Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Жоғары Сот Кеңесінің жанындағы Сот төрелігі академиясы" республикалық мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Жоғары Сот Кеңесінің жанындағы Сот төрелігі академиясы" республикалық мемлекеттік мекемесі
Конкурстың №:	№ 17972002-1
Конкурстың атауы:	Корпоративтік антивирустық бағдарламалық қамтамасыз етуге лицензиялар беру және техникалық қолдау көрсету қызметтері.
Лоттың нөмірі:	№ 83354590-ОКЗ
Лоттың атауы	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620920.000.000027
Қызметтің атауы:	Лицензиялық бағдарламалық қамтамасыз етуді техникалық қолдау жөніндегі қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	2275862.07
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	2275862.07
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шартқа қол қойылғаннан кейін күнтізбелік 15 күн ішінде.
Аванстық төлем мөлшері:	30

Кепілдік мерзімі (айлармен)	12
Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Корпоративтік антивирустық бағдарламалық қамтамасыз етуге лицензиялар беру және техникалық қолдау көрсету қызметтері.

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)	Қызметтің атауы: Корпоративтік антивирустық бағдарламалық қамтамасыз етуге лицензиялар беру және техникалық қолдау көрсету қызметтері. Тапсырыс беруші: «Қазақстан Республикасы Жоғары Сот Кеңесінің жанындағы Сот төрелігі академиясы» РММ. Бағдарламалық қамтамасыз етудің атауы: Жұмыс станцияларын қорғауға арналған корпоративтік антивирустық бағдарламалық қамтамасыз ету. Лицензиялар саны: 120 (жүз жиырма) жұмыс станциясы. Лицензиялардың қолданылу мерзімі: Лицензиялар белсендірілген күннен бастап немесе өндірушінің лицензиялау шарттарына сәйкес айқындалған лицензияның қолданылу мерзімі басталған күннен бастап кемінде 12 (он екі) ай. Техникалық талаптар 1. Тапсырыс берушінің жұмыс станцияларын қорғауға арналған корпоративтік антивирустық бағдарламалық қамтамасыз етудің 120 (жүз жиырма) лицензиясын ұсыну. 2. Жұмыс станцияларын вирустардан, зиянды бағдарламалардан, шпиондық бағдарламалық қамтамасыз етуден және өзге де киберқауіптерден қорғауды қамтамасыз ету. 3. Лицензиялардың қолданылу мерзімі ішінде антивирустық дерекқорлар мен бағдарламалық компоненттердің тұрақты жаңартылып отыруын қамтамасыз ету. 4. Таңдалған лицензиялық өнімде тиісті функционал болған жағдайда, жұмыс станцияларын қорғауды орталықтандырылған басқару жүйесіне қолжетімділікті ұсыну. 5. Сатып алынған лицензияның шарттарына сәйкес бағдарламалық қамтамасыз етуді өндірушінің техникалық қолдауын ұсыну. 6. Лицензияларды белсендіру үшін лицензиялық кілттерді, белсендіру кодтарын немесе өндіруші көздеген өзге де құралдарды ұсыну. 7. Лицензиялардың заңды түрде алынғанын және Тапсырыс берушінің оларды пайдалану құқығы бар екенін растау. Қызмет көрсету орны: Қазақстан Республикасы, Астана қаласы, Бейбітшілік көшесі, 46-ғимарат, «Қазақстан Республикасы Жоғары Сот Кеңесінің жанындағы Сот төрелігі академиясы» РММ ғимараты. Қызмет көрсету нәтижесі: Тапсырыс берушіге белгіленген мерзім ішінде жаңартулармен және техникалық қолдаумен қамтамасыз етілген, жарамды корпоративтік антивирустық бағдарламалық қамтамасыз етудің 120 (жүз жиырма) лицензиясын ұсыну. Антивирустық қорғаныс (АҚ) жұмыс станциялары мен серверлер желісінің тұрақты жұмысын қамтамасыз ететін корпоративтік шешім болуы керек. Бүкіл ұйым бірыңғай антивирустық құралдарды пайдаланады. Бұл техникалық ерекшелік антивирустық қорғау жүйесін енгізу бойынша ілеспе қызметтер көрсете отырып, жеткізілетін бағдарламалық қамтамасыз етуге қойылатын талаптарды белгілейтін іргелі құжат болып табылады. Жүйенің барлық компоненттері бір-бірімен толық интеграциялануы керек. 1. Антивирустық қорғау бағдарламалық жасақтамасына қойылатын жалпы талаптар 1.1. Қорғалатын түйіндердің жалпы саны: Лицензияның жарамдылық мерзімі: бағдарламалық жасақтама лицензиялары жасалған сәттен бастап 12 ай 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. Windows, MacOS және Linux жұмыс істейтін жұмыс станциялары мен серверлерде орнатылған жабдықты түгендеу. 4. Windows, macOS және Linux жұмыс істейтін жұмыс станциялары мен серверлерде орнатылған бағдарламалық жасақтаманы түгендеу. 5. Windows, Linux және Mac операциялық жүйелеріне арналған антивирустық бағдарламалық жасақтаманы бір уақытта бірнеше соңғы нүктеге қашықтан орнату. 6. Пайдаланушы бағдарламалық жасақтамасын қашықтан орнату. 7. Орнатылған пайдаланушы бағдарламалық жасақтамасын қашықтан жою мүмкіндігі. 8. Windows, Linux және Mac операциялық жүйелеріне арналған антивирустық бағдарламалық жасақтаманы қашықтан жою. 9. 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. 10. Оқшауланған желідегі соңғы нүктелерде, сондай-ақ қорғауды қажет ететін, бірақ әкімшілік серверге уақытша қосылмаған соңғы нүктелерде толық антивирустық қорғауды орналастыру үшін орнату бумаларын экспорттауға мүмкіндік беретін алдын ала орнатылған конфигурация параметрлері бар Windows, Linux және Mac операциялық жүйелеріне арналған орнату бумаларын жасау және өңдеу құралының болуы. 11. Әкімшілік сервердің әр түрлі пайдаланушыларын құруға және оларға жеке бөлімдерге, әкімшілік сервердегі компьютерлер топтарына әр түрлі қол жетімділік құқықтарын тағайындауға мүмкіндік беретін пайдаланушы менеджерінің болуы, бұл кең антивирустық қорғаныс жүйесінің аймақтық жүйелік әкімшілеріне әр түрлі қол жетімділік құқықтарын беруге мүмкіндік береді. 12. Active Directory қауіпсіздік топтары арқылы басқару консолінің әкімшілерін аутентификациялау мүмкіндігі. 13. Орталықтандырылған басқару серверіне рұқсатсыз қосылуды болдырмайтын әкімші тіркелгілері үшін екі факторлы аутентификацияны пайдалану мүмкіндігі. 14. Конфигурациядағы барлық өзгерістерді және әкімшілік сервер пайдаланушылары орындайтын барлық әрекеттерді тіркейтін және бақылайтын аудит журналының болуы. 15. 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. 16. Статикалық топтарды құру және өңдеу мүмкіндігі және Active Directory-ден компьютерлер ағашын импорттау мүмкіндігі. 17. Клиенттерді динамикалық топтарға автоматты түрде бөлуді көптеген критерийлер бойынша теңшеу, содан кейін тиісті қауіпсіздік саясатын тағайындау, сондай-ақ қажетті тапсырмаларды орындау мүмкіндігі. 18. Пайдаланушылар мен топтарды Active Directory-ден импорттау мүмкіндігі, оларды құрылғыны басқару және веб-бақылау ережелерін жекелендіру үшін одан әрі пайдалану. 19. Антивирустық өнімдердің конфигурация параметрлеріне үздіксіз

