Конкурстық құжаттамаға
2-3-қосымша

Сатып алынатың қызметтердің техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы	"Өскемен жылу жүйелері" акционерлік қоғамы
Ұйымдастырушының атауы	"Шығыс Қазақстан облысының мемлекеттік сатып алу басқармасы" мемлекеттік мекемесі
Лоттың №	66133986
Лоттың атауы	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	582950.000.000000
Қызметтің атауы:	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын қоспағанда бірлік бағасы:	4422384
Қосылған құн салығын қоспағанда, сатып алуға бөлінген жалпы сома:	4422384
Қызметтерді көрсету мерзімі:	веб -порталдың көмегімен хабарлама алған соң 15 жұмыс күнінде
Қызметтерді көрсету орны:	Шығыс Қазақстан облысы, Өскемен қ. Өскемен қ., М. Горький көшесі, 61
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлар)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы:	Техникалық қолдауды ұзарту мерзімі Тапсырыс берушінің атына лицензиялар берілген күннен бастап күнтізбелік 12 (он екі) айды құрайды. Антивирустық бағдарламалық қамтамасыз ету жүйесіне қойылатын жалпы талаптар Лицензиялардың талап етілетін саны – 400-ден кем емес. Жеткізу талаптары: лицензиялар Тапсырыс берушінің атына беріледі. Басқару сервері 1. Барлық желілік инфрақұрылымды антивирустық қорғауды орталықтандырылған басқару мүмкіндігі. 2. Негізгі және аймақтық бөлімшелерге тиесілі жұмыс станцияларының, серверлердің және мобильді құрылғылардың антивирустық қорғанысын орталықтандырылған басқаруға мүмкіндік беретін негізгі серверден және бағынышты серверлерден тұратын иерархиялық басқару құрылымын құру мүмкіндігі. 3. Жеке брандмауэр, нақты уақыттағы қорғаныс, электрондық пошта клиентін қорғау, Интернетке кіруді қорғау, құрылғыны басқару, веб-бақылау, жеке клиенттегі антиспам сияқты қорғаныс модульдерін қашықтан қосу және өшіру мүмкіндігі. 4. Қашықтан басқару құралының көмегімен қосымша желілік әрекеттерді орындау мүмкіндігі, мысалы: өшіру және қайта жүктеу, компьютердің ояту сигналын жіберу, хабарламалар жіберу, клиенттік компьютерде командалық жолдың нақты нұсқауларын орындау, клиенттік компьютердің амалдық жүйесін жаңартуды бастау. 5. Соңғы нүктелерде антивирустық өнімді қашықтан басқаруға, сондай-ақ жұмыс станцияларындағы антивирустық қорғаныс деңгейін және операциялық жүйенің күйін бақылауға мүмкіндік беретін тәуелсіз агентті пайдалану. 6. Келесі дерекқорларды қашықтан басқару құралымен қолдау: MS SQL Server, MySQL. 7. Үшінші тарап HTTP серверлеріне негізделген жаңарту айнасын жасау мүмкіндігі. 8. Журналдар мен есептер параметрлерін теңшеу немесе әртүрлі жүйелер/клиенттер үшін 50-ден астам шаблондарды таңдау мүмкіндігі. 9. Жұмыс станциясында орнатылған бағдарламалық жасақтаманы бақылау, сондай-ақ таңдау үшін орнатылған бағдарламалық жасақтаманы жою мүмкіндігі. 10. Тіпті физикалық немесе қашықтан қол жетімділігі жоқ жұмыс станцияларында да антивирустық өнім лицензиясын өшіру мүмкіндігі. 11. Клиенттерді динамикалық топтарға автоматты түрде бөлуді көптеген критерийлер бойынша теңшеу, содан кейін тиісті қауіпсіздік саясатын тағайындау, сондай-ақ қажетті тапсырмаларды орындау мүмкіндігі. 12. Лицензияның тиісті бөлігі бар алаңның немесе филиалдың әкімшісін анықтау үшін функционалдың болуы. 13. Клондалған машиналарды дұрыс емес сәйкестендіру туралы хабарлау үшін хабарландыру жүйесінде алдын ала орнатылған шаблондардың болуы, бұл VDI жүйелерімен дұрыс конфигурацияланбаған интеграция туралы хабарлауға мүмкіндік береді. 14. VDI жүйелерінде көшіру немесе клондау үшін қандай Виртуалды машина көзі болатынын анықтау мүмкіндігі. 15. Arm64 процессорларында басқару агентін орнату мүмкіндігі. 16. Орталықтандырылған басқару серверіне рұқсатсыз қосылуды болдырмайтын әкімші тіркелгілері үшін екі факторлы аутентификацияны пайдалану мүмкіндігі. 