Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Павлодар облысының Полиция департаменті" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Павлодар облысының Полиция департаменті" мемлекеттік мекемесі
Конкурстың №:	№ 17915519-2
Конкурстың атауы:	Антивирустық бағдарламалық қамтамасыз ету лицензиясын ұзарту бойынша қызметтер
Лоттың нөмірі:	№ 88472534-ОК1
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 есептемегенде бірлік бағасы:	4693331.89
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	4693331.89
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	Шарт күшіне енген күннен бастап 61 күнтізбелік күн.
Аванстық төлем мөлшері:	30

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	1.1. Лицензия әртүрлі типтерге жататын, оның ішінде коммерциялық және еркін таратылатын операциялық жүйелерді басқаратын 845 жұмыс станциясын, сондай-ақ 5 файлдық серверді антивирустық қорғауды қамтамасыз етуі тиіс. 1.2. Ұсынылатын лицензияның қолданылу мерзімі Тапсырыс беруші оны белсендірген күннен бастап кемінде 12 (он екі) айды құрауы тиіс. 1.3. Бағдарламалық қамтамасыз етуді өндіруші Қазақстан Республикасының аумағында техникалық қолдаудың болуын қамтамасыз етуі, сондай-ақ орыс және қазақ тілдерінде консультациялар мен техникалық көмек алу мүмкіндігін ұсынуы тиіс. 1.4. Орталықтандырылған басқару құралдарын қоса алғанда, антивирустық компоненттердің пайдаланушы интерфейсі орыс және қазақ тілдерінде қолжетімді болуы тиіс. 1.5. Жұмыс станциялары мен серверлерде пайдалануға арналған антивирустық компоненттер, оның ішінде орталықтандырылған басқару құралдары орыс және қазақ тілдеріндегі контекстік анықтамалық жүйені қамтуы тиіс. 1.6. Осы сатып алу шеңберінде жеткізілетін барлық бағдарламалық компоненттер үшін бірыңғай сериялық нөмір ұсынылуы тиіс. Барлық жеткізілетін бағдарламалық өнімдердің лицензиялық кілттерінің қолданылу мерзімі осы сериялық нөмір белсендірілген сәттен бастап есептелуі тиіс. 1.7. Бағдарламалық қамтамасыз етудің заңды түрде алынғанын растау және контрафактілік өнімді жеткізуге жол бермеу мақсатында өнім беруші бағдарламалық қамтамасыз етуді өндірушінің лицензиялардың заңды шығу тегі мен жеткізілуін растайтын ресми хатын ұсынуы тиіс. 2. Техникалық талаптарды негіздеу 2.1. Сатып алу нысанасы Тапсырыс берушінің жұмыс станцияларын, серверлері мен мобильді құрылғыларын кешенді антивирустық қорғауды қамтамасыз етуге арналған бағдарламалық қамтамасыз ету лицензиясын сатып алу болып табылады. 2.2. Техникалық талаптар ақпараттық қауіпсіздікті, Тапсырыс берушінің ақпараттық инфрақұрылымының үздіксіз жұмыс істеуін, пайдаланылатын операциялық жүйелермен үйлесімділікті, қолданыстағы қауіпсіздік баптауларын сақтауды және антивирустық қорғауды орталықтандырылған басқаруды қамтамасыз ету қажеттілігі негізінде қалыптастырылған. 2.3. Ұсынылатын бағдарламалық қамтамасыз ету өндірушісі мен бағдарламалық өнімнің атауына қарамастан, белгіленген барлық функционалдық және техникалық талаптардың орындалуын қамтамасыз етуі тиіс. 3. Антивирустық қорғауға қойылатын жалпы талаптар 3.1. Жүйенің бағдарламалық құралдары мынадай қауіп түрлерін анықтауды қамтамасыз етуі тиіс: классикалық вирустар, трояндық бағдарламалар, руткиттер, желілік құрттар, жарнамалық бағдарламалар, ақылы ресурстарға автоматты түрде қоңырау шалатын бағдарламалар, ықтимал қауіпті қосымшалар және басқа да зиянды бағдарламалар. 3.2. Антивирустық қорғау мыналарды қамтамасыз етуі тиіс: 3.2.1. 64-разрядты операциялық жүйелерге бағытталған қауіптерді, оның ішінде арнайы 64-разрядты антируткит модулінің көмегімен анықтауды; 3.2.2. Архивтер мен буып-түйілген файлдарды тексеруді жеделдету мақсатында алдын ала распаковщикті іске қоспай-ақ зиянды бағдарламаларды тануды; 3.2.3. Әртүрлі

	бағдарламалық буып-түйіштермен буып-түйілген файлдардағы вирустарды анықтауды және жоюды; 3.2.4. Кең таралған әртүрлі форматтағы контейнерлер мен архивтік файлдардың, оның ішінде архивтердің, дискілік бейнелердің, пошта контейнерлерінің, құжаттардың және шифрланған контейнерлердің ішіндегі вирустарды тексерілетін объектілердің кірістірілу деңгейіне шектеу қоймай анықтауды; 3.2.5. Қатаң форматы жоқ контейнерлердің, оның ішінде веб-құжаттар мен электрондық пошта хабарламаларының ішіндегі вирустарды анықтауды; 3.2.6. Объектінің өлшемі белгісіз немесе динамикалық түрде өзгеретін контейнерлердің ішіндегі вирустарды анықтауды; 3.2.7. Әртүрлі операциялық жүйелерге арналған орнату пакеттерін, орындалатын файлдарды, жүйелік бейнелерді, архивтерді және басқа да объектілерді антивирустық тексеруді; 3.2.8. Бағдарламалық қамтамасыз етуді әзірлеу мен буып-түюдің әртүрлі құралдарымен жасалған өздігінен ашылатын архивтер мен орнату пакеттерін антивирустық тексеруді; 3.2.9. Әртүрлі бағдарламалық буып-түйіштермен буып-түйілген орындалатын файлдарды, сондай-ақ электрондық пошта файлдарын олардың көлеміне қарамастан тексеруді; 3.2.10. Пішімделмеген пошта дерекқорларын талдауды және әртүрлі форматтағы пошта тіркемелерін қолдай отырып, жауаптар мен қайта жіберулер саны көп хат алмасуларды қоса алғанда, кірістірілу деңгейі жоғары хаттарды өңдеуді; 3.2.11. Антивирустық зертханаларда әлі талдаудан өтпеген жаңа және түрлендірілген қауіп нұсқаларын қоса алғанда, антивирустық дерекқорларда мәліметтері бар зиянды бағдарламалардан эвристикалық талдау және ұқсас зиянды объектілерді іздеу технологиялары негізінде қорғауды; 3.2.12. Веб-құжаттар мен электрондық құжаттардағы зиянды объектілерді, оның ішінде сценарийлердегі обфускацияланған эксплойттарды анықтауды, сондай-ақ күрделілігі әртүрлі жасырын элементтер мен сценарийлерді шығарып алу және талдау мүмкіндігін; 3.2.13. Орындалатын файлдардың құрылымы мен буып-түю ерекшеліктері туралы мәліметтерді талдау негізінде зиянды объектілерді анықтауды; 3.2.14. Мобильді операциялық жүйелердің орындалатын файлдарындағы зиянды объектілерді анықтауды; 3.2.15. Белгісіз немесе стандартты емес буып-түйіштерді пайдалану арқылы жасырылған вирустарды анықтауды және жоюды. 4. Жұмыс станциялары мен серверлерді антивирустық қорғауға арналған бағдарламалық құралдарға қойылатын талаптар 4.1. Жүйе сатып алу жүргізілген сәттегі бағдарламалық қамтамасыз етудің өзекті нұсқасын пайдалана отырып, мынадай санаттағы операциялық жүйелерді басқаратын жұмыс станциялары мен серверлерді қорғауды қамтамасыз етуі тиіс: 32-разрядты және 64-разрядты архитектураларды қолдайтын жұмыс үстелі операциялық жүйелері; заманауи жұмыс үстелі операциялық жүйелері; әртүрлі буындағы серверлік операциялық жүйелер; коммерциялық және еркін таратылатын платформалар негізіндегі операциялық жүйелер. Қолдау көрсетілетін операциялық жүйелердің нұсқалары ұсынылатын бағдарламалық қамтамасыз етуді өндірушінің ресми техникалық құжаттамасында көрсетілуі тиіс. 4.2. Жүйенің бағдарламалық

