Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Әділет министрлігі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Әділет министрлігі" мемлекеттік мекемесі
Конкурстың №:	№ 17985052-1
Конкурстың атауы:	Антивирустық бағдарламалық техникалық қамтамасыз ету және лицензияларды ұзарту бойынша қызметтер
Лоттың нөмірі:	№ 87894721-ОКЗ
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:	1276775.87
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	1276775.87
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	техникалық ерекшелігіне сәйкес
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Виртуалды серверлерге арналған антивирустық БЖ лицензияларын ұзарту және техникалық қолдау қызметіне техникалық сипаттама Осы техникалық ерекшелікте виртуалды серверлер үшін вирусқа қарсы бағдарламалық қамтамасыз етуді лицензиялауды және техникалық қолдауды (бұдан әрі - Қызмет) ұзарту қызметіне мынадай талаптарға сәйкес келеді: сатып алуды жүргізу нәтижесінде виртуалды орта үшін 70 бірлік көлемінде KHCS вирусқа қарсы бағдарламасына қолданыстағы лицензияны және техникалық қолдауды 2026 жылғы 7 желтоқсаннан бастап кемінде 12 ай мерзімге ұзарту талап етіледі. Қызмет көрсету мерзімі шартқа қол қойылған және заңды күшіне енген сәттен бастап есептеледі. Қызметтердің әлеуетті өнім берушісі Қазақстан Республикасының аумағында өндіруші компанияның уәкілетті серіктесі ретінде жоғарыда көрсетілген антивирустық бағдарламаға құқықты растайтын антивирустық БҚ өндіруші компаниядан осы конкурсқа қатысу құқығына авторизациялық хат ұсынуға міндетті (хаттың электрондық көшірмесі конкурстық өтінімде болуға тиіс). Тапсырыс берушіге қызметті қабылдауға және қызметті қабылдауға және ресімдеуге байланысты барлық операцияларды жүргізуге, техникалық қолдауға көмек сұрауға және қызмет көрсетушінің техникалық мамандарын тартуға құқық беріледі. Антивирустық бағдарламаның лицензиясы физикалық және виртуалды серверлерде тұрақты жұмыс істеуді, орталықтандырылған басқаруды қамтамасыз ететін корпоративтік шешімі болуы керек. 1. Антивирустық қорғаныс бағдарламалық жасақтамасына қойылатын техникалық талаптар. 1.1. Жалпы талаптар. Гибридті орталарға арналған антивирустық қорғаныс виртуалды машиналарды, жалпыға ортақ бұлттарды және Windows және Linux серверлерін қорғауы керек. Барлық антивирустық құралдардың, соның ішінде басқару құралдарының бағдарламалық интерфейсі орыс және ағылшын тілдерінде болуы керек. Барлық антивирустық құралдар, соның ішінде басқару элементтері орыс және ағылшын тілдерінде контекстік анықтамалық жүйеге ие болуы керек. Шешім мыналарды қамтуы керек: 1) виртуалды ортаға арналған антивирустық қорғаныстың агентсіз бағдарламалық құралдары; 2) агенттерді пайдалана отырып, виртуалды ортаға арналған вирусқа қарсы қорғау бағдарламалық құралдары; 3) бұлтты инфрақұрылымға арналған бағдарламалық қамтамасыз ету; 4) орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары; 5) зиянды бағдарламалар мен шабуылдардың қолтаңбаларының жаңартылатын дерекқорлары; 6) орыс тіліндегі пайдалану құжаттамасы. 1.2. Виртуалды ортаны антивирустық қорғаудың агентсіз бағдарламалық құралдарына қойылатын талаптар. VMware виртуалды инфрақұрылымы: 1) ESXi 6.5 Update 3a; 2) ESXi 6.7 Update 3; 3) ESXi 7.0 Update 1c; 4) vCenter 6.0 Update 3j; 5) vCenter 6.5 Update 3; 6) vCenter 6.7 Update 3; 7) vCenter 7.0 Update 1d; 8) VMware NSX-V Manager VMware NSX деректер орталығы vSphere 6.4.10 пакетінен; 9) VMware NSX-t Manager VMware NSX-t деректер орталығы 3.1.3; VMware NSX-T деректер орталығы 3.1.1 немесе VMware NSX-T деректер орталығы 3.0.3; 10) VMware NSX-t Manager VMware NSX-T

	деректер орталығы 3.0.3 пакетінен; 11) vCloud Director 10.1.2 немесе vCloud Director 10.3.0 for Service Providers. Жұмыс станцияларына арналған Windows операциялық жүйелері: 1) Windows 10; 2) Windows 8.1; 3) Windows 8; 4) Windows 7 Service Pack 1. Серверлерге арналған Windows операциялық жүйелері: 1) Windows Server 2019; 2) Windows Server 2016; 3) Windows Server 2012 R2 ReFS қолдауынсыз (Resilient File System); 4)Windows Server 2012 ReFS (Resilient File System) қолдауынсыз; 5) Windows Server 2008 R2 Service Pack 1. Серверлерге арналған Linux операциялық жүйелері: 1) Ubuntu Server 18.04 GA (64 биттік). 2) Ubuntu Server 16.04 GA (64 биттік). 3) Ubuntu Server 14.04 GA (64 биттік). 4) Red Hat Enterprise Linux server 7.7 ga (64 биттік). 5) Red Hat Enterprise Linux server 7.4 ga (64 биттік). 6) Red Hat Enterprise Linux Server 7.0 ga (64 биттік). 7) SUSE Linux Enterprise Server 12 GA (64 биттік). 8) CentOS 7.7 GA (64 биттік). 9) CentOS 7.4 GA (64 биттік). 10) CentOS 7.0 GA (64 биттік). Виртуалды орталарды вирусқа қарсы қорғаудың бағдарламалық құралдары мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс: 1) қонақтар машиналарына антивирустық агент орнатпай, нақты уақыт режимінде және жоспарланған тексеру режимінде зиянды бағдарламадан қорғау; 2) өшірулі қонақ машиналарын, зиянды бағдарламалардың бар-жоғын, оларды тексеру уақытына қосудың қажеті жоқ сканерлеу, оның ішінде Linux ОЖ және EXT2, EXT3, EXT4, XFS, BTRFS, VFAT, ISO9660 файлдық жүйелері бар қонақ машиналары; 3) Виртуалды машина үлгілерін тексеру; 4) қонақ машиналарының файлдық жүйесін қорғауды қамтамасыз ету үшін VMware NSX Manager технологиясымен интеграция; 5) нақты уақыт режимінде сканерлеу кезінде және жоспарланған тексеру режимінде файл бойынша үкім алу үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; 6) оқшауланған виртуалды инфрақұрылымдарды қорғау үшін VMware vCloud Director сервері басқаратын провайдер сервисі инфрақұрылымында multitenancy режимін қолдау; 7) жаңартуларды қонақ машиналарына таратудың қажеттілігінсіз базаларды орталықтандырылған жаңартулар; 8) Таңдалған файлдарды, қалталарды және бүкіл жүйені сканерлеу; 9) тексерілген файлдарды қайта сканерлеуден аулақ болатын сканерлеу режимін оңтайландыру; 10) бір гипервизор шеңберінде әртүрлі қонақ машиналарында бірдей объектілерді қайта сканерлеуді болдырмау; 11) әкімшілерді хабардар ете отырып, зиянды бағдарламаны бұғаттау, залалсыздандыру және жою; 12) барлық қорғаныс компоненттері үшін бірыңғай басқару консолі; 13) виртуалды орталар мен физикалық жұмыс станциялары үшін орталықтандырылған басқару; 14) басқарудың физикалық және логикалық құрылымын VMware vCenter-де көрсетілген түрде көрсету; 15) виртуалды машиналардағы оқиғалар және тапсырмалардың орындалуы туралы толық ақпаратты көрсету; 16) виртуалды машиналардың жекелеген топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану; 17) Бір ESXi-хосттан екіншісіне көшу кезінде виртуалды машиналарды қорғаудың

	үздіксіздігі; 18) жойылған файлдардың сақтық көшірмелерін сақтау; 19) қорғалатын виртуалды машиналар саны және физикалық CPU саны бойынша лицензиялау схемасын қолдау; 20) пайдаланушының есептік жазбасының рөліне байланысты саясат пен міндеттер параметрлеріне қол жеткізуді саралау; 21) ең жиі тексерілетін файлдар туралы статистиканы көрсету; 22) VMware NSX-t Manager басқаратын инфрақұрылымда бағдарламаны орнату және жұмыс істеу мүмкіндігі. 1.3. Агенттерді қолдана отырып, виртуалды ортаны антивирустық қорғауға қойылатын талаптар. Виртуалды Инфрақұрылым: 1) VMware ESXi 6.5, 6.7, 7.0; 2) Windows Server 2012 R2 Hyper-V; 3) Windows Server 2016 Hyper-V; 4) Windows Server 2019 Hyper-V; 5) Citrix Hypervisor 8.2 LTSR. 6) Proxmox ve платформасы: Proxmox ve 6.4 гипервизоры; 7) Huawei FusionSphere – FusionCompute CNA 8.0; 8) Nutanix Acropolis: nutanix ahv 5.19.1 гипервизоры; 9) Enterprise Cloud Platform VeiL: гипервизор VeiL Node 4.5. 10) SharxBase: sharxbase 5.10 гипервизоры.x. 11) KVM платформасы: келесі операциялық жүйелердің біріне негізделген KVM гипервизоры: 11.1) Ubuntu Server 18.04, 20.04 LTS; 11.2) Red Hat Enterprise Linux Server 7,9; 11.3) CentOS 7.9. 12) ТИОНИКС бұлтты платформасы: келесі операциялық жүйелердің біріне негізделген KVM гипервизоры: 12.1) Ubuntu Server 18.04, 20.04 LTS; 12.2) Red Hat Enterprise Linux Server 7.9; 12.3) CentOS 7.9. 13) OpenStack платформасы: келесі операциялық жүйелердің біріне негізделген KVM гипервизоры: 13.1) Ubuntu Server 18.04, 20.04 LTS; 13.2) Red Hat Enterprise Linux Server 7,9; 13.3) CentOS 7.9. Қонақ операциялық жүйелері: 1) Windows 11 Pro / Enterprise 21H2 / 22H2 / 23H2. 2) Windows 10 Desktop Pro 19h1 / 19H2 / 20H1 / 20H2 / 21H1 / 22H2 (32 / 64 бит). 3) Windows 10 Enterprise 2016 ltsc / 2019 ltsc / 19H1 / 19H2 / 20H1 / 20H2 / 21H1 / 22H2 (32 / 64 бит). 4) Windows 8.1 Update 1 professional / Enterprise (32 / 64 биттік). 5) Windows 7 Professional / Enterprise Service Pack 1 (32 / 64 бит). 6) Windows Server 2022 Standard / Datacenter / Essentials (Desktop experience / Core). 7) Windows Server 2019 Standard / Datacenter (Desktop experience / Core). 8) Windows Server 2016 Standard / Datacenter (Desktop experience / Core). 9) Windows Server 2012 R2 Standard / Datacenter / Essentials (Desktop experience / Core). 10) Windows Server 2012 Standard / Datacenter / Essentials (Desktop experience / Core). 11) Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core). 12) Debian GNU / Linux 10.1 және одан жоғары (32 / 64 бит). 13) Debian GNU / Linux 9.4 және одан жоғары (32 / 64 бит). 14) Ubuntu Server 20.04 LTS (64 биттік). 15) Ubuntu Server 18.04 LTS (64 биттік). 16) CentOS 8.0 және одан жоғары (64 биттік). 17) CentOS 7.3 және одан жоғары (64 биттік). 18) Red Hat Enterprise Linux Server 8.0 және одан жоғары (64 биттік). 19) Red Hat Enterprise Linux server 7.3 және одан жоғары (64 биттік) 20) SUSE Linux Enterprise Server 15 SP2 (64 биттік). 21) Alt Linux 8 SP (64 биттік). 22)

