

Техникалық сипаттама

Қазақстан Республикасының мемлекеттік сатып алу туралы негізгі (орнатылған) жабдықты, сондай-ақ орнатылған бағдарламалық қамтамасыз етуді (лицензияланған бағдарламалық қамтамасыз етуді) толық қамтамасыз ету, жаңғырту және қайта жабдықтау үшін

Dr.Web Enterprise Security Suite + ЦУ:

АБҚ лицензиясының қосымша жабдығымен 12 айға ұзарту: Dr.Web Desktop Security Suite – 140 жұмыс станциясын ұзарту

10 жұмыс станциясын қосымша сатып алу (бұдан әрі – Жүйе).

1 Жалпы талаптар

- 1.1 Конкурса қатысушылар Жүйе өндірушісінің авторизация хатын ұсынуы тиіс, хатта өндіруші компаниямен тауарды жеткізу және оған қолдау көрсету қарым-қатынасының жасалғаны расталуы тиіс.
- 1.2 Конкурса қатысушылар Жүйенің өндіруші компаниясы берген атаулы сертификаттың көшірмесін ұсынуы шарт, сертификатта бағдарламалық құрал пайдаланылатын бүкіл мерзім ішінде Тапсырыс берушінің мамандарына техникалық қолдау көрсету үшін Жүйені әкімшілендіру жөніндегі сертификатталған маманның бар екені расталуы тиіс.
- 1.3 Өндірушінің Қазақстан Республикасындағы жергілікті техникалық қолдауды орыс және қазақ тілінде көрсету қызметінің болуы шарт.
- 1.4 Барлық антивирус құралының бағдарламалық интерфейсі орыс және қазақ тілінде жасалған болуы керек.
- 1.5 Microsoft Windows операциялық жүйесімен басқарылатын бүкіл антивирус құралында, соның ішінде басқару құралдарында, орыс және қазақ тіліндегі мәнмәтіндік анықтамалық жүйе болуы шарт.
- 1.6 Конкурса қатысушы барлық жеткізілетін өнімдерге бірінғай сериялық нөмірді беруі керек. Бүкіл жеткізілетін бағдарламалық өнімдердің лицензиялық негізгі файлдарының жарамдылық мерзімі сериялық нөмірді іске қосқан сәттен басталуы керек.
- 1.7 Контрафактілік бағдарламалық қамтамасыз етуді жеткізуді болдырмау мақсатында әлеуетті өнім беруші бағдарламалық қамтамасыз етудің заңды шығу тегін растайтын өндіруші компаниядан хат ұсынуы тиіс.

2. Бағдарламалық құралдарға қойылатын талаптар

2.1. Антивирус қорғанысына қойылатын жалпы талаптар

- 2.1.1. Жүйенің бағдарламалық құралдары келесі түрдегі қауіптерді анықтауды қамтамасыз етуі керек: классикалық вирустар, трояндық бағдарламалар, руткиттер, желілік құрттар, жарнамалық бағдарламалар, ақылы сайттарға автоматты қоңырау шалу, ықтимал қауіпті қолданбалар және басқа да зиянды бағдарламалар.
- 2.1.2. Антивирус қорғанысы мыналарды қамтамасыз етуі тиіс:
 - 2.1.2.1. 64 разрядты операциялық жүйеге бағытталған қатерді анықтау, соның ішінде модуль антируткитінің арнайы 64 битті нұсқасының көмегімен анықтау;

- 2.1.2.2.** мұрағаттар мен қапталған файлдарды тексеруді жеделдету мақсатында ашу құралын іске қоспай зиянды бағдарламаларды анықтау;
- 2.1.2.3.** файлдағы PKLITE, LZEXE, DIET, COM2EXE және с.с. типті бағдарламалармен қапталған вирустарды тауып жою;
- 2.1.2.4.** шифрланған контейнерлері бар ACE (2.0 нұсқасына дейін), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (соның ішінде NRG, сектордың бейстандартты форматы бар және сигнатуралары жоқ бейнелер), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER форматындағы контейнерлер мен мұрағатталған файлдардағы вирустарды тексерілетін нысандардың салыну деңгейіне қойылатын шектеуге қарамастан анықтау;
- 2.1.2.5.** қатаң форматы жоқ (HTML, MIME), контейнерлердегі вирустарды анықтау;
- 2.1.2.6.** нысан мөлшері анық емес контейнер ішіндегі вирустарды анықтау (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES және т.с.с.);
- 2.1.2.7.** форматы Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 және жоғары); SETUP FACTORY (7.8 тізбегіндегі); XENOCODE; TARMA INSTALL (3-тізбек); XZ (UNIX); COMPRESS; SQUAHFS; ZAYAL; LLERIL; CHILKAT ZIP; LHA (AWARD BIOS) бумасы бар файлдар мен нысандарда вирустың болуы тексеру;
- 2.1.2.8.** қаптамадан өздігінен шығатын мұрағаттардағы вирустарды тексеру: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFX, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, ALZayc, Setup Factory, lleril; Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
- 2.1.2.9.** төмендегідей қаптағыштармен қапталған орындалатыны файлдарды тексеру: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR, ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, сондай-ақ Mozilla Thunderbird поштасындағы файлдарды олардың мөлшеріне қарамастан тексеру;
- 2.1.2.10.** форматталмаған пошта базаларын талдау және тіркемесі үлкен хаттарды өңдеу (мысалы, жауаптары көп хаттарды және қайта жіберілген хаттарды RE/FW), TNEF форматын қолдау;
- 2.1.2.11.** Тиісті ақпаратты антивирус базаларына енгізгеннен кейін жасалған және әлі антивирустық зертханаларға талдауға түсе қоймаған антивирус базаларында ақпараты бар зиянкес бағдарламалар тобына жататын зиянкес бағдарламалардан эвристикалық талдау негізінде және файл ішінде кодтардың орналасу аймағын талдауға негізделген ұқсас вирустарды іздеу технологиясы арқылы қорғау;
- 2.1.2.12.** HTML және PDF құжаттарда зиянкес нысандарды, соның ішінде осы типтегі құжаттарда тұрған JavaScript ішіндегі обфускацияланған эксплойттарды табу. «көрінбейтін» IFRAME-элементтерді шығарып талдау мүмкіндігі. Кез келген күрделі скриптілерді шығару мүмкіндігі және олардың қорғанысын алып тастау;
- 2.1.2.13.** лицензиялық деректерге келетін қатерді анықтау (ASPROTECT, PEP және ENIGMA);
- 2.1.2.14.** DEX-файлдардағы (Android) зиянкес нысандарды анықтау;
- 2.1.2.15.** белгісіз қаптағыштармен жасырынған вирустарды тауып жою.
- 2.2. Антивирус қорғанысын басқару жүйесіне қойылатын талаптар**