	құралдары жұмыс станцияларын антивирустық және спамға қарсы қорғауды, оның ішінде руткит-технологиялардан тұрақты қорғауды және резиденттік антируткит драйверінің болуын қамтамасыз етуі тиіс. 4.3. Жүйе компоненттерін вирустармен немесе басқа да зиянды бағдарламалармен зақымданған жұмыс станцияларына оларды алдын ала емдемей-ақ орнату мүмкіндігі қамтамасыз етілуі тиіс. 4.4. Компьютерде іске қосылған зиянды бағдарламаларға қарсы іс-қимыл жасау мақсатында орнату үшін операциялық жүйенің стандартты орнату қызметіне тәуелді емес, антируткит технологияларымен қорғалған орнатқыш пайдаланылуы тиіс. 4.5. Интернет желісіне қосылу арнасына қойылуы мүмкін шектеулерге байланысты қорғау жүйесін Интернет желісіне қосылмай-ақ орнату мүмкіндігі қамтамасыз етілуі тиіс. Дистрибутив жүйенің барлық қажетті компоненттерін, сондай-ақ зиянды бағдарламалар мен зиянды интернет-ресурстар белгілерінің дерекқорларын қамтуы тиіс. 4.6. Қорғау жүйесінің жұмысы тұтастығы жүйенің өзін-өзі қорғау тетіктерінің бақылауында болмайтын және бұзылуы ақпараттың дұрыс көрсетілмеуіне немесе қорғау жүйесінің интерфейсінде өзге де ақауларға әкелуі мүмкін сыртқы кітапханалар мен қосымша бағдарламалық орталарды пайдаланбауы тиіс. 4.7. Жүйе компоненттері файлдық кеңістікті сканерлеу кезінде пайдаланушылардың қалыпты жұмыс істеуін қамтамасыз ету мақсатында компьютер ресурстарын пайдалануды басқару мүмкіндігін қамтамасыз етуі тиіс. Бұл, оның ішінде оқуға ашылатын файлдарды тексеруді кейінге қалдыру және заманауи есептеу архитектураларының ерекшеліктерін пайдалану арқылы жүзеге асырылуы тиіс. 4.8. Жүйе жергілікті желіде және Интернет желісінде жұмыс істеу кезінде, веб-беттермен, электрондық поштамен, жергілікті дискілермен, алынбалы тасымалдағыштармен және желілік ресурстармен жұмыс істеу кезінде антивирустық қорғауды қамтамасыз ететін конфигурацияда жеткізілуі тиіс. Кіріс және шығыс электрондық хат-хабарларды зиянды бағдарламалардан да, қажетсіз хат-хабарлардан да қорғау қамтамасыз етілуі тиіс. 4.9. Жүйеде пайдаланушылардың Интернет желісінде жұмыс істеу уақытын, сондай-ақ компьютер алдында өткізетін уақытын шектеу мүмкіндігі болуы тиіс. 4.10. Пайдаланушылар үшін антивирустық пакет компоненттерінің баптауларына қол жеткізу құқықтары Жүйе әкімшісімен айқындалуы тиіс. Бұл ретте пайдаланушыларға әкімші берген құқықтар шегінде ғана өз бетінше баптау мүмкіндігі берілуі тиіс. 4.11. Жұмыс станцияларын қорғау жүйесі жедел хабар алмасу бағдарламаларындағы трафикті сүзуді, оның ішінде жіберілетін тіркемелерді антивирустық тексеруді, сондай-ақ хабарламалардан зиянды және фишингтік ресурстарға апаратын сілтемелерді автоматты түрде жоюды қамтамасыз етуі тиіс. 4.12. Жұмыс станцияларын қорғау жүйесі іздеу жүйелерінің нәтижелерін сүзуді және қорғау жүйесінің көзқарасы бойынша қауіпсіз ресурстарды ғана көрсетуді қамтамасыз етуі тиіс. 4.13. Қосымшалар деңгейінде желілік қосылымдарды бақылау көзделуі тиіс. Бұл нақты бағдарламалар мен процестердің желілік ресурстарға қол жеткізуін бақылауға және қол жеткізу

	әрекеттері туралы ақпаратты оқиғалар журналына тіркеуге мүмкіндік беруі тиіс. 4.14. Қосылымды бастайтын бағдарламаларға қарамастан, Интернет желісіне қол жеткізуді бақылауға мүмкіндік беретін желілік пакеттер деңгейінде сүзу көзделуі тиіс. 4.15. Жүйеде сигнатуралық және эвристикалық талдауға қосымша ретінде мынадай компоненттерден тұратын превентивті қорғау іске асырылуы тиіс: бопсалаушы бағдарламалардан қорғау, компьютерді зиянды шифрлаушы бағдарламалардан қорғау мүмкіндігін қамтамасыз етуі тиіс; эксплойттардан қорғау, кең таралған қосымшалардағы осалдықтарды пайдалануға қарсы іс-қимылды қамтамасыз етуі тиіс; іске қосылған бағдарламалардың мінез-құлқын мынадай маңызды бағыттар бойынша бақылайтын мінез-құлықты талдау: жүйелік файлдарды өзгерту, іске қосылған қосымшалардың тұтастығы, дискілерге төмен деңгейде қол жеткізу, драйверлерді жүктеу, қосымшаларды іске қосу параметрлері, жүйелік қызметтер, бағдарламаларды автоматты түрде іске қосу тетіктері, жүйелік қауіпсіздік саясаттары, жүйелік орта баптаулары және операциялық жүйенің басқа да маңызды компоненттері. 4.16. Жүйеде барлық өз объектілерін, оның ішінде маңызды файлдарды, процестерді, терезелерді, жүйелік кілттерді және басқа да компоненттерді пайдаланушылар мен зиянды бағдарламалық қамтамасыз етудің рұқсатсыз қол жеткізуінен қорғайтын өзін-өзі қорғау механизмі іске асырылуы тиіс. Өзін-өзі қорғау жүйелік деңгейде жұмыс істеуі және антивирустық Жүйе драйверлерін рұқсатсыз жүктеуден шығарудың және тоқтатудың мүмкін болмауын қамтамасыз етуі тиіс. 4.17. Виртуалды агенттерді орнату арқылы виртуалды жұмыс орындарын қорғауды іске асыру мүмкіндігі көзделуі тиіс. 5. Linux отбасына жататын операциялық жүйелерді басқаратын жұмыс станциялары мен серверлерді антивирустық қорғауға арналған бағдарламалық құралдарға қойылатын талаптар 5.1. Мынадай процессорлық архитектураларға қолдау көрсетілуі тиіс: 32-разрядты x86 архитектуралары; 64-разрядты x86-64 архитектуралары; 64-разрядты ARM архитектуралары; тиісті 64-разрядты командалар жүйесін қолдайтын IBM POWER архитектуралары. 5.2. Жүйе сатып алу жүргізілген сәттегі бағдарламалық қамтамасыз етудің өзекті нұсқасын пайдалана отырып, Samba және басқа да ұқсас технологияларды қоса алғанда, желілік файлдық қызметтер мен файлдық жүйелерді пайдаланатын, мынадай санаттағы операциялық жүйелерді басқаратын жұмыс станциялары мен серверлерді қорғауды қамтамасыз етуі тиіс: PAM және glibc кітапханасының 2.13 және одан кейінгі нұсқаларын пайдаланатын, 2.6.37 және одан кейінгі ядро нұсқалары негізіндегі Linux; BSD отбасына жататын операциялық жүйелер; Linux негізіндегі серверлік операциялық жүйелер. 5.3. Жүйені желілік файлдық қызметтермен интеграциялау виртуалды файлдық жүйе модульдері арқылы жүзеге асырылуы тиіс. 5.4. Желілік файлдық қызметтердің әртүрлі нұсқалары мен 64-разрядты платформалар үшін интеграция модульдерін бастапқы кодтардан компиляциялау мүмкіндігі болуы тиіс. 5.5. UNIX-тектес жүйелерге арналған, пайдаланылатын операциялық жүйенің түрі мен нұсқасына тәуелсіз