	Linacle Linux 8.0 және одан жоғары (64 биттік). 23) Linacle Linux 7.3 және одан жоғары (64 биттік). 24) Astra Linux se 1.6 (қол жетімділікті мандаттық шектеу режимдерін және жабық бағдарламалық ортаны қолдаусыз). 25) Astra Linux se 1.5 (қол жетімділікті мандаттық шектеу режимдерін және жабық бағдарламалық ортаны қолдаусыз). 1.4. Windows жұмыс үстелі операциялық жүйелерінде. 1) резиденттік антивирустық мониторинг; 2) бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; 3) антивирустық сканерлеуді және басқа да ресурстарды қажет ететін тапсырмаларды қонақ машиналарында емес, жеке қорғаныс машинасында орындау; 4) негізгі қорғау машинасы болмаған жағдайда ЖМ-дегі агенттерді жұмыс істеп тұрған, оның ішінде басқа хосттағы қорғау машинасына автоматты түрде анықтау және қосу; 5) қорғау машинасының қолжетімсіздігі кезеңінде қорғалатын қонақтар машинасында барлық файлдық операцияларды журналдау арқылы қорғау машинасының қысқа мерзімді қолжетімсіздігі кезеңінде файлдық қорғаудың үздіксіздігін қамтамасыз ету және қолжетімділік қалпына келтірілгеннен кейін барлық өзгерістерді автоматты түрде сканерлеуді орындау. 6) нақты уақыт режимінде сканерлеу кезінде және жоспарланған тексеру режимінде файл бойынша үкім шығару үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау. 7) электрондық хат — хабарларды трафикті тексере отырып, зиянды бағдарламалардан қорғау мынадай хаттамаларда: IMAP, SMTP, POP3-пайдаланылатын электрондық пошта клиентіне қарамастан. 8) Outlook клиентіне арналған қосымшаны тексеруді қосу/өшіру, сондай-ақ тіркемені жою немесе кірістірілген файл пішімін өзгерту мүмкіндігі бар электрондық пошта плагині. 9) веб - трафикті қорғау-HTTP, HTTPS, FTP хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін объектілерді, оның ішінде сенімді сайттарды баптау мүмкіндігімен эвристикалық талдау көмегімен тексеру. 10) веб-беттерден жүктелген баннерлер мен қалқымалы терезелерді бұғаттау. 11) фишингтік сайттарды тану және бұғаттау. 12) олардың мінез-құлқын талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау. 13) осы қолданбаның әрекеттерін талдау арқылы қолданбаның қалыптан тыс әрекетін анықтау мүмкіндігі. 14) емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару мүмкіндігі. 15) ортақ файлдар мен қалталарды сыртқы шифрлаудан қорғау. 16) тізілімге жазу, Файлдар мен қалталарға кіру сияқты орындалатын бағдарламалардың артықшылықтарын шектеу мүмкіндігі. Бағдарламаның беделіне негізделген шектеу деңгейлерін автоматты түрде анықтау. 17) барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасауға мүмкіндік беретін компоненттің болуы; 18) арнайы ережелерді құру компоненті бағдарламаны, метадеректерді, сертификатты немесе оның ізін, MD5 немесе SHA256 бақылау сомасын табу жолында

	қосымшаларды бақылауға тиіс; 19) арнайы қағидаларды құру компоненті қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі тиіс, оларға салынған файлдарды өзгерте және іске қоса алатын сенімді жаңартулар пакеттерінің тізімін жасай алуы тиіс; 20) белгілі бір протоколдар (TCP, UDP) және порттар үшін желілік пакеттік ережелерді орнатуға, сондай-ақ нақты бағдарламалар үшін желілік ережелерді құруға мүмкіндік беретін кіріктірілген желілік экранның болуы 21) кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған интрузияны анықтау және алдын-алу жүйесі (IDS/IPS) және желілік белсенділік ережелері бар брандмауэрді қолдана отырып, хакерлік шабуылдардан қорғау. 22) пайдаланушының құрылғының типі және/немесе пайдаланылатын Шина бойынша сыртқы енгізу/шығару құрылғыларымен жұмысын олардың сәйкестендіргіші бойынша сенімді құрылғылардың тізімін жасау мүмкіндігімен және ad ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігімен бақылауды жүзеге асыру. 23) пайдаланушының Интернет желісімен жұмысын бақылауды жүзеге асыру, оның ішінде белгілі бір сипаттағы ресурстарға қол жеткізуге нақты тыйым салу немесе рұқсат беру, сондайақ ақпараттың белгілі бір түрін (аудио, видео және т.б.) бұғаттау мүмкіндігі. Бағдарламалық құрал бақылаудың уақыт аралықтарын енгізуге, сондай-ақ оны тек AD ішінен белгілі бір пайдаланушыларға тағайындауға мүмкіндік беруі керек. 24) барлық виртуалды машиналарды алдын ала белгіленген кесте бойынша тексеру мүмкіндігі. 25) тексерілген файлдарды қайта сканерлеудің алдын алу. 26) әртүрлі виртуалды машиналарда орналасқан бірдей файлдарды қайта тексеруді болдырмауға мүмкіндік беретін қорғау машинасында тексерілген файлдар туралы ақпараттың болуы. 27) зиянды бағдарламаны бұғаттау, залалсыздандыру және жою, әкімшілерді хабардар ету. 28) барлық қорғаныс компоненттері үшін бірыңғай басқару консолі 29) виртуалды машиналардың жекелеген топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану мүмкіндігі. 30) жойылған файлдардың сақтық көшірмелерін сақтау. 31)антивирустық базаларды кері қайтаруды қолдау. 32) қорғалатын виртуалды машиналар саны (жұмыс станциялары) және процессорлар саны бойынша лицензиялау схемасын қолдау. 33) антивирустық параметрлерді профильдеу механизмі, оны қолдану аясын одан әрі шектеуге мүмкіндік береді. 1.5. Windows серверлік операциялық жүйелерінде. 1) резиденттік антивирустық мониторинг; 2) маскировка бағдарламаларынан, ақылы сайттарға автоматты түрде қоңырау шалу бағдарламаларынан қорғау; 3) бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; 4) антивирустық сканерлеуді және басқа да ресурстарды қажет ететін тапсырмаларды қонақ машиналарында емес, жеке қорғаныс машинасында орындау; 5) электрондық хат — хабарларды трафикті тексере отырып, зиянды бағдарламалардан қорғау мынадай хаттамаларда: IMAP, SMTP, POP3-пайдаланылатын

	электрондық пошта клиентіне қарамастан. 6) негізгі қорғау машинасы қолжетімсіз болған жағдайда жұмыс істеп тұрған, оның ішінде басқа хосттағы қорғау машинасын автоматты түрде анықтау және оған қосу; 7) қорғау машинасының қолжетімсіздігі кезеңінде қорғалатын қонақтар машинасында барлық файлдық операцияларды журналдау арқылы қорғау машинасының қысқа мерзімді қолжетімсіздігі кезеңінде файлдық қорғаудың үздіксіздігін қамтамасыз ету және қолжетімділік қалпына келтірілгеннен кейін барлық өзгерістерді автоматты түрде сканерлеуді орындау; 8) нақты уақыт режимінде сканерлеу кезінде және жоспарланған тексеру режимінде файл бойынша үкім алу үшін өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; 9) олардың мінез-құлқын талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау; 10) ортақ файлдар мен қалталарды сыртқы шифрлаудан қорғау; 11) белгілі бір протоколдар (TCP, UDP) және порттар үшін желілік пакеттік ережелерді орнатуға мүмкіндік беретін кіріктірілген желілік экранның болуы; 12) нақты бағдарламалар үшін желілік қағидалар құру; 13) кез-келген типтегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қосымшаларға арналған кіруді анықтау және алдын-алу жүйесі (IDS/IPS) және желілік белсенділік ережелері бар брандмауэрді қолдана отырып, хакерлік шабуылдардан қорғау; 14) антивирустық базалардың бір бөлігін қорғау машинасында сақтау мүмкіндігімен орталықтандырылған жаңартулар; 15) барлық виртуалды машиналарды алдын ала белгіленген кесте бойынша тексеру мүмкіндігі; 16) тексерілген файлдарды қайта сканерлеудің алдын алу; 17) әртүрлі виртуалды машиналарда орналасқан бірдей файлдарды қайта тексеруді болдырмауға мүмкіндік беретін қорғау машинасында тексерілген файлдар туралы ақпараттың болуы; 18) зиянды бағдарламаны бұғаттау, залалсыздандыру және жою, әкімшілерді хабардар ету; 19) барлық қорғаныс компоненттері үшін бірыңғай басқару консолі; 20) виртуалды орталар мен физикалық жұмыс станциялары үшін бірыңғай орталықтандырылған басқару консолі; 21) виртуалды машиналардағы оқиғалар туралы және міндеттердің орындалуы туралы толық ақпарат беру; 22) виртуалды машиналардың жекелеген топтары үшін әртүрлі қауіпсіздік параметрлерін қолдану мүмкіндігі; 23) жойылған файлдардың сақтық көшірмелерін сақтау; 24) антивирустық базаларды кері қайтаруды қолдау; 25) қорғалатын виртуалды машиналар (серверлер) саны бойынша және процессорлар бойынша лицензиялау схемасын қолдау; 26) антивирустың қолданылу аясын одан әрі шектеуге мүмкіндік беретін параметрлерін профильдеу тетігі; 1.6. Linux серверлік операциялық жүйелерінде. 1) резиденттік антивирустық мониторинг; 2) бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; 3) пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу; 4) zip мұрағаттарындағы файлдарды вирусқа қарсы тексеру;.7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz; .tbz2; .gz;.tgz; .arj.; 5)