	қызмет көрсетуге арналған кірістірілген және пайдаланушы саясаттарын пайдалану мүмкіндігі. Саясатты экспорттау/импорттау мүмкіндігі. 20. Инфрақұрылымның қауіпсіздігін қорғау деңгейіне, қорғалған соңғы нүктелердің күйіне, сондай-ақ әкімшілік сервердің күйіне қатысты барлық қажетті мәліметтерді беретін бақылау тақтасының болуы. 21. Бақылау тақтасы үшін де, әртүрлі есептерді қалыптастыру үшін де пайдалануға болатын 100-ге жуық алдын ала орнатылған есеп үлгілерінің болуы. 22. Бақылау тақтасы үшін де, PDF, CSV форматында есептер құру үшін де, көрсетілген жол бойынша әрі қарай сақтау немесе көрсетілген электрондық поштаға жіберу үшін де қолданылатын есеп шаблондарын құру және өңдеу мүмкіндігі. 23. Келесі дерекқорларды қашықтан басқару құралымен қолдау: MS SQL Server, MySQL. 24. SIEM-мен одан әрі интеграциялау үшін журналдарды syslog-қа экспорттау мүмкіндігі. 25. Журналдар мен есептер параметрлерін теңшеу немесе әртүрлі жүйелер/клиенттер үшін 50-ден астам шаблондарды таңдау мүмкіндігі. 26. Антивирустық өнімді, арнайы утилитаны немесе прокси-серверді пайдаланып жаңарту айнасын жасау мүмкіндігі. 27. Үшінші тарап HTTP серверлеріне негізделген жаңарту айнасын жасау мүмкіндігі. 28. Сертификатпен қорғалған байланыс арқылы кез-келген шолғыш арқылы серверді басқаруға мүмкіндік беретін Веб-бағытталған интерфейс. 29. Соңғы нүктелерде антивирустық өнімді қашықтан басқаруға, сондай-ақ жұмыс станцияларындағы антивирустық қорғаныс деңгейін және операциялық жүйенің күйін бақылауға мүмкіндік беретін тәуелсіз агентті пайдалану. 30. Жұмыс станциясында орнатылған бағдарламалық жасақтаманы бақылау, сондай-ақ таңдау үшін орнатылған бағдарламалық жасақтаманы жою мүмкіндігі. 31. Мобильді құрылғыларда антивирустық қорғауды басқаруға мүмкіндік беретін қосымша компонент. 32. Антивирустық қорғауды одан әрі өрістету үшін желіде қорғалмаған жұмыс станцияларын анықтауды жүзеге асыратын арнайы компонент. 33. Өздігінен шығарылған сертификаттар мен қолданыстағы сертификаттар арқылы сервер компоненттері арасындағы байланыстарды қорғау. 34. Лицензия күйін басқару құралы (тіпті әкімшілік серверді пайдаланбай). 35. Тіпті физикалық немесе қашықтан қол жетімділігі жоқ жұмыс станцияларында да антивирустық өнім лицензиясын өшіру мүмкіндігі. 36. Windows және Linux ОЖ-де әкімшілік серверді орнату мүмкіндігі. 37. Әкімшілік серверді Microsoft Hyper-V, Microsoftacle VirtualBox, VMware (ESXi/vSphere/Player/Workstation) сияқты виртуалды ортада пайдалануға дайын, кеңейтілген түрде жеткізу. 38. VMware Horizon 8 сияқты виртуализация жүйелерін қолдау.x немесе Citrix XenCenter / XenServer 8+. 39. VDI жүйелерінде көшіру немесе клондау үшін қандай Виртуалды машина көзі болатынын анықтау мүмкіндігі. 40. VDI жүйелерімен интеграциялау үшін егжей-тегжейлі параметрлерді анықтау үшін теңшеу шеберінің болуы. 41. Қолданыстағы компьютерлермен салыстыру немесе жаңа компьютерлер құру сияқты клондалған компьютер идентификаторларын өңдеу опцияларын таңдау мүмкіндігі. 42. Жылдам клондар немесе машина каталогтары үшін VDI

	атау үлгісінің параметрлерін анықтау мүмкіндігі. 43. 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. 44. Басқару агентін автоматты түрде жаңартудың болуы, бұл әкімшінің араласуынсыз ағымдағы нұсқаларды пайдалануға мүмкіндік береді. 45. Автоматты жаңарту процесін тарату механизмінің болуы, бұл желіге және жалпы компьютерлерге жүктемені азайтуға мүмкіндік береді. 46. Arm64 процессорларында басқару агентін орнату мүмкіндігі. 47. Компанияның филиалдарына сәйкес алаңдар құру функционалының болуы, бұл лицензияның белгілі бір бөлігін жеке филиалдарға тағайындауға мүмкіндік береді. 48. Лицензияның тиісті бөлігі бар алаңның немесе филиалдың әкімшісін анықтау үшін функционалдың болуы. Жұмыс станцияларын қорғау 1. Вирустардан, трояндық бағдарламалардан, жарнамалық бағдарламалардан, фишингтен, сондай-ақ шпиондық бағдарламалардан қорғауды қамтамасыз ету. 2. Компьютердегі файл кодының басына немесе соңына қосылатын зиянды бағдарламадан қорғауды қамтамасыз ету. Зиянды бағдарламаны анықтау Машиналық оқыту компонентімен бірге анықтау ядросымен жүзеге асырылуы керек. 3. 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. 4. Ықтимал қауіпті бағдарламалардан қорғауды қамтамасыз ету-рұқсатсыз қашықтан қол жеткізу, құпия сөзді ұрлау немесе бұзу, пернетақта тыңшылары және т. б. сияқты зиянды мақсаттар үшін пайдаланылуы мүмкін әртүрлі бағдарламалық құрал 5. Күдікті бағдарламалардан қорғауды қамтамасыз ету-зиянды бағдарламалық жасақтаманы анықтауға жол бермеу үшін шабуылдаушылар жиі қолданатын орауыштар немесе қорғаушылар қысатын бағдарламалар. 6. Интернеттегі шабуылдаушыларға жүйеге шектеусіз қол жеткізуге мүмкіндік беретін қауіпті руткит бағдарламаларынан қорғауды қамтамасыз ету, сонымен бірге олардың операциялық жүйеде болуын жасыру. 7. Қауіптердің әртүрлі санаттары үшін қорғаныс үшін де, есеп беру үшін де жеке жауап деңгейлерін теңшеу мүмкіндігі. 8. Зиянды емес, бірақ сканерлеу жұмыстағы ауытқуларға немесе жүйенің өнімділігіне әсер етуі мүмкін кейбір файлдарды сканерлеуден ерекшеліктер жасау мүмкіндігі. 9. Жүйелік қызметтердің жылдамдығын жақсарту және ОЖ процесіне араласуды азайту мақсатында жүйелік процестерге ерекшеліктер жасау мүмкіндігі. 10. Жүктеу секторларын негізгі жүктеу жазбасында, соның ішінде UEFI интерфейсінде вирустардың бар-жоғын тексеру мүмкіндігі. 11. Нақты уақыт режимінде антивирустық қорғауды қамтамасыз ету. 12. Сканерлеу кезінде өзіндік дамудың эвристикалық технологияларын қолдану. 13. Пайдаланушының немесе әкімшінің талабы бойынша және