	әмбебап пакеттен немесе операциялық жүйеде пайдаланылатын пакеттер менеджеріне арналған репозиторийден не пакеттен орнату мүмкіндігі қамтамасыз етілуі тиіс. 5.6. Жүйені командалық жол құралдары арқылы да, графикалық орнатқыштың көмегімен де орнату және жаңарту мүмкіндігі қамтамасыз етілуі тиіс. 5.7. Жүйе компоненттерінің жұмыс істеуіне қажетті модульдерді автоматты түрде орнату мүмкіндігі қамтамасыз етілуі тиіс. 5.8. Жүйе компоненттерін зиянды бағдарламалармен зақымданған объектілерге оларды алдын ала емдемей орнату, кейіннен белгіленген файлдық аймақтарды емдеу мүмкіндігі қамтамасыз етілуі тиіс. 5.9. Операциялық жүйелердің қосымша қауіпсіздік ішкі жүйелеріне, оның ішінде міндетті қол жеткізуді бақылау тетіктеріне, мандаттық қол жеткізуді басқаруға және тұйық бағдарламалық орта режимдеріне қолдау көрсетілуі тиіс. 5.10. Файлдық жүйені операциялық жүйенің кіріктірілген тетіктерін, сондай-ақ арнайы ядро модулін пайдалана отырып бақылау мүмкіндігі қамтамасыз етілуі тиіс. 5.11. Файлдық жүйенің жаңа томдарын, оның ішінде алынбалы жинақтауыштарды, оптикалық тасымалдағыштарды және дискілік массивтерді қосу және ажырату сәттерін автоматты түрде тану, сондай-ақ қажет болған жағдайда бақыланатын аймақтар тізімін түзету мүмкіндігі қамтамасыз етілуі тиіс. 5.12. Файлдық кеңістікті сканерлеу кезінде сервер ресурстарын пайдалануды басқару мүмкіндігі қамтамасыз етілуі тиіс. 5.13. Архивтерді, пошта файлдарын, буып-түйілген объектілерді және басқа да контейнерлерді қоса алғанда, құрамдас файлдарды тексеру параметрлерін басқару мүмкіндігі қамтамасыз етілуі тиіс. 5.14. Жүйеде SSL және TLS хаттамаларын пайдаланатын қорғалған желілік қосылымдар арқылы берілетін трафикті тексеру мүмкіндігімен бірге орнатылған желілік қосылымдарды тұрақты бақылау функциясы іске асырылуы тиіс. 5.15. Санаттар бойынша интернет-ресурстарды бұғаттау, сондай-ақ ақ және қара тізім режимдерінде жұмыс істеу мүмкіндігі бар веб-сүзгі іске асырылуы тиіс. 5.16. Жүйе бірнеше тексеру процесін бір мезгілде іске қосуды қолдауы тиіс. 5.17. Жүйенің бағдарламалық құралдары мынадай функционалдық мүмкіндіктерді қамтамасыз етуі тиіс: 5.17.1. Белгілі барлық типтегі вирустарды іздеу және жою; 5.17.2. Әкімшінің командасы бойынша және кестеге сәйкес қауіптердің бар-жоғын толық немесе іріктеп антивирустық сканерлеу; 5.17.3. Серверге жүктелетін және одан жіберілетін файлдарды нақты уақыт режимінде антивирустық тексеру; 5.17.4. Антивирустық бағдарламалық қамтамасыз етуді және басқа да қажетті компоненттерді операциялық жүйе жүктелген кезде автоматты түрде іске қосу; 5.17.5. Тапсырмаларды кесте бойынша және (немесе) операциялық жүйе жүктелгеннен кейін бірден іске қосу; 5.17.6. Іске қосу параметрлерін көрсете отырып, сканерлеу кестесін баптау. 5.18. Бағдарламаны басқару веб-интерфейс арқылы да, конфигурациялық файлдар арқылы да жүзеге асырылуы тиіс. Тексеруге жататын файлдар мен каталогтарды, сондай-ақ әртүрлі типтегі зиянды объектілерге қатысты қолданылатын әрекеттерді көрсете отырып, антивирустық сканерлеу

	параметрлерін баптау мүмкіндігі көзделуі тиіс. 5.19. Сканерлеу ядросы файлдар мен дискілік құрылғылардың жүктеу жазбаларынан, оның ішінде негізгі жүктеу жазбасынан (MBR) және бөлімдердің жүктеу жазбаларынан вирустар мен басқа да зиянды объектілерді іздеуді қамтамасыз етуі тиіс. 5.20. Файлдарды тексеру үшін ағындық тексеру әдісін, сондай-ақ проксилеу әдісін пайдалану мүмкіндігі көзделуі тиіс. 5.21. Желі арқылы алынған, файл түрінде ұсынылмаған деректерді тексеру, сондай-ақ файлдарды қауіптердің бар-жоғына үлестірілген түрде тексеруді ұйымдастыру мүмкіндігі көзделуі тиіс. 5.22. Веб-интерфейске қол жеткізу жүзеге асырылатын жергілікті құрылғыдағы файлдарды қауіптердің бар-жоғына жедел тексеру мүмкіндігі көзделуі тиіс. 5.23. Желінің қашықтағы тораптарында орналасқан файлдарды қауіптердің бар-жоғына тексеру мүмкіндігі көзделуі тиіс. Мұндай тораптар ретінде жұмыс станциялары, серверлер, желілік құрылғылар және қашықтан басқарудың қорғалған хаттамалары арқылы қол жеткізу мүмкіндігін ұсынатын желіге қосылған басқа да құрылғылар пайдаланылуы мүмкін. 5.24. Жүйе құрамында инфрақұрылымды мониторингтеу жүйелерімен интеграциялауға арналған мониторинг агенті болуы тиіс. 5.25. Жүйенің барлық компоненттерін бірыңғай басқару орталығынан басқаруды қамтамасыз ететін антивирустық қорғауды орталықтандырылған басқару жүйесіне интеграциялау мүмкіндігі көзделуі тиіс. 6. Мобильді құрылғыларды антивирустық қорғауға арналған бағдарламалық құралдарға қойылатын талаптар 6.1. Мобильді құрылғыларды антивирустық қорғауға арналған бағдарламалық құралдар Android 4.4 және одан жоғары нұсқадағы мобильді операциялық жүйелердің басқаруымен жұмыс істеуі немесе Тапсырыс беруші пайдаланатын мобильді құрылғылармен үйлесімділікті қамтамасыз етуі тиіс. 6.2. Пайдаланылатын бағдарламалық құралдар мыналарды қамтамасыз етуі тиіс: 6.2.1. Файлдық жүйені тұрақты қорғауды, мынадай объектілерді ұстап қалуды және тексеруді: мобильді деректерді беру желілері, сымсыз қосылымдар, деректерді беру интерфейстері және компьютерге қосылу арқылы келіп түсетін файлдар; браузерлер арқылы жүктелетін және электрондық пошта арқылы алынатын файлдар; мобильді құрылғыны компьютермен синхрондау кезінде алынатын файлдар; кең таралған архив форматтарындағы және орнату пакеттеріндегі файлдар; мобильді құрылғы интерфейсі арқылы орнатылатын бағдарламалар; пайдаланушының талабы бойынша және кестеге сәйкес мобильді құрылғыда немесе оған қосылған жад карталарында орналасқан файлдық жүйе объектілерін толық және іріктеп тексеру. 6.2.2. Жарнамалық таратылымдарды, белгісіз нөмірлерден келетін қоңыраулар мен SMS-хабарламаларды қоса алғанда, кіріс қоңыраулар мен SMS-хабарламаларды сүзуді қамтамасыз ету. Бұл алдын ала белгіленген және пайдаланушы жасаған қорғау профильдері негізінде жүзеге асырылуы тиіс. Әрбір профиль үшін нөмірлер тізімін қалыптастыру және осы тізімдегі нөмірлерден келетін қоңыраулар мен хабарламаларға қатысты әрекеттерді айқындау мүмкіндігі болуы тиіс. Қара тізімдер мен құрылғының телефон кітапшасын пайдалану