- 2.2.1.** Жүйе тек серверлерде ғана емес, сонымен қатар келесі операциялық жүйелерде жұмыс істейтін жұмыс станцияларында орталықтандырылған антивирустық серверді орнату мүмкіндігімен клиент-сервер архитектурасына құрылуы керек:
- Microsoft Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11;
 - Microsoft Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022;
 - Linux, егер glibc 2.13 немесе одан кейінгі нұсқасы болса;
 - FreeBSD 11.3 немесе одан кейінгі нұсқасы.
- 2.2.2.** Бұл ретте орталықтандырылған басқару сервері операциялық жүйелеріне қарамастан, барлық қорғалатын нысандар үшін бірдей болуы керек: Windows/Linux/macOS/Android.
- 2.2.3.** Басқару жүйесі Windows® Internet Explorer®, Microsoft Edge®, Mozilla® Firefox®, Google Chrome®, Opera®, Safari® (соның ішінде Microsoft Windows, Linux, FreeBSD ОЖ) браузерлері қолданылатын кез келген операциялық жүйеден қолдану үшін қолжетімді болуы керек әрі браузерлердің соңғы нұсқаларын пайдалану мүмкіндігі шектелмеген және басқару сервері жақтан да, Жүйе әкімшісі жақтан да қандай да бір бағдарламалық құралды қосымша орнату қажет болмауы шарт.
- 2.2.4.** Әкімшілердің аутентификациясы келесі тәсілдермен орындалуы тиіс:
- Сервердің дерекқорынан;
 - LDAP/AD пайдалану арқылы;
 - RADIUS пайдалану арқылы;
 - PAM пайдалану арқылы.
- 2.2.5.** Лицензияларды сервис аралық байланыстар арқылы тарату мүмкіндігі бар басты, бағыныңқы және тең құқықты басқару серверлерінің иерархиялық жүйесін құру мүмкіндігі, сондай-ақ лицензиялық негізгі файлды автоматты түрде жаңарту мүмкіндігі қарастырылған болуы тиіс.
- 2.2.6.** Басқару жүйесінің төмендегідей мүмкіндігі болуы керек:
- бірнеше серверден алынған ақпаратты бір серверге біріктіру;
 - желіге түсетін жалпы жүктемені азайту мақсатында жаңартуларды алу үшін жұмыс станцияларын серверлерге бөліп тарату;
 - нұсқалары әртүрлі антивирус серверлері арасында бір иерархиялық желі шеңберіндегі статистикамен алмасу;
 - әкімшілер мен пайдаланушылардың рөлдерін, сондай-ақ әр деңгейде берілетін есеп түрлерін баптауға болатын көп деңгейлі басқару жүйесін құру.
- 2.2.7.** iOS және Android операциялық жүйелерінде веб-браузерді пайдаланбай Жүйені мобильді басқару орталығын іске қосу мүмкіндігі қарастырылған болуы керек.
- 2.2.8.** Басқару жүйесінің төмендегідей мүмкіндігі болуы керек:
- 2.2.8.1.** сыртқы және ішкі ДҚБЖ (антивирус серверінің дистрибутивімен бірге жеткізіледі) пайдалану. Oracle, PostgreSQL, Postgres Pro, Jatoba, кез келген ДҚБЖ MS Windows және Linux операциялық жүйелеріне арналған ODBC драйвері арқылы сыртқы ДҚБЖ бола алады;
- 2.2.8.2.** Сервер бөлігін орнатқаннан кейін жұмыс барысында пайдаланылатын ДҚБЖ түрін алмастыру, бұл кезде Жүйенің сервер бөлігін қайта орнату қажет болмауы керек.
- 2.2.8.3.** басқару жүйесінің құралдарының дерекқорын басқаруы, соның ішінде дерекқорын тазарту, оны талдау мүмкіндігі, еркін түрде SQL-сұрау жасау;
- 2.2.8.4.** кірістірілген Web API арқылы сыртқы жүйе тармақтарымен біріктірілген жағдайда осы Web API функцияларының көмегімен әрекеттер аудитін жүргізу мүмкіндігі болуы шарт;