	кестеге сәйкес антивирустық сканерлеу. 14. Microsoft Office макростарын зиянды кодқа тексеруге мүмкіндік беретін құжаттарды қорғау модулі. 15. ОЖ іске қосылған кезде файлдарды сканерлеу мүмкіндігі. 16. WMI және жүйелік тізілімді, барлық бөлімдер мен кіші бөлімдерді сканерлеу мүмкіндігі, бұл зиянды бағдарламалық кодтан және деректер түрінде таратылатын зиянды сілтемелерден қорғауды қамтамасыз етеді. 17. Conficker, Sirefef, Necurs және басқалары сияқты күрделі тұрақты қауіптердің қалдықтарын тазарту үшін бірнеше утилиталарды біріктіретін кіріктірілген құралдың болуы 18. Компьютерді белсенді емес күйде сканерлеу. 19. Нысандар мен сканерлеу әдістерін анықтау, файлды сканерлеудің максималды өлшемі мен уақытын орнату, Мұрағат тіркемесінің максималды тереңдігі және ерекшеліктер жасау сияқты антивирустық сканердің егжей-тегжейлі параметрлерін анықтау мүмкіндігі. 20. Сканерлеу үшін 64 биттік ядроны пайдалану жүйеге жүктемені азайтады және ең жылдам және тиімді сканерлеуге мүмкіндік береді. 21. Зиянды бағдарламалық жасақтаманың зиянды әрекеттері мен сипаттамаларын анықтау үшін кодты тереңірек талдау үшін машиналық оқыту технологияларын қолдану мүмкіндігі. 22. Java, Flash және басқалары сияқты әртүрлі қолданбалардың осалдықтарын пайдалана алатын қауіптерден қорғауды қамтамасыз ететін эксплуатациядан қорғау модулі 23. Іске қосылған процестерді және олардың файлдық жүйедегі қызметін терең талдайтын Модуль, бұл төлем бағдарламаларынан (ransomware) қосымша қорғаныс қабатын қамтамасыз етеді. 24. Күдікті іске қосылған процестердің жұмысын бақылауға қабілетті жедел жадты сканерлеу модулі, бұл тіпті Мұқият шифрланған және жасырын қауіптермен инфекцияның алдын алады. 25. Бағдарламалардың іске қосылуын және жүйелік тізілімдегі өзгерістерді бақылайтын және компьютерді зиянды бағдарламалар мен қажетсіз әрекеттерден қорғайтын интрузияны анықтау жүйесінің (HIPS) болуы. 26. Іске қосылған процестерді, орындалатын файлдарды және тізілім бөлімдерін бақылау үшін реттелетін ережелер жасау мүмкіндігі. 27. Бұлтты бедел қызметінде іске қосылған процестерді қосымша тексеру. 28. Қосымша бағдарламалық өнімдерді орнатуды қажет етпестен жұмыс станциялары мен серверлерді қорғауды бұлтты құмсалғышпен (қосымша лицензия болған жағдайда) біріктіру мүмкіндігі. 29. Ауыстырылатын медианы автоматты антивирустық тексеру. 30. Қол жеткізу ережелерін құру арқылы ауыспалы медианың жұмыс станциясына қосылуын басқара алатын құралдың болуы, атап айтқанда құлыптау, рұқсат беру, тек оқу, оқу және жазу, ескерту. 31. Құрылғының түрі, өндірушісі, моделі немесе құрылғының сериялық нөмірі бойынша сыртқы құрылғылардың жұмыс станциясына қосылуын бақылау мүмкіндігі. 32. Рұқсат етілген немесе тыйым салынған сыртқы құрылғылар тобын құру мүмкіндігі. 33. Барлық және жеке пайдаланушылар немесе Windows немесе домен топтары үшін сыртқы құрылғыларды қосуға тыйым салу немесе рұқсат беру мүмкіндігі. 34. Құрылғыларды басқару ережелерін икемді түрде реттеуге мүмкіндік беретін уақыт аралықтарын орнату мүмкіндігі. 35. POP3,

	POP3S, SMTP, IMAP және IMAPS тексеру мүмкіндігімен электрондық пошта клиентіне интеграциялау және пошта тіркемелерін тексеру арқылы жұмыс станциясында пошта трафигін қорғаудың қосымша деңгейін қамтамасыз ету, әсіресе корпоративтік желіден тыс уақытша немесе тұрақты компьютерлерде. 36. Электрондық пошта клиентіндегі көрсетілген каталогқа вирус жұққан поштаны автоматты түрде жою немесе жылжыту мүмкіндігі. 37. Электрондық пошта клиентіне интеграциялану мүмкіндігі бар жеке әзірленген спамнан қорғау модулінің болуы, бұл спамнан қорғаудың қосымша қабатын қамтамасыз етеді, әсіресе корпоративтік желіден тыс уақытша немесе тұрақты компьютерлерде. 38. Спам-адресаттардың АҚ және қара тізімдерін пайдалану мүмкіндігі пайдаланушы (ақылды спам модулін икемді жекелендіру) және ғаламдық, оларға ақпарат жаңарту серверлерінен келеді. 39. HTTP, HTTPS трафигін тексеру арқылы Интернет-трафикті қорғаудың қосымша қабатын қамтамасыз ету, бұл осы протоколдар арқылы жіберілетін файлдарды бұғаттауға ғана емес, сонымен қатар фишингтік сайттар, ботнет серверлері, APT командалық (C&C) серверлері, сондай-ақ "ransomware" класындағы қауіптерді тарататын серверлер сияқты қауіпті ресурстардың мекен-жайларын бұғаттауға мүмкіндік береді". 40. Бұғатталған, рұқсат етілген немесе URL тексеруден шығарылған тізімдерді құру мүмкіндігі. 41. Көрсетілген кеңейтім бойынша файлдарды интернеттен жүктеуді бұғаттау мүмкіндігі, әсіресе уақытша немесе үнемі корпоративті желіден тыс компьютерлерде. 42. SSL протоколын Автоматты және интерактивті режимдерде тексеру мүмкіндігі. 43. SSL трафигі сертификаттарының жарамдылығы мен тұтастығын тексеру. 44. Тексеруден шығарылған сенімді сертификаттар мен сертификаттардың тізімдерін басқару мүмкіндігі, сондай-ақ жарамсыз, белгісіз немесе бүлінген сертификатты анықтау кезінде әрекетті таңдау мүмкіндігі. 45. 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. 46. Жеке бағдарламалар мен жеке IP-объектілер (IP-адрестер, IP-адрестер диапазондары, ішкі желілер) үшін трафикті тексеру бойынша ерекшеліктер жасау мүмкіндігі. 47. Желілік сүзуді жүзеге асыру және сыртқы және жергілікті желілік шабуылдардан қорғау үшін жеке брандмауэрдің болуы. 48. Жеке брандмауэрде интерактивті режимнің болуы, ол жаңа белгісіз желілік байланыс туралы егжей-тегжейлі ақпарат береді және компьютерде анықталған қосылым үшін жаңа Желілік сүзу ережесін құруға ғана емес, сонымен қатар ол үшін егжей-тегжейлі параметрлерді көрсетуге мүмкіндік береді. 49. Жеке брандмауэрде әкімшіге желілік қосымшалар мен жабдықтар үшін рұқсат беру ережелерін қашықтан конфигурациялауға мүмкіндік беретін оқу режимінің болуы. 50. Жасалған ережелерді өңдеуге ғана емес, сонымен қатар рұқсат етілмеген Желілік қосылыстар мен жергілікті желілік шабуылдардан алғашқы Мұқият қорғаныс

	үшін жеткілікті ендірілген ережелерді басқаруға мүмкіндік беретін ереже редакторының болуы. 51. Нақты бағдарламалар мен қызметтер үшін желіні сүзу ережелерін құру мүмкіндігі. 52. Компьютер қай желіге қосылғанына байланысты автоматты түрде ауыса алатын жеке брандмауэр үшін әртүрлі профильдер жасау мүмкіндігі. 53. Дербес брандмауэрде ДК-нің белгісіз қауіпті желілерге рұқсатсыз қосылуын болдырмау мақсатында желінің қосымша аутентификациясын пайдалану мүмкіндігі. 54. 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. 55. Компьютерге ықтимал желілік шабуылдардың әртүрлі түрлерін анықтау үшін кіруді анықтау жүйесі (IDS) Модулінің қосымша параметрлерін теңшеу мүмкіндігі. 56. "Ботнет" сияқты қауіптерден қорғауды қамтамасыз ететін технологияны пайдалану мүмкіндігі. 57. Желілік протоколдың осалдықтарын қорғау, бұл SMB, RPC, RDP және басқалары сияқты желілік протоколдардың кемшіліктерін пайдаланатын қауіптерді анықтауды жақсартады 58. Бағдарламалық жасақтаманың осалдығын пайдалануға және CVE идентификаторлары туралы толығырақ ақпарат беруге тырысатын әртүрлі шабуылдарды анықтаудың енгізілген әдістерінің болуы. 59. Компьютерде автоматты түрде бұғатталған желі қосылымдарын көру және қажет болған жағдайда белгілі бір қауіпсіз желі қосылымдарына уақытша рұқсат беру мүмкіндігі. 60. 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. 61. Жаңа рұқсат етілмеген желілік қосылыстарға алып келген желілік бағдарламалардағы өзгерістерді анықтай алатын жеке брандмауэрдің қосымша функционалдығының болуы. 62. Интернет-трафикті сүзу. 63. Веб-бақылау Модулінің болуы, бұл сайттардың белгілі бір санаттарына кіруді шектеуге мүмкіндік береді. 64. 100-ден астам ішкі санаттар бөлінген Интернет-трафикті сүзудің 27 санаты, сондай-ақ санаттар мен ішкі санаттар бойынша топтар құру мүмкіндігі. 65. Әр түрлі пайдаланушылар мен Windows ОЖ немесе домен топтары үшін Интернет-трафикті сүзу ережелерін құру мүмкіндігі. 66. Веб-сүзу ережелерін икемді түрде реттеуге мүмкіндік беретін уақыт аралықтарын орнату мүмкіндігі. 67. Вирустық базаларды тәулігіне кемінде 24 рет регламенттік жаңарту. 68. Сервердегі жергілікті жадтан клиенттердің жаңартуын алу, бұл Интернет желісіне қол жеткізе алмайтын жабық оқшауланған желілерде антивирустық қорғауды жаңартуға мүмкіндік береді. 69. Соңғы нүктелерді қорғау шешімдеріне негізделген жаңарту айнасын жасау мүмкіндігі. 70. Егер жаңартудың негізгі көзі қол жетімді болмаса, вирустық базаның жаңартуларын резервтік көздерден алу мүмкіндігі. 71. Портативті компьютерлер үшін кәсіпорын желісінен тыс болған жағдайда өндірушінің серверлерінен жаңартуларды онлайн алу мүмкіндігі. 72. Вирустық қолтаңба

