ТЕХНИКАЛЫҚ СИПАТТАМА

1267903 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № 1 (35-1 У, 4574361) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: Товарищество с ограниченной ответственностью "Өскемен Энерго"
Ұйымдастырушы: Товарищество с ограниченной ответственностью "Өскемен Энерго"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	35-1 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	Бағдарламалық жасақтаманы пайдалану құқығына лицензия (антивирус)
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Шығыс Қазақстан облысы, Өскемен Қ.Ә., Өскемен қ., проспект Ильяса Есенберлина 43, блок 2
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 15 жұмыс күніішінде
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

Жұмыс станциялары мен серверлерді антивирустық қорғауға арналған бағдарламалық қамтамасыз етудің техникалық сипаттамасы:

Антивирустық қорғау (АҚ) жұмыс станциялары мен серверлердің желіде тұрақты жұмыс істеуін қамтамасыз ететін корпоративтік шешім болуы тиіс. Бүкіл ұйым шеңберінде бірыңғай антивирустық құралдар пайдаланылуы тиіс.

Осы Техникалық сипаттама антивирустық қорғау жүйесін енгізу бойынша ілеспе қызметтерді көрсете отырып, жеткізілетін бағдарламалық қамтамасыз етуге қойылатын талаптарды белгілейтін негізгі құжат болып табылады. Жүйенің барлық компоненттері бір-бірімен толық интеграциялануы тиіс.

Бағдарламалық қамтамасыз етуге және әлеуетті өнім берушіге қойылатын талаптар осы техникалық сипаттамада көрсетілген. Ұсынылатын қызметтердің барлық сипаттамалары осы техникалық сипаттамада көрсетілген ең төменгі техникалық сипаттамаларға сәйкес келуі немесе олардан жоғары болуы тиіс.

Антивирустық қорғауға арналған бағдарламалық қамтамасыз етуге қойылатын жалпы талаптар:

1. Қорғалатын тораптардың жалпы саны: **38**

2. Лицензияның қолданылу мерзімі: бағдарламалық қамтамасыз етуге лицензиялар жасалған сәттен бастап **кемінде 12 ай**

2.1 Антивирустық қорғауға арналған бағдарламалық қамтамасыз етуге қойылатын техникалық талаптар:

Антивирустық құралдар мыналарды қамтуы тиіс:

1. Windows жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары.
2. Linux жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары.
3. Windows файлдық серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары.
4. Кәсіпорын ауқымындағы серверлер мен Windows терминалдық серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары.
5. Мобильді құрылғыларға арналған антивирустық қорғаудың бағдарламалық құралдары.
6. Орталықтандырылған басқару, мониторинг жүргізу және жаңарту бағдарламалық құралдары.
7. Зиянды бағдарламалар мен шабуылдар сигнатураларының жаңартылатын дерекқорлары.
8. Орыс тіліндегі пайдалану құжаттамасы.
9. Басқару құралдарын қоса алғанда, барлық антивирустық құралдардың бағдарламалық интерфейсі орыс тілінде болуы тиіс.
10. Басқару құралдарын қоса алғанда, барлық антивирустық құралдарда орыс тіліндегі контекстік анықтамалық жүйе болуы тиіс.

2.2 Windows жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын т алаптар:

Антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы жұмыс станцияларына арналған операциялық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Windows 7 Home / Professional / Enterprise (32 / 64-разрядты);
2. Windows 8 Professional / Enterprise (32 / 64-разрядты);
3. Windows 8.1 Professional / Enterprise (32 / 64-разрядты);
4. Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядты);
5. Windows 11 Pro / Enterprise (32 / 64-разрядты).

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу;
2. Кесте бойынша антивирустық сканерлеу;
3. Қосылатын құрылғыларды антивирустық сканерлеу;
4. Бұрын белгісіз болған зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыштың болуы;
5. Белсенді жұқтыру әрекеттерін бейтараптандыру;
6. Қосымшаның мінез-құлқын және оның жүйеде орындайтын әрекеттерін талдау арқылы зиянды белсенділікті анықтау және рұқсат етілмеген әрекеттерді айқындау;
7. Желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ бумалар мен файлдарға жүгінулерді талдау;
8. Бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау; емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалар шифрлаған файлдарды қалпына келтіру; процестер мен қосымшалардың артықшылықтарын шектеу (тізілімге жазу, файлдарға, бумаларға және басқа процестерге қол жеткізу, тапсырмаларды жоспарлаушыға жүгіну, құрылғыларға қол жеткізу, объектілерге құқықтарды өзгерту және т.б.); сенім деңгейін анықтайтын, динамикалық түрде жаңартылатын және бапталатын қосымшалар тізімдері; іске қосылатын бағдарлама немесе файл бойынша қорытынды алу үшін қосымшаның нақты уақыт режимінде өндірушінің ресурстарына жүгінуіне мүмкіндік беретін жаңа қауіптерден бұлттық қорғау;

9. Келесі форматтардағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
10. Келесі хаттамалар арқылы берілетін кіріс және шығыс трафикті тексере отырып, электрондық поштаны зиянды бағдарламалардан қорғау: IMAP, SMTP, POP3, MAPI, NNTP;
11. Белгіленген файл түрлерінің атауын өзгерту немесе оларды жою мүмкіндігі бар пошта тіркемелерінің сүзгісі;
12. Пайдаланушының компьютеріне HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP хаттамалары арқылы келіп түсетін желілік трафикті, оның ішінде эвристикалық талдау көмегімен тексеру, сенімді ресурстарды баптау және бұғаттау немесе статистика режимінде жұмыс істеу мүмкіндігімен;
13. Жүктелетін веб-беттердегі баннерлер мен қалқымалы терезелерді бұғаттау;
14. Фишингтік және қауіпті сайттарды анықтау және бұғаттау, желілік сегменттерді санаттарға бөлу мүмкіндігімен бағдарламаларға арналған желілік пакеттік қағидалар мен желілік қағидаларды жасауға мүмкіндік беретін кіріктірілген желілік экран;
15. Кез келген типтегі есептеу желілерінде қосымшалар мен порттарға арналған желілік экран қағидаларын пайдалана отырып, желілік шабуылдардан қорғау;
16. Құрылғының MAC-мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау; бірнеше желілік қосылымның бір мезгілде орнатылуын бұғаттау мүмкіндігімен «желілік көпір» түріндегі желілік қосылымдарды бақылау;
17. Барлық пайдаланушылар немесе белгілі бір пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін бағдарламаларды орнатуға және/немесе іске қосуға тыйым салатын немесе рұқсат беретін арнайы қағидаларды жасау; компонент қосымшаларды бағдарламаның орналасу жолы, метадеректер, сертификат немесе оның таңбасы, бақылау сомасы бойынша, сондай-ақ бағдарламалық қамтамасыз ету өндірушісі ұсынатын алдын ала белгіленген қосымшалар санаттары бойынша бақылауы тиіс; компонент қара немесе ақ тізім режимінде, сондай-ақ статистика жинау немесе бұғаттау режимінде жұмыс істеуі тиіс;
18. Пайдаланушының сыртқы енгізу/шығару құрылғыларымен жұмысын құрылғы түрі және/немесе пайдаланылатын шина бойынша бақылау, олардың идентификаторы бойынша сенімді құрылғылар тізімін жасау және Active Directory жүйесіндегі белгілі бір пайдаланушыларға сыртқы құрылғыларды пайдалану артықшылықтарын беру мүмкіндігімен;
19. Құрылғыларды бақылау шеңберінде MTP құрылғыларын басқару және осы типтегі құрылғыларға барлық пайдаланушылар немесе пайдаланушылар топтары (Active Directory немесе жергілікті пайдаланушылар/топтар) үшін қол жеткізу қағидаларын баптау;
20. Алынбалы дискілерге файлдарды жазу және/немесе жою туралы оқиғаларды журналға тіркеу;
21. Файлдық жүйесі бар құрылғыларға қол жеткізу қағидаларына басымдық тағайындау;
22. Пайдаланушының Интернет желісімен жұмысын бақылау, оның ішінде санаттарды қосу және редакциялау, белгілі бір мазмұндағы ресурстарға, өндіруші қалыптастыратын және динамикалық түрде жаңартып отыратын санаттарға, сондай-ақ ақпарат түрлеріне (аудио, бейне және т.б.) қол жеткізуге тікелей тыйым салу немесе рұқсат беру; бақылаудың уақыт аралықтарын белгілеу, сондай-ақ оны Active Directory жүйесіндегі белгілі бір пайдаланушыларға ғана тағайындау мүмкіндігі; BadUSB типіндегі шабуылдардан қорғау;
23. Компьютерде орнатылған қосымшалардағы осалдықтарды анықтауға арналған арнайы тапсырманы іске қосу және анықталған осалдықтар бойынша есеп беру мүмкіндігі;
24. Қосымша сервисін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ қосымша параметрлеріне қол жеткізуді құпиясөзбен қорғау;
25. Сенімді қашықтан әкімшілендіру бағдарламалары арқылы антивирус параметрлерін басқару;
26. Антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату;
27. Жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;
28. Тапсырмаларды кесте бойынша және/немесе қосымша іске қосылғаннан кейін бірден іске қосу;
29. Файлдық кеңістікті сканерлеу кезінде пайдаланушылардың қолайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару;
30. Алдыңғы тексеруден кейін күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету;
31. Антивирустық бағдарламаның тұтастығын тексеру;
32. Файлдың бақылау сомасы, атау/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден алып тастау ерекшеліктерін қосу;
33. Қағидалар мен ерекшеліктер тізімдерін XML форматына импорттау және экспорттау;
34. Антивируста жойылған жұқтырылған файлдарды кейіннен қалпына келтіру мүмкіндігі бар қорғалған сақтау орнының болуы;
35. Антивирустың жұмысы туралы есептерге арналған қорғалған сақтау орнының болуы;
36. Антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктері барынша азайтылған графикалық интерфейстің жеңілдетілген нұсқасының болуы;
37. Windows Defender Security Center жүйесімен интеграциялау; Antimalware Scan Interface (AMSI) қолдауының болуы;
38. Windows Subsystem for Linux (WSL) қолдауының болуы;

39. Резервтік сақтау орнынан объектілерді қалпына келтіруді құпиясөзбен қорғау; Интернетке қосылу лимиттелген жағдайда желілік трафикті шектеу.