	Электрондық пошта хабарламаларын мәтіндік форматта тексеру (Plain text); 6) файлдарды тексеруді оңтайландыру тетіктерінің болуы (жаһандық мониторингтен ерекшеліктер маска және жад пен процестер, сенімді процестер, тексеру уақытының лимиті, тексерілетін файл өлшемінің лимиті, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат); 7) күдікті және бүлінген объектілерді карантинге қою; 8) тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; 9) есептерді HTML және CSV форматтарында экспорттау және сақтау мүмкіндігі; 10) залалданған объектінің көшірмесін, егер ол ақпараттық құндылықты білдірсе, талап ету бойынша Объектіні ықтимал қалпына келтіру мақсатында емдеу және жою алдында резервтік қоймада сақтау; 11) бірыңғай басқару жүйесінің көмегімен жоғарыда көрсетілген барлық компоненттерді орталықтандырылған басқару; 12) Linux үшін жеңіл агент орнатылған виртуалды машиналарда GlusterFS файлдық жүйесін қолдау; 13) жүктеу секторларын, жүйелік жадты және Авто іске қосу объектілерін тексеру мүмкіндігі. 1.7. Linux жұмыс станциялары мен серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар. Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 32 биттік операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: 1) CentOS 6.7 және одан жоғары. 2) Debian GNU/Linux 9.4 және одан жоғары; 3) Debian GNU/Linux 10.1 және одан жоғары; 4) Debian GNU/Linux 11.1 және одан жоғары; 5) Linux Mint 19 және одан жоғары; 6) Mageia 4; 7) Red Hat Enterprise Linux 6.7 және одан жоғары; 8) Альт Білім 9; 9) Альт Жұмыс Станциясы 9; 10) Альт Сервер 9. Linux жұмыс станцияларына арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың 64 биттік операциялық жүйелерімен жұмыс істейтін компьютерлерде жұмыс істеуі керек: 1) AlterOS 7.5 және одан жоғары; 2) Amazon Linux 2; 3) Astra Linux Common Edition (кезекті жаңарту 2.12); 4) ASTRA Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.5); 5) ASTRA Linux Special Edition РУСБ.10015-01 (кезекті жаңарту 1.6); 6) ASTRA Linux Special Edition РУСБ.10015-16 (орындау 1) (кезекті жаңарту 1.6); 7) CentOS 6.7 және одан жоғары; 8) CentOS 7.2 және одан жоғары; 9) CentOS 8.0 және одан жоғары; 10) Debian GNU / Linux 9.4 және одан жоғары; 11) Debian GNU / Linux 10.1 және одан жоғары; 12) Debian GNU / Linux 11.1 және одан жоғары; 13) EulerOS V2.0SP2 2.2.17; 14) EulerOS V2.0SP5 2.5.6; 15) Linux Mint 19 және одан жоғары; 16) Linux Mint 20.1 және одан жоғары; 17) openSUSE Leap 15.0 және одан жоғары; 18) Linacle Linux 7.3 және одан жоғары; 19) Linacle Linux 8.0 және одан жоғары; 20) Pardus OS 19.1; 21) Red Hat Enterprise Linux 6.7 және одан жоғары; 22) Red Hat Enterprise Linux 7.2 және одан жоғары; 23) Red Hat Enterprise Linux 8.0 және одан жоғары; 24) SUSE Linux Enterprise Server 12 SP5 және одан жоғары; 25) SUSE Linux Enterprise Server 15 және одан жоғары; 26) Ubuntu 18.04 LTS және одан жоғары; 27)

	Ubuntu 20.04 LTS; 28) Альт Білім 9; 29) Альт Жұмыс Станциясы 9; 30) Альт Сервер 9; 31) Гослинукс 7.2; 32) РЕД ОС 7.3; Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек: 1) резиденттік антивирустық мониторинг; 2) іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; 3) SMB / NFS арқылы қолжетімді ресурстарды тексеру; 4) ядро жадын тексеру мүмкіндігі; 5) бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; 6) олардың мінез-құлқын талдау негізінде әлі белгісіз зиянды бағдарламалардан қорғау; 7) пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу; 8) Zip мұрағаттарындағы файлдарды вирусқа қарсы тексеру;.7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; 9) мәтіндік форматтағы электрондық пошта хабарларын тексеру (Plain text); 10) файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының лимиті, тексерілетін файл өлшемінің лимиті, кэштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат); 11) SMB / NFS хаттамалары бойынша желілік қолжетімділігі бар жергілікті каталогтардағы файлдарды қашықтықтан зиянды шифрлаудан қорғау; 12) тексеру кезінде файлдарды бұғаттау опциясын қосу мүмкіндігі; 13) күдікті және бүлінген объектілерді карантинге орналастыру; 14) SAMBA деңгейінде файлдық операцияларды ұстап алу және тексеру мүмкіндігі; 15) Қағидалардың бастапқы жай-күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару; 16) тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; 17) есептерді HTML және CSV форматтарында экспорттау және сақтау мүмкіндігі; 18) файлдық кеңістікті сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару; 19) егер ол ақпараттық құндылықты білдірсе, талап ету бойынша Объектіні ықтимал қалпына келтіру мақсатында залалданған объектінің көшірмесін емдеу және жою алдында резервтік қоймада сақтау; 20) пайдаланушы графикалық интерфейсі арқылы түбірлік құқықтарсыз басқару мүмкіндігі; 21) бірыңғай басқару жүйесі немесе веб-консоль арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; 22) пайдаланушылардың компьютерге орнатылған немесе қосылған құрылғыларға құрылғы түрлері мен қосылу шиналары бойынша қол жеткізуін басқару мүмкіндігі; 23) алынбалы дискілерді тексеру мүмкіндігі; 24) кіріс желілік трафикте желілік шабуылдарға тән әрекеттерді бақылау мүмкіндігі; 25) HTTP/HTTPS және FTP хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін трафикті тексеру мүмкіндігі, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік мекенжайларға тиесілігін орнату мүмкіндігі; 26) пайдаланушының компьютерінде бағдарламалардың әрекеттері туралы деректерді

	алу; 27) пайдаланушылардың компьютерлерінде бағдарламалардың іске қосылуын басқару (бағдарламаларды бақылау міндеті); 28) пайдаланушылардың компьютерлерінде сақталатын бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу (түгендеу міндеті); 29) бағдарламаны іске қосқан кезде бақылау файлдарын құру. 1.8. Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғаудың бағдарламалық құралдарына қойылатын талаптар. Windows файлдық серверлеріне арналған антивирустық бағдарламалық жасақтама келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: 1) Microsoft Windows 32 биттік операциялық жүйелер; 2) SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2003 Standard / Enterprise / Datacenter; 3) Windows Server 2003 R2 Foundation / Standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен; 4) SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2008 Standard / Enterprise / Datacenter; 5) Windows Server 2008 core standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен. 64 биттік Microsoft Windows операциялық жүйелері 1) SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2003 Standard / Enterprise / Datacenter; 2) Windows Server 2003 R2 standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен; 3) Windows Server 2008 core standard / Enterprise / datacenter SP2 немесе одан жоғары жаңарту бумасымен; 4) SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2008 Standard / Enterprise / Datacenter; 5) Microsoft Small Business Server 2008 Standard / Premium SP2 немесе одан жоғары; 6) Windows Server 2008 R2 Foundation / Standard / Enterprise / datacenter SP1 немесе одан жоғары жаңарту бумасымен; 7) Windows Server 2008 R2 core standard / Enterprise / datacenter SP1 немесе одан жоғары жаңарту бумасымен; 8) SP1 немесе одан жоғары жаңарту бумасы бар Windows Hyper-V Server 2008 R2; 9) Microsoft Small Business Server 2011 Essentials / standard SP1 немесе одан жоғары; 10) Microsoft Windows MultiPoint Server 2011 Standard / Premium; 11) Windows Server 2012 Foundation / Essentials / Standard / Datacenter; 12) Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; 13) Microsoft MultiPoint Server 2012 Standard / Premium; 14) Windows Storage Server 2012; 15) Windows Hyper-V Server 2012; 16) Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; 17) Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; 18) Windows Storage Server 2012 R2; 19) Windows Hyper-V Server 2012 R2; 20) Windows Server 2016 Essentials / Standard / Datacenter; 21) Windows Server 2016 MultiPoint; 22) Windows Server 2016 Core Standard / Datacenter; 23) Microsoft Windows MultiPoint Server 2016; 24) Windows Storage Server 2016; 25) Windows Hyper-V Server 2016; 26) Windows Server 2019 Essentials / Standard / Datacenter; 27) Windows Server 2019 Core; 28) Windows Storage Server 2019; 29)