- 2.2.8.5. оқиғалар өңдеушісінің Lua тілінде өз бетінше жазу, сондай-ақ басқару жүйесінің құралдары көмегімен еркін Lua-скрипттерді жасау;
- 2.2.8.6. есептерді CSV, XML, HTML және PDF форматтарына экспорттау;
- 2.2.8.7. басқару орталығының консолінде жүйе әзірлеушісінен өзекті қауіп-қатер туралы ақпарат беретін жаңалықтарды алу және сондай жаңалықтарға жазылу;
- 2.2.8.8. қолданушы мен әкімшіге пошта хабарын, дауыстық хабарлама жолдау, қалқыма терезе шығару, оқиғалар журналына жазу, SNMP-trap арқылы хабар жеткізу жолдарының көп болуы;
- 2.2.8.9. хабарлама мәтіні, интернет-ресурстардың сілтемелері, кез келген графикалық суреті бар мазмұны еркін ақпараттық хабарламаны Жүйенің Web-интерфейсінен шынайы уақыт режимінде желі арқылы жолдау;
- 2.2.8.10. агенттерді орнату және жаңарту кезінде желі трафигін шектеу;
- 2.2.8.11. Android, macOS және UNIX тобының операциялық жүйесіне арналған антивирус агенттерін қосу баптаулары бар конфигурациялық файлдарды жүктеп алу;
- 2.2.8.12. барлық қорғалатын нысандардағы, соның ішінде мобильді және off-line режимінде тұрған антивирус базаларын орталықтан жаңарту. Жаңартуларды нысандарға кесте бойынша алғаннан кейін бірден жеткізу;
- 2.2.8.13. антивирус серверінің репозиториінде тұрған өнімдердің жаңартуларының ревизиясын, соның ішінде жаңартуларды кейін шегертуді басқару;
- 2.2.8.14. топтық жаңартулар мүмкіндігінің болуы;
- 2.2.8.15. SSL-сертификаттарды пайдаланатын қорғалған арна арқылы жаңарту;
- 2.2.8.16. кейінге қалдырылған жаңартуды ұйымдастыру;
- 2.2.8.17. орнатылған бағдарламалық құралдың жаңа нұсқаларға автоматты түрде көшуі, соның ішінде ж ртылатын компоненттерді таңдау мүмкіндігімен көшуі;
- 2.2.8.18. орнатылатын компоненттерді клиент бөліктеріне антивирус топтамасын орнатқанға дейін таңдау;
- 2.2.8.19. әкімшінің және қолданушының толық құжат топтамасын басқару орталығының консолінен тікелей оқу.
- 2.2.9. Жүйе мобильді пайдаланушылар (ноутбуктер) үшін арнайы саясаты болуы керек , оны қолданған кезде мобильді пайдаланушылар антивирустық серверге қол жетімділік болмаған кезде антивирустық пакеттің параметрлерін редакциялауға және интернет арқылы жаңартуға қабілетті болуы керек. Саясатты қолдану *.xml типті конфигурация файлдарын пайдалануды қажет етпестен Web-интерфейсі арқылы жүзеге асырылуы тиіс.
- 2.2.10. Басқару жүйесінде маңызды деректерді автоматты түрде көшіру және алдын-ала белгіленген кесте бойынша антивирустық сервердің конфигурациясы, сондай-ақ серверді сақтық көшірмеден қалпына келтіру мүмкіндігі болуы керек.
- 2.2.11. Басқару орталығында алдын ала орнатылған жүйелік және қолданушылық топтар негізіндегі топтық саясат жасалған болуы тиіс,. Алдын ала орнатылған жүйелік топтар барлық қорғалатын нысандарға Active Directory нысандары, операциялық жүйелер, саясаттар, баптау профильдері, желі протоколдары, нысан мәртебесі, дербес баптаулар арқылы жүгінуге мүмкіндік беруі тиіс.
- 2.2.12. Басқару жүйесі қолданбалардың іске қосылуын тыйым салушы және рұқсат беруші ережелер негізінде әрі қолданбалардың функционалдық талдауы негізінде: қолданбаларды іске қосу, модульдерді жүктеу және орындау, скрипт түсіндірушілерін

іске қосу, драйверлерді жүктеу, MSI-топтаманы орнату, орындалатын файлдардың толықтығы сияқты топтар бойынша бақылай алуы тиіс.

- 2.2.13. Орталықтандырылған басқару сервері арқылы, антивирустық бағдарламалық құрал мониторингі бойынша есеп беру.
- 2.2.14. Антивирустық қорғау жүйесінің жай-күйі туралы есептерді құру және оларды біріктіру арқылы статистикалық ақпаратты орталықтандырып жинау, одан әрі, кейіннен әкімшіге электрондық пошта арқылы жібере отырып, көрсетілген параметрлер бойынша статистикалық есептерді автоматты түрде жасау мүмкіндігі.
- 2.2.15. Жүйеде лицензиялық кілттердің иерархиялық тізімін жүргізетін лицензиялар менеджері іске асырылуы керек. Лицензиялар менеджері келесі мүмкіндіктерді қамтамасыз етуі керек: лицензия туралы ақпаратты қарау, жаңа лицензиялық кілтті қосу, лицензиялық кілтті жаңарту, лицензиялық кілтті ауыстыру, нысанның лицензиялық кілттерінің тізімін кеңейту, лицензиялық кілтті жою және лицензиялау тізімінен нысанды жою, лицензияларды көрші басқару серверіне тасымалдау, көрші басқару серверіне тасымалданатын лицензияларды өңдеу.
- 2.2.16. Жүйе құпия ақпараттың ағып кетуіне жол бермеу үшін серверлер мен қорғалған станциялар арасындағы трафикті шифрлай алуы керек.
- 2.2.17. Жүйе өндірушісі вирус базаларының жаңартуларын тәулігіне кемінде 20 рет шығарғанда, ол Жүйе жасаған есепте расталуы тиіс;
- 2.2.18. Антивирус серверлері орналастырылған жағдайда, Интернет желісі қолжетімді емес ішкі желіде репозиториді автономды түрде жүктейтін арнайы утилитка көмегімен жаңартуларды алу мүмкіндігі болуы керек.
- 2.2.19. Виртуалды инфрақұрылымды қолдау, виртуалды жұмыс орындары инфрақұрылымымен (VDI) біріктіру, VMware, Microsoft Hyper-V, Xen, KVM (Kernel-based Virtual Machine) гипервизорларын қолдау.