	базалары мен жаңарту модульдерінің алдыңғы нұсқаларына оралу мүмкіндігімен және жаңартуларды уақытша кідірту немесе жаңаларын қолмен орнату мүмкіндігімен жаңартуларды кері қайтару. 73. Тұрақты, сынақ және кешіктірілген жаңартуларды алу режимінде жаңарту мүмкіндігі. 74. Мониторинг, қауіпсіздік жағдайын бағалау және әрекет ету құралдары: 75. ОЖ жаңартуларының қауіпсіздігі мен өзектілігін бақылау механизмінің болуы. 76. 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. 77. Операциялық жүйеде рұқсатсыз және қауіпті өзгерістерді анықтау мақсатында операциялық жүйенің әртүрлі параметрлерінің мәндерінің сыни деңгейін (қауіпті, белгісіз, аз белгілі, қауіпсіз) анықтау мүмкіндігі. 78. Жүйеде белгілі бір уақыт ішінде болған өзгерістерді анықтау үшін жүйенің күйінің әртүрлі суреттерін салыстыру мүмкіндігі. 79. Сценарийлерді жасау және қашықтан орындау мүмкіндігі, бұл қашықтағы компьютерде жұмыс істеп тұрған процестер мен қызметтерді тоқтатуға, тізілім тармақтарын жоюға, желілік қосылымдарды бұғаттауға мүмкіндік береді. 80. Жұмыс станцияларында журналдарды Жергілікті сақтау. 81. Жоспарланған тапсырмаларды құруға мүмкіндік беретін тапсырмаларды жоспарлаушының болуы, оның ішінде сыртқы бағдарламаны іске қосу, жүйені іске қосу кезінде файлдарды тексеру, жүйенің күйін суретке түсіру, Компьютерді тексеру, вирустық базалар мен бағдарлама модульдерін жаңарту. 82. Бір рет, мезгіл-мезгіл, сондай-ақ нақты оқиғалар туындаған жағдайда басталатын тапсырмаларды жоспарлау мүмкіндігі. 83. Жоспарлаушыда әр түрлі кезеңділікпен немесе әр түрлі іске қосу шарттарымен бірнеше бірдей тапсырмаларды құру мүмкіндігі. 84. Антивирустық өнімі орнатылған CD және USB медиасында жүктеу дискісін құру мүмкіндігі. 85. Соңғы нүктені қорғау үшін шешім параметрлерін құпия сөзбен қорғау мүмкіндігі. 86. Саясатты қайта анықтау режимінің болуы, бұл жүйелік әкімшіге белгілі бір ортада антивирустық бағдарламаны икемді конфигурациялау мақсатында саясат тағайындайтын және өңдеуге қол жетпейтін антивирустық бағдарламалардың параметрлерін компьютерде өзгертуге уақытша мүмкіндік береді. 87. Жоғары ажыратымдылықтағы сенсорлық экранмен үйлесімді графикалық интерфейс. 88. Пайдаланушының жұмыс үстеліндегі оқиғалар туралы хабарландырулар мен хабарламаларды икемді түрде теңшеу мүмкіндігі. 89. Клиенттік жұмыс станциясына қашықтан орнату мүмкіндігі. 90. Желіге қосылғаннан немесе VDI ортасында іске қосылғаннан кейін бірден басқару серверіне қосылуға мүмкіндік беретін кешенді инсталлятордың көмегімен жеке компьютерлерде немесе VDI кескінінде алдын ала орнату мүмкіндігі. 91. Компоненттерді автоматты режимде жаңартуға мүмкіндік беру мүмкіндігі, бұл компоненттерді әкімшінің немесе пайдаланушының араласуынсыз жүктеуге және орнатуға мүмкіндік береді. 92. Басқарылмайтын жұмыс

	станцияларында компоненттерді жаңартуға мүмкіндік беретін компоненттерді қолмен жаңарту мүмкіндігі. 93. Функцияны бастау үшін қайта жүктеуді қажет етпестен кейбір компоненттерді жаңарту мүмкіндігі. 94. Барлық хабарламаларды антивирустық бағдарламадан жасыру мүмкіндігімен толық экранда жұмыс істейтін бағдарламалардың жұмысын қолдау. 95. "Антивирустық өнімде барлық негізгі модульдер мен сервистердің тиімді жұмыс істеуі үшін қарызға алынған емес, өзінің технологиялық әзірлемелері пайдаланылуы тиіс. 96. Негізгі мүмкіндіктен басқа, резервтік әкімшілік серверлерді көрсету мүмкіндігі. 97. Қашықтан басқару құралының болуы. 98. 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. 99. Орыс тілін қамтитын көп тілді орнатушының болуы. 100. ОЖ қолдау: Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7, 8 .; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 немесе одан жоғары; Android 5 (Lollipop) немесе одан жоғары; 101. Microsoft Windows 10 Multi-session және Azure virtualized Windows 10 қолдауы 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. Зиянды бағдарламалардан, трояндық бағдарламалардан, пернетақта тыңшыларынан, жарнамалық бағдарламалардан, фишингтен, шпиондық бағдарламалардан, руткиттерден, сценарийлерден, Ықтимал қалаусыз және қауіпті бағдарламалардан қорғауды қамтамасыз ету. 3. Нақты уақыт режимінде қорғауды қамтамасыз ету. 4. Сканерлеу кезінде эвристикалық технологияны қолдану. 5. Пайдаланушының немесе әкімшінің талабы бойынша және кестеге сәйкес антивирустық сканерлеу. 6. Microsoft Hyper-V серверінің дискілерін, яғни виртуалды машиналарды (VM) тиісті виртуалды машиналарға ешқандай агенттерді орнатпай-ақ сканерлеуге мүмкіндік беретін вирустарға арналған Hyper-V сканерлеу. 7. Макростарды зиянды кодқа тексеруге мүмкіндік беретін Microsoft Office құжаттарды қорғау модулі. 8. Java, Flash және басқа қолданбалардың осалдықтарын пайдалана алатын қауіптерден қорғауды қамтамасыз ететін эксплуатациядан қорғау. 9. Пайдаланушыларды төлем бағдарламаларынан қорғаудың қосымша қабаты барлық бағдарламаларды олардың мінез-құлқы мен беделіне қарай бақылайды және бағалайды. 10. Қосымша бағдарламалық өнімдерді орнатуды қажет етпестен жұмыс станциялары мен серверлерді қорғауды бұлтты құмсалғышпен (қосымша лицензия болған жағдайда) біріктіру мүмкіндігі. 11. UEFI интерфейсін сканерлеу-негізгі жүктеу жазбасында зиянды бағдарламалық жасақтаманы тексеру. 12. Амалдық жүйені іске қосу кезінде файлдарды сканерлеу мүмкіндігі. 13. Жетілдірілген жад сканері күдікті процестерді олар пайда

