

Конкурстық құжаттамаға сатып алынатын тауарлардың техникалық ерекшелігі

Сатып алудың нөмірі:	№ 17864339-1
Сатып алудың атауы:	Компьютерге арналған лицензияланған антивирус сатып алу
Лоттың нөмірі:	№ 88378614-ОИ2
Лоттың атауы:	Желілік қауіпсіздік жабдығы кешені
Лоттың сипаттауы:	таратылған шабуылдардан қорғау үшін, шапқыншылықтың, вирустар, әр түрлі қауіптер
Лоттың қысқаша сипаттауы:	Компьютерге арналған антивирус
Саны, көлемі:	130
Өлшем бірлігі:	Дана
Жеткізу орны:	231010000, Атырау облысы, Атырау қ. Атырау Гурьев к,7а
Жеткізу мерзімі:	Шартқа қол қойлып қазынашылық департаментінен тіркеуден өткеннен кейінгі 16 күнтізбелік күн ішінде, ал егер Өнім беруші отандық өндіруші болса – 60 күнтізбелік күн ішінде
Функционалдық, техникалық, сапалық және пайдалану мінездемесін сипаттау:	<p>Бағдарламалық жасақтаманы пайдалану құқығына лицензиялар беру жөніндегі қызметтерге техникалық сипаттама</p> <p>Осы техникалық сипаттамада лицензиялық вирусқа қарсы бағдарламалық жасақтаманы (бұдан әрі - ВҚБЖ, БЖ, ЛБЖ) пайдалану құқығына лицензиялар беру бойынша қызмет көрсетуге қойылатын негізгі талаптар келтірілген. Лицензиялардың қолданылу мерзімі кемінде 12 ай. Қызмет көрсету мерзімі: аумақтық қазынашылық органында шарт тіркелген сәттен бастап 20 жұмыс күні ішінде. Қажетті саны-360 лицензия. (антивирустық бағдарламалық жасақтамаға қол жеткізуді қажет ететін жұмыс станциялары мен серверлердің жалпы саны).</p> <p>Қызметтер болуы керек</p> <p>Осы конкурс бойынша қызметтер көрсету құқығын растау мақсатында БЖ өндіруші компаниядан Қазақстан Республикасының аумағында бағдарламалық жасақтаманы өндіруші компанияның авторизацияланған әріптесі ретінде лицензиялық БЖ беру құқығын растайтын авторизациялық хат ұсыну қажет. Хаттың электрондық көшірмесі конкурстық өтінім құрамында ұсынылуы тиіс. Қызметтер көрсету шеңберінде зиянды бағдарламалардан кешенді қорғау сервисі ұсынылады. Сервис келесі талаптарға сай болуы керек.</p> <p>1. Жалпы талаптар</p> <p>Вирусқа қарсы құралдар мыналарды қамтуы керек:</p> <ul style="list-style-type: none"> ● Windows жұмыс станцияларына арналған вирусқа қарсы бағдарламалық жасақтама; ● Windows файлдық серверлеріне арналған вирусқа қарсы бағдарламалық жасақтама; ● орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары; ● сигнатуралардың зиянды бағдарламалар мен шабуылдардың жаңартылатын дерекқорлары; <p>Басқару құралдарын қоса алғанда, барлық вирусқа қарсы құралдардың бағдарламалық интерфейсі қазақ және орыс тілдерінде болуы тиіс. Басқару құралдарын қоса алғанда, барлық вирусқа қарсы құралдардың мәнмәтіндік анықтамалық жүйесі болуы тиіс. Ұсынылып отырған вирусқа қарсы қорғау құралдары, оның ішінде отандық әзірлемелер ҚР СТ ISO/IEC 15408-3-2017 сәйкес 4-тен төмен емес сенімділіктің бағалау деңгейіне сәйкес келуі тиіс.</p> <p>Windows жұмыс станцияларына арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар</p> <p>Вирусқа қарсы қорғаудың бағдарламалық құралдары мынадай нұсқадағы жұмыс станциялары үшін операциялық жүйенің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:</p> <ul style="list-style-type: none"> ● Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 және одан жоғары; ● Windows 8 Professional / Enterprise (32 / 64-разрядтық); ● Windows 8.1 Professional / Enterprise (32 / 64-разрядтық); ● Windows 10 Home / Pro / жұмыс станцияларына арналған Pro / Education / Enterprise; ● Windows 11 Home / Pro / жұмыс станцияларына арналған Pro / Education / Enterprise;