2.3. Microsoft Windows тобының операциялық жүйесімен басқарылатын жұмыс станциялары мен серверлердің антивирустық қорғаныс құралдарына қойылатын талаптар

- 2.3.1. Тендерді өткізу кезінде өзекті БҚ түрін пайдаланғанда, жүйе (орталықтандырылған басқару жүйесі көмегімен бірге) операциялық жүйенің басқаруымен жұмыс станциялары мен серверлердің қорғанысын қамтамасыз етуі тиіс.
 - MS Windows XP SP2 / Windows Vista SP2/ Windows 7 SP1/ Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
 - MS Windows Server 2003 SP1 / Windows Server 2008 SP2/ Windows Server 2008 R2 SP1/ Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022.
- 2.3.2. Жүйенің бағдарламалық құралы жұмыс станцияларында антивирус және спамға қарсы қорғанысты жүзеге асыруды, оның ішінде руткиттер технологияларынан тұрақты қорғауды, резидент антируткит драйверінің болуын қамтамасыз етуі керек.
- 2.3.3. Жүйеде зиянкес бағдарламалар вирус жұқтырған желі нысандарын алдын ала емдеместен, оларға өз компоненттерін орнату мүмкіндігі болуы керек.
- 2.3.4. Нысанда іске қосылып тұруы ықтимал зиянкес бағдарламаларға қарсы әрекет ету мақсатында, орнату үшін антируткитпен қорғалған орнатқыш бағдарлама (Windows Installer-ді қолданбай) пайдаланылуы шарт.
- 2.3.5. Интернет желісіне қосылу арнасының ықтимал шектеулеріне байланысты қорғау жүйесін орнату Интернет желісіне қосылмастан мүмкін болуы керек – дистрибутивті қорғау жүйесінің барлық компоненттері, сондай-ақ зиянкес бағдарламалар мен Интернет желісі ресурстарының дерекқоры болуы тиіс.

- 2.3.6.** Қорғаныс жүйесінің жұмысы үшін сыртқы кітапханалар және .Net Framework ортасы пайдаланылмауы тиіс, олардың бүтіндігі өзін-өзі қорғау жүйесінің бақылауында тұрмаған және оларды әшкерелеу салдарынан қорғаныс жүйесінің ақпараты қате көрсетілуі немесе қорғаныс жүйесінің интерфейсіне байланысты басқа да проблеманы туындатуы мүмкін.
- 2.3.7.** Жүйе компоненттерінде пайдаланушылардың жайлы жұмыс істеуін қамтамасыз ету үшін, соның ішінде «оқу үшін» ашылатын файлдарды кейін тексеру мүмкіндігі есебінен ДК ресурстарын пайдалануды басқару, сондай-ақ заманауи құрылым ерекшеліктерін пайдалану мүмкіндігі болуы керек.
- 2.3.8.** Жүйе жергілікті желіде және Интернет желісінде жұмыс істеген кезде қорғанысты қамтамасыз ететін конфигурациямен, Web-беттермен, электрондық поштамен, жергілікті қатты дискілермен және алмалы-салмалы тасығыштармен бірге жеткізілуі тиіс. Кіріс және шығыс электрондық хаттар зиянкес бағдарламалардан және спамнан қорғалған болуы шарт.
- 2.3.9.** Жүйе пайдаланушылардың Интернеттегі жұмыс уақытын, сонымен қатар компьютерде жұмыс істеу уақытын шектей алуы керек.
- 2.3.10.** Пайдаланушыларға арналған антивирус топтамасы компоненттерінің баптауларына кіру рұқсатының құқықтарын Жүйе әкімшісі белгілеуі тиіс және пайдаланушыларда әкімші берген құқықтар шегінде ғана оларды өз бетінше және құпия сөзді қолданбастан баптау мүмкіндігі болуы керек.
- 2.3.11.** Жұмыс станцияларын қорғау жүйелері Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin және басқа қолданбалардағы лезделік хабарламалардың трафигін сүзуді, соның ішінде қайта жолданатын тіркемелердің антивирустық тексерісін, сондай-ақ хабарламалардан зиянкес және фишингтік сайттарға апаратын сілтемелерді автоматты түрде жоюды қамтамасыз етуі керек.
- 2.3.12.** Жұмыс станцияларын қорғау жүйесі Google, Yandex, Yahoo! Bing, Rambler іздеу жүйелері нәтижелерінің шығарылуын тек іздеу жүйелері мен қорғау жүйесі тұрғысынан қауіпсіз деп саналатын ресурстарды көрсетіп сүзуі тиіс.
- 2.3.13.** Қолданбалар деңгейінде, нақты бағдарламалар мен процестердің желі ресурстарына қол жеткізуін басқаруға және қолданбалар журналында қол жеткізу әрекеттері туралы ақпаратты тіркеуге мүмкіндік беретін желілік қосылымдарды басқару.
- 2.3.14.** Қосылымға бастама болатын бағдарламаларға тәуелсіз Интернет желісіне кіруді басқаруға мүмкіндік беретін бумалар деңгейіндегі сүзу.
- 2.3.15.** Жүйеде төмендегідей компоненттерден тұратын сигнатуралық және эвристикалық талдауға қосымша алдын ала қорғау жүзеге асырылуы керек:
- бопсалаушылардан қорғағыш – трояндық-шифрлаушылардан қорғауға мүмкіндік береді;
 - эксплойттардан қорғағыш – жүйеге ену үшін танымал қолданбаларда осалдықтарды пайдалануға тырысатын зиянды нысандардан қорғауға мүмкіндік береді;
 - әрекет талдауы – жүйе тұрғысынан маңызды болып табылатын барлық салаларда іске қосылған бағдарламалардың әрекетін бақылау, мысалы: HOSTS файлы; іске қосылған қолданбалардың тұтастығы; дискіге төмен деңгейлі қол жеткізу; драйверлерді жүктеп салу; қолданбаларды іске қосу параметрлері; мультимедиялық құрылғы драйверлері; Winlogon қабықшасының параметрлері, Winlogon нотификаторлары; Windows қабықшасының автоматты іске қосылуы; орындалатын файлдардың ассоциациялары; бағдарламаларды іске қосуды шектеу саясаты (SRP); Internet Explorer плагиндері (ВНО); бағдарламаларды автоматты іске қосу; саясаттарды автоматты іске қосу; қауіпсіз режимді конфигурациялау; Windows сеансы диспетчерінің параметрлері; жүйелік қызметтер.
- 2.3.16.** Жүйе өзінің барлық объектілерін, соның ішінде маңызды файлдарды, процестерді, терезелерді, кілттерді және т.б. пайдаланушылардың рұқсатсыз кіруінен және зиянды бағдарламалардан өзін-өзі қорғауды жүзеге асыруы керек, олар жүйенің ең төменгі

деңгейінде жұмыс істеуі керек және антивирустық жүйенің драйвелреін түсіру және тоқтату мүмкіндігін шектеуі керек.