	Windows Hyper-V Server 2019; 30) Windows Server 2022; 31) Windows 10 Enterprise multi-session. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек: 1) нақты уақыт режимінде және сұраныс бойынша әртүрлі функцияларды орындайтын серверлерде антивирустық сканерлеу: терминал серверлері, баспа серверлері, қолданба серверлері және домен контроллері, файл серверлері; 2) пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу; 3) тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; 4) іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін нақты уақыт режимінде өндірушінің арнайы сайттарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; 5) RAR, ARJ, ZIP, CAB форматтарындағы файлдарды антивирустық тексеру және емдеу; 6) файлдарды, файлдық жүйелердің балама ағындарын (NTFS-streams), жүктеу жазбасын, жергілікті және алынбалы дискілердің жүктеу секторларын қорғау; 7) Microsoft Windows script Technologies (немесе Active Scripting) технологиялары бойынша құрылған VBScript және JScript сценарийлерінің қорғалатын серверінде орындау әрекеттерін үздіксіз қадағалау, сценарийлердің бағдарламалық кодын тексеру және қауіпті деп танылғандардың орындалуына автоматты түрде тыйым салу; 8) желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға өтініштерді талдау; 9) Microsoft Windows контейнерлерін тексеру мүмкіндігі; 10) процестердің жадындағы осалдықтарды пайдаланудан қорғау; 11) бұзылған процестерді автоматты түрде аяқтау мүмкіндігі, бұл ретте сыни жүйелік процестер аяқталмауы тиіс; 12) қорғалған тізімге процестерді қосу мүмкіндігі; 13) өткен тексеру уақытынан бастап жай-күйі өзгермеген объектілерді өткізу есебінен сканерлеу процесін жеделдету; 14) жеке модульдерді жеке міндет арқылы олардың тұтастығын ықтимал бұзуға тексеру; 15) жеке тапсырма ретінде сервердің маңызды аймақтарын тексеру параметрлері; 16) міндеттердің басымдылығына қарай сервер ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу; 17) фондық режимде антивирустық сканерлеуді жалғастыру мүмкіндігі; 18) болған маңызды оқиғалар туралы әкімшілерді хабардар етудің бірнеше жолдарының болуы (пошта хабарламасы, дыбыстық хабарландыру, қалқымалы терезе, Оқиғалар журналына жазу); 19) зиянды бағдарламалар, зиянкестер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшіруді болдырмауға мүмкіндік беретін, сондай-ақ антивирусты басқаруға тыйым салатын немесе рұқсат беретін рұқсаттар тізімдері арқылы қолданба мен тауар параметрлеріне рөлдік қол жеткізу; 20) SIEM жүйелерімен интеграциялау мүмкіндігі; 21) антивирустың жұмыс процестерінің санын қолмен көрсету мүмкіндігі; 22) графикалық интерфейсті өшіру мүмкіндігі; 23) қашықтан және жергілікті басқару консолінің болуы; 24) пәрмен жолынан антивирус параметрлерін басқару; 25) бірыңғай басқару жүйесінің көмегімен жоғарыда көрсетілген барлық компоненттерді

	орталықтандырылған басқару; 26) Қағидалардың бастапқы жай-күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару. 27) кез-келген типтегі есептеу желілеріндегі қосымшалар мен порттарға арналған желілік экран ережелерін қолдана отырып, желілік шабуылдардан қорғау; 28) пошта қауіптерінен қорғау (Outlook плагині); 29) HTTP және HTTPS трафигін вирустар мен фишингтен қорғау, зиянды веб-мекенжайлар базаларына сілтемелерді тексеру және веб-серверлер сертификаттарының дұрыстығын тексеру мүмкіндігімен трафикті ұстап алу ұстап алу драйверінің көмегімен немесе оны қайта бағыттау арқылы жүзеге асырылуы тиіс; 30) сенімді құрылғылардың тізімін жасау мүмкіндігімен және Active Directory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігімен пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын бақылауды жүзеге асыру; 31) желілік карталар мен модемдердің қосылуын бақылау; 32) Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде өндіруші алдын ала құрған және динамикалық жаңартатын санаттың белгілі бір мазмұндағы ресурстарына қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу; 33) әкімшіні сыртқы құрылғылардың қосылуы туралы хабардар ету; 34) құрылғылар мен қосымшаларды бақылау үшін қағидаларды автоматты генерациялау тетіктерінің болуы; 35) бағдарлама процестерін сыртқы қауіптерден қорғауды қосу немесе өшіру (функция әдепкі бойынша қосылады). Функция қосылған кезде бағдарлама өзінің процестерін, сондай-ақ әкімшілік агенттің процестерін үшінші тарап процестерінің араласуынан қорғайды. 1.9. Windows ОЖ негізіндегі орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: 1) Microsoft Windows 11 Pro 64 биттік; 2) Microsoft Windows 11 Enterprise 64 биттік; 3) Microsoft Windows 10 Pro 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит; 4) Microsoft Windows 10 Enterprise 21H2 (қазан 2021 жаңарту) 32 бит / 64 бит; 5) Microsoft Windows 10 Pro 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит; 6) Microsoft Windows 10 Enterprise 21H1 (мамыр 2021 жаңарту) 32 бит / 64 бит; 7) Microsoft Windows 10 20h2 32 биттік / 64 биттік; 8) Microsoft Windows 10 20h1 32 биттік / 64 биттік; 9) Microsoft Windows 10 Enterprise 2019 ltsc 32 биттік / 64 биттік; 10) Microsoft Windows 10 Enterprise 2016 ltsb 32 биттік / 64 биттік; 11) Microsoft Windows 10 Enterprise 2015 ltsb 32 биттік / 64 биттік; 12) Microsoft Windows 10 Pro RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік; 13) RS5 жұмыс станцияларына арналған Microsoft Windows 10 Pro (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік; 14) Microsoft Windows 10 Enterprise RS5 (қазан 2018 жаңарту, 1809) 32 биттік / 64 биттік; 15) Microsoft Windows 10 Pro 19H1 32 биттік / 64 биттік; 16) 19h1 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32 биттік / 64 биттік; 17)

	Microsoft Windows 10 Enterprise 19H1 32 биттік / 64 биттік; 18) Microsoft Windows 10 Pro 19H2 32 биттік / 64 биттік; 19) 19h2 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32 биттік / 64 биттік; 20) Microsoft Windows 10 Enterprise 19H2 32 биттік / 64 биттік; 21) Microsoft Windows 8.1 Pro 32 биттік/64 биттік; 22) Microsoft Windows 8.1 Enterprise 32 биттік / 64 биттік; 23) Microsoft Windows 8 Pro 32 биттік/64 биттік; 24) Microsoft Windows 8 Enterprise 32 биттік / 64 биттік; 25) Microsoft Windows 7 Professional Service Pack 1 32 биттік / 64 биттік; 26) Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32 биттік / 64 иттік; 27) Windows Server 2022 standard 64 биттік; 28) Windows Server 2022 Core 64 биттік; 29) Windows Server 2022 Datacenter 64 биттік; 30) Windows Server 2019 standard 64 биттік; 31) Windows Server 2019 Core 64 биттік; 32) Windows Server 2019 Datacenter 64 биттік; 33) Windows Server 2016 Standard (LTSB) 64 биттік; 34) Windows Server 2016 (Server Core орнату опциясы) (LTSB) 64 бит; 35) Windows Server 2016 Datacenter (LTSB) 64 биттік; 36) Windows Server 2012 R2 standard 64 биттік; 37) Windows Server 2012 R2 Server Core 64 биттік; 38) Windows Server 2012 R2 foundation 64 биттік; 39) Windows Server 2012 R2 Essentials 64 биттік; 40) Windows Server 2012 R2 Datacenter 64 биттік; 41) Windows Server 2012 standard 64 биттік; 42) Windows Server 2012 Server Core 64 биттік; 43) Windows Server 2012 foundation 64 биттік; 44) Windows Server 2012 essentials 64 биттік; 45) Windows Server 2012 Datacenter 64 биттік; 46) Windows Server 2008 R2 with Standard Service Pack 1 және одан жоғары 64 биттік; 47) Windows Server 2008 R2 Service Pack 1 (барлық басылымдар) 64 бит; 48) Windows Storage Server 2016 64 бит; 49) Windows Storage Server 2012 R2 64 биттік; 50) Windows Storage Server 2012 64 биттік. Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек: 1) VMware vSphere 6.7; 2) VMware vSphere 7.0; 3) VMware Workstation 16 Pro; 4) Microsoft Hyper - V Server 2012 64 бит; 5) Microsoft Hyper - V Server 2012 R2 64 биттік; 6) Microsoft Hyper - V Server 2016 64 бит; 7) Microsoft Hyper - V Server 2019 64 бит; 8) Citrix XenServer 7.1 LTSR; 9) Citrix XenServer 8.x; 10) Parallels Desktop 17; 11) Oracle VM VirtualBox 6.x (тек Windows қонақ кірісі). Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек: 1) Microsoft SQL Server 2012 express 64 биттік; 2) Microsoft SQL Server 2014 express 64 биттік; 3) Microsoft SQL Server 2016 express 64 биттік; 4) Microsoft SQL Server 2017 express 64 биттік; 5) Microsoft SQL Server 2019 express 64 биттік; 6) Microsoft SQL Server 2014 (барлық басылымдар) 64 бит; 7) Microsoft SQL Server 2016 (Барлық басылымдар) 64 бит; 8) Microsoft SQL Server 2017 (барлық басылымдар) Windows 64 биттік; 9) Linux үшін Microsoft SQL Server 2017 (барлық басылымдар) 64 биттік; 10) Microsoft SQL Server 2019

	(барлық басылымдар) Windows 64 биттік (қосымша қадамдар қажет); 11) Microsoft SQL Server 2019 (барлық басылымдар) Linux үшін 64 биттік (қосымша қадамдар қажет); 12) MySQL 5.7 Community 32 биттік / 64 биттік; 13) MySQL Standard Edition 8.0 32 биттік / 64 биттік; 14) MySQL Enterprise Edition 8.0 32 биттік / 64 биттік; 15) Amazon RDS және Microsoft Azure бұлттық платформаларында қолдау көрсетілетін SQL серверлерінің барлық нұсқалары; 16) MariaDB Server 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік; 17) MariaDB Galera Cluster 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік. Антивирустық қорғаныс бағдарламалық құралында келесі функционалдық мүмкіндіктер іске асырылуы керек: 1) қорғалатын тораптардың санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату архитектурасын таңдау; 2) ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory-дан ақпаратты оқу мүмкіндігі; 3) анықталған компьютерлерді IP-мекен-жай, ОЖ типі, OU AD-да болу ережелерін теңшеу мүмкіндігі; 4) желіде жаңа компьютерлер пайда болған жағдайда, компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; 5) IP мекенжайы, ОЖ типі, ou AD-да болу бойынша тасымалдау ережелерін теңшеу мүмкіндігі; 6) антивирустық қорғау бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; 7) орталықтандырылған баптау, әкімшілендіру; 8) қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; 9) басқару орталығының құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты); 10) саясат пен міндеттердің өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі; 11) антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары, жергілікті орнату үшін - дербес орнату пакетін құру мүмкіндігі; 12) қауіпсіздік саясатында пайдаланушы кірген есептік жазбаға, ағымдағы IPv4-мекен-жайға, сондай-ақ компьютер қай OU-да немесе қандай қауіпсіздік тобында екеніне байланысты антивирустық шешімнің параметрлерін қайта анықтайтын арнайы триггерлерді көрсету мүмкіндігі; 13) қайта бөлу орын алатын триггерлер иерархиясының мүмкіндігі; 14) клиенттік машиналарға таратпас бұрын орталықтандырылған басқару құралдарымен жүктелген жаңартуларды тестілеу; 15) жаңартуларды пайдаланушылардың жұмыс орындарына оларды алғаннан кейін бірден жеткізу; 16) виртуалды машиналар желісінде тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын міндеттердің жүктеме балансын бөлу; 17) әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын баптау мүмкіндігімен көп деңгейлі басқару жүйесін құру; 18) еркін деңгейдегі әкімшілік серверлер иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі; 19) әкімшілік серверлер иерархиясында шифрлауды басқару мүмкіндігі; 20) басқару серверлері үшін көп жалға алуды

