, SD); • Встроенная функциональность «Управление устройствами» без необходимости развертывания (установки) дополнительных модулей; • Печать КИ (сетевые и локальные принтеры); • Копирование КИ в буфер обмена; • Запись КИ на локальные диски; • Запись КИ на CD/DVD; • Контроль доступа приложений к КИ (в том числе передача файлов, содержащих КИ, через Skype и Teams); • Отправка данных КИ по протоколу HTTP; • Отправка данных КИ по протоколу HTTPS; • Контроль SMTP на уровне почтового клиента; • Копирование файлов КИ на сетевые ресурсы, включая ресурсы и сервисы Office 365; • Контроль функции Print Screen с возможностью централизованной блокировки на уровне конечных точек; • Возможность настройки и применения политик и конфигураций к агенту на конечных точках в зависимости от его местоположения: внутри корпоративной сети или за пределами корпоративной сети; • Возможность контроля массового копирования документов на внешние носители. Система должна контролировать количество файлов, которые пользователь может скопировать на внешний диск в течение определенного периода времени; • Возможность шифрования документов при копировании на внешние носители. Возможность установки пароля как пользователями, так и администратором ПО; • Возможность блокировки протокола MTP; контроль подразумевает возможность как обнаружения КИ, так и блокировки (предотвращения передачи) КИ (в соответствии с определенными политиками). 2.2. Возможность развертывания агента в ОС Windows и Linux. 2.3. Возможность реагирования на инциденты: автоматическое уведомление ответственного лица или владельца информации. 2.4. Возможность эскалации инцидента и инициирования дополнительных действий (таких как шифрование КИ, перемещение КИ и т. д.). 2.5. Распознавание (OCR — оптическое распознавание символов) должно обеспечиваться встроенной собственной технологией/механизмом без использования дополнительного стороннего программного обеспечения; оно должно осуществляться на уровне агента. • Распознавание текста должно поддерживать латинский и кириллический алфавиты с поддержкой различных языков. • Распознавание отсканированных изображений в следующих форматах: PDF, BMP, JPEG, PNG, TIFF. • Направление работы OCR: о локальное сканирование; о копирование КИ на внешний носитель; о копирование КИ на файловый сервер; о отправка КИ по HTTP/HTTPS; о отправка КИ по протоколу Webmail; • отправка по протоколу SMTP. 2.6. Возможность регулирования уровней доступа пользователей к USB. 2.7. Возможность развертывания модуля конечной точки в системах Ubuntu и CentOS с возможностью: • обнаружения КИ, находящегося в состоянии покоя; • контроля утечки КИ на съемные носители, включая блокировку и регистрацию такой информации; • контроля утечки КИ через каналы HTTP/HTTPS; • контроля утечки КИ через протокол Webmail. 2.8. Программное обеспечение должно поддерживать возможность превентивного уведомления администратора о подключении пользователем недоверенного USB-накопителя к компьютеру. 3. Требования к интерфейсу 3.1. Программное обеспечение должно поддерживать следующие языки интерфейса: английский, русский, казахский. 3.2. Программное обеспечение должно поддерживать единый веб-интерфейс для управления системой и инцидентами. 3.3. Должна быть возможность удаления агентов конечных точек с помощью интерфейса решения. 3.4. Должна быть возможность обновления агентов конечных точек с помощью интерфейса решения. 4. Требования к классификации 4.1. Программное обеспечение должно поддерживать встроенную классификацию файлов Microsoft Office, Microsoft Outlook и Web Outlook 365. 4.2. Классификация должна выполняться при сохранении файла, а не при его закрытии. 4.3. Программное обеспечение должно поддерживать классификацию текстовых документов и изображений при поиске данных в режиме реального времени и в режиме ожидания. 4.4. Программное обеспечение должно поддерживать классификацию приглашений Outlook. 4.5. Программное обеспечение должно поддерживать возможность наложения водяного знака на документ во время классификации данных. 4.6. Программное обеспечение должно иметь возможность классифицировать документы во время печати. 