

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Әділет министрлігі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Әділет министрлігі" мемлекеттік мекемесі
Конкурстың №:	№ 17855106-1
Конкурстың атауы:	Антивирустық бағдарламалық техникалық қамтамасыз ету және лицензияларды ұзарту бойынша қызметтер
Лоттың нөмірі:	№ 87894823-OK2
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:	16821551.73
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	16821551.73
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	Жұмыс станцияларына арналған антивирустық БЖ лицензияларын ұзарту және техникалық қолдау қызметіне техникалық сипаттама Осы техникалық ерекшелікте Қазақстан Республикасы Әділет министрлігі жұмыс станциялары үшін лицензияны ұзарту және антивирустық бағдарламалық қамтамасыз етуді техникалық қолдау Қызметтеріне (бұдан әрі - АБК, бұдан әрі – Қызмет) мынадай талаптар келтірілген: сатып алуды жүргізу нәтижесінде 1900 бірлік көлеміндегі жұмыс станциялары үшін KES FB Advanced бойынша қолданыстағы антивирустық лицензияны және техникалық қолдауды 2026 жылдың 7 желтоқсанынан 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 бағдарлама лицензиясы жұмыс станциялары мен серверлердің тұрақты жұмыс істеуін, орталықтандырылған басқаруды қамтамасыз ететін корпоративтік шешім болуы керек. 1. Жалпы талаптар. Антивирустық құралдар мыналарды қамтуы керек: Windows жұмыс станцияларына арналған антивирустық қорғау бағдарламалық құралдары; macOS жұмыс станцияларына арналған антивирустық қорғау бағдарламалық құралдары; Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғау бағдарламалық құралдары; Windows файлдық серверлеріне арналған антивирустық қорғау бағдарламалық құралдары; мобильді құрылғыларға (смартфондар мен планшеттерге) арналған антивирустық қорғау бағдарламалық құралдары; орталықтандырылған басқару бағдарламалық құралдары, мониторинг және жаңартулар; зиянды бағдарламалар мен шабуылдардың қолтаңбаларының жаңартылатын дерекқорлары; пайдалану құжаттамасы орыс тілінде. 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. 2. Windows жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар. Антивирустық бағдарламалық жасақтама келесі нұсқалардың жұмыс станциялары үшін операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек: Windows 7 Professional/Ultimate/Enterprise Service Pack 1 және одан жоғары (32/64 биттік); Windows 8 Professional/Enterprise (32/64 биттік); Windows 8.1 Professional/Enterprise (32/64 биттік); Windows 10 Pro/ Enterprise (32/64 биттік); Windows 11 Pro (64 биттік). Антивирустық қорғаудың бағдарламалық
--	--

	құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу; кесте бойынша антивирустық сканерлеу; қосылатын құрылғыларды антивирустық сканерлеу; бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; белсенді жұқтыру әрекеттерін бейтараптандыру; қолданбаның мінез-құлқын және ол жүргізетін әрекеттерді талдау жүйеде оның зиянды белсенділігін анықтау және рұқсат етілмеген әрекеттерді анықтау; желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау; бағдарламалық қамтамасыз етуде осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау; емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру; артықшылық шектеулері (тізілімге жазылу, файлдарға, қалталарға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға хабарласу, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т. б.) процестер мен қосымшалар үшін, сенім деңгейін анықтай отырып, динамикалық түрде жаңартылатын теңшелетін қолданбалар тізімдері; қолданбаға нақты уақыт режимінде қол жеткізуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін өндірушінің ресурстарына; RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматындағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу; келесі хаттамалар бойынша берілетін кіріс және шығыс трафикті тексере отырып, электрондық поштаны зиянды бағдарламалардан қорғау: IMAP, SMTP, POP3, MAPI, NNTP; берілген файл түрлерінің атауын өзгерту немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі; https (SSL 3.0, TLS 1.0, TLS 1.1) хаттамалары бойынша пайдаланушының компьютеріне келіп түсетін желілік трафикті тексеру, TLS 1.2), HTTP, FTP, оның ішінде эвристикалық талдау, сенімді ресурстарды теңшеу мүмкіндігі және құлыптау немесе статистика режимінде жұмыс істеу; жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді блоктау; фишингтік және қауіпті сайттарды тану және бұғаттау; желілік сегменттерді санаттауға мүмкіндік беретін бағдарламалар үшін желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желілік экран; кез-келген типтегі есептеу желілеріндегі қосымшалар мен порттар үшін желілік экран ережелерін қолдана отырып, желілік шабуылдардан қорғау; ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау құрылғының MAC мекен-жайын қолдан жасау үшін; желілік қосылымдарды басқару типі желілік көпір, бір уақытта бірнеше желілік қосылымдарды орнатуға тыйым салу мүмкіндігі бар; барлық немесе белгілі бір пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат
--	---

	беретін арнайы ережелер жасау үшін компонент бағдарламаларды бағдарламаны табу жолында, метадеректерде, сертификатта немесе оның ішінде, бақылау сомасында және өндіруші ұсынған алдын ала белгіленген қолданба санаттарында бақылауы керек бағдарламалық жасақтама, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе құлыптау режимінде жұмыс істеуі керек; пайдаланушының құрылғының типі және / немесе пайдаланылатын автобус бойынша сыртқы енгізу/шығару құрылғыларымен жұмысын бақылау, олардың идентификаторы бойынша сенімді құрылғылардың тізімін жасау мүмкіндігі және Active Directory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігі; құрылғыларды MTP басқару және барлық немесе пайдаланушылар топтары үшін осы типтегі құрылғыларға қол жеткізу ережелерін реттеу (Active Directory немесе жергілікті пайдаланушылар/топтар), құрылғыларды бақылау шеңберінде; алынбалы дискілердегі файлдарды жазу және/немесе жою туралы Оқиғалар журналына жазу; файлдық жүйесі бар құрылғыларға қол жеткізу қағидалары үшін басымдық тағайындау; пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық жаңартатын санатқа, сондай-ақ ақпарат түріне (аудио, видео және т. б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, уақыт аралықтарын енгізуге мүмкіндік беру бақылау, сондай-ақ оны тек Active Directory-ден белгілі бір пайдаланушыларға тағайындау; BadUSB типті шабуылдардан қорғау; қолданба қызметін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ пароль арқылы қолданба параметрлеріне қол жеткізуді қорғау; антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату; бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; кесте бойынша тапсырмаларды іске қосу және/немесе қолданбаны іске қосқаннан кейін бірден; ыңғайлы жұмысты қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару файл кеңістігін сканерлеу кезінде пайдаланушылар; өткен тексеру уақытынан бастап жағдайы өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету антивирустық бағдарламаның тұтастығын тексеру; файлдың бақылау сомасы, аты/каталог маскасы бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу; XML-форматқа ережелер мен ерекшеліктер тізімдерін импорттау және экспорттау; жойылған вирус жұққан файлдарға арналған қорғалған сақтау антивирусы, оларды қалпына келтіру мүмкіндігі бар; антивирустың жұмысы туралы есептер үшін қорғалған сақтау орны бар; антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктердің ең аз жиынтығымен Графикалық интерфейстің жеңілдетілген нұсқасының болуы; Windows Defender Security Center интеграциясы; Antimalware Scan Interface (AMSI) қолдауының болуы Linux үшін Windows Subsystem &#40;WSL&#41;; қолдауының болуы; TCP және UDP хаттамалары бойынша желіні
--	---