Вирусқа қарсы қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- нақты уақыт режимінде және объектінің мәнмәтіндік мәзірінен сұрау салу бойынша вирусқа қарсы сканерлеу;
- кесте бойынша вирусқа қарсы сканерлеу;
- қосылатын құрылғыларды вирусқа қарсы сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш;
- белсенді жұқтыру әрекеттерін бейтараптандыру;
- қосымшаның мінез-құлқын және оның зиянды белсенділігін және санкцияланбаған әрекеттерді анықтау үшін жүйеде жүргізетін әрекеттерін талдау;
- желі бойынша қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін жалпы папкалар мен файлдарға жүгінулерді талдау;
- бағдарламалық жасақтамада осалдықтарды пайдаланатын зиянды бағдарламалардың іс-қимылдарын, оның ішінде жүйелік процестердің жадын қорғауды бұғаттау;
- емдеу кезінде зиянды бағдарламалық жасақтаманың іс-қимылдарының кері қайтарылуы, оның ішінде шифрланған, зиянды бағдарламалармен, файлдарды қалпына келтіру;
- процестер мен қосымшалар үшін артықшылықтарды шектеу (тізілімге жазу, файлдарға, дестелерге және басқа да процестерге қол жеткізу, тапсырмаларды жоспарлаушыға жүгіну, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т.б.), сенім деңгейін айқындай отырып, қосымшалардың динамикалық жаңартылатын теңшелетін тізімдері;
- қосымшаға нақты уақыт режимінде іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлтты қорғау;
- келесі форматтағы мұрағаттардағы файлдарды вирусқа қарсы тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- келесі хаттамалар бойынша берілетін кіріс және шығыс трафигін тексере отырып, электрондық поштаны зиянды бағдарламалардан қорғау: IMAP, SMTP, POP3, MAPI, NNTP;
- файлдардың берілген түрлерін қайта атау немесе жою мүмкіндігі бар пошта тіркемелерінің сүзгісі;
- пайдаланушының компьютеріне HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары бойынша, оның ішінде эвристикалық талдау арқылы келіп түсетін желілік трафикті сенімді ресурстарды теңшеу мүмкіндігімен және блоктау немесе статистика режимінде жұмыс істеумен тексеру;
- жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
- фишингтік және қауіпсіз емес файлдарды тану және бұғаттау;
- желілік сегменттерді санаттау мүмкіндігімен бағдарламаларға арналған желілік дестелік қағидалар мен желілік қағидаларды жасауға мүмкіндік беретін жапсарлас желілік экран;
- кез келген түрдегі есептеу желілеріндегі қосымшалар мен порттар үшін желілік экран ережелерін пайдалана отырып, желілік шабуылдардан қорғау;
- құрылғының MAC-мекенжайын қолдан жасау үшін ARP-хаттамасындағы осалдықтарды пайдаланатын желілік қатерлерден қорғау;
- бірнеше желілік қосылыстарды бір мезгілде орнатуды бұғаттау мүмкіндігімен желілік көпір түріндегі желілік қосылыстарды бақылау;
- барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау, компонент бағдарламаны табу жолы, метадеректер, сертификат немесе оның таңбасы, бақылау сомасы бойынша да, сондай-ақ бағдарламалық жасақтаманы өндіруші ұсынатын қосымшалардың алдын ала берілген санаттары бойынша да қосымшаларды бақылауы тиіс, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі тиіс;
- пайдаланушының құрылғының түрі және/немесе пайдаланылатын шина бойынша сыртқы енгізу/шығару құрылғыларымен, олардың сәйкестендіргіші бойынша сенімді құрылғылардың тізімін жасау мүмкіндігімен және Active Directory-дан белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану үшін артықшылықтар беру мүмкіндігімен жұмыс істеуін бақылау;
- құрылғыларды бақылау шеңберінде барлық немесе пайдаланушылар топтары үшін (Active Directory немесе жергілікті пайдаланушылар/топтар) осы үлгідегі құрылғыларға кіру ережелерін баптау және MTP құрылғыларын басқару;
- алмалы-салмалы дискілердегі файлдарды жазу және/немесе жою туралы оқиғалар журналына жазбалар;
- файл жүйесі бар құрылғыларға қол жеткізу ережелері үшін басымдық тағайындау;
- пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде

санаттарды қосу, редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші жасаған және динамикалық жаңартып отыратын санатқа, сондай-ақ ақпарат түріне (аудио, бейне және т.б.) қол жеткізуге нақты тыйым салуды немесе рұқсатты қосу, бақылаудың уақыт аралықтарын енгізуге, сондай-ақ оны Active Directory-ден белгілі бір пайдаланушыларға ғана тағайындауға мүмкіндік беру;