	қолдау (multi-tenancy) ; 21) оқшауланған виртуалды инфрақұрылымдарды қорғау үшін провайдер сервисі инфрақұрылымында multitenancy режимін қолдау; 22) байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту; 23) басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу; 24) клиенттік компьютерлерге лицензияны автоматты түрде тарату; 25) пайдаланушылардың компьютерлерінде орнатылған БҚ мен жабдықты түгендеу; 26) орнатылған антивирустық қорғау Қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау; 27) Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару функциясы; 28) iOS MDM сервері арқылы мобильді құрылғыларды басқару мүмкіндігі; 29) берілген оқиғалар туралы SMS-хабарламалар жіберу мүмкіндігі; 30) басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; 31) басқару жүйесіне желілік жүктемені азайту үшін ұйымның кез келген компьютерін жаңартуларды қайта тарату орталығымен көрсету мүмкіндігі; 32) басқару жүйесіне желілік жүктемені азайту үшін орталықтандырылған басқару серверіне антивирустық агенттер оқиғаларын, клиенттік компьютерлердің таңдалған тобын жіберу орталығымен кез келген компьютерді көрсету мүмкіндігі; 33) виртуалды машиналарда орнатылған қосымшаларда және операциялық жүйеде осалдықтарды іздеу жөніндегі міндеттің болуы. 1.10. Linux ОЖ негізіндегі орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар. Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: 1) Ubuntu 18.04 LTS; 2) Ubuntu 20.04 LTS; 3) Debian GNU / Linux 10.5; 4) Astra Linux Common Edition, 2.12 нұсқасы; 5) Astra Linux арнайы шығарылымы, 1.6 нұсқасы; 6) CentOS 7.9.2009; 7) CentOS 8.3.2011; 8) Red Hat Enterprise Linux 7.9; 9) Red Hat Enterprise Linux 8.3; 10) ALT 8.3; 11) ALT 9.1. Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек: 1) VMware cSphere 6.7/7.0; 2) VMware Workstation 16 Pro; 3) Microsoft Hyper-V Server 2012 (64-биттік); 4) Microsoft Hyper-V Server 2016 (64- биттік); 5) Microsoft Hyper-V Server 2019 (64- биттік); 6) Microsoft Hyper-V Server 2022 (64-биттік); 7) Citrix XenServer 7.1/8.x Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек: 1) MSQL 5.7/8.0 32/64-биттік; 2) MariaDB Server 10.3 және жоғары InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік, 3) PostrfeSQL 13.x/14.x 32/64өбиттік. Орталықтандырылған басқару консолі Linux таза Linux ® ортасының талаптарына сәйкес Linux негізіндегі әкімшілік сервері арқылы Linux операциялық жүйесі бар құрылғыларды қорғауды орналастыруға және басқаруға арналған. Антивирустық қорғаныс бағдарламалық

	құралында келесі функционалдық мүмкіндіктер іске асырылуы керек: 1) антивирустық қорғау бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою; 2) Орталықтандырылған конфигурация, әкімшілік; 3) қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; 4) саясат пен міндеттердің өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі; 5) қайта бөлу орын алатын триггерлердің иерархиялары; 6) жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу; 7) виртуалды машиналар желісінде тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; 8) әкімшілер мен операторлардың құқықтарын, сондай-ақ әрбір деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру; 9) еркін деңгейдегі әкімшілік серверлер иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі; 10) басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy); 11) байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту; 12) басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу; 13) клиенттік компьютерлерге лицензияны автоматты түрде тарату; 14) орнатылған антивирустық қорғау Қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау; 15) белгіленген бағдарламаларды лицензиялау деректері бойынша вирусқа қарсы қорғау оқиғалары бойынша графикалық есептер құру; 16) жүйенің жұмысы туралы алдын ала бапталған стандартты есептердің болуы; 17) есептерді PDF және XML форматындағы файлдарға экспорттау; 18) антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару; 19) басқару серверінде аутентификация үшін ішкі есептік жазбаларды құру; 20) басқару жүйесінің кіріктірілген құралдарын басқару жүйесінің резервтік көшірмесін жасау; 21) вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы; 22) Web консолін пайдалана отырып, антивирустық қорғауды басқару. 1.11. Антивирустық базаны жаңартуға қойылатын талаптар. Жаңартылатын антивирустық мәліметтер базасы келесі функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс: 1) күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту қағидаларын құру; 2) жаңарту жолдарының көптігі, оның ішінде – байланыс арналары бойынша және ақпараттың иеліктен шығарылатын электрондық жеткізгіштерінде; 3) электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру. 1.12. Пайдалану құжаттамасына қойылатын талаптар. Басқару құралдарын қоса алғанда, вирусқа қарсы қорғаудың барлық бағдарламалық өнімдері үшін пайдалану құжаттамасында Мемлекеттік стандарттардың талаптарына сәйкес орыс тілінде дайындалған құжаттар қамтылуға тиіс,

	оның ішінде: 1) пайдаланушы (әкімші) нұсқаулығы. Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, конфигурациялау және пайдалану процесін егжей-тегжейлі сипаттауы керек. 2. Әлеуетті жеткізушіге қойылатын талаптар. 2.1. Әлеуетті өнім беруші конкурстық өтінім құрамында Тапсырыс берушінің атына жіберілген, өндіруші компаниямен немесе оның Қазақстан Республикасының аумағындағы өкілетті өкілімен ресми әріптестік қатынастарды растайтын, жеткізілетін лицензиялық бағдарламалық қамтамасыз етуді өндірушіден авторизациялық хат түпнұсқасының электрондық көшірмесін ұсынуға тиіс; 2.2. Әлеуетті өнім беруші сатылатын лицензияны тапсырыс беруші ұсынған жабдыққа орталықтандырылған әкімшілендіру консолінде орнатуы, тапсырыс берушінің серверлік жабдығына автоматты түрде тарату жөніндегі міндеттерді реттеуі, бағдарламаларды, құрылғыларды және веб-ресурстарды пайдалану қағидаларын баптауы, зиянды бағдарламаны іздеу және талдау, консоль арқылы ақпараттық қауіпсіздік міндеттері мен қағидаларын құру бойынша тапсырыс берушінің 2 (екі) маманын орталықтандырылған әкімшілендіруді оқытуы тиіс. 2.3. Жеткізуші Тапсырысшының кемінде 2 (екі) маманын үшін жеткізілетін антивирустық бағдарламалық қамтамасыз ету бойынша кейіннен курстан өткені туралы сертификат бере отырып, күндізгі уәкілетті оқу курсын өткізуі тиіс. 3. Техникалық қолдауға қойылатын талаптар. Әлеуетті өнім беруші Тапсырыс берушіге антивирустық бағдарламалық қамтамасыз етуді баптау және пайдалану мәселелері бойынша консультациялық-техникалық қызмет көрсетуі және мынадай мүмкіндіктермен қамтамасыз етуі тиіс: 1) техникалық қолдауды вирусқа қарсы БҚ өндірушінің және оның серіктестерінің мамандары Қазақстан Республикасының бүкіл аумағында мереке және демалыс күндері телефон, электрондық пошта және Интернет арқылы шарт заңды күшіне енген күннен бастап 1 жыл ішінде тәулік бойы орыс тілінде ұсынуға тиіс; 2) Әлеуетті өнім беруші электрондық пошта жүйесі арқылы нақты проблемалар бойынша сұрау салуларды жіберуді қамтитын бағдарламалық қамтамасыз ету өндірушісінің техникалық қолдауының электрондық ақпараттық жүйесіне қол жеткізуді қамтамасыз етуге тиіс; 3) жоғарыда сипатталған қызметтерге қол жеткізу қолдау көрсетудің барлық уақыты ішінде тәулік бойы ашық болуға тиіс; 4) Әлеуетті өнім беруші тапсырыс берушіге техникалық ақпаратты және/немесе қосымша бағдарламалық компоненттерді алуды, сондай-ақ антивирустық бағдарламада табылған мәселелер мен қателерді еңсеру және шешу үшін техникалық мамандарды жіберуді қамтамасыз етуі тиіс; 5) Бағдарламалық қамтамасыз етуге кепілдік беру және техникалық қолдау Тапсырыс беруші тарапынан қосымша шығыстарсыз қамтамасыз етілуі тиіс. Кепілдік қызмет көрсету және техникалық қолдау бағдарламалық қамтамасыз етудің орналасқан жері бойынша жүзеге асырылуы тиіс. Әлеуетті жеткізуші виртуалды серверлерге арналған жаңа антивирустық БЖ лицензиясын Тапсырыс берушінің орталықтандырылған әкімшілендіру консоліне жүктеуі, антивирустық базаларды жаңарту,