	мүмкіндігі қамтамасыз етілуі тиіс. 6.2.3. Бұғатталған қоңыраулар мен хабарламаларды қарау және оларға қатысты әрекеттерді таңдау мүмкіндігі; 6.2.4. Автоматты іске қосу файлдарын анықтау; 6.2.5. Зақымданған объектілерді анықталған қауіптер туралы толық ақпарат бере отырып, жою немесе карантиндік қоймаға оқшаулау; 6.2.6. Антивирустық дерекқорларды жаңартуды жүзеге асыру: деректерді берудің кіріктірілген құралдарын пайдалана отырып, HTTP хаттамасы арқылы; сымсыз қосылымдар мен деректерді беру интерфейстері арқылы; Интернет желісіне қол жеткізе алатын компьютермен синхрондау арқылы. 6.2.7. Корпоративтік саясаттар негізінде мобильді құрылғыны орталықтандырылған басқару; 6.2.8. Кіріктірілген интерактивті интерфейс элементтерін пайдалана отырып, мобильді құрылғыны басқару; 6.2.9. Баптауларды қалпына келтіру, импорттау және экспорттау; 6.2.10. Мобильді құрылғы жоғалған немесе ұрланған жағдайда оны қашықтан басқару, оның ішінде құрылғының орналасқан жерін іздеу, оны шұғыл бұғаттау, жеке деректерді жою, координаттарын алу және алдын ала орнатылған құпиясөзді пайдалана отырып, командалар арқылы құрылғыны басқару; 6.2.11. VPN технологиясына негізделген кіріктірілген желілік экранның болуы; 6.2.12. Қосымшалар сүзгісінің болуы; 6.2.13. Бопсалаушы бағдарламалардан және құрылғының жұмысын бұғаттайтын қосымшалардан қорғау; 6.2.14. Кіріктірілген браузер және үшінші тараптың мобильді браузерлері арқылы интернет-ресурстарға қол жеткізуді бақылау; 6.2.15. Арнайы компоненттің көмегімен құрылғының қауіпсіздігін диагностикалау және анықталған проблемалар мен осалдықтарды жою жөнінде ұсынымдар беру. Бұл ретте мынадай жағдайларды анықтау мүмкіндігі болуы тиіс: мобильді операциялық жүйелер мен қосымшалардың белгілі осалдықтары; қауіпсіз емес жүйелік баптаулар; қайшылық тудыратын бағдарламалық қамтамасыз ету; жасырын әкімшілер; жүйенің қауіпсіздік осалдықтарын пайдаланатын қосымшалар. 7. Антивирустық қорғауды орталықтандырылған басқару жүйесіне қойылатын талаптар 7.1. Жүйе мынадай санаттағы операциялық жүйелерді басқаратын серверлерге де, жұмыс станцияларына да орталықтандырылған басқару серверін орнату мүмкіндігі бар клиент-сервер архитектурасы негізінде құрылуы тиіс: жұмыс үстелі операциялық жүйелері; серверлік операциялық жүйелер; Linux отбасына жататын операциялық жүйелер; BSD отбасына жататын операциялық жүйелер. 7.2. Орталықтандырылған басқару сервері пайдаланылатын операциялық жүйелер мен платформаларға қарамастан, жұмыс станцияларын, серверлер мен мобильді құрылғыларды қоса алғанда, барлық қорғалатын объектілер үшін бірыңғай болуы тиіс. 7.3. Басқару жүйесіне заманауи веб-браузерлерді қолдайтын кез келген операциялық жүйеден, браузерлердің өзекті нұсқаларын пайдалануға шектеусіз және Жүйе әкімшісінің жағында да, басқару серверінің жағында да қосымша бағдарламалық қамтамасыз етуді орнату қажеттілігінсіз қол жеткізу мүмкіндігі қамтамасыз етілуі тиіс. 7.4. Әкімшілерді аутентификациялау мынадай тәсілдермен жүзеге асырылуы мүмкін болуы тиіс: сервердің ішкі дерекқорын

	пайдалану арқылы; LDAP хаттамасын және каталогтар қызметін пайдалану арқылы; RADIUS хаттамасын пайдалану арқылы; PAM операциялық жүйесінің аутентификациялау тетіктерін пайдалану арқылы. 7.5. Басқару серверлерінің иерархиялық жүйесін: негізгі, бағынысты және тең құқылы серверлерді құру мүмкіндігі іске асырылуы тиіс. Бұл ретте серверлер арасындағы байланыстар арқылы лицензияларды тарату, сондай-ақ лицензиялық кілт файлын автоматты түрде жаңарту мүмкіндігі болуы тиіс. 7.6. Басқару жүйесінде мынадай мүмкіндіктер болуы тиіс: бірнеше серверден алынған ақпаратты бір серверде біріктіру; желіге түсетін жалпы жүктемені азайту мақсатында жаңартулар алу үшін жұмыс станцияларын серверлер арасында бөлу; әртүрлі нұсқадағы серверлер арасында бір иерархиялық желі шеңберінде статистикалық ақпарат алмасу; әрбір деңгейде әкімшілер мен пайдаланушылардың рөлдерін, сондай-ақ ұсынылатын есептілік нысандарын баптау мүмкіндігі бар көпдеңгейлі басқару жүйесін құру. 7.7. Мобильді құрылғыларда мобильді операциялық жүйелердің басқаруымен жұмыс істейтін тиісті мобильді қосымшалардың көмегімен, веб-браузерлерді пайдаланбай, Жүйені басқарудың мобильді орталығын іске қосу мүмкіндігі қамтамасыз етілуі тиіс. 7.8. Басқару жүйесінде мынадай мүмкіндіктер болуы тиіс: 7.8.1. Антивирустық сервер дистрибутивінің құрамында жеткізілетін сыртқы және ішкі дерекқорларды басқару жүйесін пайдалану. Сыртқы дерекқорларды басқару жүйелері ретінде кең таралған реляциялық дерекқорларды басқару жүйелеріне, сондай-ақ серверлік және жұмыс үстелі операциялық жүйелеріне арналған ODBC драйверлері арқылы қосылуға қолдау көрсетілуі тиіс. 7.8.2. Серверлік бөлік орнатылғаннан кейін оны қайта орнату қажеттілігінсіз жұмыс барысында пайдаланылатын дерекқорды басқару жүйесінің түрін ауыстыру; 7.8.3. Дерекқорды басқару жүйесінің құралдары арқылы басқару, оның ішінде дерекқорды тазалау, талдау және еркін SQL-сұрауларын орындау мүмкіндігі; 7.8.4. Web API кіріктірілген бағдарламалық интерфейсінің функциялары арқылы орындалған әрекеттердің аудитін жүргізу; 7.8.5. Lua бағдарламалау тілінде оқиғаларды өңдеуіштерді өз бетінше жазу, сондай-ақ басқару жүйесінің құралдары арқылы еркін сценарийлерді орындау; 7.8.6. Есептерді CSV, XML, HTML және PDF форматтарына экспорттау; 7.8.7. Бағдарламалық қамтамасыз етуді өндірушіден, оның ішінде өзекті қауіптер туралы ақпарат беретін жаңалықтарға жазылу және оларды басқару орталығының консолінде тікелей алу; 7.8.8. Пайдаланушылар мен әкімшілерге хабарламаларды электрондық пошта, дыбыстық ескерту, қалқымалы терезе, оқиғалар журналына жазу, веб-консольдегі хабарлама, push-хабарламалар, желілік мониторинг хаттамалары және жүйелік журналдау арқылы жіберудің бірнеше тәсілінің болуы; 7.8.9. Жүйе әкімшісінің веб-интерфейс арқылы желі бойынша нақты уақыт режимінде пайдаланушыларға еркін мазмұндағы ақпараттық хабарламаларды, оның ішінде хабарлама мәтінін, интернет-ресурстарға гиперсілтемелерді және графикалық кескіндерді жіберуі; 7.8.10. Агенттерді орнату кезінде де, оларды жаңарту кезінде де