- BadUSB түріндегі шабуылдардан қорғау;
- қосымшаның сервисін қашықтықтан рұқсатсыз басқарудан қорғау, сондай-ақ құпия сөздің көмегімен қолданбаның параметрлеріне қол жеткізуді қорғау;
- сенімді қашықтан әкімшілендіру бағдарламалары арқылы параметрлерді басқару;
- вирусқа қарсы қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату;
- жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесінің көмегімен орталықтандырылған басқару;
- кесте бойынша және/немесе бағдарламаны іске қосқаннан кейін бірден тапсырмаларды іске қосу;
- файлдық кеңістікті сканерлеуді орындау кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- жағдайы өткен тексеруден бері өзгермеген объектілерді өткізу есебінен сканерлеу процесін жеделдету;
- вирусқа қарсы бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, атының/директориясының бетпердесі бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша вирусқа қарсы тексеруден ерекшеліктер қосу;
- вирусқа қарсы бағдарламада оларды қалпына келтіру мүмкіндігімен жойылған залалданған файлдар үшін қорғалған қойманың болуы;
- вирусқа қарсы бағдарламада жұмысы туралы есептер үшін қорғалған қойманың болуы;
- вирусқа қарсы бағдарламада графикалық интерфейсіні қосу және ажырату, сондай-ақ мүмкіндіктердің ең аз жиынтығымен графикалық интерфейстің оңайлатылған нұсқасының болуы;
- Windows Defender Security Center-мен бірігуі;
- Antimalware Scan Interface (AMSI) қолдауының болуы;
- резервтік қоймадан объектілерді қалпына келтіруді құпия сөзбен қорғау;
- интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
- TCP және UDP хаттамалары бойынша желіні бақылау құралының болуы;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- орнату мүмкіндігі тапсырманың орындалу ұзақтығын шектеу;
- егер тексеру орындалып жатса, тексеру міндеттерін кезекке қою мүмкіндігі.
- табылған осалдықтар бойынша есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу.
- арнайы жүктеу агентін құрып және Single Sign On технологиясын қолдайтын толық іздеу шифрлау, EFI-жүйелерді қолдау;
- жүктеу агенті немесе ОЖ файлдары істен шыққан жағдайда шифрланған мазмұнды қалпына келтіру, EFI жүйелерін қолдау;
- толық іздеу шифрлау кезінде қос факторлы анықтап тануды қолдау;
- шифрланатын мазмұнды икемді көрсету мүмкіндігімен файлдарды шифрлау (орналасқан жері бойынша, кеңейтім бойынша, файлды жасайтын қосымша бойынша);
- таңдалған қолданбалар тарапынан шифрланған файлдарға қол жеткізуді шектеу тетіктерінің болуы, сондай-ақ құпия сөзбен ұйымнан тыс файлдарды транскрипциялауға мүмкіндік беретін технологияның болуы;
- ұйым желісінен тыс файлдарды шифрлауға және шифрын ашуға мүмкіндік беретін жұмыс режимін орнату мүмкіндігімен алынбалы тасымалдағыштардағы деректерді шифрлау;
- мінез-құлық үлгісінен ауытқу кезінде бағдарламалардың мінез-құлық үлгісін қалыптастыру және олардың әрекеттерін бұғаттау мүмкіндігі (ауытқымаларды бейімделген бақылау)
- дискіні шифрлау кезінде анықтап тану агентінің қызметтік есептік жазбасын жасау мүмкіндігі;
- толық дискіні шифрлау кезінде SSO жұмыс істеуі үшін үшінші тарап adselfservice Plus тіркелгі деректерін жеткізушіні қолдау
- зиянкестердің жойылған ақпаратты рұқсатсыз қалпына келтіруінен қорғау
- жергілікті және сыртқы дискілерден қалпына келтірусіз деректерді жою мүмкіндігі
- жаңарту көзін таңдау мүмкіндігі. Оның ішінде құрылғыдағы жергілікті директориядан
- рұқсатсыз қалпына келтіруден қорғау үшін USB, жад карталары мен

мобильді құрылғыларды қоса алғанда, жергілікті дискілер мен сыртқы тасығыштардан деректерді қайтарымсыз жою.

Windows серверлеріне арналған вирусқа қарсы қорғау бағдарламалық құралдарына қойылатын талаптар

Вирусқа қарсы қорғаудың бағдарламалық құралдары файлдық серверлерге арналған операциялық жүйенің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

- Windows Small Business Server 2011 Essentials/Standard (64-разрядтық), Microsoft Small Business Server 2011 Standard (64-разрядтық) тек Microsoft Windows Server 2008 R2 үшін орнатылған Service Pack 1;
- Windows MultiPoint Server 2011 (64-разрядтық);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 және одан жоғары;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