	болғаннан кейін бақылайды және сканерлейді, бұл тіпті Мұқият шифрланған және жасырын қауіптермен инфекцияның алдын алады. 14. Компьютерді белсенді емес күйде сканерлеу. 15. Нысандар мен сканерлеу әдістерін анықтау, файлды сканерлеудің максималды өлшемі мен уақытын орнату, Мұрағат тіркемесінің максималды тереңдігі және ерекшеліктер жасау сияқты антивирустық сканердің егжей-тегжейлі параметрлерін анықтау мүмкіндігі. 16. Ауыстырылатын медианы автоматты антивирустық тексеру. 17. Құрылғының типі, іс-әрекеті, жасаушысы, моделі және құрылғының сериялық нөмірі бойынша ережелер жасау мүмкіндігімен ауыстырылатын тасымалдағыштарды бақылау. 18. 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. 19. Компьютерді зиянды бағдарламалардан және қажетсіз әрекеттерден қорғайтын интрузияны анықтау жүйесінің (HIPS) болуы. Сондай-ақ, Бұл модульде ережелер жасау шебері және жұмыс істеп тұрған процестерді, пайдаланылған файлдарды және тізілім бөлімдерін басқаруға арналған ережелер редакторы бар. 20. Бұлтты бедел қызметінде іске қосылған процестерді қосымша тексеру. 21. Электрондық пошта клиентіне интеграцияланатын жұмыс станциясында электрондық пошта клиентін қорғауды қамтамасыз ету, POP3, POP3S, SMTP, IMAP және IMAPS тексерулері және пошта тіркемелерін тексеруді қамтамасыз ету. 22. Электрондық пошта клиентіндегі көрсетілген каталогқа вирус жұққан поштаны автоматты түрде жою немесе жылжыту мүмкіндігі. 23. HTTP, HTTPS трафигін тексеру, тексеруден шығарылған, бұғатталған және рұқсат етілген URL мекен-жайларын құру мүмкіндігі бар. 24. Көрсетілген кеңейтім бойынша Интернеттен файлдарды жүктеуді бұғаттау мүмкіндігі. 25. SSL протоколын тексеру және сертификаттардың түпнұсқалығы мен тұтастығын тексеру мүмкіндігі. Тексеруден шығарылған сенімді сертификаттар мен сертификаттардың тізімдерін басқару мүмкіндігі, сондай-ақ жарамсыз, белгісіз немесе бүлінген сертификатты анықтау кезінде әрекетті таңдау мүмкіндігі. 26. Жеке бағдарламалар мен жеке IP объектілері (IP-адрестер, IP-адрестер диапазондары, ішкі желілер) үшін трафикті тексеруден ерекшеліктер жасау мүмкіндігі. 27. Компьютерге ықтимал желілік шабуылдардың әртүрлі түрлерін анықтау үшін кіруді анықтау жүйесі (IDS) Модулінің қосымша параметрлерін теңшеу мүмкіндігі. 28. "Ботнет" түріндегі қауіптерден қорғауды қамтамасыз ететін технологияны пайдалану мүмкіндігі. 29. SMB, RPC, RDP және т. б. сияқты желілік протоколдардың кемшіліктерін пайдаланатын қауіптерді анықтауды жақсартатын желілік протоколдың осалдығын қорғау 30. Вирустық базаларды тәулігіне кемінде 24 рет регламенттік жаңарту. 31. Сервердегі жергілікті айнадан тұтынушы жаңартуын алу. 32. Антивирустық бағдарламалық жасақтама көмегімен жаңарту айнасын құру мүмкіндігі. 33. Егер негізгі жаңарту көзі қол жетімді

	болмаса, вирустық базаларды резервтік көздерден жаңарту мүмкіндігі. 34. Вирустық қолтаңба базалары мен жаңарту модульдерінің алдыңғы нұсқаларына оралу мүмкіндігімен және жаңартуларды уақытша кідірту немесе жаңаларын қолмен орнату мүмкіндігімен жаңартуларды қайтарыңыз. 35. Тұрақты, сынақ және кешіктірілген жаңартуларды алу режимінде жаңарту мүмкіндігі. 36. Қашықтан басқару құралының болуы. 37. Негізгі мүмкіндіктен басқа, резервтік әкімшілік серверлерді көрсету мүмкіндігі. 38. Операциялық жүйенің жаңартуларының өзектілігін бақылау механизмінің болуы. 39. 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. 40. Наличие планировщика задач, который позволит создавать запланированные задачи, включая запуск внешней программы, проверку файлов при запуске системы, создание снимка состояния системы, проверку компьютера, обновление вирусных баз и модулей программы. Возможность планирования задач, которые будут запускаться однократно, периодически и при возникновении конкретных событий. 41. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска. 42. Возможность работы в кластерах как домена, так и рабочей группы. 43. Возможность настройки быстродействия, указывая количество потоков сканирования. 44. Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов. 45. Антивирустық өнім орнатылған ЫҚШАМ дискіде де, USB медиасында да жүктелетін дискіні жасау мүмкіндігі. 46. Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО. 47. Возможность защиты паролем от изменения параметров и удаления антивирусного ПО. 48. Возможность удаленной установки на файловый сервер. 49. Возможность предустановки на отдельных файловых серверах с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети. 50. Microsoft Azure бұлттық қызметімен біріктіру мүмкіндігі 51. ОЖ қолдауы: Microsoft Windows Server 2008, 2008R2, 2012r2, 2012, 2016, 2019, 2022; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise сервер (sles) 12,suse LINUX ENTERPRISE SERVER (SLES) 15,ORACLE

	LINUX 8, amazon linux 2. Бағдарламалық қамтылымның лицензиялылығын растауға қойылатын талаптар Әлеуетті өнім беруші өтінім құрамында ұсынылатын антивирустық бағдарламалық қамтылым лицензияларын Қазақстан Республикасының аумағында жеткізу құқығын растайтын антивирустық бағдарламалық қамтылым өндірушісінің немесе оның ресми өкілінің (дилерінің немесе дистрибьюторының) авторизациялық хатын ұсынады. Хатта өндірушінің атауы, ұсынылатын бағдарламалық қамтылымның атауы және әлеуетті өнім берушінің тиісті лицензияларды жеткізуге өкілеттігі расталуы тиіс. Ұсынылатын бағдарламалық қамтылым техникалық ерекшелікте көзделген мерзімге кемінде 120 жұмыс станциясын қорғауға арналған корпоративтік лицензиялармен қамтамасыз етуге мүмкіндік беруі тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Республиканское государственное учреждение "Академия правосудия при Высшем Судебном Совете Республики Казахстан"
Наименование организатора	Республиканское государственное учреждение "Академия правосудия при Высшем Судебном Совете Республики Казахстан"
№ конкурса:	№ 17972002-1
Наименование конкурса:	Услуги по предоставлению лицензий на корпоративное антивирусное программное обеспечение и технической поддержке.
Номер лота:	№ 83354590-ОКЗ
Наименование лота:	Услуги по технической поддержке лицензионного программного обеспечения
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620920.000.000027
Наименование услуги:	Услуги по технической поддержке лицензионного программного обеспечения
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	2275862.07
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	2275862.07
Срок оказания услуги:	в течение 15 календарных дней после подписания договора.
Размер авансового платежа* *:	30 %
Гарантийный срок (в месяцах)	12
Описание требуемых характеристик, параметров и иных исходных данных	Услуги по предоставлению лицензий на корпоративное антивирусное программное обеспечение и технической поддержке.