	бақылау құралының болуы; резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғау; желілік трафиктің шектеулері Егер Интернетке қосылу шектеулі болса; анықталған осалдықтар туралы есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосыңыз. арнайы жүктеу агентін құрумен және single sign технологияи технологиясын қолдаумен толық дискіні шифрлау, UEFI жүйелерін қолдау; жүктеу агенті немесе операциялық жүйе файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, UEFI жүйелерін қолдау; толық дискіні шифрлау кезінде екі факторлы аутентификацияны қолдау; шифрланатын мазмұнды икемді көрсету мүмкіндігі бар файлдарды шифрлау (орналасқан жері бойынша, кеңейтімі бойынша, файлды жасайтын қосымша бойынша); таңдалған қосымшалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөз арқылы ұйымнан тыс файлдарды шифрлауға мүмкіндік беретін технологияның болуы; алынбалы тасымалдағыштардағы деректерді шифрлау, жұмыс режимін орнату мүмкіндігі бар, бұл ұйым желісінен тыс файлдарды шифрлау және шифрын ашу; мінез-құлық үлгісінен ауытқу кезінде бағдарламалардың мінез-құлық үлгісін қалыптастыру және олардың әрекеттерін бұғаттау (ауытқуларды адаптивті бақылау). 3. Windows серверлеріне арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар. Антивирустық бағдарламалық жасақтама келесі нұсқалардың файлдық серверлері үшін операциялық жүйені басқаратын компьютерлерде жұмыс істеуі керек: Windows Small Business Server 2011 Essentials/Standard (64 биттік); Windows MultiPoint Server 2011 (64 биттік); Windows Server 2008 Standard/Enterprise Service Pack 2 (64 биттік); Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1(64 бит); Windows Server 2012 Foundation / Essentials / Standard (64 бит); Windows Server 2012 R2 Foundation / Essentials / Standard (64 биттік); Windows Server 2016 (64 биттік); Windows Server 2019 Essentials / Standard (64 биттік); Windows Server 2019 Essentials / Standard (64 биттік); Windows Server 2022 Essentials/Standard (64 биттік); Windows Server 2025 Essentials/Standard (64 биттік). Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу; кесте бойынша антивирустық сканерлеу; қосылатын құрылғыларды антивирустық сканерлеу; бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; белсенді жұқтыру әрекеттерін бейтараптандыру; қолданбаның мінез-құлқын және оның зиянды белсенділігін анықтау және рұқсат етілмеген әрекеттерді анықтау үшін жүйеде жасаған әрекеттерін талдау; желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға жүгінулерді талдау; бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде
--	---

	жүйелік процестердің жадын қорғау; емдеу кезінде зиянды бағдарламалық қамтамасыз етудің әрекеттерін кері қайтару, оның ішінде шифрланған, зиянды бағдарламалармен, файлдармен қалпына келтіру; іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін өндірушінің ресурстарына нақты уақыт режимінде қол жеткізуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы файлдарды антивирустық тексеру және емдеу; желілік пакеттік ережелер мен желілік ережелерді құруға мүмкіндік беретін кіріктірілген желілік экран желілік сегменттерді санаттау мүмкіндігі бар бағдарламалар үшін; құрылғының MAC мекенжайын қолдан жасау үшін ARP протоколындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау; қолданба сервисін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, зиянкестер немесе біліктілігі жоқ пайдаланушылар тарапынан қорғауды өшірмеуге мүмкіндік беретін пароль арқылы қолданба параметрлеріне қол жеткізуді қорғау; тек вирусқа қарсы қорғау бағдарламалық құралының таңдалған компоненттерін орнату; бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; кесте бойынша және/немесе тапсырмаларды іске қосу Операциялық жүйе жүктелгеннен кейін бірден; файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; өткен тексеру уақытынан бастап жағдайы өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету; антивирустық бағдарламаның тұтастығын тексеру; файлдың бақылау сомасы, аты/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктер қосу; антивируста жойылған вирус жұққан файлдар үшін оларды қалпына келтіру мүмкіндігімен қорғалған жадтың болуы; антивирустың жұмысы туралы есептер үшін қорғалған қойманың болуы; антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктердің ең аз жиынтығымен Графикалық интерфейсін жеңілдетілген нұсқасының болуы; Windows Defender Security Center интеграциясы; antimalware Scan Interface (AMSI) қолдауының болуы; Linux үшін Windows Subsystem &#40;WSL&#41;; қолдауының болуы; объектілерді қалпына келтіруді құпия сөзбен қорғау сақтау; ережелер мен ерекшеліктер тізімдерін XML форматына импорттау және экспорттау; желілік трафиктің шектеулері Егер Интернетке қосылу барлық немесе белгілі бір пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелерді құрудың лимиті болса, компонент бағдарламаларды бағдарламаны, метадеректерді, сертификатты немесе оның ізін табу жолындағыдай бақылауы керек, бақылау сомасы, сондай-ақ бағдарламалық жасақтама өндірушісі ұсынатын қосымшалардың алдын-ала белгіленген санаттары бойынша компонент қара немесе ақ тізім режимінде жұмыс істеуі керек, сондай-ақ статистиканы жинау немесе бұғаттау режимінде; мінез-құлық үлгісінен
--	---

	ауытқу кезінде бағдарламалардың мінез-құлық үлгісін қалыптастыру және олардың әрекеттерін бұғаттау (ауытқуларды адаптивті бақылау); анықталған осалдықтар бойынша есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу. 4. Мас жұмыс станцияларына арналған антивирустық бағдарламалық жасақтамаға қойылатын талаптар. Мас жұмыс станцияларына арналған антивирустық қорғау бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: macOS 10.13, 10.14, 10.15 немесе 11.0; антивирустық қорғау бағдарламалық құралында келесі функциялар іске асырылуы керек: резиденттік антивирустық мониторинг; іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; кесте бойынша антивирустық базаларды автоматты түрде жаңарту; қалпына келтіру мүмкіндігі үшін вирус жұққан файлдарды жоймас бұрын олардың сақтық көшірмесін жасау; бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; интрузияны анықтау және алдын алу жүйесін (IDS/IPS) және кез келген түрдегі есептеу желілерінде, соның ішінде сымсыз желілерде жұмыс істеу кезінде ең танымал қолданбаларға арналған желілік белсенділік ережелерін пайдалана отырып, желілік шабуылдардан қорғау; антивирустық қорғаныс өндірушісінің беделді бұлттық қызметтерінің үкімдеріне негізделген зиянды және фишингтік сайттарды бұғаттау; Safari браузерлері арқылы берілетін желілік трафикті тексеру, Google Chrome және Firefox (HTTP және HTTPS трафигі); пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу, редакциялау, өндіруші құрған және динамикалық түрде жаңартылатын белгілі бір ресурстарға немесе ресурстар санаттарына қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу; өткен тексеру уақытынан бастап жағдайы өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету; жоғарыда аталған барлық компоненттерді бірыңғай жүйенің көмегімен орталықтандырылған басқару басқарма; FileVault шифрлауды басқару мүмкіндігі бар бірыңғай басқару жүйесі арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; жаңа kав пәрменін қолдана отырып, пәрмен жолынан кеңейтімдерді орнату мүмкіндігі; файлдық операцияларды ұстап қалу деңгейінде көрсетілген аймақтарды тексеру кезінде ерекшеліктерді орнату мүмкіндігі; дискіге толық қол жеткізу құқықтарының пайда болуын автоматты түрде бақылау және қажетті жүйелік кеңейтімдерді орнату мүмкіндігі беріледі. 5. 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: CentOS 6.7 және одан жоғары; Debian GNU/Linux 10.1 және одан жоғары; Debian GNU/Linux 11; Mageia 4; Red Hat
--	---

	Enterprise Linux 6.7 және одан жоғары; Alt 8 SP жұмыс станциясы; Violt 8 Sp сервері; Violt білім беру 10; Violt жұмыс станциясы 10. Linux жұмыс станцияларына арналған антивирустық қорғаныс бағдарламалық жасақтамасы келесі нұсқалардың 64 биттік операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: ASTRA Linux Special Edition RUSB.10152-02 (кезекті жаңарту 4.7); EulerOS 2.0 SP8; SUSE Linux Enterprise Server 15 SP3; Ubuntu 20.04 LTS. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: резиденттік антивирустық мониторинг; іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; SMB / NFS арқылы қолжетімді ресурстарды тексеру; ядро жадын тексеру мүмкіндігі; бұрын белгісіз зиянды бағдарламаларды тиімдірек тануға және бұғаттауға мүмкіндік беретін эвристикалық анализатор; пайдаланушының пәрмені бойынша антивирустық сканерлеу немесе әкімші және кесте бойынша; zip мұрағаттарындағы файлдарды антивирустық тексеру; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj.; мәтіндік форматтағы электрондық пошта хабарламаларын тексеру (Plain text); файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының лимиті, тексерілетін файл өлшемінің лимиті, кәштеу механизмі тексерілген және тексерілгеннен кейін өзгертілмеген файлдар туралы ақпарат); SMB / NFS хаттамалары бойынша желілік қатынауы бар жергілікті каталогтардағы файлдарды қашықтықтан қорғау тексеру кезінде файлдарды бұғаттау опциясын қосу; күдікті және бүлінген объектілерді карантинге қою; SAMBA деңгейінде файлдық операцияларды ұстап алу және тексеру; ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару; тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу; есептерді HTML және CSV форматтарында экспорттау және сақтау; файл кеңістігін сканерлеу кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін дербес компьютерлердің ресурстарын пайдалануды икемді басқару; вирус жұққан объектінің көшірмесін резервтік қоймада сақтау егер ол ақпараттық құндылықты білдірсе, объектіні талап бойынша ықтимал қалпына келтіру мақсатында емдеу және жою алдында; пайдаланушының графикалық интерфейсі арқылы түбірлік құқықтарсыз басқару; бірыңғай басқару жүйесі немесе веб-консоль арқылы жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; пайдаланушылардың құрылғы түрлері мен қосылу шиналары бойынша компьютерге қосылған немесе орнатылған құрылғыларға қол жеткізуін басқару; алынбалы дискілерді тексеру; желілік шабуылдарға тән әрекетті кіріс желілік трафикте қадағалау; HTTP/HTTPS және FTP хаттамалары бойынша пайдаланушының компьютеріне түсетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік бағдарламаларға тиесілігін орнату мүмкіндігі пайдаланушының компьютеріндегі
--	---