	желілік трафикті шектеу; 7.8.11. Әртүрлі операциялық жүйелерге арналған антивирустық агенттердің қосылу баптаулары бар конфигурациялық файлдарды жүктеп алу; 7.8.12. Барлық қорғалатын объектілерде антивирустық дерекқорларды орталықтандырылған түрде жаңарту және жаңартуларды пайдаланушылардың жұмыс орындарына кесте бойынша да, жаңартулар алынғаннан кейін бірден де жеткізу; 7.8.13. Антивирустық сервер репозиторийінде орналасқан өнімдердің жаңартулар нұсқаларын басқару, оның ішінде жаңартуларды кері қайтару мүмкіндігі; 7.8.14. Топтық жаңартуларды жүргізу; 7.8.15. SSL-сертификаттарын пайдалана отырып, қорғалған арна арқылы жаңарту; 7.8.16. Кейінге қалдырылған жаңартуды ұйымдастыру; 7.8.17. Орнатылған бағдарламалық қамтамасыз етуді оның жаңа нұсқаларына автоматты түрде көшіру, оның ішінде жаңартылатын компоненттерді таңдау мүмкіндігі; 7.8.18. Антивирустық пакетті клиенттік құрылғыларға орнату басталғанға дейін орнатылатын компоненттерді таңдау және баптау; 7.8.19. Әкімші мен пайдаланушыға арналған құжаттаманың толық пакетін басқару орталығының консолінде тікелей оқу. 7.9. Жүйеде мобильді пайдаланушыларға, оның ішінде ноутбук пайдаланушыларына арналған арнайы саясат болуы тиіс. Осы саясатты қолданған кезде пайдаланушылар антивирустық пакет баптауларын редакциялау және антивирустық серверге қол жеткізу болмаған жағдайда Интернет желісі арқылы жаңартулар алу мүмкіндігіне ие болуы тиіс. Саясатты қолдану конфигурациялық файлдарды пайдалануды қажет етпей, веб-интерфейс арқылы жүзеге асырылуы тиіс. 7.10. Басқару жүйесінде алдын ала белгіленген кесте бойынша антивирустық сервердің маңызды деректері мен конфигурациясының автоматты түрде резервтік көшірмесін жасауға, сондай-ақ резервтік көшірмеден серверді қалпына келтіруге мүмкіндік беретін кіріктірілген компонент болуы тиіс. 7.11. Басқару орталығында жұмыс станцияларын анықтау және оларға антивирустық агенттің орнатылғанын айқындау мақсатында желіні сканерлеуге мүмкіндік беретін компонент іске асырылуы тиіс. Сканерлеу каталогтар қызметі, желілік атаулар, ICMP және TCP хаттамаларын пайдалану арқылы іздеу режимдерінде жүзеге асырылуы тиіс. 7.12. Басқару орталығында алдын ала орнатылған жүйелік және пайдаланушы топтары негізінде топтық саясат іске асырылуы тиіс. Алдын ала орнатылған жүйелік топтар мынадай объектілерге қол жеткізуге мүмкіндік беруі тиіс: барлық қорғалатын объектілерге; каталогтар қызметінің объектілеріне; операциялық жүйелердің түрлері бойынша объектілерге; қолданылатын саясаттар бойынша объектілерге; баптау профильдері бойынша объектілерге; желілік хаттамалар бойынша объектілерге; мәртебесі бойынша объектілерге; дербес баптаулары бойынша объектілерге. 7.13. Басқару жүйесінде қосымшалардың іске қосылуын тыйым салатын және рұқсат беретін қағидалар негізінде де, қосымшаларды функционалдық талдау негізінде де бақылау мүмкіндігі болуы тиіс. Бұл ретте мынадай санаттарға бақылау жүргізілуі тиіс: қосымшаларды іске қосу; модульдерді жүктеу және орындау; сценарийлік интерпретаторларды іске

	қосу; драйверлерді жүктеу; бағдарламалық пакеттерді орнату; орындалатын файлдардың тұтастығын бақылау. 7.14. Орталықтандырылған басқару серверін пайдалана отырып, антивирустық бағдарламалық қамтамасыз етудің мониторингі бойынша есептілік қамтамасыз етілуі тиіс. 7.15. Антивирустық қорғаудың жай-күйі туралы есептерді қалыптастыру және оларды біріктіру арқылы статистикалық ақпаратты орталықтандырылған түрде жинау, сондай-ақ белгіленген параметрлер бойынша статистикалық есептерді автоматты түрде қалыптастырып, кейіннен әкімшіге электрондық пошта арқылы жіберу мүмкіндігі көзделуі тиіс. 7.16. Жүйеде лицензиялық кілттердің иерархиялық тізімін қолдайтын лицензиялар менеджері болуы тиіс. Лицензиялар менеджері мынадай мүмкіндіктерді ұсынуы тиіс: лицензия туралы ақпаратты қарау; жаңа лицензиялық кілтті қосу; лицензиялық кілтті жаңарту; лицензиялық кілтті ауыстыру; объектінің лицензиялық кілттер тізімін кеңейту; лицензиялық кілтті жою; объектіні лицензиялау тізімінен алып тастау; лицензияларды көршілес басқару серверіне беру; көршілес басқару серверіне берілген лицензияларды редакциялау. 7.17. Құпия ақпараттың таралып кетуіне жол бермеу мақсатында серверлер мен қорғалатын жұмыс станциялары арасындағы трафикті шифрлау мүмкіндігі болуы тиіс. 7.18. Жүйені өндіруші антивирустық дерекқорлардың жаңартуларын тәулігіне кемінде 20 рет шығаруды қамтамасыз етуі тиіс. Бұл Жүйе құралдарымен қалыптастырылатын есеп арқылы расталуы тиіс. 7.19. Антивирустық серверлер Интернет желісіне қол жеткізе алмайтын ішкі желіде орналасқан жағдайда, жаңартуларды репозиторийді автономды түрде жүктеуге арналған арнайы утилитаның көмегімен алу мүмкіндігі қамтамасыз етілуі тиіс. 7.20. Виртуалды инфрақұрылымға және виртуалды жұмыс орындарының инфрақұрылымымен (VDI) интеграциялауға, сондай-ақ кең таралған виртуалдандыру технологиялары мен гипервизорларға қолдау көрсетілуі тиіс.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	Сатып алудың жеңімпазы болып айқындалған өнім беруші лицензияны беру және (немесе) ілеспе қызметтерді көрсету кезінде ұсынылатын бағдарламалық қамтамасыз етуді өндірушімен қолданыстағы әріптестік қатынастардың болуын құжаттамалық растауды ұсынуға тиіс. Растау ретінде әріптестік сертификат, өндірушінің авторизациялық хаты не өндірушінің ресми интернет-ресурсында орналастырылған өнім берушінің ресми мәртебесі туралы ақпарат қабылданады.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Департамент полиции Павлодарской области Министерства внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Департамент полиции Павлодарской области Министерства внутренних дел Республики Казахстан"
№ конкурса:	№ 17915519-2
Наименование конкурса:	Услуги по продлению лицензии антивирусного программного обеспечения
Номер лота:	№ 88472534-ОК1
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:	4693331.89
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	4693331.89
Срок оказания услуги:	61 календарных дней со дня вступления договора в силу.
Размер авансового платежа* *:	30 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	1.1. Лицензия должна обеспечивать антивирусную защиту 845 рабочих станций под управлением настольных операционных систем различных семейств, включая коммерческие и свободно распространяемые операционные системы, а также 5 файловых серверов. 1.2. Срок действия предоставляемой лицензии должен составлять не менее 12 (двенадцати) месяцев с даты ее активации Заказчиком. 1.3. Производитель программного обеспечения должен обеспечивать наличие технической поддержки на территории Республики Казахстан с возможностью получения консультаций и технической помощи на русском и казахском языках. 1.4. Пользовательский интерфейс антивирусных компонентов, в том числе средств централизованного управления системой, должен быть доступен на русском и казахском языках. 1.5. Антивирусные компоненты, предназначенные для эксплуатации на рабочих станциях и серверах, включая средства централизованного управления, должны содержать контекстную справочную систему на русском и казахском языках. 1.6. Для всех поставляемых в рамках настоящей закупки программных компонентов должен предоставляться единый серийный номер. Срок действия лицензионных ключей на все поставляемые программные продукты должен исчисляться с момента активации данного серийного номера. 1.7. В целях подтверждения легального происхождения программного обеспечения и исключения поставки контрафактной продукции поставщик должен предоставить официальное письмо производителя программного обеспечения, подтверждающее легальность происхождения и поставки лицензий. 2. Обоснование технических требований 2.1. Предметом закупки является приобретение лицензии на программное обеспечение для обеспечения комплексной антивирусной защиты рабочих станций, серверов и мобильных устройств Заказчика. 2.2. Технические требования сформированы исходя из необходимости обеспечения информационной безопасности, непрерывности функционирования информационной инфраструктуры Заказчика, совместимости с используемыми операционными системами, сохранения действующих настроек безопасности и централизованного управления антивирусной защитой. 2.3. Предлагаемое программное обеспечение должно обеспечивать выполнение всех установленных функциональных и технических требований независимо от производителя и наименования программного продукта. 3. Общие требования к антивирусной защите 3.1. Программные средства Системы должны обеспечивать определение угроз следующих типов: классических вирусов, троянских программ, руткитов, сетевых червей, рекламных программ, программ автоматического дозвона на платные ресурсы, потенциально опасных приложений и прочих вредоносных программ. 3.2. Антивирусная защита должна обеспечивать: 3.2.1. обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специализированного 64-разрядного антируткит-модуля; 3.2.2. распознавание вредоносных программ без предварительного запуска распаковщика в целях ускорения проверки архивов и упакованных файлов; 3.2.3. обнаружение и удаление вирусов из файлов,