2.3. Windows серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар

Антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы файлдық серверлерге арналған операциялық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Windows Small Business Server 2011 Essentials / Standard (64-разрядты);
2. Windows MultiPoint Server 2011 (64-разрядты);
3. Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядты);
4. Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядты);
5. Windows Server 2012 Foundation / Essentials / Standard (64-разрядты);
6. Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядты);
7. Windows Server 2016 (64-разрядты) (шектеулермен);
8. Windows Server 2019 (64-разрядты) (шектеулермен);
9. Windows Server 2022 Standard (64-разрядты).

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Нақты уақыт режимінде және объектінің контекстік мәзірінен сұрау бойынша антивирустық сканерлеу;
2. Кесте бойынша антивирустық сканерлеу;
3. Қосылатын құрылғыларды антивирустық сканерлеу;
4. Бұрын белгісіз зиянды бағдарламаларды анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыштың болуы;
5. Белсенді жұқтыру әрекеттерін бейтараптандыру;
6. Қосымшаның мінез-құлқын және оның жүйеде орындайтын әрекеттерін талдау арқылы зиянды белсенділікті анықтау және рұқсат етілмеген әрекеттерді айқындау;
7. Желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ бумалар мен файлдарға жүгінулерді талдау;
8. Бағдарламалық қамтамасыз етудегі осалдықтарды пайдаланатын зиянды бағдарламалардың әрекеттерін бұғаттау, оның ішінде жүйелік процестердің жадын қорғау;
9. Емдеу кезінде зиянды бағдарламалық қамтамасыз ету әрекеттерін кері қайтару, оның ішінде зиянды бағдарламалармен шифрланған файлдарды қалпына келтіру;
10. Іске қосылатын бағдарлама немесе файл бойынша қорытынды алу үшін қосымшаның нақты уақыт режимінде өндірушінің ресурстарына жүгінуіне мүмкіндік беретін жаңа қауіптерден бұлттық қорғау;
11. RAR, ARJ, ZIP, CAB, LHA, JAR, ICE форматтарындағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу;
12. Желілік сегменттерді санаттарға бөлу мүмкіндігімен бағдарламаларға арналған желілік пакеттік қағидалар мен желілік қағидаларды жасауға мүмкіндік беретін кіріктірілген желілік экран;
13. Құрылғының MAC-мекенжайын қолдан жасау үшін ARP хаттамасындағы осалдықтарды пайдаланатын желілік қауіптерден қорғау;
14. Компьютерде орнатылған қосымшалардағы осалдықтарды анықтау үшін арнайы тапсырманы іске қосу және анықталған осалдықтар бойынша есеп беру мүмкіндігі;
15. Қосымша сервисін қашықтан рұқсатсыз басқарудан қорғау, сондай-ақ зиянды бағдарламалар, қаскүнемдер немесе біліктілігі жеткіліксіз пайдаланушылар тарапынан қорғаудың өшірілуіне жол бермеуге мүмкіндік беретін қосымша параметрлеріне қол жеткізуді құпиясөзбен қорғау;
16. Антивирустық қорғау бағдарламалық құралының тек таңдалған компоненттерін орнату;
17. Жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;
18. Тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
19. Файлдық кеңістікті сканерлеу кезінде пайдаланушылардың қолайлы жұмысын қамтамасыз ету үшін компьютер ресурстарын пайдалануды икемді басқару; алдыңғы тексеруден кейін күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету;
20. Антивирустық бағдарламаның тұтастығын тексеру; файлдың бақылау сомасы, атау/каталог маскасы немесе файлда сенімді цифрлық қолтаңбаның болуы бойынша антивирустық тексеруден ерекшеліктерді қосу;
21. Антивируста жойылған жұқтырылған файлдарды кейіннен қалпына келтіру мүмкіндігі бар қорғалған сақтау орнының болуы;
22. Антивирустың жұмысы туралы есептерге арналған қорғалған сақтау орнының болуы;
23. Антивирустың графикалық интерфейсін қосу және өшіру, сондай-ақ мүмкіндіктері барынша азайтылған графикалық интерфейстің жеңілдетілген нұсқасының болуы;
24. Windows Defender Security Center жүйесімен интеграциялау; Antimalware Scan Interface (AMSI) қолдауының болуы;

25. Windows Subsystem for Linux (WSL) қолдауының болуы;
26. Резервтік сақтау орнынан объектілерді қалпына келтіруді құпиясөзбен қорғау;
27. Қағидалар мен ерекшеліктер тізімдерін XML форматына импорттау және экспорттау;
28. Интернетке қосылу лимиттелген жағдайда желілік трафикті шектеу.

2.4. Linux жұмыс станциялары мен серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар

Linux жұмыс станцияларына арналған антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы 32-биттік операциялық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Ubuntu 16.04 LTS және одан жоғары.
2. Red Hat Enterprise Linux 6.7 және одан жоғары.
3. CentOS 6.7 және одан жоғары.
4. Debian GNU / Linux 9.4 және одан жоғары.
5. Debian GNU / Linux 10.
6. Linux Mint 18.2 және одан жоғары.
7. Linux Mint 19 және одан жоғары.
8. Альт 8 СП Рабочая Станция.
9. Альт 8 СП Сервер. Альт Рабочая Станция 8.
10. Альт Рабочая Станция К 8.
11. Альт Сервер 8.
12. Альт Образование 8.
13. Альт Сервер 9.
14. Альт Рабочая Станция 9.
15. Альт Образование 9.
16. Гослинукс 6.6.
17. Mageia 4.
18. Ubuntu 16.04 LTS және одан жоғары.
19. Ubuntu 18.04 LTS және одан жоғары.
20. Red Hat Enterprise Linux 6.7 және одан жоғары.
21. Red Hat Enterprise Linux 7.2 және одан жоғары.
22. Red Hat Enterprise Linux 8.0 және одан жоғары.
23. CentOS 6.7 және одан жоғары.
24. CentOS 7.2 және одан жоғары.
25. CentOS 8.0 және одан жоғары.
26. Debian GNU / Linux 9.4 және одан жоғары.
27. Debian GNU / Linux 10.1 және одан жоғары.
28. Oracle Linux 6.7 және одан жоғары.
29. Oracle Linux 7.3 және одан жоғары.
30. Oracle Linux 8 және одан жоғары.
31. SUSE Linux Enterprise Server 12 SP3 және одан жоғары.
32. SUSE Linux Enterprise Server 15 және одан жоғары.
33. openSUSE Leap 15 және одан жоғары.
34. Альт 8 СП Рабочая Станция.
35. Альт 8 СП Сервер.
36. Альт Рабочая Станция 8.
37. Альт Рабочая Станция К 8.
38. Альт Сервер 8.
39. Альт Образование 8.
40. Альт Рабочая Станция 9.
41. Альт Сервер 9.
42. Альт Образование 9.
43. Amazon Linux 2.
44. Linux Mint 18.2 және одан жоғары.
45. Linux Mint 19 және одан жоғары.
46. Astra Linux Special Edition, 1.5 нұсқасы (стандартты ядро және PaX ядросы).
47. Astra Linux Special Edition, 1.6 нұсқасы (стандартты ядро және PaX ядросы).
48. Astra Linux Common Edition, 2.12 нұсқасы.
49. Клиенттік жүйелерге арналған РОСА «КОБАЛЬТ» 7.3 ОЖ.
50. Серверлік жүйелерге арналған РОСА «КОБАЛЬТ» 7.3 ОЖ.

51. Гослинукс 6.6.
52. Гослинукс 7.2.
53. AlterOS 7.5 және одан жоғары.
54. Pardus OS 19.1. RED OS 7.2.