	бағдарламалардың әрекеттері туралы деректерді алу; компьютерлерде сақталатын бағдарламалардың барлық орындалатын файлдары туралы ақпарат алу (тапсырма түгендеу); бағдарламаны іске қосу кезінде бақылау файлдарын жасау; бағдарламаның компьютерлерде орнатылған бағдарламалардың барлық орындалатын файлдары туралы ақпарат; автоматты іске қосу объектілерін тексеру, жүктеу секторлары, процесс жады және ядро жады; емдеу немесе жою алдында файлдардың сақтық көшірмелерін сақтау және сақтық көшірмелерден файлдарды қалпына келтіру. 6. Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді, Windows терминалдық серверлерін вирусқа қарсы қорғаудың бағдарламалық құралдарына қойылатын талаптар. Windows файлдық серверлеріне арналған антивирустық қорғау бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: 32 биттік Microsoft Windows операциялық жүйелері: SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2008 Standard/Enterprise/Datacenter; SP2 немесе одан жоғары жаңарту бумасы бар Windows Server 2008 Core Standard/Enterprise/Datacenter. 64 биттік Microsoft Windows операциялық жүйелері: Windows Server 2003 Standard/Enterprise/Datacenter SP2 немесе одан жоғары жаңарту бумасымен; Windows Server 2003 R2 Standard/Enterprise/datacenter SP2 немесе одан жоғары жаңарту бумасымен; Windows Server 2008 Core Standard/Enterprise/ Datacenter SP2 немесе одан жоғары жаңарту бумасымен; Windows Server 2008 Standard/Enterprise/Datacenter SP2 немесе одан жоғары жаңарту бумасы бар Enterprise/Datacenter; Microsoft Small Business Server 2008 Standard/Premium SP2 немесе одан жоғары; Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter SP1 немесе одан жоғары жаңарту бумасымен; Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1 немесе одан жоғары жаңарту бумасымен; Windows Hyper-V SP1 немесе одан жоғары жаңарту бумасы бар Server 2008 R2; Microsoft Small Business Server 2011 Essentials/Standard SP1 немесе одан жоғары; Microsoft Windows MultiPoint Server 2011 Standard/Premium; Windows Server 2012 Foundation/Essentials/Standard/Datacenter; Windows Server 2012 Core Foundation/Essentials/Standard/ Datacenter; Microsoft MultiPoint Server 2012 Standard/Premium; Windows Storage Server 2012; Windows Hyper-V Server 2012; Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter; Windows Server 2012 R2 Core Foundation/Essentials/Standard/Datacenter; Windows Storage Server 2012 R2; Windows Hyper-V Server 2012 R2; Windows Server 2016 Essentials/Standard/Datacenter; Windows Server 2016 MultiPoint; Windows Server 2016 Core Standard / Datacenter; Microsoft Windows MultiPoint Server 2016; Windows Storage Server 2016; Windows Hyper-V Server 2016; Windows Server 2019 Essentials / Standard / Datacenter; Windows Server 2019 Core; Windows Storage Server 2019; Windows Hyper-V Server 2019; Windows Server 2022; Windows 10 Enterprise multi-session. Антивирустық қорғаудың бағдарламалық құралында мынадай функционалдық
--	---

	мүмкіндіктер іске асырылуы тиіс: нақты уақыт режимінде және сұраныс бойынша әртүрлі функцияларды орындайтын серверлерде антивирустық сканерлеу: терминал серверлері, баспа серверлері, қолданба серверлері және домен контроллерлері, файлдық серверлер; пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу; тапсырмаларды кесте бойынша және/немесе амалдық жүйе жүктелгеннен кейін бірден іске қосу; іске қосылатын бағдарлама немесе файл бойынша үкім шығару үшін нақты уақыт режимінде өндірушінің арнайы сайттарына жүгінуге мүмкіндік беретін жаңа қауіптерден бұлтты қорғау; RAR, ARJ, ZIP, CAB форматындағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу; RAR, ARJ, ZIP, CAB форматындағы файлдарды қорғау файлдық жүйелер ағындары (NTFS-streams), жүктеу жазбасы, жергілікті және алынбалы дискілердің жүктеу секторлары; 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; желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ қалталар мен файлдарға қоңырауларды талдау; контейнерлерді тексеру Microsoft Windows; процесс жадындағы осалдықтарды пайдаланудан қорғау; бұзылған процестерді автоматты түрде аяқтау мүмкіндігі болуы керек, ал маңызды жүйелік процестер аяқталмауы керек; қорғалған тізімге процестерді қосу; өткен тексеру уақытынан бастап жағдайы өзгермеген объектілерді өткізіп жіберу арқылы сканерлеу процесін жеделдету; жеке модульдерді жеке тапсырма арқылы олардың тұтастығын бұзуы мүмкін екенін тексеру; сервердің маңызды аймақтарын жеке тапсырма ретінде тексеру параметрлері тапсырмалар; тапсырмалардың басымдылығына байланысты сервер ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу; фондық режимде антивирустық сканерлеуді жалғастыру; болған маңызды оқиғалар туралы әкімшілерді хабардар етудің бірнеше жолдарының болуы (пошта хабарламасы, дыбыстық ескерту, қалқымалы терезе, Оқиғалар журналына жазу); зиянды бағдарламалардан, зиянкестерден немесе біліктілігі жоқ пайдаланушылардан қорғауды өшірмеуге мүмкіндік беретін рұқсаттар тізімдері арқылы қолданба мен қызмет параметрлеріне рөлдік қол жеткізу, сондай-ақ антивирусты басқаруға тыйым салу немесе рұқсат беру; SIEM жүйелерімен интеграция; антивирустың жұмыс процестерінің санын қолмен көрсету; графикалық интерфейсті өшіру; қашықтан және жергілікті басқару консолінің болуы; пәрмен жолынан антивирус параметрлерін басқару; бірыңғай басқару жүйесінің көмегімен жоғарыда аталған барлық компоненттерді орталықтандырылған басқару; ережелердің бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару; желілік шабуылдардың белгілеріне кіріс трафигін талдауды қамтамасыз ететін желілік қауіптерден қорғау; қорғауды қосу немесе өшіру сыртқы қауіптерден
--	---