Вирусқа қарсы қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

- нақты уақыт режимінде және объектінің мәнінің мәзірінен сұрау салу бойынша вирусқа қарсы сканерлеу;
- кесте бойынша вирусқа қарсы сканерлеу;
- қосылатын құрылғыларды вирусқа қарсы сканерлеу;
- бұрын белгісіз зиянды бағдарламаларды тануға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш;
- белсенді жұқтыру әрекеттерін бейтараптандыру;
- қосымшаның мінез-құлқын және оның зиянды белсенділігін және санкцияланбаған әрекеттерді анықтау үшін жүйеде жүргізетін әрекеттерін талдау;
- желі бойынша қол жетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін жалпы папкалар мен файлдарға жүгінулерді талдау;
- бағдарламалық жасақтамада осалдықтарды пайдаланатын зиянды бағдарламалардың іс-қимылдарын, оның ішінде жүйелік процестердің жадын қорғауды бұғаттау;
- емдеу кезінде зиянды бағдарламалық жасақтаманың іс-қимылдарының кері қайтарылуы, оның ішінде шифрланған, зиянды бағдарламалармен, файлдарды қалпына келтіру;
- қосымшаға нақты уақыт режимінде іске қосылатын бағдарлама немесе файл бойынша үкім алу үшін өндірушінің ресурстарына жүгінуге мүмкіндік беретін жаңа қатерлерден бұлтты қорғау;
- келесі форматтағы мұрағаттардағы файлдарды вирусқа қарсы тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- желілік сегменттерді санаттау мүмкіндігімен бағдарламаларға арналған желілік дестелік қағидалар мен желілік қағидаларды жасауға мүмкіндік беретін жапсарлас желілік экран;
- құрылғының MAC-мекенжайын қолдан жасау үшін ARP-хаттамасындағы осалдықтарды пайдаланатын желілік қатерлерден қорғау;
- қосымшаның сервисін қашықтықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, жәбірленушілер немесе білікті емес пайдаланушылар тарапынан қорғауды ажыратуды болдырмауға мүмкіндік беретін құпия сөздің көмегімен қосымшаның параметрлеріне қол жеткізуді қорғау;
- вирусқа қарсы қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату;
- жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесінің көмегімен орталықтандырылған басқару;
- кесте бойынша және/немесе операциялық жүйені жүктегеннен кейін бірден тапсырмаларды іске қосу;
- файлдық кеңістікті сканерлеуді орындау кезінде пайдаланушылардың ыңғайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
- жағдайы өткен тексеруден бері өзгермеген объектілерді өткізу есебінен сканерлеу процесін жеделдету;
- вирусқа қарсы бағдарламаның тұтастығын тексеру;
- файлдың бақылау сомасы, атының/директориясының бетпердесі бойынша немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша вирусқа қарсы тексеруден ерекшеліктер қосу;
- вирусқа қарсы бағдарламада оларды қалпына келтіру мүмкіндігімен жойылған залалданған файлдар үшін қорғалған қойманың болуы;
- вирусқа қарсы бағдарламада жұмысы туралы есептер үшін қорғалған қойманың болуы;
- вирусқа қарсы бағдарламада графикалық интерфейсін қосу және ажырату, сондай-ақ мүмкіндіктердің ең аз жиынтығымен графикалық

интерфейстің оңайлатылған нұсқасының болуы;

- Windows Defender Security Center-мен бірігуі;
- Antimalware Scan Interface (AMSI) қолдауының болуы;
- нысандарды сақтық қоймадан қалпына келтіруді құпия сөзбен қорғау.
- интернет байланысы шектеулі болған жағдайда желілік трафиктің шектеулері;
- барлық немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы ережелер жасау, компонент бағдарламаны табу жолы, метадеректер, сертификат немесе оның таңбасы, бақылау сомасы бойынша да, сондай-ақ бағдарламалық жасақтаманы өндіруші ұсынатын қосымшалардың алдын ала берілген санаттары бойынша да қосымшаларды бақылауы тиіс, компонент қара немесе ақ тізім режимінде, сондай-ақ статистиканы жинау немесе бұғаттау режимінде жұмыс істеуі тиіс;
- мінез-құлық үлгісінен ауытқу кезінде бағдарламалардың мінез-құлық үлгісін қалыптастыру және олардың әрекеттерін бұғаттау мүмкіндігі (ауытқымаларды бейімделген бақылау)
- табылған осалдықтар бойынша есеп беру мүмкіндігімен компьютерде орнатылған қосымшалардағы осалдықтарды анықтау және жабу үшін арнайы тапсырманы іске қосу.
- компоненттерді қолдау Веб-қатерлерден қорғау, Пошталық қатерлерден қорғау, Веб-бақылау және серверлер үшін Windows операциялық жүйесі басқаратын компьютерлерге арналған құрылғыларды бақылау;
- тексеру үзілген жерден қайта жүктелгеннен кейін тексеру тапсырмасын жалғастыру;
- тапсырманың орындалу ұзақтығына шектеу қою мүмкіндігі;
- егер тексеру орындалып жатса, тексеру міндеттерін кезекке қою мүмкіндігі.
- жаңарту көзін таңдау мүмкіндігі. Оның ішінде құрылғыдағы жергілікті директориядан