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Резиденттік антивирустық мониторинг;
2. Қосымшаның іске қосылатын бағдарлама немесе файл бойынша қорытынды алу үшін нақты уақыт режимінде өндірушінің арнайы ресурстарына жүгінуіне мүмкіндік беретін жаңа қауіптерден бұлттық қорғау;
3. SMB / NFS арқылы қолжетімді ресурстарды тексеру;
4. Ядро жадын тексеру мүмкіндігі;
5. Бұрын белгісіз зиянды бағдарламаларды неғұрлым тиімді анықтауға және бұғаттауға мүмкіндік беретін эвристикалық талдағыш;
6. Пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
7. zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz; .bz2; .tbz; .tbz2; .gz; .tgz; .arj форматтарындағы мұрағаттардағы файлдарды антивирустық тексеру;
8. Мәтіндік форматтағы (Plain text) электрондық пошта хабарламаларын тексеру;
9. Файлдарды тексеруді оңтайландыру тетіктерінің болуы (ерекшеліктер, сенімді процестер, тексеру уақытының шегі, тексерілетін файл өлшемінің шегі, тексерілген және тексеруден кейін өзгертілмеген файлдар туралы ақпаратты кэштеу тетігі);
10. SMB / NFS хаттамалары арқылы желілік қолжетімділігі бар жергілікті каталогтардағы файлдарды қашықтан зиянды шифрлаудан қорғау;
11. Тексеру кезінде файлдарды бұғаттау опциясын қосу;
12. Күдікті және зақымдалған объектілерді карантинге орналастыру;
13. SAMBA деңгейінде файлдық операцияларды ұстап қалу және тексеру;
14. Қағидалардың бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
15. Тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
16. Есептерді HTML және CSV форматтарында экспорттау және сақтау;
17. Файлдық кеңістікті сканерлеу кезінде пайдаланушылардың қолайлы жұмысын қамтамасыз ету үшін ДК ресурстарын пайдалануды икемді басқару;
18. Объект ақпараттық құндылыққа ие болған жағдайда, талап бойынша оны қалпына келтіру мүмкіндігін қамтамасыз ету мақсатында емдеу және жою алдында жұқтырылған объектінің көшірмесін резервтік сақтау орнына сақтау;
19. Root құқықтарынсыз пайдаланушының графикалық интерфейсі арқылы басқару;
20. Жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі немесе веб-консоль арқылы орталықтандырылған басқару;
21. Алынбалы дискілерді тексеру; кіріс желілік трафикте желілік шабуылдарға тән белсенділікті қадағалау; пайдаланушының компьютеріне HTTP/HTTPS және FTP хаттамалары арқылы келіп түсетін трафикті тексеру, сондай-ақ веб-мекенжайлардың зиянды немесе фишингтік ресурстарға жататынын анықтау мүмкіндігі;
22. Пайдаланушының компьютеріндегі бағдарламалардың әрекеттері туралы деректерді алу;
23. Ядро жадын тексеру.

2.5. Файлдық серверлерді, кәсіпорын ауқымындағы серверлерді және Windows терминалдық серверлерін антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар

Windows файлдық серверлеріне арналған антивирустық қорғаудың бағдарламалық құралдары келесі нұсқалардағы операциялық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Microsoft Windows 32-разрядты операциялық жүйелері: Windows Server 2003 Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
2. Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
3. Windows Server 2008 Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
4. Windows Server 2008 Core Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
5. Microsoft Windows 64-разрядты операциялық жүйелері: Windows Server 2003 Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
6. Windows Server 2003 R2 Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
7. Windows Server 2008 Core Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
8. Windows Server 2008 Standard / Enterprise / Datacenter, SP2 жаңарту пакетімен немесе одан жоғары;
9. Microsoft Small Business Server 2008 Standard / Premium, SP2 немесе одан жоғары;
10. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter, SP1 жаңарту пакетімен немесе одан жоғары;
11. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter, SP1 жаңарту пакетімен немесе одан жоғары;

12. Windows Hyper-V Server 2008 R2, SP1 жаңарту пакетімен немесе одан жоғары;
13. Microsoft Small Business Server 2011 Essentials / Standard, SP1 немесе одан жоғары;
14. Microsoft Windows MultiPoint Server 2011 Standard / Premium;
15. Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
16. Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
17. Microsoft MultiPoint Server 2012 Standard / Premium;
18. Windows Storage Server 2012;
19. Windows Hyper-V Server 2012;
20. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; Windows Storage Server 2012 R2;
21. Windows Hyper-V Server 2012 R2;
22. Windows Server 2016 Essentials / Standard / Datacenter; Windows Server 2016 MultiPoint;
23. Windows Server 2016 Core Standard / Datacenter;
24. Microsoft Windows MultiPoint Server 2016;
25. Windows Storage Server 2016;
26. Windows Hyper-V Server 2016;
27. Windows Server 2019 Essentials / Standard / Datacenter;
28. Windows Server 2019 Core;
29. Windows Storage Server 2019;
30. Windows Hyper-V Server 2019;
31. Windows 10 Enterprise multi-session.

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Әртүрлі функцияларды орындайтын серверлерде: терминалдық серверлерде, принт-серверлерде, қосымшалар серверлерінде және домен контроллерлерінде, файлдық серверлерде нақты уақыт режимінде жа
2. Пайдаланушының немесе әкімшінің пәрмені бойынша және кесте бойынша антивирустық сканерлеу;
3. Тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
4. Іске қосылатын бағдарлама немесе файл бойынша қорытынды алу үшін қосымшаның нақты уақыт режимінде өндірушінің
5. RAR, ARJ, ZIP, CAB форматтарындағы мұрағаттардағы файлдарды антивирустық тексеру және емдеу;
6. Файлдарды, файлдық жүйелердің балама ағындарын (NTFS-streams), жүктеу жазбасын, жергілікті және алынбалы дискілердің жүктеу секторларын қорғау;
7. Microsoft Windows Script Technologies (немесе Active Scripting) технологиялары бойынша жасалған VBScript және JScript скрипттерін қорғалатын серверде орындау әрекеттерін
8. Желі арқылы қолжетімді қорғалатын ресурстарды шифрлау әрекеттерін анықтау үшін ортақ бумалар мен файлдарға жүгін
9. Microsoft Windows контейнерлерін тексеру;
10. Процестер жадындағы осалдықтарды пайдаланудан қорғау;
11. Бұзылған процестерді автоматты түрде аяқтау мүмкіндігі болуы тиіс, бұл ретте маңызды жүйелік процестер аяқталмауы тиіс;
12. Процестерді қорғалатын процестер тізіміне қосу;
13. Алдыңғы тексеруден кейін күйі өзгермеген объектілерді өткізіп жіберу есебінен сканерлеу процесін жеделдету;
14. Жеке тапсырма арқылы бағдарламаның өз модульдерінің тұтастығының ықтимал бұзылуын тексеру;
15. Сервердің маңызды аймақтарын тексеруді жеке тапсырма ретінде баптау;
16. Тапсырмалардың басымдығына байланысты сервер ресурстарын антивирус пен басқа қосымшалар арасында бөлуді реттеу;
17. Антивирустық сканерлеуді фондық режимде жалғастыру; әкімшілерді орын алған маңызды оқиғалар туралы хабардар етудің бірнеше тәсілінің болуы (электрондық пошта хабарламасы, дыбыстық хабарландыру, қалқымалы терезе, оқиғалар журналына жазу);
18. Рұқсаттар тізімдері арқылы қосымша параметрлері мен қызметіне рөлдік қол жеткізу, бұл зиянды бағдарламалар, қаскүнемдер немесе біліктілігі жеткіліксіз пайдаланушылар тарапынан қорғаудың өшірілуіне жол бермеуге, сондай-ақ антивирусты басқаруға тыйым салуға немесе рұқсат беруге мүмкіндік береді; SIEM жүйелерімен интеграциялау; антивирустың жұмыс процестерінің санын қолмен белгілеу;
19. Графикалық интерфейсті өшіру;
20. Қашықтан және жергілікті басқару консольдерінің болуы;
21. Антивирус параметрлерін пәрмен жолы арқылы басқару;
22. Жоғарыда көрсетілген барлық компоненттерді бірыңғай басқару жүйесі арқылы орталықтандырылған басқару;
23. Қағидалардың бастапқы күйін қалпына келтіру мүмкіндігімен операциялық жүйенің желілік экранын басқару;
24. Кіріс трафикті желілік шабуыл белгілерінің бар-жоғына талдауды қамтамасыз ететін желілік қауіптерден қорғау.