17. Компанияның филиалдарына сәйкес алаңдар құру функционалының болуы, бұл лицензияның белгілі бір бөлігін жеке филиалдарға тағайындауға мүмкіндік береді. 18. Антивирустық өнімдерді пайдалану мүмкіндігі, егер олар барлық бөлімшелердің антивирустық қорғаныс инфрақұрылымының барлық тармақталған жүйелерін орталықтандырылған бақылауға және басқаруға конфигурацияланған қолданыстағы әкімшілік серверлермен басқарылатын болса. 19. Қолданыстағы орталықтандырылған басқару серверімен үйлесімділік және бар басқару серверіне кілт қосу арқылы антивирустық бағдарламаны іске қосу. Қатысушының ұсынысының Осы сипаттамаға сәйкестігін растау үшін тапсырыс берушінің талабы бойынша қатысушы қолданыстағы басқару серверіне қосу үшін 5 күндік сынақ кілтін ұсынады. Жұмыс станцияларын қорғау 1. Компьютердегі файл кодының басына немесе соңына қосылатын зиянды бағдарламадан қорғауды қамтамасыз ету. Зиянды бағдарламаны анықтау Машиналық оқыту компонентімен бірге анықтау ядросымен жүзеге асырылуы керек. 2. Вирустар немесе трояндар сияқты сөзсіз зиянды бағдарламаларға ұқсастығы бойынша зиянды бағдарламаларға біржақты жатқызуға болмайтын Ықтимал қалаусыз бағдарламалардан қорғауды қамтамасыз ету, бірақ бұл бағдарламалар қосымша қажетсіз бағдарламалық жасақтаманы орната алады, жүйе параметрлерін өзгерте алады және күтпеген әрекеттерді немесе пайдаланушы растамаған әрекеттерді орындай алады. 3. Интернеттегі шабуылдаушыларға жүйеге шектеусіз қол жеткізуге мүмкіндік беретін қауіпті руткит бағдарламаларынан қорғауды қамтамасыз ету, сонымен бірге олардың операциялық жүйеде болуын жасыру. 4. Зиянды емес, бірақ сканерлеу жұмыстағы ауытқуларға немесе жүйенің өнімділігіне әсер етуі мүмкін кейбір файлдарды сканерлеуден ерекшеліктер жасау мүмкіндігі. 5. Нақты уақыт режимінде антивирустық қорғауды қамтамасыз ету. 6. "Ботнет" сияқты қауіптерден қорғауды қамтамасыз ететін технологияны пайдалану мүмкіндігі. 7. Пайдаланушының немесе әкімшінің талабы бойынша және кестеге сәйкес антивирустық сканерлеу. 8. Зиянды бағдарламалық жасақтаманың зиянды әрекеттері мен сипаттамаларын анықтау үшін кодты тереңірек талдау үшін машиналық оқыту технологияларын қолдану мүмкіндігі. 9. Рұқсат етілген немесе тыйым салынған сыртқы құрылғылар тобын құру мүмкіндігі. 10. Браузердің жад аймағына және оның терезелерінің мазмұнына араласу әрекеттерін бұғаттау, сондай-ақ интернет төлемдері мен Интернет-банкинг және т. б. сияқты маңызды Интернет байланыстарын қосымша қорғау мақсатында браузерлерді қорғалған режимде іске қосуға мүмкіндік беретін қосымша модульдің болуы. 11. Жеке брандмауэрде әкімшіге желілік қосымшалар мен жабдықтар үшін рұқсат беру ережелерін қашықтан конфигурациялауға мүмкіндік беретін оқу режимінің болуы. 12. Дербес брандмауэрде ДК-нің белгісіз қауіпті желілерге рұқсатсыз қосылуын болдырмау мақсатында желінің қосымша аутентификациясын пайдалану мүмкіндігі. 13. Жаңа рұқсат етілмеген желілік қосылыстарға алып келген желілік бағдарламалардағы өзгерістерді анықтай алатын жеке брандмауэрдің қосымша функционалдығының болуы. 14. Сервердегі жергілікті жадтан клиенттердің жаңартуын алу, бұл Интернет желісіне қол жеткізе алмайтын жабық оқшауланған желілерде антивирустық қорғауды жаңартуға мүмкіндік береді. 15. Тұрақты, сынақ және кешіктірілген жаңартуларды алу режимінде жаңарту мүмкіндігі. 16. Жеке брандмауэрдің қосымша функционалдығының болуы, бұл барлық қол жетімді Желілік қосылыстар туралы барлық мәліметтерді көруге, сондай-ақ пайдаланушыға қорғалмаған Wi-Fi желісіне қосылу туралы ескертуге мүмкіндік береді. 17. Жеке брандмауэрдің қосымша функционалдығының болуы, бұл компьютерде бұғатталған IP мекенжайларының тізімін көруге мүмкіндік береді, қара тізімге ену себептері туралы ақпарат береді және нақты қауіпсіз мекенжайларға ерекшеліктер жасауға мүмкіндік береді. 