	вирустар мен осалдықтарды іздеу саясаттары мен міндеттерін реттеуі, орталықтандырылған әкімшілендіру консолі арқылы ақпараттық қауіпсіздік міндеттері мен ережелерін жасау бойынша Тапсырыс берушінің 2 (екі) маманын оқыту 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)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Министерство юстиции Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство юстиции Республики Казахстан"
№ конкурса:	№ 17985052-1
Наименование конкурса:	Услуги по продлению лицензии и технической поддержки антивирусного программного обеспечения
Номер лота:	№ 87894721-ОКЗ
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:	1276775.87
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	1276775.87
Срок оказания услуги:	согласно технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	В настоящей технической спецификации на услугу продление лицензии и технической поддержки антивирусного программного обеспечения для виртуальных серверов (далее - Услуга), соответствующий следующим требованиям: в результате проведения закупок требуется продлить действующую лицензию с 7 декабря 2026 года на антивирусное ПО KHCS для виртуальных сред в количестве 70 единиц и техническую поддержку на срок не менее 12 месяцев. Срок оказания услуги исчисляется с момента подписания договора и вступления в законную силу. Потенциальный Поставщик услуг обязан предоставить авторизационное письмо на право участия в настоящем конкурсе от компании производителя антивирусного ПО, подтверждающее право на вышеуказанное антивирусное ПО в качестве авторизованного партнера компании производителя на территории Республики Казахстан (электронная копия письма должна быть в конкурсной заявке). Заказчику предоставляется право принять услугу и проводить все операции, связанные с приемкой и оформлением услуги, обращаться за помощью в техническую поддержку и привлекать технических специалистов Поставщика услуг. Лицензия антивирусного ПО должна представлять собой корпоративное решение, обеспечивающее устойчивое функционирование в физических и виртуальных серверов, централизованное управление. 1. Технические требования к программному обеспечению по антивирусной защите. 1.1. Общие требования. Антивирусные средства защиты для виртуальных сред должны защищать виртуальные машины, публичные облака и серверы Windows и Linux. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке. Решение должно включать: 1) безагентные программные средства антивирусной защиты для виртуальных сред; 2) программные средства антивирусной защиты для виртуальных сред с использованием агентов; 3) программные средства защиты для облачной инфраструктуры; 4) программные средства централизованного управления, мониторинга и обновления; 5) обновляемые базы данных сигнатур вредоносных программ и атак; 6) эксплуатационную документацию на русском языке. 1.2. Требования к безагентным программным средствам антивирусной защиты виртуальных сред. Виртуальная инфраструктура VMware: 1) ESXi 6.5 Update 3a; 2) ESXi 6.7 Update 3; 3) ESXi 7.0 Update 1c; 4) vCenter 6.0 Update 3j; 5) vCenter 6.5 Update 3; 6) vCenter 6.7 Update 3; 7) vCenter 7.0 Update 1d; 8) VMware NSX-V Manager из пакета VMware NSX Data Center for vSphere 6.4.10; 9) VMware NSX-T Manager из пакета VMware NSX-T Data Center 3.1.3; VMware NSX-T Data Center 3.1.1 или VMware NSX-T Data Center 3.0.3; 10) VMware NSX-T Manager из пакета VMware NSX-T Data Center 3.0.3; 11) vCloud Director 10.1.2 или vCloud Director 10.3.0 for Service Providers. Операционные системы Windows для рабочих станций: 1) Windows 10; 2) Windows 8.1; 3) Windows 8; 4) Windows 7 Service Pack 1.

	Операционные системы Windows для серверов: 1) Windows Server 2019; 2) Windows Server 2016; 3) Windows Server 2012 R2 без поддержки ReFS (Resilient File System); 4) Windows Server 2012 без поддержки ReFS (Resilient File System); 5) Windows Server 2008 R2 Service Pack 1. Операционные системы Linux для серверов: 1) Ubuntu Server 18.04 GA (64-разрядная). 2) Ubuntu Server 16.04 GA (64-разрядная). 3) Ubuntu Server 14.04 GA (64-разрядная). 4) Red Hat Enterprise Linux Server 7.7 GA (64-разрядная). 5) Red Hat Enterprise Linux Server 7.4 GA (64-разрядная). 6) Red Hat Enterprise Linux Server 7.0 GA (64-разрядная). 7) SUSE Linux Enterprise Server 12 GA (64-разрядная). 8) CentOS 7.7 GA (64-разрядная). 9) CentOS 7.4 GA (64-разрядная). 10) CentOS 7.0 GA (64-разрядная). Программные средства антивирусной защиты виртуальных сред должны обеспечивать реализацию следующих функциональных возможностей: 1) защита от вредоносного ПО в режиме реального времени и в режиме запланированной проверки без установки антивирусного агента на гостевые машины; 2) сканирование выключенных гостевых машин, на наличие вредоносного ПО, без необходимости включать их на время проверки, в том числе и гостевые машины с ОС Linux и файловыми системами EXT2, EXT3, EXT4, XFS, BTRFS, VFAT, ISO9660; 3) проверка шаблонов виртуальных машин; 4) интеграция с технологией VMware NSX Manager для обеспечения защиты файловой системы гостевых машин; 5) облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу; 6) поддержка режима multitenancy в инфраструктуре сервис провайдера под управлением сервера VMware vCloud Director для защиты изолированных виртуальных инфраструктур; 7) централизованные обновления баз без необходимости распространения обновлений на гостевые машины; 8) сканирование выбранных файлов, папок и всей системы; 9) оптимизация режима сканирования, которая позволяет избегать повторного сканирования уже проверенных файлов; 10) предотвращение повторного сканирования одинаковых объектов на разных гостевых машинах рамках одного гипервизора; 11) блокирование, обезвреживание и удаление вредоносного ПО с уведомлением администраторов; 12) единая консоль управления для всех компонентов защиты; 13) централизованное управление для виртуальных сред и физических рабочих станций; 14) отображение как физической, так и логической структуры администрирования в том виде, в котором она представлена в VMware vCenter; 15) отображение подробной информации о событиях на виртуальных машинах и о выполнении задач; 16) применение различных параметров безопасности для отдельных групп виртуальных машин; 17) непрерывность защиты виртуальных машин, при миграции с одного ESXi-хоста на другой; 18) хранение резервных копий удаленных файлов; 19) поддержка схемы лицензирования по числу защищаемых виртуальных машин и по количеству физических CPU; 20) разграничение доступа к

	параметрам политик и задач в зависимости от роли учетной записи пользователя; 21) отображение статистики о наиболее часто проверяемых файлах; 22) возможность установки и работы программы в инфраструктуре под управлением VMware NSX-T Manager. 1.3. Требования к программным средствам антивирусной защиты виртуальных сред с использованием агентов. Виртуальная инфраструктура: 1) VMware ESXi 6.5, 6.7, 7.0; 2) Windows Server 2012 R2 Hyper-V; 3) Windows Server 2016 Hyper-V; 4) Windows Server 2019 Hyper-V; 5) Citrix Hypervisor 8.2 LTSR. 6) Платформа Proxmox VE: гипервизор Proxmox VE 6.4; 7) Huawei FusionSphere – FusionCompute CNA 8.0; 8) Nutanix Acropolis: гипервизор Nutanix AHV 5.19.1; 9) Enterprise Cloud Platform VeiL: гипервизор VeiL Node 4.5. 10) SharxBase: гипервизор SharxBase 5.10.x. 11) Платформа KVM: гипервизор KVM на базе одной из следующих операционных систем: 11.1) Ubuntu Server 18.04, 20.04 LTS; 11.2) Red Hat Enterprise Linux Server 7.9; 11.3) CentOS 7.9. 12) Облачная платформа ТИОНИКС: гипервизор KVM на базе одной из следующих операционных систем: 12.1) Ubuntu Server 18.04, 20.04 LTS; 12.2) Red Hat Enterprise Linux Server 7.9; 12.3) CentOS 7.9. 13) Платформа OpenStack: гипервизор KVM на базе одной из следующих операционных систем: 13.1) Ubuntu Server 18.04, 20.04 LTS; 13.2) Red Hat Enterprise Linux Server 7,9; 13.3) CentOS 7.9. Гостевые операционные системы: 1) Windows 11 Pro / Enterprise 21H2 / 22H2 / 23H2 (32 / 64-разрядная). 2) Windows 10 Desktop Pro 19H1 / 19H2 / 20H1 / 20H2 / 21H1 / 22H2 (32 / 64-разрядная). 3) Windows 10 Enterprise 2016 LTSC / 2019 LTSC / 19H1 / 19H2 / 20H1 / 20H2 / 21H1 (32 / 64-разрядная). 4) Windows 8.1 Update 1 Professional / Enterprise (32 / 64-разрядная). 5) Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-разрядная). 6) Windows Server 2022 Standard / Datacenter / Essentials (Desktop experience / Core). 7) Windows Server 2019 Standard / Datacenter (Desktop experience / Core). 8) Windows Server 2016 Standard / Datacenter (Desktop experience / Core). 9) Windows Server 2012 R2 Standard / Datacenter / Essentials (Desktop experience / Core). 10) Windows Server 2012 Standard /Datacenter / Essentials (Desktop experience / Core). 11) Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core). 12) Debian GNU / Linux 10.1 и выше (32 / 64-разрядная). 13) Debian GNU / Linux 9.4 и выше (32 / 64-разрядная). 14) Ubuntu Server 20.04 LTS (64-разрядная). 15) Ubuntu Server 18.04 LTS (64-разрядная). 16) CentOS 8.0 и выше (64-разрядная). 17) CentOS 7.3 и выше (64-разрядная). 18) Red Hat Enterprise Linux Server 8.0 и выше (64-разрядная). 19) Red Hat Enterprise Linux Server 7.3 и выше (64-разрядная) 20) SUSE Linux Enterprise Server 15 SP2 (64-разрядная). 21) ALT Linux 8 SP (64-разрядная). 22) Oracle Linux 8.0 и выше (64-разрядная). 23) Oracle Linux 7.3 и выше (64-разрядная). 24) Astra Linux SE 1.6 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды).

	25) Astra Linux SE 1.5 (без поддержки режимов Мандатного разграничения доступа и Замкнутой программной среды). 1.4. На настольных операционных системах Windows и Linux: 1) резидентный антивирусный мониторинг; 2) эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; 3) выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты; 4) автоматическое обнаружение и подключение агентов на ВМ к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты; 5) обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа. 6) облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу. 7) защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента. 8) почтовый плагин для клиента Outlook с возможностью включения/отключения проверки вложений, а также возможностью удаления вложения или изменения формата вложенного файла. 9) защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов. 10) блокировка баннеров и всплывающих окон, загружаемых с Web-страниц. 11) распознавание и блокировка фишинг-сайтов. 12) защита от еще не известных вредоносных программ на основе анализа их поведения. 13) возможность определения аномального поведения приложения с помощью анализа действий этого приложения. 14) возможность совершить откат действий вредоносного программного обеспечения при лечении. 15) защита от внешнего шифрования общих файлов и папок. 16) возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы. 17) наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп); 18) компонент создания специальных правил должен контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256; 19) компонент создания специальных правил должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должен иметь возможность создания списка доверенных пакетов обновлений, которые могут