2.6. Мобильді құрылғыларды антивирустық қорғаудың бағдарламалық құралдарына қойылатын талаптар

Смартфондарды антивирустық қорғауға арналған бағдарламалық құралдар келесі мобильді операциялық жүйелердің басқаруымен жұмыс істеуі тиіс:

1. Android 4.2–11.0;
2. iOS 10.0–14.0 немесе iPadOS;
3. Android ОЖ-ге арналған смартфондарды антивирустық қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс: смартфонның файлдық жүйесін тұрақты антивирустық қорғау, антивирустық қорғау құралдарын өндірушінің бұлттық бедел сервисін пайдалана отырып, қосымша тексеру деңгейімен;
4. Құрылғының файлдық жүйесін сұрау бойынша және кесте бойынша тексеру;
5. Орнатылатын қосымшаларды жедел тексеру; антивирустық қорғау құралдарын өндірушінің бұлттық бедел сервистерінің қорытындылары негізінде зиянды және фишингтік сайттарды бұғаттау;
6. Жұқтырылған объектілерді оқшаулауға арналған сақтау орнының болуы; зиянды бағдарламаларды іздеу және қауіпті объектілерді жою кезінде пайдаланылатын антивирустық дерекқорларды кесте бойынша жаңарту;
7. Көрсетілген қосымшалардың іске қосылуын, оның ішінде алдын ала белгіленген қосымшалар санаттарының көмегімен бұғаттау;
8. Рұқсат етілген қосымшалардың ақ тізімдерін қолдау;
9. Қосымшалардың іске қосылуын бақылау шеңберінде жүйелік қосымшаларды бұғаттау;
10. Firebase Cloud Messaging (FCM) сервисі арқылы пәрмендер мен push-хабарламаларды жіберу;
11. Wi-Fi және Bluetooth модульдерін, сондай-ақ мобильді құрылғы камерасын пайдалануды бұғаттау;
12. Wi-Fi желілеріне қосылу параметрлерін көрсету; міндетті түрде орнатылуы тиіс қосымшаларды белгілеу;
13. Мобильді құрылғыны бұғаттау, деректерді жою, жұмыс қызметіне байланысты деректерді жою, құрылғының орналасқан жерінің координаттарын алу, зауыттық баптауларға қашықтан қайтару (factory reset);
14. Мобильді құрылғының корпоративтік саясаттарға сәйкестігін тексеру жүзеге асырылатын қағидалар тізімін жасау, сәйкессіздіктер анықталған жағдайда құрылғыны автоматты түрде бұғаттау, деректерді жою және корпоративтік қосымшалардың іске қосылуына тыйым салу мүмкіндігімен;
15. Samsung KNOX1 және KNOX2 технологияларын қолдау.

Apple iOS ОЖ-ге арналған смартфондарды қорғау бағдарламалық құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Топтық саясаттардың көмегімен iOS MDM құрылғыларының параметрлерін қашықтан баптау;
2. Құрылғыны бұғаттау және деректерді жою пәрмендерін жіберу;
3. Мобильді құрылғылардың топтық қауіпсіздік саясаттарын жасау;
4. Exchange ActiveSync / iOS MDM хаттамасы арқылы қосылған құрылғылардың конфигурациялық параметрлерін қашықтан баптау;
5. Пайдаланушылардың мобильді құрылғыларының жұмысы туралы есептер мен статистиканы алу;
6. Supervised mode режимін пайдалану кезінде антивирустық қорғау құралдарын өндірушінің бұлттық бедел сервистерінің қорытындылары негізінде зиянды және фишингтік сайттарды бұғаттау;
7. Бірыңғай басқару консолі арқылы орталықтандырылған басқару;
8. Басқарылатын құрылғыда iTunes, Safari немесе Game Center сияқты құрылғының кіріктірілген қосымшаларын пайдалануға болатын-болмайтынын бақылауға мүмкіндік беретін компоненттің болуы.

2.7. Windows ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі операциялық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Microsoft Windows 10 20H2 32-разрядты / 64-разрядты;
2. Microsoft Windows 10 20H1 32-разрядты / 64-разрядты;
3. Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядты / 64-разрядты;
4. Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядты / 64-разрядты;
5. Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядты / 64-разрядты;
6. Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядты / 64-разрядты;
7. Microsoft Windows 10 Pro жұмыс станцияларына арналған RS5 (October 2018 Update, 1809) 32-разрядты / 64-разрядты;
8. Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядты / 64-разрядты;
9. Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядты / 64-разрядты;
10. Microsoft Windows 10 Pro 19H1 32-разрядты / 64-разрядты;
11. Microsoft Windows 10 Pro жұмыс станцияларына арналған 19H1 32-разрядты / 64-разрядты;
12. Microsoft Windows 10 Enterprise 19H1 32-разрядты / 64-разрядты;

13. Microsoft Windows 10 Education 19H1 32-разрядты / 64-разрядты;
14. Microsoft Windows 10 Pro 19H2 32-разрядты / 64-разрядты;
15. Microsoft Windows 10 Pro жұмыс станцияларына арналған 19H2 32-разрядты / 64-разрядты;
16. Microsoft Windows 10 Enterprise 19H2 32-разрядты / 64-разрядты;
17. Microsoft Windows 10 Education 19H2 32-разрядты / 64-разрядты;
18. Microsoft Windows 8.1 Pro 32-разрядты / 64-разрядты;
19. Microsoft Windows 8.1 Enterprise 32-разрядты / 64-разрядты;
20. Microsoft Windows 8 Pro 32-разрядты / 64-разрядты;
21. Microsoft Windows 8 Enterprise 32-разрядты / 64-разрядты;
22. Microsoft Windows 7 Professional Service Pack 1 32-разрядты / 64-разрядты;
23. Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядты / 64-разрядты;
24. Windows Server 2019 Standard 64-разрядты;
25. Windows Server 2019 Standard 64-разрядты;
26. Microsoft Windows Server 2019 Datacenter 64-разрядты;
27. Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядты;
28. Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-разрядты;
29. Microsoft Windows Server 2016 (Server Core RS3 (v1709) (LTSB/CBB) орнату нұсқасы) 64-разрядты;
30. Microsoft Windows Server 2016 Standard (LTSB) 64-разрядты;
31. Microsoft Windows Server 2016 (Server Core орнату нұсқасы) (LTSB) 64-разрядты;
32. Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядты;
33. Microsoft Windows Server 2012 R2 Standard 64-разрядты;
34. Microsoft Windows Server 2012 R2 Server Core 64-разрядты;
35. Microsoft Windows Server 2012 R2 Foundation 64-разрядты;
36. Microsoft Windows Server 2012 R2 Essentials 64-разрядты;
37. Microsoft Windows Server 2012 R2 Datacenter 64-разрядты;
38. Microsoft Windows Server 2012 Standard 64-разрядты;
39. Microsoft Windows Server 2012 Server Core 64-разрядты;
40. Microsoft Windows Server 2012 Foundation 64-разрядты;
41. Microsoft Windows Server 2012 Essentials 64-разрядты;
42. Microsoft Windows Server 2012 Datacenter 64-разрядты;
43. Microsoft Windows Storage Server 2016 64-разрядты;
44. Microsoft Windows Storage Server 2012 R2 64-разрядты;
45. Microsoft Windows Storage Server 2012 64-разрядты.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі виртуалды платформаларда орнатуды қолдауы тиіс:

1. VMware vSphere 6.7;
2. VMware vSphere 7.1;
3. VMware Workstation 15 Pro;
4. VMware Workstation 16 Pro;
5. Microsoft Hyper-V Server 2012 64-разрядты;
6. Microsoft Hyper-V Server 2012 R2 64-разрядты;
7. Microsoft Hyper-V Server 2016 64-разрядты;
8. Microsoft Hyper-V Server 2019 64-разрядты;
9. Citrix XenServer 7.1 LTSR;
10. Citrix XenServer 8.x;
11. Parallels Desktop 16;
12. Oracle VM VirtualBox 6.x.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардағы дерекқорды басқару жүйелерімен (ДҚБЖ) жұмыс істеуі тиіс:

1. Microsoft SQL Server 2012 Express 64-разрядты;
2. Microsoft SQL Server 2014 Express 64-разрядты;
3. Microsoft SQL Server 2016 Express 64-разрядты;
4. Microsoft SQL Server 2017 Express 64-разрядты;
5. Microsoft SQL Server 2019 Express 64-разрядты;
6. Microsoft SQL Server 2014 (барлық редакциялары) 64-разрядты;
7. Microsoft SQL Server 2016 (барлық редакциялары) 64-разрядты;
8. Windows жүйесіне арналған Microsoft SQL Server 2017 (барлық редакциялары) 64-разрядты;

9. Linux жүйесіне арналған Microsoft SQL Server 2017 (барлық редакциялары) 64-разрядты;
10. Windows жүйесіне арналған Microsoft SQL Server 2019 (барлық редакциялары) 64-разрядты;
11. Linux жүйесіне арналған Microsoft SQL Server 2019 (барлық редакциялары) 64-разрядты;
12. MySQL Standard Edition 5.7 32-разрядты / 64-разрядты;
13. MySQL Enterprise Edition 5.7 32-разрядты / 64-разрядты;
14. Amazon RDS және Microsoft Azure бұлттық платформаларында қолдау көрсетілетін SQL-серверлердің барлық нұсқалары;
15. InnoDB сақтау ішкі жүйесі бар MariaDB Server 10.3 32-разрядты / 64-разрядты.