2.3.17. Виртуалды агенттерді орнату арқылы виртуалды жұмыс орындарын қорғауды жүзеге асыру мүмкіндігі.

2.4. Linux тобының операциялық жүйесімен басқарылатын жұмыс станциялары мен серверлердің антивирустық қорғаныс құралдарына қойылатын талаптар

2.4.1. Құрылымы төмендегідей процессорларды және пәрмендер жүйесін қолдау:

- Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64);
- ARM64;
- IBM POWER (ppc64el).

2.4.2. Жүйе операциялық жүйелердің басқаруымен 3.6 - 4.16 Samba немесе Novell Storage Services (NSS) версияларын пайдаланатын жұмыс станциялары мен серверлердің қорғанысын қамтамасыз етуі тиіс:

- 2.6.37 және жаңа нұсқалы ядро негізінде жасалған, PAM және 2.13 мен жаңа нұсқалы glibc кітапханасын пайдаланатын Linux;
- FreeBSD 11, 12;
- Novell Open Enterprise Server SP2 на базе SUSE Linux Enterprise Server 10 SP3 және жаңалары.

2.4.3. Жүйенің Samba-мен бірігуі VFS (Virtual File System) модулінің көмегімен жасалуы тиіс.

2.4.4. Нұсқасы жоғарыда көрсетілгендерден басқа Samba нұсқасын немесе Linux тобының 64-битті платформаларына арналған Samba пайдаланылған жағдайда, біріктіру модульдерін бастапқы кодтардан компиляциялау мүмкіндігі болуы тиіс.

2.4.5. Операциялық жүйенің типі мен нұсқасына қарамастан, UNIX-жүйелеріне арналған әмбебап топтамадан репозиторийді немесе операциялық жүйеде топтама менеджері пайдаланатын жұмысқа есептелген топтаманы орнату мүмкіндігі.

2.4.6. Жүйені пәрмен жолағынан және графикалық орнатқыш көмегімен орнату және жанарту мүмкіндігі.

2.4.7. Жүйенің қажетті компоненттерін орнату үшін қажет модульдерді автоматты түрде орнату мүмкіндігі.

2.4.8. Жүйенің компоненттерін зиянкес бағдарламалар вирус жұқтырған нысандарды алдын ала емдемей сол нысандарға орнатып, одан кейін белгіленген файл аймақтарын емдеу мүмкіндігі.

2.4.9. SELinux қосымша қауіпсіздікті қамтамасыз ететін ішкі жүйелерге, PARSEC рұқсатын мандаттық басқару жүйесін, сондай-ақ тұйық бағдарлама ортасын (ТБО) режимін қолдау.

2.4.10. Операциялық жүйе ұсынатын fanotify механизмін пайдалану арқылы және Linux (Linux kernel module) ядросының арнайы модулінің көмегімен файл жүйесін мониторингілеу мүмкіндігі.

2.4.11. Файл жүйесінің жаңа томдарын орнату және бөлшектеу сәтін (мысалы, USB-flash, CD/DVD жинақтағыштарында, RAID массивтері және т.б.) автоматты түрде анықтау және қажетіне қарай бақылау жасалатын аймақтар тізімін түзету мүмкіндігі.

2.4.12. Файл кеңістігін сканерлеу кезінде сервер ресурстарын пайдалану процесін басқару мүмкіндігі.

2.4.13. Мұрағат, пошта файлдары, қапталған нысандар мен басқа да контейнерлер сияқты құрамдас файлдарды тексеру параметрлерін басқару мүмкіндігі.

- 2.4.14. Жүйеде SSL және TLS негізіндегі протоколдарды пайдаланатын қорғалған желі қосылыстары арқылы берілетін трафикті тексеру мүмкіндігі бар орнаған желі қосылыстарын тұрақты түрде бақылау функциясы қарастырылуы тиіс.
- 2.4.15. Жүйеде Интернет ресурстарын санаттары бойынша құлыптау, сондай-ақ Ақ/Қара тізімдер режимінде жұмыс істеу мүмкіндігі бар веб-сүзгі болуы тиіс.
- 2.4.16. Жүйе бір уақытта бірнеше тексеру процесін жасау мүмкіндігін қолдауы тиіс.
- 2.4.17. Жүйенің бағдарламалық құралдары келесі функционалдық мүмкіндіктердің орындалуын қамтамасыз етуі керек:
- 2.4.17.1. түрі белгілі барлық вирустарды тауып жою;
- 2.4.17.2. қауіп-қатердің болуын толық немесе таңдап тексеруге негізделген және әкімшінің пәрмені бойынша не кесте бойынша жасалатын антивирустық сканерлеу;
- 2.4.17.3. Серверге жүктелетін не одан шығатын файлдарды «жолдан ұстап» орындалатын антивирустық тексеру;
- 2.4.17.4. Операциялық жүйе жүктелген кезде антивирустық бағдарламалық құралдың және басқа да қажеті компоненттердің автоматты түрде бірге іске қосылуы;
- 2.4.17.5. тапсырмаларды кесте бойынша және/немесе операциялық жүйе жүктелгеннен кейін бірден іске қосу;
- 2.4.17.6. іске қосу параметрлері көрсетілген сканерлеу кестесін баптау.
- 2.4.18. Бағдарлама веб-интерфейс арқылы да, тікелей конфигурациялық файлдар арқылы да басқарылуы тиіс. Антивирустық тексеріс жүргізілуі тиіс файлдар мен каталогтарды, сондай-ақ әртүрлі зиянкес нысандарға қатысты қолданылатын әрекеттерді көрсетуге болатын антивирустық сканерлеу параметрлерін баптау мүмкіндігі.
- 2.4.19. Сканерлеуші ядро файлдардағы және диск құрылғыларының жүктеу жазбаларынан MBR - Master Boot Record, VBR - Volume Boot Record) вирустарды және басқа да зиянкес нысандарды іздеуді қамтамасыз етуі тиіс.
- 2.4.20. Файлдарды тексеру үшін лектік тексеру әдісін (flow), сондай-ақ проксилеу әдісін (proxy) қолдану мүмкіндігі.
- 2.4.21. Желі арқылы алынған файл түрінде көрсетілмеген деректерді тексеру, сондай-ақ файлдарда қауіп-қатердің болуын бөліп тексеруді ұйымдастыру мүмкіндігі.
- 2.4.22. Басқару веб-интерфейсіне кіруге болатын жергілікті құрылғыдағы файлдарда қауіп-қатердің болуын шұғыл тексеру мүмкіндігі.
- 2.4.23. Жойылған желі тораптарында тұрған файлдарда қауіп-қатердің болуын тексеру мүмкіндігі. Осындай тораптар ретінде жұмыс станцияларымен және серверлермен қатар, роутерлер, ТД-тіркемелер және Secure Shell немесе Telnet кіру рұқсатын беретін «Интернет заттарды» құрайтын өзге де «ақылды» құрылғылар бола алады.
- 2.4.24. Жүйе құрамында мониторинг жүйелерімен (Munin, Nagios, Zabbix) біріктіруге арналған SNMP-агент болуы тиіс.
- 2.4.25. Антивирус қорғанысын орталықтан басқаратын жүйеге біріктіру жүйе әкімшісіне барынша қолайлы болатын антивирус қорғанысы жүйесін «бір жерден» басқаруға мүмкіндік береді.
- 2.5. Жұмыс станциялары мен macOS серверлерінің антивирустық қорғаныс бағдарламалық құралдарына қойылатын талаптар**
- 2.5.1. Заманауи қауіп-қатерді анықтау және жою технологияларын пайдаланып, macOS басқаруындағы құрылғыларды кез келген түрдегі келесідей қатерден қорғау: вирустар,