	упакованных различными программными упаковщиками; 3.2.4. обнаружение вирусов внутри контейнеров и архивных файлов различных распространенных форматов, включая архивы, образы дисков, почтовые контейнеры, документы и зашифрованные контейнеры, без ограничений на уровень вложенности проверяемых объектов; 3.2.5. обнаружение вирусов внутри контейнеров, не имеющих строгого формата, включая веб-документы и почтовые сообщения; 3.2.6. обнаружение вирусов внутри контейнеров с неопределенным или динамически изменяемым размером объекта; 3.2.7. антивирусную проверку установочных пакетов, исполняемых файлов, системных образов, архивов и других объектов различных операционных систем; 3.2.8. антивирусную проверку самораспаковывающихся архивов и установочных пакетов, созданных различными средствами разработки и упаковки программного обеспечения; 3.2.9. проверку исполняемых файлов, упакованных различными программными упаковщиками, а также почтовых файлов независимо от их размера; 3.2.10. разбор неформатированных почтовых баз и обработку писем с высокой вложенностью, включая переписки с большим количеством ответов и пересылок, с поддержкой различных форматов почтовых вложений; 3.2.11. защиту от вредоносных программ, сведения о которых имеются в антивирусных базах, включая новые и модифицированные разновидности угроз, еще не прошедшие анализ в антивирусных лабораториях, на основе эвристического анализа и технологий поиска похожих вредоносных объектов; 3.2.12. обнаружение вредоносных объектов в веб-документах и электронных документах, включая обфусцированные эксплойты в сценариях, а также возможность извлечения и анализа скрытых элементов и сценариев различной сложности; 3.2.13. обнаружение вредоносных объектов на основании анализа сведений о структуре и особенностях упаковки исполняемых файлов; 3.2.14. обнаружение вредоносных объектов в исполняемых файлах мобильных операционных систем; 3.2.15. обнаружение и удаление вирусов, скрытых с использованием неизвестных или нестандартных упаковщиков. 4. Требования к программным средствам антивирусной защиты рабочих станций и серверов 4.1. Система, используя актуальную на момент проведения закупки версию программного обеспечения, должна обеспечивать защиту рабочих станций и серверов под управлением следующих категорий операционных систем: • настольные операционные системы с поддержкой 32-разрядной и 64-разрядной архитектур; • современные настольные операционные системы; • серверные операционные системы различных поколений; • операционные системы на основе коммерческих и свободно распространяемых платформ. Поддерживаемые версии операционных систем должны быть указаны производителем предлагаемого программного обеспечения в официальной технической документации. 4.2. Программные средства Системы должны обеспечивать антивирусную и антиспам-защиту рабочих станций, включая постоянную защиту от руткит-технологий и наличие резидентного антируткит-драйвера. 4.3. Система должна поддерживать возможность установки своих компонентов на

	зараженные вирусами или другими вредоносными программами рабочие станции без их предварительного лечения. 4.4. С целью противодействия вредоносным программам, запущенным на компьютере, для установки должен использоваться защищенный антируткит-технологиями инсталлятор, не зависящий от стандартной службы установки операционной системы. 4.5. В связи с возможными ограничениями канала доступа к сети Интернет установка системы защиты должна быть возможной без доступа к сети Интернет. Дистрибутив должен содержать все необходимые компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных интернет-ресурсов. 4.6. Для работы системы защиты не должны использоваться внешние библиотеки и дополнительные программные среды, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации либо другим нарушениям функционирования интерфейса системы защиты. 4.7. Компоненты системы должны иметь возможность управления использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых для чтения, и использования особенностей современных вычислительных архитектур. 4.8. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и сети Интернет, при работе с веб-страницами, электронной почтой, локальными дисками, съемными носителями и сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции как от вредоносных программ, так и от нежелательной корреспонденции. 4.9. Система должна иметь возможность ограничения времени работы пользователей в сети Интернет, а также времени работы за компьютером. 4.10. Права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав. 4.11. Система защиты рабочих станций должна обеспечивать фильтрацию трафика в программах обмена мгновенными сообщениями, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые ресурсы. 4.12. Система защиты рабочих станций должна обеспечивать фильтрацию результатов работы поисковых систем с отображением только безопасных с точки зрения системы защиты ресурсов. 4.13. Должен быть предусмотрен контроль сетевых подключений на уровне приложений, позволяющий контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале событий. 4.14. Должна быть предусмотрена фильтрация на уровне сетевых пакетов, позволяющая контролировать доступ к сети Интернет независимо от программ, инициирующих подключение. 4.15. В Системе должна быть реализована превентивная защита в дополнение к