Windows ОЖ негізіндегі орталықтандырылған басқару, бақылау және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардың операциялық жүйелерін басқаратын компьютерлерде жұмыс істеуі керек:

- Microsoft Windows 10 Enterprise 2015 LTSC 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 2016 LTSC 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro 19H1 32-разрядтық/64-разрядтық;
- 19H1 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 19H1 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 19H1 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro 19H2 32-разрядтық/64-разрядтық;
- 19H2 жұмыс станцияларына арналған Microsoft Windows 10 Pro 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 19H2 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 19H2 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядтық/64-

разрядтық;

- Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядтық/64-разрядтық;
- Microsoft Windows 11 Home 64-разрядтық;
- Microsoft Windows 11 Pro 64-разрядтық;
- Microsoft Windows 11 Enterprise 64-разрядтық;
- Microsoft Windows 11 Education 64-разрядтық;
- Microsoft Windows 8.1 Pro 32-разрядтық/64-разрядтық;
- Microsoft Windows 8.1 Enterprise 32-разрядтық/64-разрядтық;
- Microsoft Windows 8 Pro 32-разрядтық/64-разрядтық;
- Microsoft Windows 8 Enterprise 32-разрядтық/64-разрядтық;
- Microsoft Windows 7 Professional Service Pack 1 32-разрядтық/64-разрядтық;

- Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядтық/64-разрядтық;
- Windows Server 2008 R2 with Standard Service Pack 1 және одан жоғары 64-разрядтық;

- Windows Server 2008 R2 Service Pack 1 (барлық редакциялары) 64-разрядтық;
- Windows Server 2012 Server Core 64-разрядтық;
- Windows Server 2012 Datacenter 64-разрядтық;
- Windows Server 2012 Essentials 64-разрядтық;
- Windows Server 2012 Foundation 64-разрядтық;
- Windows Server 2012 Standard 64-разрядтық;
- Windows Server 2012 R2 Server Core 64-разрядтық;
- Windows Server 2012 R2 Datacenter 64-разрядтық;
- Windows Server 2012 R2 Essentials 64-разрядтық;
- Windows Server 2012 R2 Foundation 64-разрядтық;
- Windows Server 2012 R2 Standard 64-разрядтық;
- Windows Server 2016 Datacenter (LTSC) 64-разрядтық;
- Windows Server 2016 Standard (LTSC) 64-разрядтық;
- Windows Server 2016 (Server Core орнату нұсқасы) (LTSC) 64-разрядтық;
- Windows Server 2019 Standard 64-разрядтық;
- Windows Server 2019 Datacenter 64-разрядтық;
- Windows Server 2019 Core 64-разрядтық;
- Windows Server 2022 Standard 64-разрядтық;
- Windows Server 2022 Datacenter 64-разрядтық;
- Windows Server 2022 Core 64-разрядтық;
- Windows Storage Server 2012 64-разрядтық;
- Windows Storage Server 2012 R2 64-разрядтық;
- Windows Storage Server 2016 64-разрядтық;
- Windows Storage Server 2019 64-разрядтық;

Орталықтандырылған басқарудың, мониторингтің және жаңартудың бағдарламалық құралдары келесі виртуалды платформаларда орнатуды қолдауы тиіс:

- VMware vSphere 6.7;
- VMware vSphere 7.0;
- VMware Workstation 16 Pro;
- Microsoft Hyper-V Server 2012 64-разрядтық;
- Microsoft Hyper-V Server 2012 R2 64-разрядтық;
- Microsoft Hyper-V Server 2016 64-разрядтық;
- Microsoft Hyper-V Server 2019 64-разрядтық;
- Microsoft Hyper-V Server 2022 64-разрядтық;
- Citrix XenServer 7.1 LTSR;
- Citrix XenServer 8.x;
- Parallels Desktop 17;
- Oracle VM VirtualBox 6.x.