руткиттер, трояндық бағдарламалар, тыңшылық және жарнамалық бағдарламалар, хакерлік утилиттер және әртүрлі зиянды нысандар.

- 2.5.2. Операциялық жүйелердің келесі нұсқаларымен жұмыс істейтін құрылғыларды қорғау: OS X 10.11 El Capitan / macOS 10.12 Sierra / macOS 10.13 High Sierra / macOS 10.14 Mojave / macOS 10.15 Catalina / macOS 11 Big Sur / macOS 12 Monterey / macOS 13 Ventura / macOS 14 Sonoma.
- 2.5.3. Автоматты іске қосу нысандарын, ауыстырылатын ақпарат тасымалдауыштарын, желілік және логикалық дискілерді, пошталық форматтарды, файлдар мен каталогтерді, соның ішінде қапталған және мұрағатталғандарын тексеру.
- 2.5.4. Нақты уақыт режимінде файлдық жүйені бақылау, тексеруден жеке қалталар мен файлдарды алып тастау мүмкіндігімен іске қосылған бағдарламалар мен процестерді басқару.
- 2.5.5. Интернет трафикті нақты уақыт режимінде HTTP/HTTPS хаттамасы бойынша онда қатердің бар-жоғын бақылау, ұсынылмаған сайттарға, сондай-ақ жекелеген сайттар мен интернет-ресурстардың санаттарына кіруді шектеу, пайдаланушы анықтаған белгілі бір қолданбаларға арналған жекелеген сайттардың веб-трафигін және желілік қосылыстарын тексеруден алып тастау.
- 2.5.6. Барлық шығыс және кіріс желілік трафикті басқару, таңдалған жұмыс режиміне және жеке сүзу ережелеріне сәйкес қолданбаның желі ресурстарына қол жеткізу мүмкіндігін бұғаттау.
- 2.5.7. Қолданбаның веб-камералар мен микрофондарға қол жеткізуін басқару арқылы құпиялылықты қорғау.
- 2.5.8. Қатердің анықталғаны, оларды жою немесе компоненттер жұмысында қателік туындағаны туралы хабарламаларды көрсететін macOS жүйелік хабарламаларын пайдалану.
- 2.5.9. Пайдаланушыны вирусталған файлдардан және қажетсіз сайттарға кіруінен қорғау үшін әзірлеуші компаниялардың қарапайым сервистерге қосылу мүмкіндігі.

И.о. начальника службы АСУ:



Котова Е.В.

Руководитель по материально-
техническому снабжению и
управлению персоналом и офицер-
комплаенс
_____Какимов Т.Б.

Техническая спецификация

Согласно закону РК о государственных закупках для доукомплектования, модернизации и дооснащения основного (установленного) оборудования, а также установленного программного обеспечения (лицензионного программного обеспечения)

Наименование:

Продление

Dr.Web Enterprise Security Suite

Продление с доукомплектованием лицензии АПО на 12 месяцев:

**Dr.Web Desktop Security Suite + ЦУ – 140 рабочих станций продление
10 рабочих станций дозакуп, (далее - Система).**

Наименование: Система комплексной антивирусной защиты с централизованным управлением для защиты рабочих станций, файловых серверов, почтовых серверов, интернет-шлюзов и мобильных устройств (далее - Система).

1 Общие требования

- 1.1** Участники конкурса должны представить авторизационное письмо от производителя Системы, подтверждающее наличие партнерских отношений с компанией-производителем на поставку и поддержку товара.
- 1.2** Участники конкурса должны предоставить копию именного сертификата, выданного компанией-производителем Системы, подтверждающего наличие сертифицированного специалиста по администрированию Системы для оказания технической поддержки специалистов Заказчика в течение всего срока использования программного обеспечения.
- 1.3** Наличие локальной службы технической поддержки от производителя в Республике Казахстан как на русском, так и на казахском языках.