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Қорғалатын тораптар санына байланысты орталықтандырылған басқару, мониторинг және жаңарту құралын орнату архит
2. Ұйымдағы компьютерлер мен пайдаланушылардың есептік жазбалары туралы деректерді алу мақсатында Active Directory жүйесінен ақпаратты оқу;
3. Анықталған компьютерлерді IP-мекенжайы, ОЖ түрі, AD OU-да орналасуы бойынша ауыстыру қағидаларын баптау;
4. Желіде жаңа компьютерлер пайда болған жағдайда компьютерлердің есептік жазбаларын басқару топтары бойынша автом
5. IP-мекенжайы, ОЖ түрі, AD OU-да орналасуы бойынша ауыстыру қағидаларын баптау мүмкіндігі;
6. Антивирустық қорғаудың бағдарламалық құралдарын орталықтандырылған орнату, жаңарту және жою;
7. Орталықтандырылған баптау және әкімшілендіру; қорғау құралдарының жұмысы туралы есептер мен статистикалық ақпа
8. Басқару орталығының құралдарымен үйлесімсіз қосымшаларды орталықтандырылған түрде жою (қолмен және автоматты
9. Антивирустық агенттерді орнатудың әртүрлі әдістерінің болуы: қашықтан орнату үшін – RPC, GPO, басқару жүйесінің құралдары арқылы; жергілікті орнату үшін – автономды орнату пакетін жасау мүмкіндігі; қауіпсі
10. Қайта бөлу жүзеге асырылатын триггерлер иерархиясы;
11. Клиенттік компьютерлерге таратпас бұрын жүктелген жаңартуларды орталықтандырылған басқару бағдарламалық құрал
12. Жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
13. Желідегі виртуалды машиналарды анықтау және егер олар бір физикалық серверде орналасқан болса, іске қосылатын тапс
14. Әрбір деңгейде әкімшілер мен операторлардың құқықтарын, сондай-ақ ұсынылатын есептілік нысандарын баптау мүмкіндігі бар көпдеңгейлі басқару жүйесін құру;
15. Еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтанд
16. Басқару серверлері үшін мультиарендалықты (multi-tenancy) қолдау;
17. Бағдарламалық құралдар мен антивирустық дерекқорларды әртүрлі көздерден, байланыс арналары арқылы да, машиналы
18. Басқару сервері арқылы антивирустық бағдарламалық қамтамасыз ету өндірушісінің бұлттық серверлеріне қол жеткізу;
19. Лицензияны клиенттік компьютерлерге автоматты түрде тарату;
20. Пайдаланушылардың компьютерлерінде орнатылған бағдарламалық қамтамасыз ету мен жабдықтарды түгендеу;
21. Орнатылған антивирустық қорғау қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы электрондық пошта хабарламаларын таратуды баптау;
22. Exchange ActiveSync сервері арқылы мобильді құрылғыларды басқару функциясы;
23. iOS MDM сервері арқылы мобильді құрылғыларды басқару функциясы; белгіленген оқиғалар туралы SMS-хабарламаларды жіберу;
24. Басқарылатын мобильді құрылғыларға сертификаттарды орталықтандырылған түрде орнату;
25. Басқару жүйесіне түсетін желілік жүктемені азайту үшін ұйымның кез келген компьютерін жаңартуларды ретрансляциялау орталығы ретінде белгілеу;
26. Басқару жүйесіне түсетін желілік жүктемені азайту үшін ұйымның кез келген компьютерін клиенттік компьютерлердің таңдалған тобының антивирустық агенттері оқиғаларын орталықтандырылған басқару серверіне жіберу орталығы ретінде белгілеу;
27. Антивирустық қорғау оқиғалары, түгендеу деректері және орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру;
28. Жүйенің жұмысы туралы алдын ала бапталған стандартты есептердің болуы;
29. Есептерді PDF және XML форматтарындағы файлдарға экспорттау;
30. Антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстарындағы резервтік сақтау орындары мен карантин объектілерін орталықтандырылған басқару;
31. Басқару серверінде аутентификациялау үшін ішкі есептік жазбаларды жасау;
32. Басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау;
33. Windows Failover Clustering қолдауы;
34. Windows Certificate Authority сервисімен интеграцияны қолдау;
35. Пайдаланушылардың өзіне-өзі қызмет көрсету порталының болуы;
36. Өзіне-өзі қызмет көрсету порталы басқару агентін мобильді құрылғыға орнату мақсатында пайдаланушыларды қосу, мобильді қ
37. Вирустық эпидемиялардың туындауын бақылау жүйесінің болуы;
38. Microsoft Azure және Google Cloud бұлттық инфрақұрылымында орнату;

39. OpenAPI арқылы интеграциялау;
40. Microsoft Azure және Google Cloud бұлттық инфрақұрылымында орнату;
41. OpenAPI арқылы интеграциялау;
42. WEB-консольді пайдалана отырып, антивирустық қорғауды басқару;
43. Әкімшілендіру консоліне рұқсатсыз қол жеткізу қаупін азайту үшін екі кезеңді тексеру;
44. Пайдаланушының есептік жазба параметрлері өзгертілгеннен кейін қосымша аутентификацияны пайдалану.

2.8. Linux ОЖ негізіндегі орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдарына қ ойылатын талаптар

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардағы операциял ық жүйелердің басқаруымен жұмыс істейтін компьютерлерде жұмыс істеуі тиіс:

1. Ubuntu 18.04 LTS;
2. Ubuntu 20.04 LTS;
3. Debian GNU / Linux 10.5;
4. Astra Linux Common Edition, 2.12 нұсқасы;
5. Astra Linux Special Edition, 1.6 нұсқасы;
6. CentOS 7.9.2009;
7. CentOS 8.3.2011;
8. Red Hat Enterprise Linux 7.9;
9. Red Hat Enterprise Linux 8.3;
10. ALT 8.3;
11. ALT 9.1.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі виртуалды платформаларда орнатуды қолдауы тиіс:

1. FusionCompute 8.0;
2. FusionSphere OpenStack 6.5.13.

Орталықтандырылған басқару, мониторинг және жаңарту бағдарламалық құралдары келесі нұсқалардағы **дерекқор ды басқару жүйелерімен (ДҚБЖ)** жұмыс істеуі тиіс:

1. InnoDB сақтау ішкі жүйесі бар MariaDB Server 10.3 32-разрядты / 64-разрядты.
2. Антивирус Linux® таза орталарының талаптарына сәйкес Linux негізіндегі әкімшілендіру серверінің көмегімен Linux операциялық жүйесі бар құрылғыларды қорғауды өрістетуге және басқаруға арналған.

Бағдарламалық антивирустық қорғау құралында мынадай функционалдық мүмкіндіктер іске асырылуы тиіс:

1. Антивирустық қорғаудың бағдарламалық құралдарын орталықтандырылған түрде орнату, жаңарту және жою;
2. Орталықтандырылған баптау және әкімшілендіру;
3. Қорғау құралдарының жұмысы туралы есептер мен статистикалық ақпаратты қарау;
4. Саясаттар мен тапсырмалардың өзгеру тарихын сақтау, алдыңғы нұсқаларға қайтару мүмкіндігі;
5. Қайта бөлу жүзеге асырылатын триггерлер иерархиясы;
6. Жаңартуларды алғаннан кейін бірден пайдаланушылардың жұмыс орындарына жеткізу;
7. Желідегі виртуалды машиналарды анықтау және егер бұл машиналар бір физикалық серверде орналасқан болса, іске қосылатын тапсырмалардың жүктемесін олардың арасында теңгерімді бөлу;
8. Әрбір деңгейде әкімшілер мен операторлардың құқықтарын, сондай-ақ ұсынылатын есептілік нысандарын баптау мүмкіндігі бар көпдеңгейлі басқару жүйесін құру;
9. Еркін деңгейдегі әкімшілендіру серверлерінің иерархиясын құру және бүкіл иерархияны жоғарғы деңгейден орталықтандырылған басқару мүмкіндігі;
10. Басқару серверлері үшін мультиарендалықты (multi-tenancy) қолдау;
11. Бағдарламалық құралдар мен антивирустық дерекқорларды әртүрлі көздерден, байланыс арналары арқылы да, машиналық ақпарат тасымалдағыштар арқылы да жаңарту;
12. Басқару сервері арқылы антивирустық бағдарламалық қамтамасыз ету өндірушісінің бұлттық серверлеріне қол жеткізу;
13. Лицензияны клиенттік компьютерлерге автоматты түрде тарату;
14. Орнатылған антивирустық қорғау қосымшаларының жұмысындағы оқиғалар туралы хабарлау тетігінің болуы және олар туралы электрондық пошта хабарламаларын таратуды баптау;
15. Антивирустық қорғау оқиғалары және орнатылған бағдарламаларды лицензиялау деректері бойынша графикалық есептер құру;

16. Жүйенің жұмысы туралы алдын ала бапталған стандартты есептердің болуы;
17. Есептерді PDF және XML форматтарындағы файлдарға экспорттау;
18. Антивирустық бағдарламалық қамтамасыз ету орнатылған желінің барлық ресурстарындағы резервтік сақтау орындары мен карантин объектілерін орталықтандырылған басқару;
19. Басқару серверінде аутентификациялау үшін ішкі есептік жазбаларды жасау;
20. Басқару жүйесінің кіріктірілген құралдарымен басқару жүйесінің резервтік көшірмесін жасау;
21. Вирустық эпидемиялардың туындауын бақылау жүйесінің болуы;
22. WEB-консольді пайдалана отырып, антивирустық қорғауды басқару.

2.9. Антивирустық дерекқорларды жаңартуға қойылатын талаптар

Жаңартылатын антивирустық дерекқорлар мынадай функционалдық мүмкіндіктерді іске асыруды қамтамасыз етуі тиіс:

1. Антивирустық дерекқорларды бір күнтізбелік тәулік ішінде кемінде 24 рет жаңарту қағидаларын жасау;
2. Жаңартудың бірнеше тәсілінің болуы, оның ішінде байланыс арналары арқылы және алынбалы электрондық ақпарат тасымалдағыштарында;
3. Электрондық цифрлық қолтаңба құралдары арқылы жаңартулардың тұтастығы мен түпнұсқалығын тексеру.