Орталықтандырылған басқарудың, мониторингтің және жаңартудың бағдарламалық құралдары ДҚБЖ-мен мынадай нұсқаларда жұмыс істеуі тиіс:

- Microsoft SQL Server 2012 Express 64-разрядтық;
- Microsoft SQL Server 2014 Express 64-разрядтық;
- Microsoft SQL Server 2016 Express 64-разрядтық;
- Microsoft SQL Server 2017 Express 64-разрядтық;

- Microsoft SQL Server 2019 Express 64-разрядтық;
 - Microsoft SQL Server 2014 (барлық редакциялар) 64-разрядтық;
 - Microsoft SQL Server 2016 (барлық редакциялар) 64-разрядтық;
 - Microsoft SQL Server 2017 (барлық редакциялар) Windows үшін 64-разрядтық;
 - Microsoft SQL Server 2017 (барлық редакциялар) үшін Linux 64-разрядтық;
 - Microsoft SQL Server 2019 (барлық редакциялар) Windows үшін 64-разрядтық (қосымша әрекеттер қажет);
 - Microsoft SQL Server 2019 (барлық редакциялар) Linux үшін 64-разрядтық (қосымша әрекеттер қажет);
 - MySQL 5.7 Community 32-разрядтық/64-разрядтық;
 - MySQL Standard Edition 8.0 (8.0.20 релиз және одан жоғары) 32-разрядтық/64-разрядтық;
 - MySQL Enterprise Edition 8.0 (8.0.20 релиз және одан жоғары) 32-разрядтық/64-разрядтық;
 - MariaDB 10.3.22 және одан жоғары 32-разрядтық/64-разрядтық;
 - MariaDB Server 10.3 32-разрядтық/64-разрядтық InnoDB қоймасының кіші жүйесімен;
 - MariaDB Galera Cluster 10.3 32-разрядтық/64-разрядтық InnoDB қоймасының кіші жүйесімен.
- Вирусқа қарсы қорғаудың бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:
- қорғалатын тораптардың санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату құрылымын таңдау;
 - ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory-дан ақпаратты оқу;
 - анықталған компьютерлерді IP мекенжайы, ОЖ түрі, OU AD орналасқан жері бойынша тасымалдау ережелерінің баптаулары;
 - желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автоматты түрде бөлу; IP мекенжайы, ОЖ түрі, OU AD-да болу бойынша тасымалдау ережелерін баптау мүмкіндігі;
 - вирусқа қарсы қорғаудың бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою;
 - орталықтандырылған теңшеу, әкімшілендіру;
 - қорғау құралдарының жұмысы бойынша есептер мен статистикалық ақпаратты қарау;
 - басқару орталығының құралдарымен үйлеспейтін қосымшаларды орталықтандырылған жою (қолмен және автоматты);
 - саясат пен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға оралу мүмкіндігі;
 - пайдаланушы жүйеге кірген есептік жазбаға, ағымдағы IPv4 мекенжайына, сондай-ақ компьютердің қандай OU-да немесе қауіпсіздік тобында болуына байланысты вирусқа қарсы шешімнің баптауларын қайта анықтайтын арнайы триггерлердің қауіпсіздік саясатындағы нұсқаулар;
 - қайта бөлу орын алатын триггерлердің иерархиялары;
 - клиенттік машиналарға тарату алдында орталықтандырылған басқару БЖ құралдарымен жүктелген жаңартуларды тестілеу;
 - жаңартуларды пайдаланушылардың жұмыс орындарына оларды алғаннан кейін бірден жеткізу;
 - виртуалды машиналар желісінде анықтап тану және егер бұл машиналар бір физикалық серверде болса, олардың арасында іске қосылатын тапсырмалардың жүктеме теңгерімін бөлу;
 - әкімшілер мен операторлардың құқықтарын, сондай-ақ әр деңгейде ұсынылатын есептілік нысандарын теңшеу мүмкіндігімен көп деңгейлі басқару жүйесін құру;
 - еркін деңгейдегі басқару серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
 - басқару серверлері үшін көп жалға алуды қолдау (multi-tenancy);
 - байланыс арналары арқылы да, машиналық ақпарат тасығыштарда да әртүрлі көздерден бағдарламалық құралдар мен вирусқа қарсы базаларды жаңарту;
 - басқару сервері арқылы вирусқа қарсы БЖ өндірушінің бұлтты серверлеріне қол жеткізу;
 - клиенттік компьютер лицензиясын автоматты түрде тарату;
 - пайдаланушылардың компьютерлерінде орнатылған БЖ мен жабдықтарды түгендеу;
 - вирусқа қарсы қорғаудың белгіленген қосымшаларының жұмысында оқиғалар туралы хабарлау және олар туралы пошта хабарламаларын жіберуді баптау тетігінің болуы;
 - басқару жүйесіне желілік жүктемені төмендету үшін жаңартуларды ретрансляциялау орталығымен ұйымның кез келген компьютерін көрсету;
 - ұйымның кез келген компьютерін вирусқа қарсы агенттердің оқиғаларын жіберу орталығы, клиенттік компьютерлердің таңдалған тобы басқару жүйесіне желілік жүктемені төмендету үшін орталықтандырылған басқару