18. Күдікті іске қосылған процестердің жұмысын бақылауға қабілетті жедел жадты сканерлеу модулі, бұл тіпті Мұқият шифрланған және жасырын қауіптермен инфекцияның алдын алады. 19. Операциялық жүйеде рұқсатсыз және қауіпті өзгерістерді анықтау мақсатында операциялық жүйенің әртүрлі параметрлерінің мәндерінің сыни деңгейін (қауіпті, белгісіз, аз белгілі, қауіпсіз) анықтау мүмкіндігі. 20. SSL протоколын Автоматты және интерактивті режимдерде тексеру мүмкіндігі. 21. SSL трафигі сертификаттарының жарамдылығы мен тұтастығын тексеру. 22. Сценарийлерді жасау және қашықтан орындау мүмкіндігі, бұл қашықтағы компьютерде жұмыс істеп тұрған процестер мен қызметтерді тоқтатуға, тізілім тармақтарын жоюға, желілік қосылымдарды бұғаттауға мүмкіндік береді. 23. Компьютерде автоматты түрде бұғатталған желі қосылымдарын көру және қажет болған жағдайда белгілі бір қауіпсіз желі қосылымдарына уақытша рұқсат беру мүмкіндігі. 24. Саясатты қайта анықтау режимінің болуы, бұл жүйелік әкімшіге белгілі бір ортада антивирустық бағдарламаны икемді конфигурациялау мақсатында саясат тағайындайтын және өндеуге қол жетпейтін антивирустық бағдарламалардың параметрлерін компьютерде өзгертуге уақытша мүмкіндік береді. 25. Құрылғыларды басқару ережелерін икемді түрде реттеуге мүмкіндік беретін уақыт аралықтарын орнату мүмкіндігі. 26. ДК ресурстарын өзекті антивирустық өнімдермен аз тұтыну (барлық процестермен бірге: графикалық интерфейс, кешенді қорғау процесі, қашықтан басқару қызметі): 50-100 МБ жедел жады, 2-35% орталық процессор. 27. Тұрақты, сынақ және кешіктірілген жаңартуларды алу режимінде жаңарту мүмкіндігі. 28. Барлық және жеке пайдаланушылар немесе Windows немесе домен топтары үшін сыртқы құрылғыларды қосуға тыйым салу немесе рұқсат беру мүмкіндігі. 29. Сканерлеу үшін 64 биттік ядроны пайдалану жүйеге жүктемені азайтады және ең жылдам және тиімді сканерлеуге мүмкіндік береді. 30. Компьютерді белсенді емес күйде сканерлеу. 31. Conficker, Sirefef, Necurs және басқалары сияқты күрделі тұрақты қауіптердің қалдықтарын тазарту үшін бірнеше утилиталарды біріктіретін кіріктірілген құралдың болуы 32. Жүктеу секторларын негізгі жүктеу жазбасында, соның ішінде UEFI интерфейсінде вирустардың бар-жоғын тексеру мүмкіндігі. 33. ОЖ қолдауы: Microsoft Windows Vista (кәсіби немесе одан жоғары); Microsoft Windows 7 (кәсіби немесе одан жоғары); Microsoft Windows 8 (кәсіби немесе одан жоғары); Microsoft Windows 8.1 (кәсіби немесе одан жоғары); Microsoft Windows 10. Серверді қорғау 1. Серверлік операциялық жүйенің жұмысына әсерін азайтуға мүмкіндік беретін арнайы файлдар, қалталар, қосымшалар үшін автоматты ерекшеліктер жасау үшін сервер рөлдерін автоматты түрде анықтау. 2. UEFI интерфейсін сканерлеу-негізгі жүктеу жазбасында зиянды бағдарламалық жасақтаманы тексеру. 3. Компьютерді белсенді емес күйде сканерлеу. 4. Сканерлеу кезінде эвристикалық технологияны қолдану. 5. Зиянды бағдарламалардан, трояндық бағдарламалардан, пернетақта тыңшыларынан, жарнамалық бағдарламалардан, фишингтен, шпиондық бағдарламалардан, руткиттерден, сценарийлерден, Ықтимал қалаусыз және қауіпті бағдарламалардан қорғауды қамтамасыз ету. 6. Вирустық базаларды тәулігіне кемінде 24 рет регламенттік жаңарту. 7. Негізгі мүмкіндіктен басқа, резервтік әкімшілік серверлерді көрсету мүмкіндігі. 8. Құрылғының типі, қол жеткізу деңгейі, өндіруші, модель немесе құрылғының сериялық нөмірі бойынша қол жеткізу ережелерін жасау арқылы перифериялық құрылғылардың жұмыс станциясына қосылуын бақылауды жүзеге асыра алатын құралдың болуы. Ережелер барлық және жеке пайдаланушылар немесе Windows топтары үшін жасалуы мүмкін. 