2.10. Пайдалану құжаттамасына қойылатын талаптар

Басқару құралдарын қоса алғанда, антивирустық қорғаудың барлық бағдарламалық өнімдеріне арналған пайдалану құжаттамасы мемлекеттік стандарттардың талаптарына сәйкес дайындалған орыс тіліндегі құжаттарды қамтуы тиіс, оның ішінде:

1. «Пайдаланушы (әкімші) нұсқаулығы»;
2. Антивирустық құралдармен бірге жеткізілетін құжаттама тиісті антивирустық қорғау құралын орнату, баптау және пайдалану процесін егжей-тегжейлі сипаттауы тиіс.

3. Өнім берушіге қойылатын талаптар

Өнім беруші Қазақстан Республикасының аумағында антивирустық қорғау жүйесін өндірушінің ресми серіктесі болуы тиіс.

Бағдарламалық қамтамасыз етуге арналған лицензияны беру кезінде өнім беруші қолданыстағы серіктестік сертификатының электрондық көшірмесін ұсынуы тиіс.

4. Техникалық қолдауға қойылатын талаптар

Өнім беруші Тапсырыс берушіге антивирустық бағдарламалық қамтамасыз етуді баптау және пайдалану мәселелері бойынша консультациялық-техникалық қызмет көрсетуі және мынадай мүмкіндіктерді қамтамасыз етуі тиіс:

1. Техникалық қолдау лицензиялар ұзартылған сәттен бастап **1 жыл бойы**, мереке және демалыс күндерін қоса алғанда, тәулік бойы Қазақстан Республикасының бүкіл аумағында антивирустық бағдарламалық қамтамасыз етуді өндірушінің және оның серіктестерінің мамандары тарапынан орыс тілінде телефон, электрондық пошта және Интернет арқылы көрсетілуі тиіс;
2. Өнім беруші бағдарламалық қамтамасыз етуді өндірушінің техникалық қолдау жөніндегі электрондық ақпараттық жүйесіне қол жеткізуді қамтамасыз етуі тиіс, оның ішінде нақты мәселелер бойынша сұрау салуларды электрондық пошта жүйесі арқылы жіберу мүмкіндігі болуы тиіс;
3. Жоғарыда сипатталған қызметтерге қол жеткізу техникалық қолдау көрсетілетін бүкіл кезең ішінде тәулік бойы ашық болуы тиіс;
4. Өнім беруші Тапсырыс берушіні өндірушінің бағдарламалық өнімдерінде анықталған проблемалар мен қателерді жою және шешу үшін қажетті техникалық ақпаратпен және/немесе қосымша бағдарламалық компоненттермен қамтамасыз етуі тиіс;
5. Бағдарламалық қамтамасыз етуге кепілдік қызмет көрсету және техникалық қолдау Тапсырыс беруші тарапынан қосымша шығындарсыз қамтамасыз етілуі тиіс;
6. Кепілдік қызмет көрсету және техникалық қолдау бағдарламалық қамтамасыз ету орналасқан жерде жүзеге асырылуы тиіс.

Шартқа қол қойылған күннен бастап 5 (бес) жұмыс күні ішінде өнім беруші Тапсырыс берушіге серіктестік қатынастардың болуын және өнім берушінің Қазақстан Республикасының аумағында тиісті лицензиялық бағдарламалық қамтамасыз етуді іске асыруға және/немесе пайдалану құқығын беруге құқығын растайтын бағдарламалық қамтамасыз

етуді өндірушіден (құқық иеленушіден) қолданыстағы авторизациялық хат, сертификат немесе өзге де растау беруге міндетті. Көрсетілген құжатты ұсыну міндетті талап болып табылады. Жоғарыда көрсетілген құжаттар ұсынылмаған жағдайда Тапсырыс беруші Шартты орындаудан біржақты тәртіппен бас тартуға құқылы (авторизациялық хаттың мәтіні және/немесе шет тілінде өзге де растайтын құжаттар болған жағдайда оларға мемлекеттік немесе орыс тіліне нотариалды куәландырылған аударма қоса берілуге тиіс).

Жеткізуші жеткізілетін бағдарламалық қамтамасыз етудің лицензияланған, контрафактілі емес екендігіне, ал берілетін лицензиялардың жарамды екендігіне кепілдік береді және Тапсырыс берушіге бағдарламалық қамтамасыз етуді шартта және техникалық ерекшелікте көзделген көлемде және мерзімге пайдалану құқығын береді.

Өнім беруші Шарт бойынша өз міндеттемелерін орындаудан бас тартқан және/немесе мүмкін болмаған, сондай-ақ тауарды жеткізу мерзімі күнтізбелік 30 (отыз) күннен асатын мерзімге кешіктірілген жағдайда, өнім беруші Тапсырыс берушіге Шарт сомасының 10% мөлшерінде айыппұл төлеуге міндетті.

Қол қойған	Сатубалдина Зарина Малкаждаровна
Қол қойылған күні	02.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1267903
способом Запрос ценовых предложений на понижение

Лот № 1 (35-1 У, 4574361) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Өскемен Энерго"
Организатор: Товарищество с ограниченной ответственностью "Өскемен Энерго"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	35-1 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Лицензия на право использования программного обеспечения (антивирус)
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Восточно-Казахстанская область, Усть-Каменогорск Г.А., г.Усть-Каменогорск, проспект Ильяса Есенберлина 43, блок 2
Условия поставки	-
Срок поставки	С даты подписания договора в течение 15 рабочих дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

Техническая спецификация на программное обеспечение по антивирусной защите рабочих станций и серверов.

Антивирусная защита (АЗ) должна представлять собой корпоративное решение, обеспечивающее устойчивое функционирование в сети рабочих станций и серверов. В рамках всей организации должны использоваться единые антивирусные средства.

Настоящая Техническая спецификация является основополагающим документом, устанавливающим требования к поставляемому программному обеспечению с оказанием сопутствующих услуг по внедрению системы антивирусной защиты. Все компоненты системы должны иметь полную интеграцию между собой.

Требования к программному обеспечению и потенциальному поставщику указаны в настоящей технической спецификации, все предложенные характеристики услуг должны соответствовать или превосходить минимальные технические характеристики, указанные в данной технической спецификации.

Общие требования к программному обеспечению по антивирусной защите:

1. Общее количество защищаемых узлов: 38

2. Срок действия лицензии: не менее 12 месяцев с момента генерации лицензий на программное обеспечение.

2.1 Технические требования к программному обеспечению по антивирусной защите:

Антивирусные средства должны включать:

1. Программные средства антивирусной защиты для рабочих станций Windows.
2. Программные средства антивирусной защиты для рабочих станций Linux.
3. Программные средства антивирусной защиты для файловых серверов Windows.
4. Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows.
5. Программные средства антивирусной защиты мобильных устройств.
6. Программные средства централизованного управления, мониторинга и обновления.
7. Обновляемые базы данных сигнатур вредоносных программ и атак.
8. Эксплуатационную документацию на русском языке.
9. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.
10. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

2.2 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:

1. Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
2. Windows 8 Professional / Enterprise (32 / 64-разрядная);
3. Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
4. Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).
5. Windows 11 Pro / Enterprise (32 / 64-разрядная).

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
2. антивирусное сканирование по расписанию;
3. антивирусное сканирование подключаемых устройств;
4. эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
5. нейтрализации действий активного заражения;
6. анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
7. анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
8. 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;

9. антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
10. защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
11. фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
12. 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;
13. блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
14. 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;
15. защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
16. 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;
17. 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;
18. 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;
19. 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;
20. записи в журнал событий о записи и/или удалении файлов на съемных дисках;
21. назначение приоритета для правил доступа к устройствам с файловой системой;
22. 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;
23. запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
24. защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
25. управления параметрами антивируса через доверенные программы удаленного администрирования;
26. установки только выбранных компонентов программного средства антивирусной защиты;
27. централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
28. запуска задач по расписанию и/или сразу после запуска приложения;
29. гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
30. ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
31. проверки целостности антивирусной программы;
32. добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
33. импорта и экспорта списков правил и исключений в XML-формат;
34. наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
35. наличие защищенного хранилища для отчетов о работе антивируса;

36. включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
37. интеграции с Windows Defender Security Center; наличие поддержки Antimalware Scan Interface (AMSI);
38. наличие поддержки Windows Subsystem for Linux (WSL);
39. защитить паролем восстановление объектов из резервного хранилища; ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

2.3. 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:

1. Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
2. Windows MultiPoint Server 2011 (64-разрядная);
3. Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
4. Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64- разрядная);
5. Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
6. Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
7. Windows Server 2016 (64-разрядная) (с ограничениями);
8. Windows Server 2019 (64-разрядная) (с ограничениями);
9. Windows Server 2022 Standard (64-разрядная).