- 1.4 Программный интерфейс всех антивирусных средств, включая средства управления, должен быть реализован как на русском, так и на казахском языках.
- 1.5 Все антивирусные средства, функционирующие под управлением операционных систем семейства Microsoft Windows, включая средства управления, должны обладать контекстной справочной системой как на русском, так и на казахском языках.
- 1.6 Участник конкурса должен предоставить единый серийный номер для всех поставляемых продуктов. Срок действия лицензионных ключевых файлов на все поставляемые программные продукты должен начинаться с момента активации серийного номера.
- 1.7 В целях исключения поставки контрафактного программного обеспечения потенциальный поставщик должен предоставить письмо от компании производителя подтверждающего легальное происхождение программного обеспечения.

2 Требования к программным средствам

2.1 Общие требования к антивирусной защите

- 2.1.1 Программные средства Системы должны обеспечивать определение угроз следующих типов: классических вирусов, троянских программ, руткитов, сетевых червей, рекламных программ, программ автодозвона на платные сайты, потенциально опасных приложений, прочих вредоносных программ.
- 2.1.2 Антивирусная защита должна обеспечивать:
 - 2.1.2.1 обнаружение угроз, направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля;
 - 2.1.2.2 опознание вредоносных программ без запуска распаковщика - в целях ускорения проверки архивов и упакованных файлов;
 - 2.1.2.3 обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
 - 2.1.2.4 обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
 - 2.1.2.5 обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME);
 - 2.1.2.6 обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE, ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.);
 - 2.1.2.7 антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); LLERIL; INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; ZAYAL; CHILKAT ZIP; пакеты LHA (AWARD BIOS);
 - 2.1.2.8 антивирусную проверку в самораспаковывающихся архивах: AppPackager, Astrum Install Wizard, Create Install, Fly Studio, GSFx, Hot Soup, Inno Setup, Install Essen, Install Factory, Linder Setup, NSIS (NullSoft Installation System), RSFX, SEA, ALZayc, LLERIL, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy;
 - 2.1.2.9 проверку исполняемых файлов, упакованных следующими упаковщиками: PELOCK, ENIGMA Protector, NSPACK, NTKRNL, EXECRYPTOR, PESPIN, EXPRESSOR,

ASPROTECT, PECOMPACT, PACKMAN, SEA, ULTRAPROTECT, ASPACK, PETITE, NEOLITE, GENPACKER, BERO, RCRYPTOR, PECRYPT, а также почтовых файлов Mozilla Thunderbird- вне зависимости от их размера;

- 2.1.2.10** разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF;
- 2.1.2.11** защиту от вредоносных программ, принадлежащих семействам вредоносных программ, информация о которых имеется в антивирусных базах, созданных после занесения соответствующей информации в антивирусные базы и еще не попавших на анализ в антивирусные лаборатории - как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
- 2.1.2.12** обнаружение вредоносных объектов в HTML- и PDF-документах, включая обфусцированные эксплойты в JavaScript, находящиеся в документах данных типов. Возможность извлечения и анализа «невидимых» IFRAME-элементов. Возможность извлечения для проверки скриптов любой сложности и снятие с них защиты;
- 2.1.2.13** обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA);
- 2.1.2.14** обнаружение вредоносных объектов в DEX-файлах (Android);
- 2.1.2.15** обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками.

2.2 Требования к системе управления антивирусной защитой

- 2.2.1** Система должна быть построена по клиент-серверной архитектуре с возможностью установки антивирусного сервера централизованного управления не только на серверы, но и на рабочие станции под управлением следующих ОС:

- 3** Microsoft Windows 7 / Windows 8 / Windows 8.1 / Windows 10 / Windows 11;
- 4** Microsoft Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022;
- 5** Linux, при наличии библиотеки glibc 2.13 или более поздней версии;
- 6** FreeBSD 11.3 или более поздней версии.

- 6.1.1** Сервер централизованного управления должен быть единым для всех защищаемых объектов, не зависимо от их операционных систем: Windows/Linux/macOS/Android.

- 6.1.2** Система управления должна быть доступной из любой операционной системы, поддерживающей браузеры Windows® Internet Explorer®, Microsoft Edge®, Mozilla® Firefox®, Google Chrome®, Opera®, Safari® (в том числе с ОС Microsoft Windows, Linux, FreeBSD), без ограничений на использование последних версий браузеров и без доустановки какого-либо программного обеспечения как на стороне сервера управления, так и на стороне администратора Системы.

- 6.1.3** Аутентификация администраторов должна быть возможна следующими способами:

- 7** из БД Сервера;
- 8** с использованием LDAP/AD;
- 9** с использованием RADIUS;
- 10** с использованием PAM.

- 10.1.1** Должна быть реализована возможность построения иерархической системы серверов управления - главных, подчиненных и равноправных, с возможностью распространения лицензий по межсерверным связям, а также возможность автоматического обновления лицензионного ключевого файла.

- 10.1.2** Система управления должна иметь возможность:

- 11 объединения информации от нескольких серверов на одном;
- 12 распределения рабочих станций между серверами для получения обновлений в целях снижения общей нагрузки на сеть;
- 13 обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий;
- 14 построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне.
 - 14.1.1 Должна быть реализована возможность запуска мобильного центра управления Системой на операционных системах iOS и Android с помощью соответствующих мобильных приложений, без использования веб-браузеров.
 - 14.1.2 Система управления должна иметь возможность:
 - 14.1.2.1 использования как внешней, так и внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера). В качестве внешних могут выступать Oracle, PostgreSQL, Postgres Pro, Jatoba, любая СУБД через ODBC-драйвер для операционных систем MS Windows и Linux;
 - 14.1.2.2 замены типа используемой СУБД в ходе работы, после установки серверной части – без необходимости переустановки серверной части Системы.
 - 14.1.2.3 управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов;
 - 14.1.2.4 в случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API;
 - 14.1.2.5 самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления;
 - 14.1.2.6 экспорта отчетов в форматы CSV, XML, HTML и PDF;
 - 14.1.2.7 подписки и получения новостей от компании разработчика, в том числе информирующих об актуальных угрозах, в консоли центра управления;
 - 14.1.2.8 наличия множественных путей уведомления пользователей и администраторов путем отправки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap;
 - 14.1.2.9 отправки системным администратором информационных сообщений пользователям произвольного содержания, включающих: текст сообщения; гиперссылки на интернет-ресурсы; любое графическое изображение, по сети в режиме реального времени через Web-интерфейс Системы;
 - 14.1.2.10 ограничения сетевого трафика как при установке агентов, так и при их обновлении;
 - 14.1.2.11 скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС Android, Mac OS X и ОС семейства UNIX;
 - 14.1.2.12 централизованного обновления антивирусных баз на всех защищаемых объектах. Доставки обновлений на рабочие места пользователей как по расписанию, так и сразу после их получения;
 - 14.1.2.13 управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений;
 - 14.1.2.14 наличия возможности групповых обновлений;
 - 14.1.2.15 обновлений по защищенному каналу с использованием SSL-сертификатов;