	бағдарламаның процестері (әдепкі бойынша функция қосылады). Функция қосылған кезде бағдарлама өзінің процестерін, сондай-ақ әкімшілік агент процестерін үшінші тарап процестерінің араласуынан қорғайды; құрылғыларды, соның ішінде желілік карталар мен модемдерді бақылау; веб-бақылау; пошта қауіптерінен қорғау (Outlook плагині); HTTP және HTTPS трафигін вирустар мен фишингтен, зиянды веб-базаларға сілтемелерді тексерумен қорғаңыз-веб-сервер сертификаттарының дұрыстығын тексеру мүмкіндігімен трафикті ұстап алу ұрлау драйверінің көмегімен немесе оны қайта бағыттау арқылы жүзеге асырылуы тиіс; барлық немесе белгілі бір пайдаланушы топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау; арнайы ережелер жасау бағдарламаны, метадеректерді, сертификатты немесе оның басып шығаруын, бақылау сомасын табу жолында қосымшаларды бақылауы тиіс; арнайы ережелерді құру қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі керек, оларға салынған файлдарды өзгерте және іске қоса алатын сенімді жаңартулар пакеттерінің тізімін жасау мүмкіндігі болуы керек; пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын сенімді құрылғылар тізімін құру мүмкіндігімен және оларды ұсыну мүмкіндігімен бақылауды жүзеге асыру. Active Directory ішінен белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану артықшылықтары; Интернет желісімен жұмысты бақылауды жүзеге асыру, оның ішінде белгілі бір мазмұндағы ресурстарға, өндіруші алдын ала жасаған және динамикалық жаңартатын санатқа қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу; әкімшіні сыртқы құрылғылардың қосылуы туралы хабардар ету; құрылғылар мен қосымшаларды бақылау үшін ережелерді автоматты түрде генерациялау тетіктерінің болуы. 7. Мобильді құрылғыларды антивирустық қорғау бағдарламалық құралдарына қойылатын талаптар. Смартфондарды антивирустық қорғауға арналған бағдарламалық құралдар келесі мобильді ОЖ - де жұмыс істеуі керек: Android 5.0-13 (Go Edition қоспағанда, Android 12L қоса алғанда); iOS 10-16 немесе iPadOS 13-15. Android ОЖ үшін смартфондарды вирусқа қарсы қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: антивирустық қорғау құралдарын өндірушінің бұлттық беделді сервисін пайдалана отырып, қосымша тексеру деңгейімен смартфонның файлдық жүйесін тұрақты антивирустық қорғау; талап бойынша және кесте бойынша құрылғының файлдық жүйесін тексеру; беделдік және фишингтік сайттардың үкімдері негізінде зиянды және фишингтік сайттарды бұғаттаудың Орнатылатын қосымшаларын лезде тексеру антивирустық қорғаныс өндірушісінің бұлтты қызметтері; вирус жұқтырған объектілерді оқшаулауға арналған қойманың болуы; зиянды бағдарламаларды іздеу және қауіпті объектілерді жою кезінде пайдаланылатын антивирустық базаларды кесте бойынша жаңарту; көрсетілген қосымшалардың іске қосылуын, оның ішінде алдын ала белгіленген қосымшалар
--	---

	санаттарының көмегімен бұғаттау; рұқсат етілген қосымшалардың ақ тізімдерін қолдау; қосымшалардың іске қосылуын бақылау шеңберінде жүйелік қосымшаларды бұғаттау; командалар мен push хабарламалар жіберу Firebase Cloud Messaging (FCM) қызметі арқылы; wi-fi және bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалану; Wi-fi желілеріне қосылу параметрлерін көрсету; орнатуға міндетті қосымшаларды көрсету; мобильді құрылғыны бұғаттау, деректерді жою, жұмыс қызметіне байланысты деректерді жою, құрылғының орналасқан жерінің координаттарын алу, зауыттық параметрлерге қашықтан оралу (factory reset); олардың негізінде мобильді құрылғының корпоративтік саясатқа сәйкестігін тексеру жүзеге асырылатын ережелер тізімін жасау. құрылғыны автоматты түрде құлыптау, деректерді жою, сәйкессіздіктер анықталған кезде корпоративті қосымшаларды іске қосуға тыйым салу мүмкіндігі; Samsung Knox1 және Knox2 технологияларын қолдау. Apple iOS операциялық жүйелеріне арналған смартфондарды қорғау бағдарламалық құралында келесі функциялар іске асырылуы керек: топтық саясаттарды қолдана отырып, IOS MDM құрылғыларының параметрлерін қашықтан конфигурациялау; деректерді блоктау және жою пәрменін жіберу; мобильді құрылғылардың топтық қауіпсіздік саясаттарын құру; Exchange ActiveSync\ iOS MDM протоколы бойынша қосылған құрылғылардың конфигурация параметрлерін қашықтан конфигурациялау; есептер алу пайдаланушылардың мобильді құрылғыларының жұмысы туралы Статистика; supervised mode пайдалану кезінде антивирустық қорғаныс өндірушісінің беделді бұлттық қызметтерінің үкімдеріне негізделген зиянды және фишингтік сайттарды бұғаттау; бір басқару консолі арқылы орталықтандырылған басқару; басқарылатын құрылғыда iTunes, Safari немесе Game Center сияқты құрылғының жергілікті қолданбаларын пайдалануға болатынын бақылауға мүмкіндік беретін компоненттің болуы. 8. Windows операциялық жүйелеріне негізделген орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар. Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: Microsoft Windows 10 Enterprise 2015 LTSC 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 2016 LTSC 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 2019 LTSC 32 биттік/64 биттік-бит; Microsoft Windows 10 Pro RS5 (қазан 2018 жаңарту, 1809) 32 бит / 64 бит; RS5 жұмыс станцияларына арналған Microsoft Windows 10 Pro (қазан 2018 жаңарту, 1809) 32 биттік/64 биттік; Microsoft Windows 10 Enterprise RS5 (қазан 2018 жаңарту, 1809) 32 биттік/64 биттік; Microsoft Windows 10 Pro 19H1 32 биттік / 64 биттік; 19H1 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 19H1 32 биттік/64 биттік; Microsoft Windows 10 Pro 19H2 32 биттік / 64 биттік; 19H2 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 19H2 32 биттік / 64 биттік;
--	---

	Microsoft Windows 10 Pro 20H1 (мамыр 2020 жаңарту) 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 20h1 (мамыр 2020 жаңарту) 32 биттік/64 биттік; Microsoft Windows 10 Pro 20H2 (қазан 2020 жаңарту) 32 бит/64 бит; Microsoft Windows 10 Enterprise 20h2 (қазан 2020 жаңарту) 32 бит/64 бит; Microsoft Windows 10 Pro 21h1 (мамыр 2021 жаңарту) 32 биттік/64 биттік; Microsoft Windows 10 Enterprise 21H1 (мамыр 2021 жаңарту) 32-бит/64 бит; Microsoft Windows 10 Pro 21H2 (қазан 2021 жаңарту) 32 бит/64 бит; Microsoft Windows 10 Enterprise 21h2 (October 2021 Update) 32 биттік/64 биттік; Microsoft Windows 11 Enterprise 64 биттік; Microsoft Windows 8.1 Pro 32 биттік/64 биттік; Microsoft Windows 8.1 Enterprise 32 биттік/64 биттік; Microsoft Windows 8 Pro 32 биттік / 64 биттік; Microsoft Windows 8 Enterprise 32 биттік / 64 биттік; Microsoft Windows 7 Professional Service Pack 1 32 биттік / 64 биттік-биттік; Microsoft Windows 7 Enterprise/ultimate Service Pack 1 32 биттік/64 биттік; Windows Server 2008 R2 with Standard Service Pack 1 және одан жоғары 64 биттік; Windows Server 2008 R2 Service Pack 1 (барлық басылымдар) 64 биттік; Windows Server 2012 Server Core 64 биттік;; Windows Server 2012 Datacenter 64 биттік; Windows Server 2012 Essentials 64 биттік; Windows Server 2012 Foundation 64 биттік; Windows Server 2012 Standard 64 биттік; Windows Server 2012 R2 Server Core 64 биттік; Windows Server 2012 R2 Datacenter 64 биттік; Windows Server 2012 R2 Essentials 64 биттік; Windows Server 2012 R2 Foundation 64 биттік; Windows Server 2012 R2 Standard 64 биттік; Windows Server 2016 Datacenter (LTSB) 64 биттік; Windows Server 2016 Standard (LTSB) 64 биттік; Windows Server 2016 (орнату нұсқасы Server Core) (LTSB) 64-разрядты; Windows Server 2019 Standard 64 бит; Windows Server 2019 Datacenter 64 бит; Windows Server 2019 Core 64 бит; Windows Server 2022 Standard 64 бит; Windows Server 2022 Datacenter 64 бит; Windows Server 2022 Core 64 бит; Windows Storage Server 2012 64 биттік; Windows storage Server 2012 R2 64 биттік; Windows Storage Server 2016 64 биттік; Windows Storage Server 2019 64 биттік. Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық жасақтамасы келесі виртуалды платформаларда орнатуды қолдауы керек: VMware vSphere 6.7; VMware vSphere 7.0; VMware Workstation 16 Pro; Microsoft Hyper-V Server 2012 64 бит; Microsoft Hyper-V Server 2012 R2 64 бит; Microsoft Hyper-V Server 2016 64 бит; Microsoft Hyper-V Server 2019 64 бит; Microsoft Hyper-V Server 2022 64 биттік; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Parallels Desktop 17; Oracle VM VirtualBox 6.x. орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдары келесі нұсқалардың ДҚБЖ-мен жұмыс істеуі керек: Microsoft SQL Server 2012 express 64 биттік; Microsoft SQL Server 2014 express 64 биттік; Microsoft SQL Server 2016 express 64 бит; Microsoft SQL Server 2017 express 64 бит; Microsoft SQL Server 2019 Express 64 бит; Microsoft SQL Server 2014 (барлық басылымдар) 64 бит; Microsoft SQL
--	--