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
2. антивирусное сканирование по расписанию;
3. антивирусное сканирование подключаемых устройств;
4. эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
5. нейтрализации действий активного заражения;
6. анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
7. анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
8. блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
9. откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
10. облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
11. антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, L HA, JAR, ICE;
12. встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
13. защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
14. запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
15. 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;
16. установки только выбранных компонентов программного средства антивирусной защиты;
17. централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

18. запуск задач по расписанию и/или сразу после загрузки операционной системы;
19. 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;
20. проверки целостности антивирусной программы; добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
21. наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
22. наличие защищенного хранилища для отчетов о работе антивируса;
23. включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
24. интеграции с Windows Defender Security Center; наличие поддержки Antimalware Scan Interface (AMSI);
25. наличие поддержки Windows Subsystem for Linux (WSL);
26. защитить паролем восстановление объектов из резервного хранилища.
27. импорта и экспорта списков правил и исключений в XML-формат;
28. ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

2.4. Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux:

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:

1. Ubuntu 16.04 LTS и выше.
2. Red Hat Enterprise Linux 6.7 и выше.
3. CentOS 6.7 и выше.
4. Debian GNU / Linux 9.4 и выше.
5. Debian GNU / Linux 10.
6. Linux Mint 18.2 и выше.
7. Linux Mint 19 и выше.
8. Альт 8 СП Рабочая Станция.
9. Альт 8 СП Сервер. Альт Рабочая Станция 8.
10. Альт Рабочая Станция К 8.
11. Альт Сервер 8.
12. Альт Образование 8.
13. Альт Сервер 9.
14. Альт Рабочая Станция 9.
15. Альт Образование 9.
16. Гослинукс 6.6.
17. Mageia 4.
18. Ubuntu 16.04 LTS и выше.
19. Ubuntu 18.04 LTS и выше.
20. Red Hat Enterprise Linux 6.7 и выше.
21. Red Hat Enterprise Linux 7.2 и выше.
22. Red Hat Enterprise Linux 8.0 и выше.
23. CentOS 6.7 и выше.
24. CentOS 7.2 и выше.
25. CentOS 8.0 и выше.
26. Debian GNU / Linux 9.4 и выше.
27. Debian GNU / Linux 10.1 и выше.
28. Oracle Linux 6,7 и выше.
29. Oracle Linux 7,3 и выше.
30. Oracle Linux 8 и выше.
31. SUSE Linux Enterprise Server 12 SP3 и выше.
32. SUSE Linux Enterprise Server 15 и выше.
33. openSUSE Leap 15 и выше.

34. Альт 8 СП Рабочая Станция.
35. Альт 8 СП Сервер.
36. Альт Рабочая Станция 8.
37. Альт Рабочая Станция К 8.
38. Альт Сервер 8.
39. Альт Образование 8.
40. Альт Рабочая Станция 9.
41. Альт Сервер 9.
42. Альт Образование 9.
43. Amazon Linux 2.
44. Linux Mint 18.2 и выше.
45. Linux Mint 19 и выше.
46. Astra Linux Special Edition, версия 1.5 (стандартное ядро и ядро PaX).
47. Astra Linux Special Edition, версия 1.6 (стандартное ядро и ядро PaX).
48. Astra Linux Common Edition, версия 2.12.
49. ОС РОСА "КОБАЛЬТ" 7.3 для клиентских систем.
50. ОС РОСА "КОБАЛЬТ" 7.3 для серверных систем.
51. Гослинукс 6.6.
52. Гослинукс 7.2.
53. AlterOS 7.5 и выше.
54. Pardus OS 19.1. RED OS 7.2.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. резидентного антивирусного мониторинга;
2. облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
3. проверку ресурсов доступных по SMB / NFS;
4. возможность проверки памяти ядра;
5. эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
6. антивирусное сканирование по команде пользователя или администратора и по расписанию;
7. антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz ;.tbz2; .gz;.tgz; .arj.;
8. проверку сообщений электронной почты в текстовом формате (Plain text);
9. наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
10. защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / N FS от удаленного вредоносного шифрования;
11. включения опции блокирования файлов во время проверки;
12. помещение подозрительных и поврежденных объектов на карантин;
13. перехвата и проверки файловых операций на уровне SAMBA;
14. управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
15. запуск задач по расписанию и/или сразу после загрузки операционной системы;
16. экспортировать и сохранять отчеты в форматах HTML и CSV;
17. гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
18. сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
19. управления через пользовательский графический интерфейс без root прав;
20. централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
21. проверки съемных дисков; отслеживания во входящем сетевом трафике активности, характерной для сетевых атак проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/H TTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым;

22. получения данных о действиях программ на компьютере пользователя;
23. проверки памяти ядра.

2.5. Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows:

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. 32-разрядных операционных систем Microsoft Windows Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
2. Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
3. Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
4. Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.
5. 64-разрядных операционных систем Microsoft Windows Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
6. Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
7. Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
8. Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
9. Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;
10. Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
11. Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
12. Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
13. Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше;
14. Microsoft Windows MultiPoint Server 2011 Standard / Premium;
15. Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
16. Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
17. Microsoft MultiPoint Server 2012 Standard / Premium;
18. Windows Storage Server 2012;
19. Windows Hyper-V Server 2012;
20. Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; Windows Storage Server 2012 R2;
21. Windows Hyper-V Server 2012 R2;
22. Windows Server 2016 Essentials / Standard / Datacenter; Windows Server 2016 MultiPoint;
23. Windows Server 2016 Core Standard / Datacenter;
24. Microsoft Windows MultiPoint Server 2016;
25. Windows Storage Server 2016;
26. Windows Hyper-V Server 2016;
27. Windows Server 2019 Essentials / Standard / Datacenter;
28. Windows Server 2019 Core;
29. Windows Storage Server 2019;
30. Windows Hyper-V Server 2019;
31. Windows 10 Enterprise multi-session.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
2. антивирусное сканирование по команде пользователя или администратора и по расписанию;
3. запуск задач по расписанию и/или сразу после загрузки операционной системы;

4. облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
5. антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
6. защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
7. непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Tech nologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
8. анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
9. проверки контейнеров Microsoft Windows;
10. защиты от эксплуатирования уязвимостей в памяти процессов;
11. должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
12. добавлять процессы в список защищаемых;
13. ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
14. проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
15. настройки проверки критических областей сервера в качестве отдельной задачи;
16. регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
17. 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);
18. 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;
19. отключить графический интерфейс;
20. наличие удаленной и локальной консоли управления;
21. управления параметрами антивируса из командной строки;
22. централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
23. управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
24. защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак.

2.6. Требования к программным средствам антивирусной защиты мобильных устройств:

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:

1. Android 4.2-11.0.
2. iOS 10.0-14.0 или iPadOS.
3. 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;
4. проверка файловой системы устройства по требованию и по расписанию;
5. мгновенная проверка устанавливаемых приложений блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
6. наличие хранилища для изолирования зараженных объектов; обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
7. блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
8. поддержка белых списков разрешенных приложений;
9. блокировка системных приложений, в рамках контроля запуска приложений;

10. отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
11. заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
12. указать параметры подключения к wi-fi сетям; указать обязательные к установке приложения;
13. блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
14. 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;
15. поддержка технологий Samsung KNOX1 и KNOX2.

В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:

1. удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
2. отправки команды блокирования и удаления данных;
3. создавать групповые политики безопасности мобильных устройств;
4. удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
5. получать отчеты и статистику о работе мобильных устройств пользователей;
6. блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
7. централизованного управления с помощью единой консоли управления;
8. наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства,
9. такие как iTunes, Safari или Game Center, на управляемом устройстве.

2.7. 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:

1. Microsoft Windows 10 20H2 32-разрядная / 64-разрядная;
2. Microsoft Windows 10 20H1 32-разрядная / 64-разрядная;
3. Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная / 64-разрядная;
4. Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная / 64-разрядная;
5. Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная / 64-разрядная;
6. Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная / 64- разрядная;
7. Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32- разрядная / 64-разрядная;
8. Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная / 64- разрядная;
9. Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная / 64- разрядная;
10. Microsoft Windows 10 Pro 19H1 32-разрядная / 64-разрядная;
11. Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная / 64-разрядная;
12. Microsoft Windows 10 Enterprise 19H1 32-разрядная / 64-разрядная;
13. Microsoft Windows 10 Education 19H1 32-разрядная / 64-разрядная;
14. Microsoft Windows 10 Pro 19H2 32-разрядная / 64-разрядная;
15. Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная / 64-разрядная;
16. Microsoft Windows 10 Enterprise 19H2 32-разрядная / 64-разрядная;
17. Microsoft Windows 10 Education 19H2 32-разрядная / 64-разрядная;
18. Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная;
19. Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная;
20. Microsoft Windows 8 Pro 32-разрядная / 64-разрядная;