	изменять и запускать вложенные в них файлы; 20) наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов, а также создание сетевых правил для конкретных программ 21) защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные. 22) осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из AD. 23) осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD. 24) возможность проверки всех виртуальных машин по заранее заданному расписанию. 25) предотвращение повторного сканирования уже проверенных файлов. 26) наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах. 27) блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов. 28) единая консоль управления для всех компонентов защиты 29) возможность применять различные параметры безопасности для отдельных групп виртуальных машин. 30) хранение резервных копий удаленных файлов. 31) поддержка отката антивирусных баз. 32) поддержка схемы лицензирования по числу защищаемых виртуальных машин (рабочие станции) и по количеству процессоров. 33) механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения. 1.5. На серверных операционных системах Windows: 1) резидентный антивирусный мониторинг; 2) защита от программ-маскировщиков, программ автодозвона на платные сайты; 3) эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; 4) выполнение антивирусного сканирования и других ресурсоемких задач не на гостевых машинах, а на отдельной машине защиты; 5) защита электронной корреспонденции от вредоносных программ с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента. 6) автоматическое обнаружение и подключение к функционирующей машине защиты, в том числе находящейся на другом хосте, в случае недоступности основной машины защиты; 7) обеспечение непрерывности файловой защиты в период кратковременной недоступности машины защиты посредством журналирования всех файловых операций на защищаемой гостевой машине в период недоступности

	машины защиты, и выполнение автоматического сканирования всех изменений после восстановления доступа; 8) облачная защита от новых угроз, позволяющая приложению при сканировании в режиме реального времени и в режиме запланированной проверки обращаться к специальным ресурсам производителя, для получения вердикта по файлу; 9) защита от еще не известных вредоносных программ на основе анализа их поведения; 10) защита от внешнего шифрования общих файлов и папок; 11) наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов; 12) создание сетевых правил для конкретных программ; 13) защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; 14) централизованные обновления с возможностью хранения части антивирусных баз на машине защиты; 15) возможность проверки всех виртуальных машин по заранее заданному расписанию; 16) предотвращение повторного сканирования уже проверенных файлов; 17) наличие информации о проверенных файлах на машине защиты, позволяющей исключить повторную проверку одних и тех же файлов, находящихся на разных виртуальных машинах; 18) блокирование, обезвреживание и удаление вредоносного ПО, уведомление администраторов; 19) единая консоль управления для всех компонентов защиты; 20) консоль централизованного управления, единая для виртуальных сред и физических рабочих станций; 21) предоставление подробной информации о событиях на виртуальных машинах и о выполнении задач; 22) возможность применять различные параметры безопасности для отдельных групп виртуальных машин; 23) хранение резервных копий удаленных файлов; 24) поддержка отката антивирусных баз; 25) поддержка схемы лицензирования по числу защищаемых виртуальных машин (серверов) и по процессорам; 26) механизм профилирования настроек антивируса, позволяющий дополнительно ограничить область ее применения. 1.6. На серверных операционных системах Linux: 1) резидентный антивирусный мониторинг; 2) эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; 3) антивирусное сканирование по команде пользователя или администратора и по расписанию; 4) антивирусная проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz; .tbz2; .gz;.tgz; .arj.; 5) проверка сообщений электронной почты в текстовом формате (Plain text); 6) наличие механизмов оптимизации проверки файлов (глобальные исключения из мониторинга, по маске, памяти и процессов, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); 7) помещение подозрительных и поврежденных объектов на карантин; 8) запуск задач по расписанию и/или сразу после загрузки операционной системы; 9) возможность экспортировать

	и сохранять отчеты в форматах HTML и CSV; 10) сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; 11) централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; 12) поддержка файловой системы GlusterFS на виртуальных машинах с установленным Легким агентом для Linux; 13) возможность проверки загрузочных секторов, системной памяти и объектов автозапуска. 1.7. Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий: 1) CentOS 6.7 и выше. 2) Debian GNU/Linux 9.4 и выше; 3) Debian GNU/Linux 10.1 и выше; 4) Debian GNU/Linux 11.1 и выше; 5) Linux Mint 19 и выше; 6) Mageia 4; 7) Red Hat Enterprise Linux 6.7 и выше; 8) Альт Образование 9; 9) Альт Рабочая Станция 9; 10) Альт Сервер 9. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий: 1) AlterOS 7.5 и выше; 2) Amazon Linux 2; 3) Astra Linux Common Edition (очередное обновление 2.12); 4) Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5); 5) Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6); 6) Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6); 7) CentOS 6.7 и выше; 8) CentOS 7.2 и выше; 9) CentOS 8.0 и выше; 10) Debian GNU / Linux 9.4 и выше; 11) Debian GNU / Linux 10.1 и выше; 12) Debian GNU / Linux 11.1 и выше; 13) EulerOS V2.0SP2 2.2.17; 14) EulerOS V2.0SP5 2.5.6; 15) Linux Mint 19 и выше; 16) Linux Mint 20.1 и выше; 17) openSUSE Leap 15.0 и выше; 18) Oracle Linux 7.3 и выше; 19) Oracle Linux 8.0 и выше; 20) Pardus OS 19.1; 21) Red Hat Enterprise Linux 6.7 и выше; 22) Red Hat Enterprise Linux 7.2 и выше; 23) Red Hat Enterprise Linux 8.0 и выше; 24) SUSE Linux Enterprise Server 12 SP5 и выше; 25) SUSE Linux Enterprise Server 15 и выше; 26) Ubuntu 18.04 LTS и выше; 27) Ubuntu 20.04 LTS; 28) Альт Образование 9; 29) Альт Рабочая Станция 9; 30) Альт Сервер 9; 31) Гослинукс 7.2; 32) РЕД ОС 7.3; В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: 1) резидентного антивирусного мониторинга; 2) облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; 3) проверку ресурсов доступных по SMB / NFS; 4) возможность проверки памяти ядра; 5) эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; 6) защита от еще не известных вредоносных программ на основе анализа их поведения; 7)

	антивирусное сканирование по команде пользователя или администратора и по расписанию; 8) антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; 9) проверку сообщений электронной почты в текстовом формате (Plain text); 10) наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); 11) защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; 12) возможность включения опции блокирования файлов во время проверки; 13) помещение подозрительных и поврежденных объектов на карантин; 14) возможность перехвата и проверки файловых операций на уровне SAMBA; 15) управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; 16) запуск задач по расписанию и/или сразу после загрузки операционной системы; 17) возможность экспортировать и сохранять отчеты в форматах HTML и CSV; 18) гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; 19) сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; 20) возможность управления через пользовательский графический интерфейс без root прав; 21) централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли; 22) возможность управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения; 23) возможность проверки съемных дисков; 24) возможность отслеживания во входящем сетевом трафике активности, характерные для сетевых атак; 25) возможность проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым; 26) получения данных о действиях программ на компьютере пользователя; 27) управления запуском программ на компьютерах пользователей (задача Контроль программ); 28) получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах пользователей (задача Инвентаризация); 29) создание файлов трассировки при запуске программы. 1.8. Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows. Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 1) 32-разрядных операционных систем Microsoft Windows; 2) Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 3) Windows Server 2003 R2 Foundation / Standard /

	Enterprise / Datacenter с пакетом обновлений SP2 или выше; 4) Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 5) Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше. 64-разрядных операционных систем Microsoft Windows 1) Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 2) Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 3) Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 4) Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; 5) Microsoft Small Business Server 2008 Standard / Premium SP2 или выше; 6) Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; 7) Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; 8) Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; 9) Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше; 10) Microsoft Windows MultiPoint Server 2011 Standard / Premium; 11) Windows Server 2012 Foundation / Essentials / Standard / Datacenter; 12) Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter; 13) Microsoft MultiPoint Server 2012 Standard / Premium; 14) Windows Storage Server 2012; 15) Windows Hyper-V Server 2012; 16) Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; 17) Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; 18) Windows Storage Server 2012 R2; 19) Windows Hyper-V Server 2012 R2; 20) Windows Server 2016 Essentials / Standard / Datacenter; 21) Windows Server 2016 MultiPoint; 22) Windows Server 2016 Core Standard / Datacenter; 23) Microsoft Windows MultiPoint Server 2016; 24) Windows Storage Server 2016; 25) Windows Hyper-V Server 2016; 26) Windows Server 2019 Essentials / Standard / Datacenter; 27) Windows Server 2019 Core; 28) Windows Storage Server 2019; 29) Windows Hyper-V Server 2019; 30) Windows Server 2022; 31) Windows 10 Enterprise multi-session. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: 1) антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов; 2) антивирусное сканирование по команде пользователя или администратора и по расписанию; 3) запуск задач по расписанию и/или сразу после загрузки операционной системы; 4) облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу; 5) антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; 6) защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной

	записи, загрузочных секторов локальных и съемных дисков; 7) непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными; 8) анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; 9) возможность проверки контейнеров Microsoft Windows; 10) защита от эксплуатирования уязвимостей в памяти процессов; 11) возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться; 12) возможность добавлять процессы в список защищаемых; 13) ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; 14) проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; 15) настройки проверки критических областей сервера в качестве отдельной задачи; 16) регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач; 17) возможность продолжать антивирусное сканирование в фоновом режиме; 18) наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); 19) ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом; 20) возможность интеграции с SIEM системами; 21) возможность указания количества рабочих процессов антивируса вручную; 22) возможность отключить графический интерфейс; 23) наличие удаленной и локальной консоли управления; 24) управления параметрами антивируса из командной строки; 25) централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; 26) управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил. 27) защита от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; 28) защита от почтовых угроз (плагин для Outlook); 29) защита HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов вебсерверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления; 30) осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory; 31) контроль подключения сетевых карт и модемов; 32) осуществление

	контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания категории, заранее созданной и динамически обновляемой производителем; 33) информирование администратора о подключении внешних устройств; 34) наличие механизмов автоматической генерации правил для контроля устройств и приложений; 35) включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов. 1.9. Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Windows Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 1) Microsoft Windows 11 Pro 64-разрядная; 2) Microsoft Windows 11 Enterprise 64-разрядная; 3) Microsoft indows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная; 4) Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная; 5) Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная; 6) Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная; 7) Microsoft Windows 10 20H2 32-разрядная/64-разрядная; 8) Microsoft Windows 10 20H1 32-разрядная/64-разрядная; 9) Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная; 10) Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная; 11) Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная; 12) Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; 13) Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; 14) Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; 15) Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная; 16) Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная; 17) Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная; 18) Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная; 19) Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная; 20) Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная; 21) Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная; 22) Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная; 23) Microsoft Windows 8 Pro 32-разрядная/64-разрядная; 24) Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная; 25) Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная; 26) Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная/64-разрядная; 27) Windows Server 2022 Standard 64-разрядная; 28) Windows Server 2022 Core 64-разрядная; 29) Windows Server 2022 Datacenter 64-разрядная; 30) Windows Server 2019 Standard 64-разрядная; 31) Windows Server 2019 Core