серверіне көрсету;

- вирусқа қарсы қорғау оқиғалары, түгендеу деректері, белгіленген бағдарламаларды лицензиялау деректері бойынша графикалық есептерді құру;
- жүйенің жұмысы туралы алдын ала бапталған стандартты есептердің болуы;
- есептерді PDF, HTML, XML форматындағы файлдарға экспорттау;
- вирусқа қарсы бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстары бойынша сақтық қоймалар мен карантиндер объектілерін орталықтандырылған басқару;
- басқару серверінде анықтап тану үшін ішкі есептік жазбаларды құру;
- басқару жүйесінің кірістірілген құралдарын басқару жүйесінің сақтық көшірмесін жасау;
- Windows Certificate Authority қызметімен бірігуді қолдау;
- вирустық эпидемиялардың пайда болуын бақылау жүйесінің болуы;
- OpenAPI бойынша бірігу;
- WEB консолін пайдалана отырып, вирусқа қарсы қорғауды басқару;
- орталықтандырылған басқару құралдарын пайдаланушылардың алдын ала бапталған рөлдерінің болуы;
- пайдаланушылардың есептік жазбаларына байланыстыру үшін нақты көрсетілген өкілеттіктер жиынтығымен мамандандырылған рөлдерді құру мүмкіндігі іске асырылуы тиіс
- басқару консолінен RDP немесе штаттық құралдар арқылы қосылу мүмкіндігі;
- Windows жұмыс үстеліне (Windows Desktop Sharing) ортақ қосылу мүмкіндігінің болуы;
- пайдаланушыға қашықтан қосылуға рұқсат сұрауы көрсетілуі керек;
- лицензияны пайдаланудың бұзылуы немесе лицензияның қолданылу мерзімінен асып кетуі туралы әкімшіге хабарлау мүмкіндігімен компьютерде орнатылған бөгде БЖ лицензияларын бақылау жүйесінің болуы;
- деректерді шифрлауды басқару функционалдығын қолдау;
- SIEM жүйелерімен интеграциялану мүмкіндігі және оқиғаларды syslog немесе CEF\LEEF форматында беру
- IPv6 және IPv4-мекенжайлармен жұмыс істеу және IPv6-мекенжайлары бар құрылғылары бар желілерден пікіртерім алу мүмкіндігі.
- пайдаланушылардың компьютерлерінде орнатылған қолданбалар мен операциялық жүйеде осалдықтарды автоматтандырылған іздеу және жабу;
- жаңартуларды орнату және оқшауланған желідегі үшінші тарап бағдарламаларының (Microsoft бағдарламаларынан басқа) осалдықтарын жабу мүмкіндігі.

2. Вирусқа қарсы базаларды жаңартуға қойылатын талаптар
 Жаңартылатын вирусқа қарсы дерекқорлар мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс:

- күнтізбелік тәулік ішінде кемінде 24 рет вирусқа қарсы базаларды жаңарту қағидаларын жасау;
- жаңарту жолдарының көптігі, оның ішінде - байланыс арналары бойынша және иеліктен шығарылатын электрондық ақпарат тасығыштарда;
- электрондық цифрлық қолтаңба құралдарымен жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

3. Пайдалану құжаттамасына қойылатын талаптар
 Басқару құралдарын қоса алғанда, вирусқа қарсы қорғаудың барлық бағдарламалық өнімдеріне арналған пайдалану құжаттамасы мынадай құжаттарды қамтуы тиіс:
 «Пайдаланушы (әкімші) нұсқаулығы»
 Вирусқа қарсы құралдармен жеткізілетін құжаттама вирусқа қарсы қорғаныстың тиісті құралын орнату, баптау және пайдалану процесін егжей-тегжейлі сипаттауы тиіс.

4. Техникалық қолдауға қойылатын талаптар
 Вирусқа қарсы бағдарламалық жасақтаманы техникалық қолдау:

- Вирусқа қарсы қорғаныс құралдарын өндірушінің және оның серіктестерінің сертификатталған мамандары телефон, электрондық пошта және Интернет арқылы қазақ және орыс тілдерінде ұсынылады.