21. Microsoft Windows 8 Enterprise 32-разрядная / 64-разрядная;
22. Microsoft Windows 7 Professional Service Pack 1 32-разрядная / 64-разрядная;
23. Microsoft Windows 7 Enterprise / Ultimate Service Pack 1 32-разрядная / 64-разрядная;
24. Windows Server 2019 Standard 64-разрядная;
25. Windows Server 2019 Standard 64-разрядная;
26. Microsoft Windows Server 2019 Datacenter 64-разрядная;
27. Microsoft Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-разрядная;
28. Microsoft Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64- разрядная;
29. Microsoft Windows Server 2016 (вариант установки Server Core RS3 (v1709) (LTSB /CBB) 64-разрядная;
30. Microsoft Windows Server 2016 Standard (LTSB) 64-разрядная;
31. Microsoft Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
32. Microsoft Windows Server 2016 Datacenter (LTSB) 64-разрядная;
33. Microsoft Windows Server 2012 R2 Standard 64-разрядная;
34. Microsoft Windows Server 2012 R2 Server Core 64-разрядная;
35. Microsoft Windows Server 2012 R2 Foundation 64-разрядная;
36. Microsoft Windows Server 2012 R2 Essentials 64-разрядная;
37. Microsoft Windows Server 2012 R2 Datacenter 64-разрядная;
38. Microsoft Windows Server 2012 Standard 64-разрядная;
39. Microsoft Windows Server 2012 Server Core 64-разрядная;
40. Microsoft Windows Server 2012 Foundation 64-разрядная;
41. Microsoft Windows Server 2012 Essentials 64-разрядная;
42. Microsoft Windows Server 2012 Datacenter 64-разрядная;
43. Microsoft Windows Storage Server 2016 64-разрядная;
44. Microsoft Windows Storage Server 2012 R2 64-разрядная;
45. Microsoft Windows Storage Server 2012 64-разрядная;

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

1. VMware vSphere 6.7;
2. VMware vSphere 7.1;
3. VMware Workstation 15 Pro;
4. VMware Workstation 16 Pro;
5. Microsoft Hyper-V Server 2012 64-разрядная;
6. Microsoft Hyper-V Server 2012 R2 64-разрядная;
7. Microsoft Hyper-V Server 2016 64-разрядная;
8. Microsoft Hyper-V Server 2019 64-разрядная;
9. Citrix XenServer 7.1 LTSR;
10. Citrix XenServer 8.x;
11. Parallels Desktop 16;
12. Oracle VM VirtualBox 6.x.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

1. Microsoft SQL Server 2012 Express 64-разрядная;
2. Microsoft SQL Server 2014 Express 64-разрядная;
3. Microsoft SQL Server 2016 Express 64-разрядная;
4. Microsoft SQL Server 2017 Express 64-разрядная;
5. Microsoft SQL Server 2019 Express 64-разрядная;
6. Microsoft SQL Server 2014 (все редакции) 64-разрядная;
7. Microsoft SQL Server 2016 (все редакции) 64-разрядная;
8. Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;
9. Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;
10. Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная;
11. Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная;
12. MySQL Standard Edition 5.7 32-разрядная / 64-разрядная;

13. MySQL Enterprise Edition 5.7 32-разрядная / 64-разрядная;
14. Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и M icrosoft Azure;
15. MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
2. чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
3. настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
4. автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети;
5. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
6. централизованные установка, обновление и удаление программных средств антивирусной защиты;
7. централизованная настройка, администрирование; просмотр отчетов и статистической информации по работе средств защиты;
8. централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
9. 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;
10. иерархии триггеров, по которым происходит перераспределение;
11. тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
12. доставка обновлений на рабочие места пользователей сразу после их получения;
13. распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
14. построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
15. создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
16. поддержка мультиарендности (multi-tenancy) для серверов управления;
17. обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
18. доступ к облачным серверам производителя антивирусного ПО через сервер управления;
19. автоматическое распространение лицензии на клиентские компьютеры;
20. инвентаризация установленного ПО и оборудования на компьютерах пользователей;
21. наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
22. функция управления мобильными устройствами через сервер Exchange ActiveSync;
23. функция управления мобильными устройствами через сервер iOS MDM; отправки SMS-оповещений о заданных событиях;
24. централизованная установка сертификатов на управляемые мобильные устройства;
25. указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
26. указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
27. построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
28. наличие преднастроенных стандартных отчетов о работе системы;
29. экспорт отчетов в файлы форматов PDF и XML;

30. централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
31. создание внутренних учетных записей для аутентификации на сервере управления;
32. создание резервной копии системы управления встроенными средствами системы управления;
33. поддержка Windows Failover Clustering;
34. поддержка интеграции с Windows сервисом Certificate Authority;
35. наличие портала самообслуживания пользователей;
36. 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;
37. наличие системы контроля возникновения вирусных эпидемий;
38. установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
39. интеграции по OpenAPI;
40. установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
41. интеграции по OpenAPI;
42. управления антивирусной защитой с использованием WEB консоли;
43. двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
44. использования дополнительной аутентификация после изменения параметров учетной записи пользователя.

2.8. Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux:

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

1. Ubuntu 18.04 LTS;
2. Ubuntu 20.04 LTS;
3. Debian GNU / Linux 10.5;
4. Astra Linux Common Edition, версия 2.12;
5. Astra Linux Special Edition, версия 1.6;
6. CentOS 7.9.2009;
7. CentOS 8.3.2011;
8. Red Hat Enterprise Linux 7.9;
9. Red Hat Enterprise Linux 8.3;
10. ALT 8.3;
11. ALT 9.1.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

1. FusionCompute 8.0;
2. FusionSphere OpenStack 6.5.13.

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

1. MariaDB Server 10.3 32-разрядная / 64-разрядная с подсистемой хранилища InnoDB.
2. Антивирус предназначен для развертывания и управления защитой устройств с операционной системой Linux с помощью Сервера администрирования на базе Linux в соответствии с требованиями чистых сред Linux®.

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

1. централизованные установка, обновление и удаление программных средств антивирусной защиты;
2. централизованная настройка, администрирование;
3. просмотр отчетов и статистической информации по работе средств защиты;
4. сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
5. иерархии триггеров, по которым происходит перераспределение;
6. доставка обновлений на рабочие места пользователей сразу после их получения;
7. распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
8. построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
9. создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
10. поддержка мультиарендности (multi-tenancy) для серверов управления;
11. обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
12. доступ к облачным серверам производителя антивирусного ПО через сервер управления;
13. автоматическое распространение лицензии на клиентские компьютеры;
14. наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
15. построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
16. наличие преднастроенных стандартных отчетов о работе системы;
17. экспорт отчетов в файлы форматов PDF и XML;
18. централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
19. создание внутренних учетных записей для аутентификации на сервере управления;
20. создание резервной копии системы управления встроенными средствами системы управления;
21. наличие системы контроля возникновения вирусных эпидемий;
22. управления антивирусной защитой с использованием WEB консоли;

2.9. Требования к обновлению антивирусных баз:

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

1. создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
2. множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
3. проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

2.10. Требования к эксплуатационной документации:

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

1. «Руководство пользователя (администратора)»
2. Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной за щиты.

3. Требования к поставщику:

Поставщик должен являться официальным партнером производителя системы антивирусной защиты на территории Республики Казахстан.

При передаче лицензии на программное обеспечение поставщик должен предоставить, электронную копию действующего партнерского сертификата.

4. Требования к технической поддержке:

Поставщик должен оказать Заказчику консультационно-техническое обслуживание по вопросам настройки и эксплуатации антивирусного программного обеспечения и обеспечить следующими возможностями:

1. Техническая поддержка должна предоставляться на русском языке специалистами производителя антивирусного ПО и его партнеров на всей территории Республики Казахстан круглосуточно в праздничные и выходные дни по телефону, электронной почте и через Интернет в течении 1 года с момента продления лицензий.
2. Поставщик должен обеспечить доступ к электронной информационной системе технической поддержки производителя программного обеспечения, включающей в себя направление запросов по конкретным проблемам через систему электронной почты.
3. Доступ к вышеописанным службам должен быть открыт круглосуточно в течение всего времени оказания поддержки.
4. Поставщик должен обеспечить Заказчика получением технической информации и/или дополнительных программных компонентов для преодоления и разрешения проблем и ошибок, обнаруженных в программных продуктах производителя.
5. Гарантийное обслуживание и техническая поддержка программного обеспечении должно обеспечиваться без дополнительных расходов со стороны Заказчика.
6. Гарантийное обслуживание и техническая поддержка должны осуществляться по месту нахождения программного обеспечения.

В течение 5 (пяти) рабочих дней с даты подписания Договора Поставщик обязан предоставить Заказчику действующее авторизационное письмо, сертификат или иное подтверждение от производителя (правообладателя) программного обеспечения, подтверждающее наличие партнерских отношений и право Поставщика на реализацию и/или предоставление права использования соответствующего лицензионного программного обеспечения на территории Республики Казахстан. Предоставление указанного документа является обязательным требованием. В случае непредоставления вышеуказанных документов Заказчик вправе отказаться от исполнения Договора в одностороннем порядке (в случае наличия текста авторизационного письма и/или иных подтверждающих документов на иностранном языке к ним должен быть приложен нотариально заверенный перевод на государственный или русский язык).

Поставщик гарантирует, что поставляемое программное обеспечение является лицензионным, не является контрафактным, а предоставляемые лицензии являются действительными и предоставляют Заказчику право использования программного обеспечения в объеме и на срок, предусмотренные Договором и технической спецификацией.

В случае отказа и/или невозможности Поставщика выполнить свои обязательства по Договору, а также просрочки поставки товара на срок свыше 30 (тридцати) календарных дней, Поставщик обязан оплатить Заказчику штраф в размере 10% от суммы Договора.

Подписал	Сатубалдина Зарина Малкаждаровна
Дата подписания	02.11.2026