9. Операциялық жүйенің жұмысының әр түрлі аспектілерін, соның ішінде жұмыс істеп тұрған процестерді, тізілім мазмұнын, орнатылған бағдарламалық жасақтаманы, желілік байланыстарды одан әрі терең талдау үшін операциялық жүйенің күйінің суреттерін жасай алатын жүйені диагностикалау құралының болуы. Жүйе күйінің әртүрлі суреттерін салыстыру қабілетінің арқасында бұл құрал жүйеде болған өзгерістерді анықтай алады. Сондай-ақ, ол сценарийлерді жасай алады және орындай алады, бұл сізге жұмыс істеп тұрған процестерді тоқтатуға, тізілім тармақтарын жоюға, желілік қосылымдарды бұғаттауға мүмкіндік береді. 10. Көрсетілген кеңейтім бойынша Интернеттен файлдарды жүктеуді бұғаттау мүмкіндігі. 11. Тұрақты, сынақ және кешіктірілген жаңартуларды алу режимінде жаңарту мүмкіндігі. 12. Виртуалды жұмыс станцияларына, сондай-ақ жалпы гипервизорға жүктемені едәуір төмендететін арнайы технологияның болуы. 13. Терминал пайдаланушылары үшін графикалық интерфейсті өшіру арқылы іске қосу режимін теңшеу мүмкіндігі, бұл терминал сервері режимінде жұмыс істейтін серверге жүктемені азайтуға мүмкіндік береді. Техникалық қолдауға қойылатын талаптар Антивирустық бағдарламалық жасақтаманы техникалық қолдау: - Қазақстан Республикасының бүкіл аумағында вируспен қарсы қорғаныс құралдарын өндірушінің сертификатталған мамандары орыс тілінде мереке және демалыс күндерінсіз (24х7) электрондық пошта және Интернет арқылы, сондай-ақ телефон арқылы тәулік бойы ұсынады; - AZ өндірушісінің орыс тіліндегі веб-сайтында техникалық қолдауға арналған арнайы бөлім, жаңартылатын білім базасы және орыс тілді форум бар. Бағдарламалық қамтамасыз етуді техникалық қолдауды ұзарту бойынша қызмет көрсету кезінде өнім беруші ілеспе қызметтер көрсетеді: - Антивирустық бағдарламалық жасақтаманың параметрлері мен ағымдағы күйінің аудиті Қажет болған жағдайда қолтаңбалар базасын және бағдарламалық жасақтаманың барлық модульдерін өзекті нұсқасына дейін жаңартуды жүзеге асыру; - Антивирустық жүйенің дұрыс жұмыс істеуі үшін үшінші тарап бағдарламалық жасақтамасын орнатуды және/немесе жоюды жүзеге асыру қажет болған жағдайда (Тапсырыс берушімен келісім бойынша); - Қажет болған жағдайда бағдарламалық қамтамасыз етудің жұмысына қажетті қосымша агенттерді орнатуды жүзеге асыру; - Жүйеге қол жеткізудің рөлдік моделінің саясатына аудит жүргізу және өзектендіру; - Тапсырыс берушінің сұрауы бойынша қосымша қауіпсіздік және қауіп қатерге әрекет ету саясатын орнатуды жүзеге асыру; - Тапсырыс берушінің сұранысы бойынша пайдаланушылардың екі факторлы аутентификациясын орнату. Енгізу процесінде өнім беруші консультациялар береді (ауызша, телефон арқылы, эл. пошта арқылы, ал қажет болған жағдайда Тапсырыс берушінің жұмыс орнында) жүйенің тиімді жұмыс істеуіне бағытталған. Техникалық қолдауды ұзартқаннан кейін жеткізуші жұмыс қабілеттілігін тексеруді және қажет болған жағдайда қажетті нәтижеге жету үшін түзетуді жүргізеді. Жеткізуші жүйенің өндірушісінің өз тәжірибесі мен ұсыныстарына сүйене отырып, теңшеу бойынша кеңестер мен ұсыныстар береді.
Орындаушы жеңімпаз деп анықталған жағдайда әлеуетті өнім берушіге қойылатын талаптар және онымен мемлекеттік сатып алу туралы шарт жасасу (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені немесе бермегені үшін қабылдамауға жол берілмейді)	

Приложение 2-3
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Усть-Каменогорские тепловые сети"
Наименование организатора	Государственное учреждение "Управление государственных закупок Восточно-Казахстанской области"
Номер лота	66133986
Наименование лота:	Услуги по продлению лицензий на право использования программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	582950.000.000000
Наименование услуги:	Услуги по продлению лицензий на право использования программного обеспечения
Единица измерения:	Одна услуга
Количество(объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	4422384
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	4422384
Срок оказания услуги:	15 рабочих дней после получения уведомления посредством веб-портала