	Server 2016 (Барлық басылымдар) 64 бит; Microsoft SQL Server 2016 (Барлық басылымдар) 64 бит; Microsoft SQL Server 2017 (барлық басылымдар) үшін Windows 64 биттік; Linux үшін Microsoft SQL Server 2017 (барлық басылымдар) 64 биттік; Windows үшін Microsoft SQL Server 2019 (барлық басылымдар) 64 биттік (қосымша қадамдар қажет); Linux үшін Microsoft SQL Server 2019 (барлық басылымдар) 64 биттік (қосымша қадамдар қажет); Microsoft Azure SQL Database; Amazon RDS және Microsoft Azure бұлттық платформаларында қолдау көрсетілетін SQL серверлерінің барлық нұсқалары; MySQL 5.7 Community 32 биттік/64 биттік; MySQL Standard Edition 8.0 (8.0.20 және одан жоғары шығарылым) 32 биттік/64 биттік; MySQL Enterprise Edition 8.0 (8.0.20 және одан жоғары шығарылым) 32 биттік / 64 биттік; MariaDB 10.5.x 32 биттік / 64 биттік; MariaDB 10.4.x 32 биттік / 64 биттік; MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік; MariaDB Server 10.3 32 биттік / 64 биттік InnoDB сақтау ішкі жүйесі бар; MariaDB Galera Cluster 10.3 InnoDB сақтау ішкі жүйесі бар 32 биттік / 64 биттік; MariaDB 10.1.30 және одан жоғары 32 биттік/64 биттік. Вирусқа қарсы қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: қорғалатын тораптардың санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату архитектурасын таңдау; ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory-дан ақпаратты оқу; табылған компьютерлерді IP-мекен-жайы бойынша, операциялық жүйелердің типі бойынша ои AD-да болу ережелерін баптау; желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; IP-мекен-жайы, операциялық жүйелердің типі, ои AD-да болу бойынша тасымалдау ережелерін теңшеу мүмкіндігі; орталықтандырылған бағдарламалық жасақтаманы орнату, жаңарту және жою антивирустық қорғау құралдары; орталықтандырылған баптау, әкімшілендіру; қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; басқару орталығының құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты); саясат пен міндеттердің өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі; антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін-RPC, GPO, басқару жүйесінің құралдары - жергілікті орнату үшін-дербес орнату пакетін құру мүмкіндігі; пайдаланушы кірген есептік жазбаға, ағымдағы IPv4 мекенжайына және компьютердің қай ои немесе қауіпсіздік тобына байланысты антивирустық шешімнің параметрлерін қайта анықтайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар; қайта бөлу орын алатын триггер иерархиялары; бағдарламалық құрал арқылы жүктелген жаңартуларды сынау клиенттік машиналарға таратпас бұрын орталықтандырылған басқару; жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу; виртуалды машиналар желісінде тану және егер бұл машиналар бір физикалық серверде болса, олардың
--	---

	арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; әкімшілер мен операторлардың құқықтарын, сондай-ақ әр деңгейде ұсынылатын есеп беру нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру; еркін деңгейдегі әкімшілік серверлер иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі басқару серверлері үшін көп жалға алуды (multi-tenancy) қолдау; байланыс арналары арқылы да, машиналық ақпарат тасығыштар арқылы да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту; басқару сервері арқылы антивирустық бағдарламалық жасақтама өндірушісінің бұлтты серверлеріне қол жеткізу; клиенттік компьютерлерге лицензияны автоматты түрде тарату; пайдаланушылардың компьютерлерінде орнатылған бағдарламалық жасақтама мен жабдықты түгендеу; орнатылған антивирустық қосымшалардың жұмысындағы оқиғалар туралы хабарлау механизмінің болуы олар туралы пошта хабарламаларын қорғау және тарату параметрлері; Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару функциясы; IOS MDM сервері арқылы мобильді құрылғыларды басқару функциясы; берілген оқиғалар туралы SMS-ескертулерді жіберу; басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған орнату; басқару жүйесіне желілік жүктемені азайту үшін жаңартуларды қайта жіберу орталығының ұйымның кез келген компьютерін көрсетуі. 9. Linux операциялық жүйесіне негізделген орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар. Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек: Debian GNU/Linux 11.x (Bullseye) 32 биттік/64 биттік; Debian GNU/Linux 10.x (Buster) 32 биттік/64 биттік; Debian GNU/Linux 9.x (Stretch) 32 биттік/64 биттік; Ubuntu Server 20.04 LTS (Focal Fossa) 64 биттік; Ubuntu Server 18.04 LTS (Bionic Beaver) 64 биттік; CentOS 7.x 64 биттік; Red Hat Enterprise Linux server 8.x 64 биттік; Red Hat Enterprise Linux server 7.x 64 биттік; SUSE Linux Enterprise Server 12 (барлық жаңарту бумалары) 64 биттік; SUSE Linux Enterprise Server 15 (барлық жаңарту бумалары) 64 биттік; Astra Linux Special Edition 1.7 (жабық бағдарламалық жасақтама режимі мен мандат режимін қоса) 64 биттік; Astra Linux Special Edition 1.6 (режимді қосқанда 64-биттік; Astra Linux Common Edition 2.12 64-биттік; Linacle Linux 7 64 биттік; Linacle Linux 8 64 биттік; . Орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдары келесі виртуалды платформаларда орнатуды қолдауы керек: VMware vSphere 6.7; VMware vSphere 7.0; VMware Workstation 16 Pro; Microsoft Hyper-V Server 2012 64 бит; Microsoft Hyper-V Server 2012 R2 64 бит; Microsoft Hyper-V Server 2016 64 бит; Microsoft Hyper-V Server 2019 64 бит; Microsoft Hyper-V Server 2022 64 бит; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Parallels Desktop 17; келесі операциялық жүйелерді қолдайтын ядроға негізделген Виртуалды машина: Alt 8 SP сервері
--	---

	(LKNV.11100-01) 64-биттік; Astra Linux Special Edition 1.7 (тұйық бағдарламалық орта режимі мен мандат режимін қоса алғанда) 64-биттік; Debian GNU/Linux 11.x (Bullseye) 32 биттік / 64 биттік; Ubuntu Server 20.04 LTS (Focal Fossa) 64 биттік; РЕД ОС 7.3 Сервер 64-биттік; РЕД ОС 7.3 сертификатталған редакция 64-биттік; орталықтандырылған басқару, мониторинг және жаңартудың бағдарламалық құралдары мынадай нұсқалардың ДҚБЖ-мен жұмыс істеуі тиіс: MySQL 5.7 community 32-биттік/64-биттік; MySQL 8.0 32-биттік/64-биттік; MariaDB 10.5.x 32 биттік / 64 биттік; MariaDB 10.4.x 32 биттік/64 биттік; MariaDB 10.3.22 және одан жоғары 32 биттік/64 биттік; MariaDB Server 10.3 32 биттік/64 биттік InnoDB сақтау ішкі жүйесі бар; MariaDB 10.1.30 және одан жоғары 32 биттік / 64 биттік. Антивирустық қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: орталықтандырылған антивирустық қорғау бағдарламалық құралдарын орнату, жаңарту және жою; орталықтандырылған баптау, әкімшілендіру; қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау; саясат пен міндеттердің өзгеру тарихын сақтау, алдыңғы нұсқаларға кері қайтаруды орындау мүмкіндігі; қайта бөлу жүргізілетін триггерлер иерархиялары; жаңартуларды пайдаланушылардың жұмыс орындарына оларды алғаннан кейін бірден жеткізу; виртуалды машиналар желісінде тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме балансын бөлу; әкімшілер мен операторлардың құқықтарын, сондай-ақ әр деңгейде ұсынылатын есеп беру нысандарын теңшеу мүмкіндігі бар көп деңгейлі басқару жүйесін құру; еркін деңгейдегі әкімшілік серверлер иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі басқару серверлері үшін көп жалға алуды (multi-tenancy) қолдау; байланыс арналары арқылы да, машиналық ақпарат тасығыштар арқылы да әртүрлі көздерден бағдарламалық құралдар мен антивирустық базаларды жаңарту; басқару сервері арқылы антивирустық бағдарламалық қамтамасыз етуді өндірушінің бұлттық серверлеріне қол жеткізу; клиенттік компьютерлерге лицензияны автоматты түрде тарату; орнатылған антивирустық қорғау Қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы пошта хабарламаларын жіберуді баптау; белгіленген бағдарламаларды лицензиялау деректері бойынша антивирустық қорғау оқиғалары бойынша графикалық есептерді құру; жүйенің жұмысы туралы алдын ала конфигурацияланған стандартты есептердің болуы; есептерді PDF және XML форматындағы файлдарға экспорттау; антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша резервтік сақтау және карантин объектілерін орталықтандырылған басқару; басқару серверінде аутентификациялау үшін ішкі есептік жазбаларды құру; басқару жүйесінің кіріктірілген құралдарын басқару жүйесінің резервтік көшірмесін жасау; пайда болуын бақылау жүйесінің болуы вирустық эпидемиялар; web консолін пайдалана отырып, антивирустық қорғауды басқару;
--	--