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)	ТЕХНИЧЕСКОЕ СПЕЦИФИКАЦИЯ Наименование услуги: Услуги по предоставлению лицензий на корпоративное антивирусное программное обеспечение и технической поддержке. Заказчик: РГУ «Академия правосудия при Высшем Судебном Совете Республики Казахстан». Наименование программного обеспечения: Корпоративное антивирусное программное обеспечение для защиты рабочих станций. Количество лицензий: 120 (сто двадцать) рабочих станций. Срок действия лицензий: не менее 12 (двенадцати) месяцев с даты активации лицензий либо с даты начала срока действия лицензии, определенной условиями лицензирования производителя. Технические требования: 1. Предоставление 120 (сто двадцать) лицензий на корпоративное антивирусное программное обеспечение для защиты рабочих станций Заказчика. 2. Обеспечение защиты рабочих станций от вирусов, вредоносных программ, шпионского программного обеспечения и иных киберугроз. 3. Обеспечение регулярного обновления антивирусных баз и программных компонентов в течение всего срока действия лицензий. 4. Предоставление доступа к централизованному управлению защитой рабочих станций при наличии соответствующей функциональности в выбранном лицензионном продукте. 5. Предоставление технической поддержки производителя программного обеспечения в соответствии с условиями приобретенной лицензии. 6. Предоставление лицензионных ключей, кодов активации либо иных предусмотренных производителем средств активации лицензий. 7. Подтверждение легальности происхождения лицензий и права их использования Заказчиком. Место оказания услуг: Республика Казахстан, город Астана, улица Бейбітшілік, 46, здание РГУ «Академия правосудия при Высшем Судебном Совете Республики Казахстан». Результат оказания услуг: Предоставление Заказчику 120 (сто двадцать) действующих корпоративных лицензий на антивирусное программное обеспечение с обеспечением обновлений и технической поддержки в течение установленного срока. Антивирусная защита (АЗ) должна представляет собой корпоративное решение, обеспечивающее устойчивое функционирование в сети рабочих станций и серверов. В рамках всей организации используются единые антивирусные средства. Настоящая Техническая спецификация является основополагающим документом, устанавливающим требования к поставляемому программному обеспечению с оказанием сопутствующих услуг по внедрению системы антивирусной защиты. Все компоненты системы должны имеют полную интеграцию между собой. 1. Общие требования к программному обеспечению по антивирусной защите 1.1. Общее количество защищаемых узлов: Срок действия лицензии: 12 (двенадцать) месяцев с момента генерации лицензий на программное обеспечение. 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. Инвентаризация оборудования, которое установлено на рабочих станциях и серверах под управлением Windows, MacOS и Linux. 4. Инвентаризация программного обеспечения, которое установлено на рабочих станциях и серверах под управлением Windows, macOS и Linux. 5. Удаленная установка антивирусного программного обеспечения для операционных систем Windows, Linux и Mac на несколько конечных точек одновременно. 6. Удаленная установка пользовательского программного обеспечения. 7. Возможность удаленного удаления установленного пользовательского программного обеспечения. 8. Удаленное удаление антивирусного программного обеспечения для операционных систем Windows, Linux и Mac. 9. 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. 10. Наличие инструмента для создания и редактирования установочных пакетов для операционных систем Windows, Linux и Mac с предварительно установленными настройками конфигурации, что позволяет экспортировать установочные пакеты для развертывания полноценной антивирусной защиты на конечных точках в изолированной сети, а также на конечных точках, которые нуждаются в защите, но временно не подключены к серверу администрирования. 11. Наличие диспетчера пользователей, который позволяет создавать разных пользователей сервера администрирования и назначать им разные права доступа к отдельным разделам, группам компьютеров на сервере администрирования, что дает возможность предоставить разные права доступа для региональных системных администраторов разветвленной системы антивирусной защиты. 12. Возможность аутентифицировать администраторов консоли управления с помощью групп безопасности Active Directory. 13. Возможность использования двухфакторной аутентификации для учетных записей администраторов, что позволяет предотвратить несанкционированное подключение к серверу централизованного управления. 14. Наличие журнала аудита, в котором регистрируются и отслеживаются все изменения в конфигурации и все действия, которые выполняют пользователи сервера администрирования. 15. 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. 16. Возможность создавать и редактировать статические группы и возможность импорта из Active Directory дерева компьютеров. 17. Возможность настройки автоматического распределения клиентов по динамическим группам по многим критериям с последующим назначением соответствующих политик безопасности, а также запуском необходимых задач. 18. Возможность импорта

	пользователей и групп из Active Directory для дальнейшего использования их для персонализации правил контроля устройств и веб-контроля. 19. Возможность использовать как встроенные, так и пользовательские политики, предназначенные для постоянного обслуживания конфигурационных настроек антивирусных продуктов. Возможность осуществлять экспорт/импорт политик. 20. Наличие панели мониторинга, которая предоставляет всю необходимую подробную информацию относительно уровня защиты безопасности инфраструктуры, состояния защищенных конечных точек, а также состояния самого сервера администрирования. 21. Наличие около 100 предустановленных шаблонов отчетов, которые могут использоваться как для панели мониторинга, так и для формирования различных отчетов. 22. Возможность создавать и редактировать шаблоны отчетов, которые используются как для панели мониторинга, так и для формирования отчетов в форматах PDF, CSV и дальнейшего хранения по указанному пути или отправки на указанную электронную почту. 23. Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL. 24. Возможность экспортировать журналы в syslog для дальнейшей интеграции с SIEM. 25. Возможность настраивать параметры журналов и отчетов или выбрать из более чем 50 шаблонов для различных систем/клиентов. 26. Возможность создавать зеркало обновлений с помощью антивирусного продукта, специальной утилиты или прокси сервера. 27. Возможность создания зеркала обновлений на основе сторонних HTTP-серверов. 28. Веб-ориентированный интерфейс, который дает возможность управлять сервером через любой браузер путем соединения, защищенного сертификатом. 29. 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. 30. Возможность отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор. 31. Дополнительный компонент, что позволяет управлять антивирусной защитой на мобильных устройствах. 32. Специальный компонент, который осуществляет обнаружение в сети незащищенных рабочих станций для дальнейшего развертывания антивирусной защиты. 33. Защита соединений между компонентами сервера с помощью как самостоятельно выпущенных сертификатов, так и существующих сертификатов. 34. Инструмент для управления состоянием лицензий (даже без использования сервера администрирования). 35. Возможность деактивировать лицензию антивирусных продуктов даже на рабочих станциях, к которым нет физического или удаленного доступа. 36. Возможность установки сервера администрирования на ОС Windows и Linux. 37. Поставка сервера администрирования в развернутом виде, готовом для использования в виртуальных средах, таких как Microsoft Hyper-V, Oracle VirtualBox, VMware (ESXi/vSphere/Player/Workstation). 38. Поддержка систем виртуализации, таких как VMware Horizon 8.x или Citrix XenCenter/XenServer 8+. 39.

	Возможность определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI. 40. Наличие мастера настройки для определения подробных параметров для интеграции с системами VDI. 41. Возможность выбирать варианты обработки идентификаторов клонированных компьютеров, такие как сопоставление существующими компьютерами или создание новых компьютеров. 42. Возможность определять параметры шаблона именования VDI для мгновенных клонов или каталогов машин. 43. Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI. 44. Наличие автоматического обновления агента управления, что дает возможность без вмешательства администраторов использовать актуальные версии. 45. Наличие механизма распределения автоматического процесса обновления, что дает возможность снизить нагрузку на сеть и компьютеры в целом. 46. Возможность установки агента управления на ARM64 процессорах. 47. Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам. 48. Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии. Защита рабочих станций 1. Предоставление защиты от вирусов, троянского ПО, рекламного ПО, фишинга, а также шпионского ПО. 2. 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. 3. 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. 4. Предоставление защиты от потенциально опасных программ – разнообразного ПО, которое может использоваться для вредоносных целей, таких как несанкционированный удаленный доступ, кража или взлом паролей, клавиатурные шпионы и другие 5. Предоставление защиты от подозрительных программ – программ, которые сжатые упаковщиками или протекторами, которые часто используют злоумышленники для предотвращения обнаружения вредоносного программного обеспечения. 6. 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. 7. Возможность для различных категорий угроз настраивать отдельные уровни реагирования как для защиты, так и для отчетности. 8. Возможность делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может