	сигнатурному и эвристическому анализу, состоящая из следующих компонентов: • защита от программ-вымогателей, позволяющая защитить компьютер от вредоносных программ-шифровальщиков; • защита от эксплойтов, позволяющая противодействовать использованию уязвимостей в распространенных приложениях; • поведенческий анализ, контролирующий поведение запущенных программ по критическим направлениям, включая изменение системных файлов, целостность запущенных приложений, низкоуровневый доступ к дискам, загрузку драйверов, параметры запуска приложений, системные службы, механизмы автоматического запуска программ, системные политики безопасности, настройки системного окружения и другие критически важные компоненты операционной системы. 4.16. В Системе должна быть реализована самозащита всех собственных объектов, включая критические файлы, процессы, окна, системные ключи и другие компоненты, от несанкционированного доступа пользователей и вредоносного программного обеспечения. Самозащита должна работать на системном уровне и обеспечивать невозможность несанкционированной выгрузки и остановки драйверов антивирусной Системы. 4.17. Должна быть предусмотрена возможность реализации защиты виртуальных рабочих мест с помощью установки виртуальных агентов. 5. Требования к программным средствам антивирусной защиты рабочих станций и серверов под управлением операционных систем семейства Linux 5.1. Должна обеспечиваться поддержка следующих процессорных архитектур: • 32-разрядные архитектуры x86; • 64-разрядные архитектуры x86-64; • 64-разрядные архитектуры ARM; • архитектуры IBM POWER с поддержкой соответствующих 64-разрядных систем команд. 5.2. Система, используя актуальную на момент проведения закупки версию программного обеспечения, должна обеспечивать защиту рабочих станций и серверов, использующих сетевые файловые службы и файловые системы, включая Samba и другие аналогичные технологии, под управлением следующих категорий операционных систем: • Linux на основе ядра версии 2.6.37 и новее, с использованием PAM и библиотеки glibc версии 2.13 и новее; • операционные системы семейства BSD; • серверные операционные системы на основе Linux. 5.3. Интеграция Системы с сетевыми файловыми службами должна осуществляться посредством модулей виртуальной файловой системы. 5.4. Должна существовать возможность компиляции модулей интеграции из исходных кодов для различных версий сетевых файловых служб и 64-разрядных платформ. 5.5. Должна обеспечиваться возможность установки из универсального пакета для UNIX-подобных систем, независимого от типа и версии используемой операционной системы, либо из репозитория или пакета, рассчитанного на работу с используемым в операционной системе менеджером пакетов. 5.6. Должна обеспечиваться возможность установки и обновления Системы как через средства командной строки, так и с помощью графического установщика. 5.7. Должна обеспечиваться возможность автоматической установки модулей, необходимых для функционирования компонентов Системы. 5.8. Должна

	обеспечиваться возможность установки компонентов Системы на зараженные вредоносными программами объекты без их предварительного лечения с последующим лечением заданных файловых областей. 5.9. Должна обеспечиваться поддержка дополнительных подсистем безопасности операционных систем, включая механизмы обязательного контроля доступа, мандатного управления доступом и режимы замкнутой программной среды. 5.10. Должна обеспечиваться возможность мониторинга файловой системы с использованием как встроенных механизмов операционной системы, так и специального модуля ядра. 5.11. Должна обеспечиваться возможность автоматического распознавания моментов монтирования и отмонтирования новых томов файловой системы, включая съемные накопители, оптические носители и дисковые массивы, с корректировкой списка наблюдаемых областей по мере необходимости. 5.12. Должна обеспечиваться возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства. 5.13. Должна обеспечиваться возможность управления параметрами проверки составных файлов, включая архивы, почтовые файлы, упакованные объекты и прочие контейнеры. 5.14. В Системе должна быть реализована функция постоянного контроля установленных сетевых соединений с возможностью проверки трафика, передаваемого через защищенные сетевые соединения с использованием протоколов SSL и TLS. 5.15. В Системе должен быть реализован веб-фильтр с возможностью блокировки интернет-ресурсов по категориям, а также работы в режимах белых и черных списков. 5.16. Система должна поддерживать возможность одновременного запуска нескольких процессов проверки. 5.17. Программные средства Системы должны обеспечивать следующие функциональные возможности: 5.17.1. поиск и удаление вирусов всех известных типов; 5.17.2. полное или выборочное антивирусное сканирование на наличие угроз по команде администратора и по расписанию; 5.17.3. антивирусную проверку в режиме реального времени загружаемых на сервер и передаваемых с него файлов; 5.17.4. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой операционной системы; 5.17.5. запуск задач по расписанию и (или) сразу после загрузки операционной системы; 5.17.6. настройку расписания сканирования с указанием параметров запуска. 5.18. Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Должна быть предусмотрена возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих проверке, а также действий по отношению к вредоносным объектам различных типов. 5.19. Сканирующее ядро должно обеспечивать поиск вирусов и других вредоносных объектов в файлах и загрузочных записях дисковых устройств, включая главную загрузочную запись и загрузочные записи разделов. 5.20. Должна быть предусмотрена возможность использования для проверки файлов метода потоковой проверки, а также метода проксирования. 5.21. Должна быть

	предусмотрена возможность проверки данных, не представленных в виде файлов, полученных через сеть, а также организации распределенной проверки файлов на наличие угроз. 5.22. Должна быть предусмотрена возможность оперативной проверки на наличие угроз файлов, находящихся на локальном устройстве, с которого осуществляется доступ к веб-интерфейсу управления. 5.23. Должна быть предусмотрена возможность проверки на наличие угроз файлов, находящихся на удаленных узлах сети. В качестве таких узлов могут выступать рабочие станции, серверы, сетевые устройства и другие устройства, подключенные к сети и предоставляющие доступ по защищенным протоколам удаленного управления. 5.24. В состав Системы должен входить агент мониторинга, предназначенный для интеграции с системами мониторинга инфраструктуры. 5.25. Должна быть предусмотрена интеграция в систему централизованного управления антивирусной защитой, позволяющая обеспечить управление всеми компонентами Системы из единого центра управления. 6. Требования к программным средствам антивирусной защиты мобильных устройств 6.1. Программные средства антивирусной защиты мобильных устройств должны функционировать под управлением мобильных операционных систем на базе Android версии 4.4 и выше либо обеспечивать совместимость с используемыми Заказчиком мобильными устройствами. 6.2. Используемые программные средства должны обеспечивать: 6.2.1. постоянную защиту файловой системы, перехват и проверку: • файлов, поступающих через мобильные сети передачи данных, беспроводные соединения, интерфейсы передачи данных и подключения к компьютеру; • файлов, загружаемых через браузеры и получаемых посредством электронной почты; • файлов во время синхронизации мобильного устройства с компьютером; • файлов в распространенных форматах архивов и установочных пакетов; • программ, устанавливаемых из интерфейса мобильного устройства; • полную и выборочную проверку объектов файловой системы, находящихся на мобильном устройстве или подключенных картах памяти, по требованию пользователя и по расписанию. 6.2.2. фильтрацию входящих звонков и SMS-сообщений, включая рекламные рассылки, звонки и сообщения с неизвестных номеров, на основе предопределенных и созданных пользователем профилей защиты, для каждого из которых можно сформировать список номеров и определить действия для звонков и сообщений с номеров этого списка. Использование черных списков и телефонной книги устройства. 6.2.3. просмотр и выбор действий для заблокированных звонков и сообщений; 6.2.4. обнаружение файлов автоматического запуска; 6.2.5. удаление или изоляцию зараженных объектов в карантинное хранилище с предоставлением подробной информации о выявленных угрозах; 6.2.6. проведение обновления антивирусных баз: • по протоколу HTTP с использованием встроенных средств передачи данных; • через беспроводные соединения и интерфейсы передачи данных; • путем синхронизации с компьютером, имеющим доступ к сети Интернет. 6.2.7. централизованное управление мобильным устройством на основе