Место оказания услуги:	Восточно-Казахстанская область, г.Усть-Каменогорск г. Усть - Каменогорск, ул. М. Горького, 61
Размер авансового платежа:	0
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Срок продления технической поддержки составляет 12 (двенадцать) календарных месяцев со дня предоставления лицензий в адрес Заказчика. Общие требования к системе антивирусного программного обеспечения Требуемое количество лицензий – 400. Требования к поставке: лицензии выдаются на имя заказчика. Сервер управления 1. Возможность централизованного управления антивирусной защитой всей сетевой инфраструктуры. 2. Возможность построения иерархической структуры администрирования, которая состоит из главного сервера и подчиненных серверов, что дает возможность осуществлять централизованное управление антивирусной защитой рабочих станций, серверов и мобильных устройств, что принадлежат как главному, так и региональным подразделениям. 3. Возможность удаленно активировать и деактивировать модули защиты, такие как персональный брандмауэр, защита в режиме реального времени, защита почтового клиента, защита доступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельно взятом клиенте. 4. Возможность выполнять с помощью инструмента удаленного управления дополнительные сетевые действия, такие как: завершение работы и перезагрузка, отправка сигнала пробуждения компьютера, отправка сообщений, выполнение конкретных инструкций командной строки на клиентском компьютере, старт обновления операционной системы клиентского компьютера. 5. Использование независимого агента, который позволяет осуществлять удаленное управление антивирусным продуктом на конечных точках, а также контролировать уровень антивирусной защиты на рабочих станциях и состояние операционной системы. 6. Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL. 7. Возможность создания зеркала обновлений на основе сторонних HTTP-серверов. 8. Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов. 9. Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор. 10. Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа. 11. Возможность настройки автоматического распределения клиентов по динамическим группам по многим критериям с последующим назначением соответствующих политик безопасности, а также запуском необходимых задач. 12. Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии. 13. Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI. 14. Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI. 15. Возможность установки агента управления на ARM64 процессорах. 16. Возможность использования двухфакторной аутентификации для учетных записей администраторов, что позволяет предотвратить несанкционированное подключение к серверу централизованного управления. 17. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам. 18. Возможность использования антивирусных продуктов при условии, что они будут управляться существующими серверами администрирования, настроенными на централизованный мониторинг и управление всеми разветвленными системами инфраструктуры антивирусной защиты всех подразделений. 19. Совместимость с существующим сервером централизованного управления и активация антивирусного ПО путем добавления ключа к существующему серверу управления. В подтверждение соответствия предложения участника этой характеристике по требованию Заказчика участник предоставляет тестовый ключ продолжительностью 5 дней для добавления к существующему серверу управления. Защита рабочих станций 1. Предоставление защиты от вредоносного ПО – определенного вредоносного кода, который добавляется в начало или конец кода файлов на компьютере. Выявление вредоносного ПО должно осуществляться ядром обнаружения в сочетании с компонентом машинного обучения. 