	привести к отклонениям в работе или влиять на продуктивность системы. 9. Возможность создания исключений для общесистемных процессов с целью улучшить скорость работы системных служб и минимизировать вмешательство в процесс работы ОС. 10. Возможность осуществлять проверку загрузочных секторов на наличие вирусов в главной загрузочной записи, в том числе интерфейса UEFI. 11. Обеспечение антивирусной защиты в режиме реального времени. 12. Использование эвристических технологий собственной разработки во время сканирования. 13. Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком. 14. Модуль защиты документов, которые дают возможность проверять макросы Microsoft Office на наличие вредоносного кода. 15. Возможность сканирования файлов во время запуска ОС. 16. Возможность сканирования WMI и системного реестра, всех разделов и подразделов, что обеспечивает защиту от вредоносного программного кода и злонамеренных ссылок, которые распространяются в виде данных. 17. Наличие встроенного инструмента, что объединяет несколько утилит для очистки остатков сложных устойчивых угроз, таких как Conficker, Sirefef, Necurs и других 18. Сканирование компьютера в неактивном состоянии. 19. Возможность определения подробных параметров работы антивирусного сканера, таких как определение объектов и методов сканирования, возможность установки максимального размера и времени сканирования файла, максимальная глубина вложения архива и создание исключений. 20. Использование 64-битного ядра для сканирования, что уменьшает нагрузку на систему и позволяет сделать самые быстрые и эффективные сканирования. 21. Возможность использования технологий машинного обучения для более углубленного анализа кода с целью выявления вредоносного поведения и характеристик вредоносного программного обеспечения. 22. Модуль защиты от эксплойтов, который обеспечивает защиту от угроз, способных использовать уязвимости различных приложений, таких как Java, Flash и других 23. Модуль, который глубоко анализирует запущенные процессы и их деятельность в файловой системе, что обеспечивает дополнительный уровень защиты от программ-вымогателей (ransomware). 24. Модуль сканирования оперативной памяти, который способный отслеживать работу подозрительных запущенных процессов, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами. 25. Наличие системы обнаружения вторжений (HIPS), которая отслеживает запуск программ и изменения в системном реестре и защищает компьютер от вредоносных программ и нежелательной активности. 26. Возможность создавать собственные правила для контроля запущенных процессов, исполняемых файлов и разделов реестра. 27. Дополнительная проверка запущенных процессов в облачном репутационном сервисе. 28. Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов. 29. Автоматическая антивирусная

	проверка сменных носителей. 30. Наличие инструмента, который сможет осуществлять контроль подключения к рабочей станции сменных носителей путем создания правил доступа, а именно блокировка, разрешение, только чтение, чтение и запись, предупреждение. 31. Возможность осуществлять контроль подключения к рабочей станции внешних устройств по типу устройства, по производителю, модели или серийному номеру устройства. 32. Возможность создавать группы разрешенных или запрещенных внешних устройств. 33. Возможность запрещать или разрешать подключение внешних устройств как для всех, так и для отдельных пользователей или групп Windows или домена. 34. Возможность задавать временные интервалы, что позволяет более гибко настраивать правила контроля устройств. 35. Обеспечение дополнительного уровня защиты почтового трафика на рабочей станции путем интеграции в почтовый клиент с возможностью проверки POP3, POP3S, SMTP, IMAP и IMAPS и проверки почтовых вложений, особенно на тех ПК, которые временно или постоянно находятся за пределами корпоративной сети. 36. Возможность автоматически удалять или перемещать зараженную почту в указанный каталог в почтовом клиенте. 37. Наличие модуля защиты от спама собственной разработки с возможностью интеграции в почтовый клиент, что обеспечивает дополнительный уровень защиты от спама, особенно на тех ПК, которые временно или постоянно находятся за пределами корпоративной сети. 38. Возможность использовать белые и черные списки спам-адресатов как пользовательские (гибкая персонализация интеллектуального спам-модуля), так и глобальные, информация к которым приходит с серверов обновления. 39. Обеспечение дополнительного уровня защиты Интернет-трафика путем проверки HTTP, HTTPS трафика, что позволяет не только блокировать файлы, которые передаются этими протоколами, но и блокировать адреса таких опасных ресурсов, как фишинговые сайты, серверы ботнетов, командные (C&C) серверы APT, а также серверы, которые распространяют угрозы класса «ransomware». 40. Возможность создания списков заблокированных, разрешенных или исключенных из проверки URL-адресов. 41. Возможность блокировать загрузку из Интернета файлов по указанному расширению, особенно на тех ПК, которые временно или постоянно находятся за пределами корпоративной сети. 42. Возможность проверки протокола SSL как в автоматическом, так и в интерактивном режимах. 43. Проверка действительности и целостности сертификатов SSL-трафика. 44. Возможность управлять списками доверенных сертификатов и сертификатов, исключенных из проверки, а также возможность выбора действия при определении сертификата недействительным, неопределенным или поврежденным. 45. 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. 46. Возможность создания исключений по проверке

	трафика для отдельных программ и отдельных IP-объектов (IP-адресов, диапазонов IP-адресов, подсетей). 47. Наличие персонального брандмауэра для осуществления сетевой фильтрации и защиты как от внешних, так и от локальных сетевых атак. 48. Наличие в персональном брандмауэре интерактивного режима, что предоставляет подробную информацию о новом неизвестном сетевом соединении и дает возможность не только создавать на ПК новое правило сетевой фильтрации для обнаруженного соединения, но и указывать подробные настройки для него. 49. Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования. 50. Наличие редактора правил, что позволяет не только редактировать созданные правила, но и управлять встроенными правилами, которых достаточно для первичной тщательной защиты от несанкционированных сетевых соединений и локальных сетевых атак. 51. Возможность создания правил сетевой фильтрации для конкретных программ и сервисов. 52. Возможность создания для персонального брандмауэра различных профилей, которые могут автоматически переключаться, в зависимости от того, к какой сети подключен компьютер. 53. Возможность использовать в персональном брандмауэре дополнительную аутентификацию сети с целью предотвращения несанкционированного подключения ПК к неизвестным опасным сетям. 54. 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. 55. Возможность настройки дополнительных параметров модуля системы обнаружения вторжений (IDS) с целью выявления различных типов возможных сетевых атак на компьютер. 56. Возможность использования технологии, которая обеспечивает защиту от угроз типа «ботнет». 57. Защита уязвимостей сетевого протокола, что улучшает выявление угроз, которые используют недостатки сетевых протоколов, таких как SMB, RPC, RDP и других 58. Наличие внедренных методов выявления различных атак, которые пытаются использовать уязвимости программного обеспечения и предоставить более подробную информацию об идентификаторах CVE. 59. Возможность просматривать на ПК автоматически заблокированные сетевые соединения и при необходимости временно разрешать конкретные безопасные сетевые соединения. 60. 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. 61. Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения. 62. Фильтрация Интернет-трафика. 63. Наличие модуля веб-контроля, что позволяет ограничивать доступ к определенным категориям

	сайтов. 64. 27 категорий фильтрации Интернет-трафика, в которых распределены более 100 подкатегорий, а также возможность создавать группы по категориям и подкатегориям. 65. Возможность создавать правила фильтрации Интернет-трафика для разных пользователей и групп ОС Windows или домена. 66. Возможность задавать временные интервалы, что позволяет более гибко настраивать правила веб-фильтрации. 67. Регламентное обновление вирусных баз не менее 24 раз в сутки. 68. 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. 69. Возможность создания зеркала обновлений на основе решений для защиты конечных точек. 70. Возможность получения обновлений вирусных баз из резервных источников, если основной источник обновления будет недостижим. 71. Возможность для портативных компьютеров получать обновления с серверов производителя онлайн, в случае нахождения за пределами корпоративной сети. 72. Откат обновлений с возможностью вернуться к предыдущим версиям баз вирусных сигнатур и модулей обновления и возможностью временно приостановить обновления или устанавливать новые вручную. 73. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений. 74. Инструменты мониторинга, оценки состояния безопасности и реагирование: 75. Наличие механизма контроля за состоянием безопасности и актуальностью обновлений ОС. 76. 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. 77. Возможность определения уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы с целью выявления несанкционированных и опасных изменений в операционной системе. 78. Возможность сравнивать различные снимки состояния системы с целью обнаружения изменений, которые произошли в системе за определенное время. 79. Возможность создавать и удаленно выполнять скрипты, что позволит на удаленном ПК останавливать запущенные процессы и службы, удалять ветки реестра, блокировать сетевые соединения. 80. Локальное хранение журналов на рабочих станциях. 81. Наличие планировщика задач, который позволит создавать запланированные задачи, среди которых запуск внешней программы, проверка файлов при запуске системы, создание снимка состояния системы, проверка компьютера, обновление вирусных баз и модулей программы. 82. Возможность планирования задач, которые будут запускаться однократно, периодически, а также при условии возникновения конкретных событий. 83. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска. 84. Возможность создания загрузочного диска как на CD-, так и USB-носителях с установленным антивирусным