	64-разрядная; 32) Windows Server 2019 Datacenter 64-разрядная; 33) Windows Server 2016 Standard (LTSB) 64-разрядная; 34) Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная; 35) Windows Server 2016 Datacenter (LTSB) 64-разрядная; 36) Windows Server 2012 R2 Standard 64-разрядная; 37) Windows Server 2012 R2 Server Core 64-разрядная; 38) Windows Server 2012 R2 Foundation 64-разрядная; 39) Windows Server 2012 R2 Essentials 64-разрядная; 40) Windows Server 2012 R2 Datacenter 64-разрядная; 41) Windows Server 2012 Standard 64-разрядная; 42) Windows Server 2012 Server Core 64-разрядная; 43) Windows Server 2012 Foundation 64-разрядная; 44) Windows Server 2012 Essentials 64-разрядная; 45) Windows Server 2012 Datacenter 64-разрядная; 46) Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная; 47) Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная; 48) Windows Storage Server 2016 64-разрядная; 49) Windows Storage Server 2012 R2 64-разрядная; 50) Windows Storage Server 2012 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: 1) VMware vSphere 6.7; 2) VMware vSphere 7.0; 3) VMware Workstation 16 Pro; 4) Microsoft Hyper-V Server 2012 64-разрядная; 5) Microsoft Hyper-V Server 2012 R2 64-разрядная; 6) Microsoft Hyper-V Server 2016 64-разрядная; 7) Microsoft Hyper-V Server 2019 64-разрядная; 8) Citrix XenServer 7.1 LTSR; 9) Citrix XenServer 8.x; 10) Parallels Desktop 17; 11) Oracle VM VirtualBox 6.x (только гостевой вход Windows). Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: 1) Microsoft SQL Server 2012 Express 64-разрядная; 2) Microsoft SQL Server 2014 Express 64-разрядная; 3) Microsoft SQL Server 2016 Express 64-разрядная; 4) Microsoft SQL Server 2017 Express 64-разрядная; 5) Microsoft SQL Server 2019 Express 64-разрядная; 6) Microsoft SQL Server 2014 (все редакции) 64-разрядная; 7) Microsoft SQL Server 2016 (все редакции) 64-разрядная; 8) Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная; 9) Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная; 10) Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия); 11) Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия); 12) MySQL 5.7 Community 32-разрядная / 64-разрядная; 13) MySQL Standard Edition 8.0 32-разрядная / 64-разрядная; 14) MySQL Enterprise Edition 8.0 32-разрядная / 64-разрядная; 15) Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure; 16) MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB; 17) MariaDB Galera Cluster 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: 1) выбор

	архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; 2) возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; 3) возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD; 4) автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; 5) возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD; 6) централизованные установка, обновление и удаление программных средств антивирусной защиты; 7) централизованная настройка, администрирование; 8) просмотр отчетов и статистической информации по работе средств защиты; 9) централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; 10) сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; 11) наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки; 12) возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; 13) возможность иерархии триггеров, по которым происходит перераспределение; 14) тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; 15) доставка обновлений на рабочие места пользователей сразу после их получения; 16) распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; 17) построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; 18) создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; 19) возможность управления шифрованием в иерархии серверов администрирования; 20) поддержка мультиарендности (multi-tenancy) для серверов управления; 21) поддержка режима multitenancy в инфраструктуре сервис провайдера для защиты изолированных виртуальных инфраструктур; 22) обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; 23) доступ к облачным серверам производителя антивирусного ПО через сервер управления; 24) автоматическое распространение лицензии на клиентские компьютеры; 25) инвентаризация установленного ПО и оборудования на компьютерах пользователей; 26) наличие механизма оповещения о событиях в

	работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; 27) функция управления мобильными устройствами через сервер Exchange ActiveSync; 28) функция управления мобильными устройствами через сервер iOS MDM; 29) возможность отправки SMS-оповещений о заданных событиях; 30) централизованная установка сертификатов на управляемые мобильные устройства; 31) возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; 32) возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления; 33) наличие задачи по поиску уязвимостей в установленных приложениях и операционной системе на виртуальных машинах; 34) построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ; 35) наличие преднастроенных стандартных отчетов о работе системы; 36) экспорт отчетов в файлы форматов PDF и XML; 37) экспорт событий во внешние системы по протоколу Syslog; 38) централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; 39) создание внутренних учетных записей для аутентификации на сервере управления; 40) создание резервной копии системы управления встроенными средствами системы управления; 41) поддержка Windows Failover Clustering; 42) поддержка интеграции с Windows сервисом Certificate Authority; 43) наличие портала самообслуживания пользователей; 44) наличие системы контроля возникновения вирусных эпидемий; 45) возможность установки в облачной инфраструктуре Microsoft Azure и Google Cloud; 46) возможность интеграции по OpenAPI; 47) возможность управления антивирусной защитой с использованием WEB консоли; 48) консоль централизованного управления, единая для виртуальных сред и физических рабочих станций; 49) двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования; 50) использования дополнительной аутентификация после изменения параметров учетной записи пользователя; 51) возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; 52) возможность развернуть сервер администрирования как систему высокой доступности. 1.10. Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux. Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: 1) Ubuntu 18.04 LTS; 2) Ubuntu 20.04 LTS; 3) Debian GNU / Linux 10.5; 4) Astra Linux Common Edition, версия 2.12; 5) Astra Linux Special Edition, версия 1.6; 6) CentOS 7.9.2009; 7) CentOS 8.3.2011; 8) Red Hat Enterprise Linux 7.9; 9) Red Hat Enterprise

	Linux 8.3; 10) ALT 8.3; 11) ALT 9.1. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: 1) VMware cSphere 6.7/7.0; 2) VMware Workstation 16 Pro; 3) Microsoft Hyper-V Server 2012 (64-разрядная); 4) Microsoft Hyper-V Server 2016 (64-разрядная); 5) Microsoft Hyper-V Server 2019 (64-разрядная); 6) Microsoft Hyper-V Server 2022 (64-разрядная); 7) Citrix XenServer 7.1/8.x.13. Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: 1) MSQL 5.7/8.0 32-разрядная/64-разрядная; 2) MariaDB Server 10.3 и выше 32-разрядная/64-разрядная с подсистемой хранилища InnoDB, 3) PostrfeSQL 13.x/14.x 32-разрядная/64-разрядная. Централизованная консоль администрирования предназначенная для развертывания и управления защитой устройств с операционной системой Linux с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux®. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: 1) централизованные установка, обновление и удаление программных средств антивирусной защиты; 2) централизованная настройка, администрирование; 3) просмотр отчетов и статистической информации по работе средств защиты; 4) сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; 5) иерархии триггеров, по которым происходит перераспределение; 6) доставка обновлений на рабочие места пользователей сразу после их получения; 7) распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; 8) построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; 9) создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; 10) поддержка мультиарендности (multitenancy) для серверов управления; 11) обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; 12) доступ к облачным серверам производителя антивирусного ПО через сервер управления; 13) автоматическое распространение лицензии на клиентские компьютеры; 14) наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; 15) построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ; 16) наличие преднастроенных стандартных отчетов о работе системы; 17) экспорт отчетов в файлы форматов PDF и XML; 18) централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; 19) создание внутренних учетных записей для

	аутентификации на сервере управления; 20) создание резервной копии системы управления встроенными средствами системы управления; 21) наличие системы контроля возникновения вирусных эпидемий; 22) управления антивирусной защитой с использованием WEB консоли. 1.11. Требования к обновлению антивирусных баз. Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: 1) создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток; 2) множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; 3) проверку целостности и подлинности обновлений средствами электронной цифровой подписи. 1.12. Требования к эксплуатационной документации. Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе: 1) руководство пользователя (администратора). Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты. 2. Требования к потенциальному поставщику. 2.1. Потенциальный Поставщик в составе конкурсной заявки должен предоставить электронную копию оригинала авторизационного письма от производителя лицензионного антиврусного программного обеспечения, подтверждающее официальные партнерские отношения с компанией-производителем или его полномочного представителя на территории Республики Казахстан, направленное в адрес Заказчика. 2.2. Потенциальный поставщик должен произвести инсталляцию продляемой лицензии в консоли централизованного администрирования на предоставленном заказчиком оборудовании, настроить задачи по автоматическому распространению на серверное оборудование Заказчика, произвести настройку правил использования программ, устройств и веб-ресурсов, обучить 2 (двух) специалистов Заказчика по поиску вредоносного ПО и анализу, создания задач и правил информационной безопасности посредством консоли централизованного администрирования. 2.3. Поставщик услуг должен провести очный авторизованный учебный курс по поставляемому антивирусному программному обеспечению для не менее 2 (двух) специалистов Заказчика с последующим предоставлением сертификата о прохождении курса. 3. Требования к технической поддержке. Потенциальный поставщик должен оказать Заказчику консультационно-техническое обслуживание по вопросам настройки и эксплуатации антивирусного программного обеспечения и обеспечить следующими возможностями: 1) Техническая поддержка должна предоставляться на русском языке специалистами производителя антивирусного ПО и его партнеров на всей территории Республики Казахстан круглосуточно в праздничные и выходные дни по телефону, электронной почте и через Интернет в течении 1 года с даты вступления Договора в законную силу; 2) Потенциальный поставщик должен

	обеспечить доступ к электронной информационной системе технической поддержки производителя программного обеспечения, включающей в себя направление запросов по конкретным проблемам через систему электронной почты; 3) Доступ к вышеописанным службам должен быть открыт круглосуточно в течение всего времени оказания поддержки; 4) Потенциальный поставщик должен обеспечить Заказчика получением технической информации и/или дополнительных программных компонентов, а также направлением технических специалистов для преодоления и разрешения проблем и ошибок, обнаруженных в антивирусном ПО; 5) Гарантийное обслуживание и техническая поддержка программного обеспечения должны обеспечиваться без дополнительных расходов со стороны Заказчика. Гарантийное обслуживание и техническая поддержка должны осуществляться по месту нахождения программного обеспечения. Потенциальный поставщик должен загрузить новую лицензию антивирусного ПО для виртуальных серверов на консоль централизованного администрирования оборудования заказчика, произвести настройку политик и задач обновления антивирусных баз, поиска вирусов и уязвимостей, обучить 2 (двух) специалистов Заказчика по созданию задач и правил информационной безопасности посредством консоли централизованного администрирования.
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)	