	корпоративных политик; 6.2.8. управление мобильным устройством с использованием встроенных интерактивных элементов интерфейса; 6.2.9. сброс, импорт и экспорт настроек; 6.2.10. удаленное управление мобильным устройством в случае его утери или кражи, включая поиск, экстренное блокирование устройства, удаление личных данных, получение координат и управление устройством посредством команд с использованием заранее установленного пароля; 6.2.11. наличие встроенного сетевого экрана на базе технологии VPN; 6.2.12. наличие фильтра приложений; 6.2.13. защиту от программ-вымогателей и приложений, блокирующих работу устройства; 6.2.14. контроль доступа к интернет-ресурсам через встроенный браузер и сторонние мобильные браузеры; 6.2.15. диагностику безопасности устройства и предоставление рекомендаций по устранению выявленных проблем и уязвимостей с помощью специального компонента, с возможностью обнаружения: • известных уязвимостей мобильных операционных систем и приложений; • небезопасных системных настроек; • конфликтующего программного обеспечения; • скрытых администраторов устройства; • приложений, использующих уязвимости системы безопасности. 7. Требования к системе централизованного управления антивирусной защитой 7.1. Система должна быть построена по клиент-серверной архитектуре с возможностью установки сервера централизованного управления как на серверы, так и на рабочие станции под управлением следующих категорий операционных систем: • настольные операционные системы; • серверные операционные системы; • операционные системы семейства Linux; • операционные системы семейства BSD. 7.2. Сервер централизованного управления должен быть единым для всех защищаемых объектов независимо от используемых операционных систем и платформ, включая рабочие станции, серверы и мобильные устройства. 7.3. Система управления должна быть доступна из любой операционной системы, поддерживающей современные веб-браузеры, без ограничений на использование актуальных версий браузеров и без необходимости установки дополнительного программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы. 7.4. Аутентификация администраторов должна быть возможна следующими способами: • из внутренней базы данных сервера; • с использованием протокола LDAP и служб каталогов; • с использованием протокола RADIUS; • с использованием механизмов аутентификации операционной системы PAM. 7.5. Должна быть реализована возможность построения иерархической системы серверов управления: главных, подчиненных и равноправных, с возможностью распространения лицензий по межсерверным связям, а также автоматического обновления лицензионного ключевого файла. 7.6. Система управления должна иметь возможность: • объединения информации от нескольких серверов на одном сервере; • распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть; • обмена статистикой в рамках одной иерархической сети между серверами различных версий; •

	построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне. 7.7. Должна быть реализована возможность запуска мобильного центра управления Системой на мобильных устройствах под управлением мобильных операционных систем с помощью соответствующих мобильных приложений без использования веб-браузеров. 7.8. Система управления должна иметь возможность: 7.8.1. использования как внешней, так и внутренней системы управления базами данных, поставляемой в составе дистрибутива антивирусного сервера. В качестве внешних должны поддерживаться распространенные реляционные системы управления базами данных, а также подключение через ODBC-драйверы для серверных и настольных операционных систем; 7.8.2. замены типа используемой системы управления базами данных в ходе работы после установки серверной части без необходимости ее переустановки; 7.8.3. управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа и выполнения произвольных SQL-запросов; 7.8.4. аудита действий, произведенных с помощью функций встроенного программного интерфейса Web API; 7.8.5. самостоятельного написания обработчиков событий на языке программирования Lua, а также выполнения произвольных сценариев с помощью средств системы управления; 7.8.6. экспорта отчетов в форматы CSV, XML, HTML и PDF; 7.8.7. подписки и получения новостей от производителя программного обеспечения, в том числе информирующих об актуальных угрозах, непосредственно в консоли центра управления; 7.8.8. наличия нескольких способов уведомления пользователей и администраторов путем отправки электронной почты, звукового оповещения, всплывающего окна, записи в журнал событий, оповещения в веб-консоли, push-уведомлений, сетевых протоколов мониторинга и системного журналирования; 7.8.9. отправки системным администратором информационных сообщений пользователям произвольного содержания, включающих текст сообщения, гиперссылки на интернет-ресурсы и графические изображения, по сети в режиме реального времени через веб-интерфейс Системы; 7.8.10. ограничения сетевого трафика как при установке агентов, так и при их обновлении; 7.8.11. скачивания конфигурационных файлов с настройками подключения антивирусных агентов для различных операционных систем; 7.8.12. централизованного обновления антивирусных баз на всех защищаемых объектах и доставки обновлений на рабочие места пользователей как по расписанию, так и сразу после их получения; 7.8.13. управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая возможность отката обновлений; 7.8.14. проведения групповых обновлений; 7.8.15. обновления по защищенному каналу с использованием SSL-сертификатов; 7.8.16. организации отложенного обновления; 7.8.17. автоматического перехода установленного программного обеспечения на более новые версии, в том числе с возможностью выбора обновляемых компонентов; 7.8.18.

	выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские устройства; 7.8.19. чтения полного пакета документации администратора и пользователя непосредственно в консоли центра управления. 7.9. Система должна обладать специальной политикой для мобильных пользователей, в том числе пользователей ноутбуков, при применении которой пользователи должны иметь возможность редактирования настроек антивирусного пакета и получения обновлений через сеть Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно осуществляться через веб-интерфейс без необходимости использования файлов конфигурации. 7.10. Система управления должна обладать возможностью встроенного автоматического копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также возможностью восстановления сервера из резервной копии. 7.11. В системе управления должен быть реализован компонент, позволяющий проводить сканирование сети с целью обнаружения рабочих станций и определения наличия антивирусного агента в режимах поиска по службе каталогов, по сетевым именам, с использованием ICMP и TCP. 7.12. В центре управления должна быть реализована групповая политика на основе предустановленных системных и пользовательских групп. Предустановленные системные группы должны позволять обращаться: • ко всем защищаемым объектам; • к объектам службы каталогов; • к объектам по типам операционных систем; • к объектам по применяемым политикам; • к объектам по профилям настроек; • к объектам по сетевым протоколам; • к объектам по статусу; • к объектам по персональным настройкам. 7.13. Система управления должна обладать возможностью контроля запуска приложений как на основе запрещающих и разрешающих правил, так и на основе функционального анализа приложений по следующим группам: • запуск приложений; • загрузка и исполнение модулей; • запуск сценарных интерпретаторов; • загрузка драйверов; • установка программных пакетов; • контроль целостности исполняемых файлов. 7.14. Должна обеспечиваться отчетность по мониторингу антивирусного программного обеспечения с использованием сервера централизованного управления. 7.15. Должен быть предусмотрен централизованный сбор статистической информации с созданием отчетов о состоянии антивирусной защиты и их консолидацией, а также возможность автоматического формирования статистических отчетов по заданным параметрам с последующей отправкой администратору по электронной почте. 7.16. В Системе должен быть реализован менеджер лицензий, поддерживающий иерархический список лицензионных ключей. Менеджер лицензий должен предоставлять следующие возможности: • просмотр информации о лицензии; • добавление нового лицензионного ключа; • обновление лицензионного ключа; • замена лицензионного ключа; • расширение списка лицензионных ключей объекта; • удаление лицензионного ключа; • удаление объекта из списка лицензирования; • передача лицензий на соседний сервер управления; •

	редактирование лицензий, переданных на соседний сервер управления. 7.17. Система должна иметь возможность шифрования трафика между серверами и защищаемыми рабочими станциями в целях предотвращения утечки конфиденциальной информации. 7.18. Производитель Системы должен обеспечивать выпуск обновлений антивирусных баз не менее 20 раз в сутки, что должно подтверждаться отчетом, формируемым средствами Системы. 7.19. В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория. 7.20. Должна обеспечиваться поддержка виртуальной инфраструктуры и интеграция с инфраструктурой виртуальных рабочих мест (VDI), а также поддержка распространенных технологий виртуализации и гипервизоров.
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)	Поставщик, определенный победителем закупки, при поставке лицензии и (или) оказании сопутствующих услуг должен предоставить документальное подтверждение наличия действующих партнерских отношений с производителем предлагаемого программного обеспечения. В качестве подтверждения принимаются партнерский сертификат, авторизационное письмо производителя либо информация об официальном статусе поставщика, размещенная на официальном интернет-ресурсе производителя.