басқару серверіне жүктемені азайту және кәсіпорын желісіндегі деректер трафигін оңтайландыру үшін басқару сервері арқылы да, тарату нүктелері арқылы да басқарылатын құрылғыларда антивирустық базалар мен бағдарламалық модульдерді жаңарту және тарату мүмкіндігі; Жаңартуларды тексеру тапсырмасы арқылы жүктелетін жаңартуларды басқарылатын құрылғыларға орнатпас бұрын өнімділік пен қателерді тексеру мүмкіндігі; антивирустық базалар мен бағдарламалық модульдерді жүктеу үшін айырмашылық файлдары мүмкіндігін пайдалану мүмкіндігі. 10. Антивирустық базаны жаңартуға қойылатын талаптар. Жаңартылатын антивирустық деректер базасы мынадай функционалдық мүмкіндіктердің іске асырылуын қамтамасыз етуі тиіс: күнтізбелік тәулік ішінде кемінде 24 рет антивирустық базаларды жаңарту қағидаларын құру; жаңарту жолдарының көптігі, оның ішінде – байланыс арналары бойынша және ақпараттың иеліктен шығарылатын электрондық жеткізгіштерінде; электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру. 11. 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, оның ішінде: «пайдаланушы (әкімші) нұсқаулығы» қамтылуға тиіс. Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғаныс құралын орнату, конфигурациялау және пайдалану процесін егжей-тегжейлі сипаттауы керек. 12. Әлеуетті өнім берушіге қойылатын талаптар: 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 хаттың түпнұсқасының электрондық көшірмесін ұсынуға тиіс. 13. Жеткізуші Тапсырыс берушінің кемінде 2 (екі) маманы үшін жеткізілетін антивирустық бағдарламалық қамтамасыз ету бойынша сертификат бере отырып оқыту курсын өткізуі тиіс. 14. Техникалық қолдауға қойылатын талаптар. Антивирустық бағдарламалық қамтамасыз етуді техникалық қолдау: техникалық қолдауды антивирустық бағдарламалық қамтамасыз етуді өндірушінің мамандары және оның серіктестері 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; әлеуетті өнім беруші электрондық пошта жүйесі арқылы нақты мәселелер бойынша сұрауларды жіберуді қамтитын бағдарламалық қамтамасыз ету өндірушісінің техникалық қолдауының электрондық ақпараттық жүйесіне қол жеткізуді қамтамасыз етуі тиіс; жоғарыда сипатталған қызметтерге қол жеткізу қолдау көрсетудің барлық уақыты ішінде тәулік бойы ашық болуы тиіс. Әлеуетті Жеткізуші Тапсырыс берушіге өндірушінің бағдарламалық өнімдерінде кездесетін мәселелер мен қателерді жеңу және шешу үшін техникалық

	ақпаратты және/немесе қосымша бағдарламалық компоненттерді алуды қамтамасыз етуі керек сондай-ақ, антивирустық бағдарламада кездесетін мәселелер мен қателерді жеңу және шешу үшін техникалық мамандарды жіберуі керек; Бағдарламалық жасақтамаға кепілдік беру және техникалық қолдау Тапсырыс берушінің қосымша шығындарынсыз қамтамасыз етілуі керек.Кепілдік қызмет көрсету және техникалық қолдау бағдарламалық қамтамасыз етудің орналасқан жері бойынша жүзеге асырылуы 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)	

**Техническая спецификация
закупаемых услуг
(заполняется заказчиком)**

Наименование заказчика	Государственное учреждение "Министерство юстиции Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство юстиции Республики Казахстан"
№ конкурса:	№ 17855106-1
Наименование конкурса:	Услуги по продлению лицензии и технической поддержки антивирусного программного обеспечения
Номер лота:	№ 87894823-OK2
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:	16821551.73
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	16821551.73
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 услуги продления лицензии и технической поддержки антивирусного программного обеспечения (далее АПО, далее - Услуга) для рабочих станций МЮ РК приведены следующие требования: в результате проведения закупок требуется продлить действующую лицензию с 7 декабря 2026 года антивирусного ПО KES FB Advanced для рабочих станций в количестве 1900 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 рабочих станций и серверов, централизованное управление. 1. Общие требования. АПО должны включать: программные средства антивирусной защиты для рабочих станций Windows; программные средства антивирусной защиты для рабочих станций MacOS; программные средства антивирусной защиты для рабочих станций и серверов Linux; программные средства антивирусной защиты для файловых серверов Windows; программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов); программные средства централизованного управления, мониторинга и обновления; обновляемые базы данных сигнатур вредоносных программ и атак; эксплуатационную документацию на русском языке. 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. 2. Требования к программным средствам антивирусной защиты для рабочих станций Windows. Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: Windows 7 Professional/Ultimate/Enterprise Service Pack 1 и выше (32/64-разрядная); Windows 8 Professional/Enterprise (32/64-разрядная); Windows 8.1 Professional/Enterprise (32/64-разрядная); Windows 10 Pro/Enterprise (32/64-разрядная); Windows 11 Pro (64-разрядная). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; антивирусное сканирование по расписанию; антивирусное сканирование подключаемых устройств; эвристического анализатора,
---	---

	позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; нейтрализации действий активного заражения; анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP; фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; блокировку баннеров и всплывающих окон на загружаемых Web-страницах; распознавания и блокировку фишинговых и небезопасных сайтов; встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений; создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; 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 Active Directory; управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств; записи в журнал событий о записи и/или удалении файлов на съемных дисках; назначение приоритета для правил доступа к устройствам с файловой системой; контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; защиты от атак типа BadUSB; защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля; установки только выбранных компонентов программного средства антивирусной защиты; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; запуска задач по расписанию и/или сразу после запуска приложения; гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; проверки целостности антивирусной программы; добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; импорта и экспорта списков правил и исключений в XML-формат; наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; наличие защищенного хранилища для отчетов о работе антивируса; включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей; интеграции с Windows Defender Security Center; наличие поддержки Antimalware Scan Interface (AMSI); наличие поддержки Windows Subsystem for Linux (WSL); наличие инструмента мониторинга сети по протоколам TCP и UDP; защитить паролем восстановление объектов из резервного хранилища; ограничения сетевого трафика в том случае, если подключение к интернету является лимитным; запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка
--	---