4.7. Программное обеспечение должно иметь возможность наносить водяной знак на экран пользователя с возможностью выбора положения, видимости, а также возможность наносить водяной знак на весь экран. 4.8. Программное обеспечение должно классифицировать не только файлы, но и папки в режиме реального времени. 4.9. Программное обеспечение должно контролировать копирование файлов на уровне буфера обмена и иметь возможность блокировать такую операцию в зависимости от уровня классификации файла. 4.10. Программное обеспечение должно контролировать скриншоты файлов Microsoft Office и блокировать попытки создания скриншотов для классифицированных файлов. 4.11. Возможность присваивать уникальный цвет каждому уровню классификации. 4.12. Возможность запретить переклассификацию файлов кем-либо, кроме автора классификации. 4.13. Возможность изменять тему засекреченного электронного письма. 4.14. Возможность классифицировать веб-письма Office 365. 4.15. Возможность интеграции со сторонними системами классификации. 5. Дополнительные требования 5.1. ПО должно поддерживать интеграцию со сторонними почтовыми сервисами с использованием специализированных стандартных протоколов (MTA). 5.2. ПО должно поддерживать интеграцию со сторонними веб-сервисами (шлюзами) с использованием специализированных стандартных протоколов (ICAP). 5.3. ПО должно поддерживать интеграцию с облачной средой Office 365 с возможностью просмотра инцидентов, связанных с КИ в этой среде, в централизованной консоли ПО. Это включает в себя возможность работы с файлами в OneDrive и OneDrive for Business. 5.4. Участник должен быть способен обеспечить в рамках технической поддержки (ТП) полную реализацию и настройку системы на территории Заказчика, а также консультационную поддержку по эксплуатации и администрированию системы и ее компонентов. • Требования к ТП системы: О Полная реализация и настройка системы на территории Заказчика с предоставлением консультационной поддержки не менее чем трем специалистам Заказчика по эксплуатации и администрированию системы и ее компонентов. о Проведение технических консультаций для персонала Заказчика (не менее 3 человек) по установке и настройке системы предотвращения утечки конфиденциальной информации. 5.5. Наличие функции «Off-Premise DLP», при которой агент должен применять один набор политик защиты при подключении к центральной консоли и другой набор политик в автономном режиме. 5.6. Перехват трафика агентом должен осуществляться без установки плагина в браузере пользователя. 5.7. Система должна иметь возможность устанавливать максимальное время сканирования файлов для каждой функции отдельно. 5.8. Должна быть возможность создавать пользовательские группы без привязки к Active Directory. 5.9. ПО должно иметь возможность полностью обходить проверку без расшифровки пакетов для определенных веб-сайтов. 5.10. Наличие функционала для блокировки возможности удаления файлов со съемных носителей. 5.11. Возможность указывать локально разрешенные IP-адреса для агентов. 5.12. Наличие AI-помощника для более удобного взаимодействия с системой. 5.13. ПО должно поддерживать возможность аудита сетевого хранилища, Sharepoint, OneDrive; должен осуществляться мониторинг открытия, изменения, удаления и переименования файлов. 5.14. Агент ПО должен поддерживать работу в скрытом режиме; все процессы должны быть скрыты от конечного пользователя. 5.15 Агент ПО должен поддерживать онлайн- и локальную проверку Telegram для текстовых сообщений и файлов.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о закупках (указываются при наличии) (потенциальный поставщик за не указание и непредставление указанных сведений не отклоняется)	

* сведения подтягиваются из плана закупок (отображаются автоматически).

Примечание:

1. Каждые характеристики, параметры, исходные данные и дополнительные условия к исполнителю указываются отдельной строкой.

2. В технической спецификации квалификационные требования, предъявляемые к потенциальному поставщику, не устанавливаются.

3. Требования технической спецификации в иных документах не устанавливаются.