2. Предоставление защиты от потенциально нежелательных программ, которые нельзя однозначно отнести к вредоносному ПО по аналогии с такими безусловно вредоносными программами, как вирусы или трояны, но эти программы могут устанавливать дополнительное нежелательное ПО, менять настройки системы, а также выполнять неожиданные действия или действия, не подтвержденные пользователем. 3. Предоставление защиты от опасных программ руткитов, которые предоставляют злоумышленникам из Интернета неограниченный доступ к системе, в то же время скрывая свое присутствие в операционной системе. 4. Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы. 5. Обеспечение антивирусной защиты в режиме реального времени. 6. Возможность использования технологии, которая обеспечивает защиту от угроз типа «ботнет». 7. Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком. 8. Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения. 9. Возможность создавать группы разрешенных или запрещенных внешних устройств. 10. Наличие дополнительного модуля, который позволяет запускать браузеры в защищенном режиме с целью блокирования попыток вмешательства в область памяти браузера и содержимого его окон, а также дополнительной защиты критических Интернет-соединений, таких как Интернет-платежи и Интернет-банкинг и т.д. 11. Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования. 12. Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям. 13. Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения. 14. Получение обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых изолированных сетях, у которых нет доступа к сети Интернет. 15. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений. 16. Наличие дополнительного функционала персонального брандмауэра, что позволяет просматривать всю подробную информацию по всем имеющимся сетевым соединениям, а также предупреждать пользователя о подключении к незащищенной сети Wi-Fi. 17. Наличие дополнительного функционала персонального брандмауэра, что дает возможность просматривать на ПК перечень заблокированных IP-адресов, предоставляет информацию о причинах попадания в черный список и позволяет сделать исключения для конкретных безопасных адресов. 18. Модуль сканирования оперативной памяти, который способный отслеживать работу подозрительных запущенных процессов, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами. 19. Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе. 20. Возможность проверки протокола SSL как в автоматическом, так и в интерактивном режимах. 21. Проверка действительности и целостности сертификатов SSL-трафика. 22. Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения. 23. Возможность просматривать на ПК автоматически заблокированные сетевые соединения и при необходимости временно разрешать конкретные безопасные сетевые соединения. 24. Наличие режима переопределения политики, что дает системному администратору временную возможность изменять на ПК те настройки антивирусного ПО, которые назначаются политикой и недостижимые для редактирования, с целью гибкой настройки антивирусного ПО в специфической среде. 25. Возможность задавать временные интервалы, что позволяет более гибко настраивать правила контроля устройств. 26. Низкое потребление ресурсов ПК актуальными антивирусными продуктами (совместно с всеми процессами: графический интерфейс, процесс комплексной защиты, служба удаленного администрирования): 50-100 МБ оперативной памяти, 2-35 % центрального процессора. 27. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений. 28. Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена. 29. Использование 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования. 30. Сканирование компьютера в неактивном состоянии. 31. Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и других 32. Возможность осуществлять проверку загрузочных секторов на наличие вирусов в главной загрузочной записи, в том числе интерфейса UEFI. 33. Поддержка ОС: Microsoft Windows Vista (Professional или выше); Microsoft Windows 7 (Professional или выше); Microsoft Windows 8 (Professional или выше); Microsoft Windows 8.1 (Professional или выше); Microsoft Windows 10. Защита серверов 1. Автоматическое определение ролей сервера для создания автоматических исключений для специфических файлов, папок, приложений, позволяющее минимизировать влияние на работу серверной операционной системы. 2. Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи. 3. Сканирование компьютера в неактивном состоянии. 4. Использование эвристических технологий во время сканирования. 5. Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО. 6. Регламентное обновление вирусных баз не менее 24 раз в сутки. 7. Возможность помимо основного указать резервные серверы администрирования. 8. Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции периферийных устройств путем создания правил доступа по типу устройства, по уровню доступа, по производителю, модели или серийному номеру устройства. Правила могут быть созданы как для всех, так и для отдельных пользователей или групп Windows. 9. Наличие инструмента для диагностики системы, который может создавать снимки состояния операционной системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения. Благодаря умению сравнивать различные снимки состояния системы, этот инструмент может обнаружить изменения, которые произошли в системе. Также он может создавать и выполнять скрипты, что позволит останавливать запущенные процессы, удалять ветки реестра, блокировать сетевые соединения. 10. Возможность блокировать загрузку из Интернета файлов по указанному расширению. 11. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений. 12. Наличие специальной технологии, значительно снижающей нагрузку на виртуальные рабочие станции, а также на гипервизор в целом. 13. Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов. Требования к технической поддержке Техническая поддержка антивирусного программного обеспечения: • предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Республики Казахстан круглосуточно без праздников и выходных (24x7) по электронной почте и через Интернет, а также по телефону; • Web-сайт производителя АЗ на русском языке, имеет специальный раздел, посвящённый технической поддержке, пополняемую базу знаний и русскоязычный форум. • При оказании услуги по продлению технической поддержки программного обеспечения поставщик оказывает сопутствующие услуги: • - Аудит настроек и текущего состояния антивирусного программного обеспечения • В случае необходимости осуществить обновление базы сигнатур и всех модулей программного обеспечения до актуальной версии; • В случае необходимости осуществить установку и/или удаление стороннего программного обеспечения для корректной работы антивирусной системы (по согласованию с заказчиком); • В случае необходимости осуществить установку дополнительных агентов, необходимых для работы программного обеспечения; • Провести аудит и актуализацию политик ролевой модели доступа к системе; • По запросу заказчика осуществить настройку дополнительных политик безопасности и реагирования на угрозы; • По запросу заказчика осуществить настройка двухфакторной аутентификации пользователей. • В процессе внедрения поставщик оказывает консультации, (устно, по телефону, по эл. почте, а в случае необходимости на рабочем месте Заказчика) направленные на эффективное функционирование системы. • Поставщик после продления технической поддержки производит тестирование работоспособности и в случае необходимости подстройку для достижения желаемого результата. • Поставщик оказывает консультации и рекомендации по настройке ПО исходя из собственного опыта и рекомендаций производителя системы.
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)	