Техническая спецификация закупаемых товаров к конкурсной документации

Номер закупки:	№ 17864339-1
Наименование закупки:	Приобретение лицензионного антивируса для компьютера
Номер лота:	№ 88378614-ОИ2
Наименование лота:	Комплекс оборудования сетевой безопасности
Описание лота:	для защиты от распределенных атак, вторжений, вирусов, угроз различного типа
Дополнительное описание лота:	Антивирус для компьютера
Количество:	130
Единица измерения:	Штука
Места поставки:	231010000, Атырауская область, г.Атырау Атырау ул.Гурьевская, 7а
Срок поставки:	В течение 16 календарных дней после подписания и регистрации договора в органах Казначейства, в случае если Поставщик отечественный товаропроизводитель 60 календарных дней
Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров:	<p>Техническая спецификация на услуги по предоставлению лицензий на право использования программного обеспечения</p> <p>В настоящей технической спецификации приведены основные требования к оказанию услуги по предоставлению лицензий на право использования лицензионного антивирусного программного обеспечения (далее - АПО, ПО, ЛПО). Срок действия лицензий не менее 12 месяцев. Срок оказания услуги: в течение 20 рабочих дней. Необходимое количество – 82 лицензий. (общее количество рабочих станций и серверов, для которых необходимо предоставить доступ к антивирусному программному обеспечению).</p> <p>В целях подтверждения права на оказание услуг по настоящему конкурсу необходимо предоставить авторизационное письмо от компании – производителя программного обеспечения, подтверждающее право на предоставление лицензионного ПО в качестве авторизованного партнера компании производителя ПО на территории Республики Казахстан. Электронная копия письма должна быть предоставлена в составе конкурсной заявки.</p> <p>В рамках оказания услуг предоставляется сервис комплексной защиты от вредоносных программ. Сервис должен отвечать следующим требованиям.</p> <p>1. Общие требования</p> <p>Антивирусные средства должны включать:</p> <ul style="list-style-type: none"> • программные средства антивирусной защиты для рабочих станций Windows; • программные средства антивирусной защиты для файловых серверов Windows; • программные средства централизованного управления, мониторинга и обновления; • обновляемые базы данных сигнатур вредоносных программ и атак; <p>Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на казахском и русском языках.</p> <p>Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой.</p> <p>Предлагаемые средства антивирусной защиты, в том числе отечественной разработки, должна соответствовать оценочному уровню доверия не ниже 4, согласно СТ РК ISO/IEC 15408-3-2017.</p> <p>Требования к программным средствам антивирусной защиты для рабочих станций Windows</p> <p>Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:</p> <ul style="list-style-type: none"> • Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше; • Windows 8 Professional / Enterprise (32 / 64-разрядная); • Windows 8.1 Professional / Enterprise (32 / 64-разрядная); • Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise; • Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise <p>В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:</p>

- 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 веб-ресурсов;
- 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;
- управления параметрами через доверенные программы удаленного администрирования;
- 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;
- 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);
- защитить паролем восстановление объектов из резервного хранилища;
- ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
- наличие инструмента мониторинга сети по протоколам TCP и UDP;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничение длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется.
- 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 сбоя 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;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
- поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании
- защита от несанкционированного восстановления удаленной информации злоумышленниками
- возможность удалять данные без возможности восстановления с локальных и внешних дисков
- возможность выбора источника обновления. В том числе из локальной директории на устройстве
- безвозвратное удаление данных с локальных дисков и внешних носителей, включая USB, карты памяти и мобильные устройства, для защиты от несанкционированного восстановления.

Требования к программным средствам антивирусной защиты для 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), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;
- Windows MultiPoint Server 2011 (64-разрядная);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
- Windows Server 2016 Essentials / Standard / Datacenter;
- Windows Server 2019 Essentials / Standard / Datacenter;
- Windows Server 2022.

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);
- защитить паролем восстановление объектов из резервного хранилища.
- 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;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов;
- возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
- возможность установки ограничения длительности выполнения задачи;
- возможность ставить задачи проверки в очередь, если проверка уже выполняется.
- возможность выбора источника обновления. В том числе из локальной директории на устройстве.

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 Education 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 Education 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 Education 19H2 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H1 (May 2020 Update) 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 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 20H2 (October 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 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 10 Home 21H1 (May 2021 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 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

- Microsoft Windows 10 Home 21H2 (October 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 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
- Microsoft Windows 11 Home 64-разрядная;
- Microsoft Windows 11 Pro 64-разрядная;
- Microsoft Windows 11 Enterprise 64-разрядная;
- Microsoft Windows 11 Education 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 Datacenter 64-разрядная;
- Windows Server 2022 Core 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);
- 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 10.3.22 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.

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;
 - 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;
 - 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, HTML, XML;
 - централизованное управление объектами резервных хранилищ и карантинных 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 интеграции с Windows сервисом Certificate Authority;
- наличие системы контроля возникновения вирусных эпидемий;
- интеграции по OpenAPI;
- управления антивирусной защитой с использованием WEB консоли;
- 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 системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF
- 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 устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.

2. 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.

3. Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать следующие документы:

«Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

4. Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

- Предоставляться на казахском и русском языках сертифицированными специалистами производителя средств антивирусной защиты и его партнеров по телефону, электронной почте и через Интернет.