	UEFI-систем; восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем; поддержка двухфакторной аутентификации при полнодисковом шифровании; шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению); наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля; шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации; формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий). 3. Требования к программным средствам антивирусной защиты для физических серверов Windows. Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: Windows Small Business Server 2011 Essentials/Standard (64-разрядная); Windows MultiPoint Server 2011 (64-разрядная); Windows Server 2008 Standard/Enterprise Service Pack 2 (64-разрядная); Windows Server 2008 R2 Foundation/Standard/Enterprise Service Pack 1 (64-разрядная); Windows Server 2012 Foundation/Essentials/Standard (64-разрядная); Windows Server 2012 R2 Foundation/Essentials/Standard (64-разрядная); Windows Server 2016 Essentials/Standard (64-разрядная); Windows Server 2019 Essentials/Standard (64-разрядная); Windows Server 2022 Essentials/Standard (64-разрядная), Windows Server 2025 Essentials/Standard (64-разрядная). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; антивирусное сканирование по расписанию; антивирусное сканирование подключаемых устройств; эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; нейтрализации действий активного заражения; анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; встроенного
--	---

	сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей; установки только выбранных компонентов программного средства антивирусной защиты; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; запуск задач по расписанию и/или сразу после загрузки операционной системы; гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; проверки целостности антивирусной программы; добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; наличие защищенного хранилища для отчетов о работе антивируса; включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей; интеграции с Windows Defender Security Center; наличие поддержки Antimalware Scan Interface (AMSI); наличие поддержки Windows Subsystem for Linux (WSL); защитить паролем восстановление объектов из резервного хранилища; импорта и экспорта списков правил и исключений в XML-формат; ограничения сетевого трафика в том случае, если подключение к интернету является лимитным 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), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий); запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. 4. Требования к программным средствам антивирусной защиты для рабочих станций Mac. Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих
--	--

	под управлением операционных систем следующих версий: macOS 10.13, 10.14, 10.15 или 11.0; В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: резидентный антивирусный мониторинг; облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; автоматическое обновление антивирусных баз по расписанию; резервное копирование зараженных файлов перед их удалением, для возможности восстановления; эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы; защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные; блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты; проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик); контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем; ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault; возможность установки расширений из командной строки с помощью новой команды kav; возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций; возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены. 5. 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: CentOS 6.7 и выше; Debian GNU/Linux 10.1 и выше; Debian GNU/Linux 11; Mageia 4; Red Hat Enterprise Linux 6.7 и выше. Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий: Astra Linux Special Edition ПУСБ.10152-02 (очередное обновление 4.7); EulerOS 2.0 SP8; SUSE Linux Enterprise Server 15 SP3; Ubuntu 20.04 LTS. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: резидентного антивирусного мониторинга; облачной
--	--

	защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; проверку ресурсов доступных по SMB / NFS; возможность проверки памяти ядра; эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; антивирусное сканирование по команде пользователя или администратора и по расписанию; антивирусную проверку файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj.; проверку сообщений электронной почты в текстовом формате (Plain text); наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информации о проверенных и не измененных после проверки файлах); защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; включения опции блокирования файлов во время проверки; помещения подозрительных и поврежденных объектов на карантин; перехвата и проверки файловых операций на уровне SAMBA; управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; запуск задач по расписанию и/или сразу после загрузки операционной системы; экспортировать и сохранять отчеты в форматах HTML и CSV; гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; управления через пользовательский графический интерфейс без root прав; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли; управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения; проверки съемных дисков; отслеживания во входящем сетевом трафике активности, характерной для сетевых атак; проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым; получения данных о действиях программ на компьютере пользователя; получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация); создание файлов трассировки при запуске программы; получение информации обо всех исполняемых файлах программ, установленных на компьютерах; проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра; сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий. 6. 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: 32-разрядных операционных систем Microsoft Windows: Windows Server 2008 Standard/Enterprise/Datacenter с пакетом обновлений SP2 или выше; Windows Server 2008 Core Standard/Enterprise/Datacenter с пакетом обновлений SP2 или выше. 64-разрядных операционных систем Microsoft Windows: Windows Server 2008 Core Standard/Enterprise/Datacenter с пакетом обновлений SP2 или выше; Windows Server 2008 Standard/Enterprise/Datacenter с пакетом обновлений SP2 или выше; Microsoft Small Business Server 2008 Standard/Premium SP2 или выше; Windows Server 2008 R2 Foundation/Standard/Enterprise/Datacenter с пакетом обновлений SP1 или выше; Windows Server 2008 R2 Core Standard/Enterprise/Datacenter с пакетом обновлений SP1 или выше; Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; Microsoft Small Business Server 2011 Essentials/Standard SP1 или выше; Microsoft Windows MultiPoint Server 2011 Standard/Premium; Windows Server 2012 Foundation/Essentials/Standard/Datacenter; Windows Server 2012 Core Foundation/Essentials/Standard/Datacenter; Microsoft MultiPoint Server 2012 Standard/Premium; Windows Storage Server 2012; Windows Hyper-V Server 2012; Windows Server 2012 R2 Foundation/Essentials/Standard/Datacenter; Windows Server 2012 R2 Core Foundation/Essentials/Standard/Datacenter; Windows Storage Server 2012 R2; Windows Hyper-V Server 2012 R2; Windows Server 2016 Essentials/Standard/Datacenter; Windows Server 2016 MultiPoint; Windows Server 2016 Core Standard / Datacenter; Microsoft Windows MultiPoint Server 2016; Windows Storage Server 2016; Windows HyperV Server 2016; Windows Server 2019 Essentials / Standard / Datacenter; Windows Server 2019 Core; Windows Storage Server 2019; Windows Hyper-V Server 2019; Windows Server 2022 Foundation/Essentials/Standard/Datacenter (64-разрядная); Windows Server 2025 Foundation/Essentials/Standard/Datacenter (64-разрядная), Windows 10 Enterprise multi-session. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: 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; антивирусное сканирование по команде пользователя или администратора и по расписанию; запуск задач по расписанию и/или сразу после загрузки операционной системы; облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу; антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; 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 выполнения тех из них, которые признаются опасными; анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; проверки контейнеров Microsoft Windows; защиты от эксплуатации уязвимостей в памяти процессов; должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться; добавлять процессы в список защищаемых; ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; настройки проверки критических областей сервера в качестве отдельной задачи; регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач; продолжать антивирусное сканирование в фоновом режиме; наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий); 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; интеграции с SIEM системами; указания количества рабочих процессов антивируса вручную; отключить графический интерфейс; наличие удаленной и локальной консоли управления; управления параметрами антивируса из командной строки; централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак; 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; контроль устройств, в том числе сетевых карт и модемов; веб-контроль; защита от почтовых угроз (плагин для Outlook); защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления; 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); создания специальных правил должно контролировать приложения по пути
--	---

	нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме; создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы; 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; 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; информирование администратора о подключении внешних устройств; наличие механизмов автоматической генерации правил для контроля устройств и приложений. 7. Требования к программным средствам антивирусной защиты мобильных устройств. Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС: Android 5.0-13 (включая Android 12L, исключая Go Edition); iOS 10-16 или iPadOS 13-15. В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности: постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты; проверка файловой системы устройства по требованию и по расписанию; мгновенная проверка устанавливаемых приложений блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты; наличие хранилища для изолирования зараженных объектов; обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию; блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений; поддержка белых списков разрешенных приложений; блокировка системных приложений, в рамках контроля запуска приложений; отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM); заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства; указать параметры подключения к wi-fi сетям; указать обязательные к установке приложения; блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset); создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий; поддержка технологий Samsung KNOX1 и
--	---

	KNOX2. В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности: удаленной настройки параметров iOS MDM-устройств с помощью групповых политик; отправки команды блокирования и удаления данных; создавать групповые политики безопасности мобильных устройств; удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM; получать отчеты и статистику о работе мобильных устройств пользователей; блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode; централизованного управления с помощью единой консоли управления; наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве. 8. 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: Microsoft Windows 10 Enterprise 2015 LTSC 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 2016 LTSC 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная; Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная; Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная; Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная; Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная; Microsoft Windows 11 Pro 64-разрядная; Microsoft Windows 11 Enterprise 64-разрядная; Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная; Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная; Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
--	--

	Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная; Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная; Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная; Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная; Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная; Windows Server 2012 Server Core 64-разрядная; Windows Server 2012 Datacenter 64-разрядная; Windows Server 2012 Essentials 64-разрядная; Windows Server 2012 Foundation 64-разрядная; Windows Server 2012 Standard 64-разрядная; Windows Server 2012 R2 Server Core 64-разрядная; Windows Server 2012 R2 Datacenter 64-разрядная; Windows Server 2012 R2 Essentials 64-разрядная; Windows Server 2012 R2 Foundation 64-разрядная; Windows Server 2012 R2 Standard 64-разрядная; Windows Server 2016 Datacenter (LTSC) 64-разрядная; Windows Server 2016 Standard (LTSC) 64-разрядная; Windows Server 2016 (вариант установки Server Core) (LTSC) 64-разрядная; Windows Server 2019 Standard 64-разрядная; Windows Server 2019 Datacenter 64-разрядная; Windows Server 2019 Core 64-разрядная; Windows Server 2022 Standard 64-разрядная; Windows Server 2022 Core 64-разрядная; Windows Server 2025 Essentials/Standard (64-разрядная), Windows Storage Server 2012 64-разрядная; Windows Storage Server 2012 R2 64-разрядная; Windows Storage Server 2016 64-разрядная; Windows Storage Server 2019 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: VMware vSphere 6.7; VMware vSphere 7.0; VMware Workstation 16 Pro; Microsoft Hyper-V Server 2012 64-разрядная; Microsoft Hyper-V Server 2012 R2 64-разрядная; Microsoft Hyper-V Server 2016 64-разрядная; Microsoft Hyper-V Server 2019 64-разрядная; Microsoft Hyper-V Server 2022 64-разрядная; Citrix XenServer 7.1 LTSR; Citrix XenServer 8.x; Parallels Desktop 17; Oracle VM VirtualBox 6.x. Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: Microsoft SQL Server 2012 Express 64-разрядная; Microsoft SQL Server 2014 Express 64-разрядная; Microsoft SQL Server 2016 Express 64-разрядная; Microsoft SQL Server 2017 Express 64-разрядная; Microsoft SQL Server 2019 Express 64-разрядная; Microsoft SQL Server 2014 (все редакции) 64-разрядная; Microsoft SQL Server 2016 (все редакции) 64-разрядная; Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная; Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная; Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуется дополнительные действия); Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуется дополнительные действия); Microsoft Azure SQL Database; Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure; MySQL 5.7 Community 32-разрядная/64-разрядная; MySQL Standard Edition 8.0 (релиз 8.0.20 и выше)
--	---

	32-разрядная/64-разрядная; MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная; MariaDB 10.5.x 32-разрядная/64-разрядная; MariaDB 10.4.x 32-разрядная/64-разрядная; MariaDB 10.3.22 и выше 32-разрядная/64-разрядная; MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; MariaDB 10.1.30 и выше 32-разрядная/64-разрядная. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD; автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD; централизованные установка, обновление и удаление программных средств антивирусной защиты; централизованная настройка, администрирование; просмотр отчетов и статистической информации по работе средств защиты; централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки - возможность создать автономный пакет установки; 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; иерархии триггеров, по которым происходит перераспределение; тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения; распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; поддержка мультиарендности (multi-tenancy) для серверов управления; обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; доступ к облачным серверам производителя
--	---

	антивирусного ПО через сервер управления; автоматическое распространение лицензии на клиентские компьютеры; инвентаризация установленного ПО и оборудования на компьютерах пользователей; наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; функция управления мобильными устройствами через сервер Exchange ActiveSync; функция управления мобильными устройствами через сервер iOS MDM; отправки SMS-оповещений о заданных событиях; централизованная установка сертификатов на управляемые мобильные устройства; указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления; указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления; построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ; наличие преднастроенных стандартных отчетов о работе системы; экспорт отчетов в файлы форматов PDF и XML; централизованное управление объектами резервных хранилищ и карантин по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; создание внутренних учетных записей для аутентификации на сервере управления; создание резервной копии системы управления встроенными средствами системы управления; поддержка Windows Failover Clustering; поддержка интеграции с Windows сервисом Certificate Authority; наличие портала самообслуживания пользователей; портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; наличие системы контроля возникновения вирусных эпидемий; установки в облачной инфраструктуре Microsoft Azure и Google Cloud; интеграции по OpenAPI; управления антивирусной защитой с использованием WEB консоли; возможность управления развертыванием ОС Windows через консоль управления; наличие преднастроенных ролей пользователей средств централизованного управления; должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей; возможность подключения по RDP или штатными средствами из консоли управления; наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing) пользователю должен выводиться запрос на разрешение дистанционного подключения; наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal); должна быть обеспечена возможность добавления наборов драйверов в ранее созданный
--	---

	образ; возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС; возможность импортировать образ операционной системы из дистрибутивов (WIM); наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии; автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры; поддержка функциональности управления шифрованием данных; возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\LEEF; двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования; использования дополнительной аутентификация после изменения параметров учетной записи пользователя; возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами; автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей; возможность развернуть Сервер администрирования как систему высокой доступности; возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети. 9. 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: Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; Debian GNU/Linux 10.x (Buster) 32-разрядная/64-разрядная; Debian GNU/Linux 9.x (Stretch) 32-разрядная/64-разрядная; Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная; CentOS 7.x 64-разрядная; Red Hat Enterprise Linux Server 8.x 64-разрядная; Red Hat Enterprise Linux Server 7.x 64-разрядная; SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная; SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная; Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная; Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная; Astra Linux Common Edition 2.12 64-разрядная; Oracle Linux 7 64-разрядная; Oracle Linux 8 64-разрядная. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: VMware vSphere 6.7; VMware vSphere 7.0; VMware Workstation 16 Pro; Microsoft Hyper-V Server 2012 64-разрядная; Microsoft Hyper-V Server 2012 R2 64-разрядная; Microsoft Hyper-V Server 2016 64-разрядная; Microsoft Hyper-V Server 2019 64-разрядная; Microsoft Hyper-V Server 2022 64-разрядная; Citrix XenServer
--	---

	7.1 LTSR; Citrix XenServer 8.x; Parallels Desktop 17; Виртуальная машина на основе Kernel, поддерживающая следующие операционные системы: Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная; Debian GNU/Linux 11.x (Bullseye) 32-разрядная/64-разрядная; Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная; РЕД ОС 7.3 Сервер 64-разрядная; РЕД ОС 7.3 Сертифицированная редакция 64-разрядная; Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: MySQL 5.7 Community 32-разрядная/64-разрядная; MySQL 8.0 32-разрядная/64-разрядная; MariaDB 10.5.x 32-разрядная/64-разрядная; MariaDB 10.4.x 32-разрядная/64-разрядная; MariaDB 10.3.22 и выше 32-разрядная/64-разрядная; MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB; MariaDB 10.1.30 и выше 32-разрядная/64-разрядная. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: централизованные установка, обновление и удаление программных средств антивирусной защиты; централизованная настройка, администрирование; просмотр отчетов и статистической информации по работе средств защиты; сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям; иерархии триггеров, по которым происходит перераспределение; доставка обновлений на рабочие места пользователей сразу после их получения; распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; поддержка мультиарендности (multi-tenancy) для серверов управления; обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации; доступ к облачным серверам производителя антивирусного ПО через сервер управления; автоматическое распространение лицензии на клиентские компьютеры; наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ; наличие преднастроенных стандартных отчетов о работе системы; экспорт отчетов в файлы форматов PDF и XML; централизованное управление объектами резервных хранилищ и карантин по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; создание внутренних учетных записей для аутентификации на сервере управления; создание резервной копии системы управления встроенными средствами системы управления; наличие системы контроля возникновения
--	--

	вирусных эпидемий; управления антивирусной защитой с использованием WEB консоли; возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети; возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства; возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули. 10. Требования к обновлению антивирусных баз. Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток; множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; проверку целостности и подлинности обновлений средствами электронной цифровой подписи. 11. Требования к эксплуатационной документации. Эксплуатационная документация для 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. 12. Требования к потенциальному поставщику: Потенциальный Поставщик в составе конкурсной заявки должен предоставить электронную копию оригинала авторизационного письма от производителя поставляемого лицензионного программного обеспечения, подтверждающее официальные партнерские отношения с компанией-производителем или его полномочного представителя на территории Республики Казахстан, направленное в адрес Заказчика. Потенциальный 13. Поставщик 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. 14. Требования к технической поддержке. Техническая поддержка антивирусного программного обеспечения должна: 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; 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; доступ к вышеописанным службам должен быть открыт круглосуточно в течение всего времени
--	---

	оказания поддержки. 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; 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
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)	