	продуктом. 85. Возможность защиты паролем параметров решения для защиты конечной точки. 86. 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. 87. Графический интерфейс, совместимый с сенсорным экраном высокого разрешения. 88. Возможность гибко настраивать уведомления и сообщения о событиях на рабочем столе пользователя. 89. Возможность удаленной установки на клиентскую рабочую станцию. 90. Возможность предустановки на отдельных ПК или в образе VDI с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети или запуска в среде VDI. 91. Возможность разрешить обновление компонентов в автоматическом режиме, что позволяет загрузить и установить компоненты без вмешательства администратора или пользователя. 92. Возможность обновления компонентов в ручном режиме, что позволяет обновлять компоненты на неуправляемых рабочих станциях. 93. Возможность обновления некоторых компонентов без необходимости перезагрузки для начала функционирования. 94. Поддержка работы программ, которые работают в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО. 95. "В антивирусном продукте должны использоваться не заимствованные, а собственные технологические разработки для эффективной работы всех основных модулей и сервисов. 96. Возможность, кроме основного, указать резервные сервера администрирования. 97. Наличие инструмента удаленного управления. 98. 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. 99. Наличие многоязычного инсталлятора, который включает в себя в том числе русский язык. 100. Поддержка ОС: Microsoft Windows 7 (SP1); Microsoft Windows 8; Microsoft Windows 8.1; Microsoft Windows 10; Microsoft Windows 11; Ubuntu Desktop 18.04 LTS 64-bit; Ubuntu Desktop 20.04 LTS; Ubuntu Desktop 22.04 LTS; Red Hat Enterprise Linux 7, 8 .; SUSE Linux Enterprise Desktop 15; Linux Mint 20; macOS 10.12 или выше; Android 5 (Lollipop) или выше; 101. Поддержка Microsoft Windows 10 Multi-session и Azure virtualized 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. Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО. 3. Обеспечение защиты в режиме реального времени. 4. Использование эвристических технологий во время сканирования. 5. Антивирусное сканирование по требованию

	пользователя или администратора и согласно графику. 6. Сканирование Hyper-V на наличие вирусов, позволяющее сканировать диски сервера Microsoft Hyper-V Server, то есть виртуальные машины (ВМ), без необходимости установки каких-либо агентов на соответствующих виртуальных машинах. 7. Модуль защиты документов Microsoft Office, позволяющий проверять макросы на наличие вредоносного кода. 8. Защита от эксплойтов, которая обеспечивает защиту от угроз, способных использовать уязвимости Java, Flash и других приложений. 9. Дополнительный уровень защиты пользователей от программ-вымогателей контролирует и оценивает все программы на основе их поведения и репутации. 10. Возможность интеграции защиты рабочих станций и серверов с облачной песочницей (при наличии дополнительной лицензии) без необходимости установки дополнительных программных продуктов. 11. Сканирование интерфейса UEFI – проверка на наличие вредоносного программного обеспечения в главной загрузочной записи. 12. Возможность сканирования файлов во время запуска операционной системы. 13. Расширенный сканер памяти отслеживает и сканирует подозрительные процессы, как только они возникают, что позволяет предотвратить заражение даже тщательно зашифрованными и скрытыми угрозами. 14. Сканирование компьютера в неактивном состоянии. 15. Возможность определения подробных параметров работы антивирусного сканера, таких как определение объектов и методов сканирования, возможность установки максимального размера и времени сканирования файла, максимальная глубина вложения архива и создание исключений. 16. Автоматическая антивирусная проверка сменных носителей. 17. Контроль сменных носителей с возможностью создания правил по типу устройства, действиям, изготовителю, модели и серийному номеру устройства. 18. 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. 19. Наличие системы обнаружения вторжений (HIPS), защищающей компьютер от вредоносных программ и нежелательной активности. Также этот модуль содержит мастер для создания правил и редактор правил для контроля запущенных процессов, используемых файлов и разделов реестра. 20. Дополнительная проверка запущенных процессов в облачном репутационном сервисе. 21. Обеспечение защиты почтового клиента на рабочей станции с возможностью интеграции в почтовый клиент, проверка POP3, POP3S, SMTP, IMAP и IMAPS и обеспечение проверки почтовых вложений. 22. Возможность автоматически удалять или перемещать зараженную почту в указанный каталог в почтовом клиенте. 23. Проверка HTTP, HTTPS трафика с возможностью создания писем исключенных из проверки, заблокированных и разрешенных URL. 24. Возможность блокировать загрузку из Интернета файлов по указанному расширению. 25. Возможность проверки протокола SSL и

	проверки подлинности и целостности сертификатов. Возможность управления списками доверенных сертификатов и сертификатов исключенных из проверки, а также возможность выбора действия при определении сертификата недействующим, неопределенным или поврежденным. 26. Возможность создания исключений из проверки трафика для отдельных программ и отдельных IP-объектов (IP-адресов, диапазонов IP-адресов, подсетей). 27. Возможность настройки дополнительных параметров модуля системы обнаружения вторжений (IDS) для выявления различных типов возможных сетевых атак на компьютер. 28. Возможность использования технологии, обеспечивающей защиту от угроз типа «ботнет». 29. Защита уязвимостей сетевого протокола, улучшающая обнаружение угроз, использующих недостатки сетевых протоколов, таких как SMB, RPC, RDP и других 30. Регламентное обновление вирусных баз не менее 24 раз в сутки. 31. Получение обновления клиентов из локального зеркала на сервере. 32. Возможность создания зеркала обновления средствами антивирусного ПО. 33. Возможность обновления вирусных баз из резервных источников, если основной источник обновления будет недоступным. 34. Откат обновлений с возможностью вернуться к предыдущим версиям баз вирусных сигнатур и модулей обновления, и возможностью временно приостановить обновления или устанавливать новые вручную. 35. Возможность обновления в режиме получения регулярных, тестовых и отложенных обновлений. 36. Наличие инструмента удаленного управления. 37. Возможность помимо основного указать резервные серверы администрирования. 38. Наличие механизма контроля актуальности обновлений операционной системы. 39. 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. 40. Наличие планировщика задач, который позволит создавать запланированные задачи, включая запуск внешней программы, проверку файлов при запуске системы, создание снимка состояния системы, проверку компьютера, обновление вирусных баз и модулей программы. Возможность планирования задач, которые будут запускаться однократно, периодически и при возникновении конкретных событий. 41. Возможность создания в планировщике нескольких однотипных задач с разной периодичностью или разными условиями запуска. 42. Возможность работы в кластерах как домена, так и рабочей группы. 43. Возможность настройки быстродействия, указывая количество потоков сканирования. 44. Возможность настройки режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер,

	работающий в режиме сервера терминалов. 45. Возможность создания загрузочного диска как на CD-, так и на USB-носителях с установленным антивирусным продуктом. 46. Поддержка работы программ, работающих в полноэкранном режиме, с возможностью скрыть все сообщения от антивирусного ПО. 47. Возможность защиты паролем от изменения параметров и удаления антивирусного ПО. 48. Возможность удаленной установки на файловый сервер. 49. Возможность предустановки на отдельных файловых серверах с помощью комплексного инсталлятора, что позволит соединяться с сервером управления сразу после подключения к сети. 50. Возможность интеграции с облачным сервисом Microsoft Azure 51. Поддержка ОС: Microsoft Windows Server 2012, 2016, 2019, 2022; RedHat Enterprise Linux (RHEL) 7, RedHat Enterprise Linux (RHEL) 8, RedHat Enterprise Linux (RHEL) 9, CentOS 7, Ubuntu Server 18.04 LTS, Ubuntu Server 20.04 LTS, Ubuntu Server 22.04 LTS, Debian 10, Debian 11, SUSE Linux Enterprise Server (SLES) 12,SUSE Linux Enterprise Server (SLES) 15,Oracle Linux 8, Amazon Linux 2. Требование к подтверждению лицензионности программного обеспечения В составе заявки потенциальный поставщик предоставляет авторизационное письмо от производителя антивирусного программного обеспечения либо его официального представителя (дилера или дистрибьютора), подтверждающее право потенциального поставщика осуществлять поставку лицензий на предлагаемое программное обеспечение на территории Республики Казахстан. Письмо должно содержать наименование производителя, наименование предлагаемого программного обеспечения и подтверждение полномочий поставщика на поставку соответствующих лицензий. Предлагаемое программное обеспечение должно обеспечивать предоставление корпоративных лицензий на защиту не менее 120 рабочих станций на срок, предусмотренный технической спецификацией.