- 14.1.2.16 организации отложенного обновления;
- 14.1.2.17 автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов;
- 14.1.2.18 выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части;
- 14.1.2.19 чтения полного пакета документации администратора и пользователя непосредственно в консоли центра управления.
- 14.1.3 Система должна обладать специальной политикой для мобильных пользователей (ноутбуки), при применении которой, мобильные пользователи должны иметь возможность редактирования настроек антивирусного пакета и обновления через Интернет при отсутствии доступа к антивирусному серверу. Применение политики должно происходить через Web-интерфейс, без необходимости использования файлов конфигурации типа *.xml.
- 14.1.4 Система управления должна обладать возможностью встроенного автоматического копирования критически важных данных и конфигурации антивирусного сервера по заранее заданному расписанию, а также опцию восстановления сервера из резервной копии.
- 14.1.5 В системе управления должен быть реализован компонент позволяющий проводить сканирование сети с целью обнаружения рабочих станций и определения наличия антивирусного агента в режимах поиска в Active Directory, по NetBIOS, по ICMP, по TCP.
- 14.1.6 В центре управления должна быть реализована групповая политика на основе предустановленных системных и пользовательских групп. Предустановленные системные группы должны позволять обращаться: ко всем защищаемым объектам, по объектам Active Directory, по операционным системам, по политикам, по профилям настроек, по сетевым протоколам, по статусу объекта, по персональным настройкам.
- 14.1.7 Система управления должна обладать возможностью контроля запуска приложений, как на основе запрещающих и разрешающих правил, так и на основе функционального анализа приложений по следующим группам: запуск приложений, загрузка и исполнение модулей, запуск скриптовых интерпретаторов, загрузка драйверов, установка MSI-пакетов, целостность исполняемых файлов.
- 14.1.8 Предоставление отчетности по мониторингу антивирусного программного обеспечения, с использованием сервера централизованного управления.
- 14.1.9 Централизованный сбор статистической информации с созданием отчетов о состоянии антивирусной защиты и их консолидация, возможность автоматического формирования статистических отчетов по заданным параметрам с последующей отправкой администратору по электронной почте.
- 14.1.10 В Системе должен быть реализован менеджер лицензий, поддерживающий иерархический список лицензионных ключей. Менеджер лицензий должен предоставлять следующие возможности: просмотр информации о лицензии, добавление нового лицензионного ключа, обновление лицензионного ключа, замена лицензионного ключа, расширение списка лицензионных ключей объекта, удаление лицензионного ключа и удаление объекта из списка лицензирования, передачу лицензий на соседний сервер управления, редактирование лицензий, переданных на соседний сервер управления.
- 14.1.11 Система должна иметь возможность шифрования трафика между серверами и защищаемыми станциями в целях предотвращения утечки конфиденциальной информации.

- 14.1.12** Выпуск обновлений вирусных баз производителем Системы не менее 20 раз в сутки, что должно подтверждаться созданным Системой отчетом;
- 14.1.13** В случае размещения антивирусных серверов во внутренней сети без доступа к сети Интернет получение обновлений должно быть возможно с помощью специальной утилиты автономной загрузки репозитория.
- 14.1.14** Поддержка виртуальной инфраструктуры, интеграция с инфраструктурой виртуальных рабочих мест (VDI), поддержка гипервизоров VMware, Microsoft Hyper-V, Xen, KVM (Kernel-based Virtual Machine).

14.2 Требования к программным средствам антивирусной защиты рабочих станций и серверов под управлением ОС семейства Microsoft Windows

- 14.2.1** Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения тендера версию ПО должна обеспечивать защиту рабочих станций и серверов под управлением операционных систем:
- 15** MS Windows XP SP2 / Windows Vista SP2/ Windows 7 SP1/ Windows 8 / Windows 8.1 / Windows 10 / Windows 11.
- 16** MS Windows Server 2003 SP1 / Windows Server 2008 SP2/ Windows Server 2008 R2 SP1/ Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019 / Windows Server 2022.
- 16.1.1** Программные средства Системы должны обеспечивать осуществление антивирусной и антиспам защиты на рабочих станциях, включая постоянную защиту от руткит-технологий, наличие резидентного антируткит драйвера.
- 16.1.2** Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения.
- 16.1.3** С целью противодействия вредоносным программам, запущенным на компьютере, для установки должен использоваться защищенный антируткитом инсталлятор (без использования Windows Installer).
- 16.1.4** В связи с возможными ограничениями канала доступа в сеть Интернет установка системы защиты должна быть возможной без доступа в сеть Интернет - дистрибутив должен содержать все компоненты системы защиты, а также базы данных признаков вредоносных программ и вредоносных ресурсов сети Интернет, доступ к которым может регулироваться системой защиты.
- 16.1.5** Для работы системы защиты не должны использоваться внешние библиотеки, а также среда .Net Framework, целостность которых не находится под контролем системы самозащиты и компрометация которых может привести к ошибкам отображения информации системы защиты или иным проблемам, связанным с интерфейсом системы защиты.
- 16.1.6** Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства, в том числе за счет возможности отложенной проверки файлов, открываемых «на чтение», а также использования особенностей современных архитектур.
- 16.1.7** Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ, так и от спама.

- 16.1.8** Система должна иметь возможность ограничения времени работы пользователей в сети Интернет, а также времени работы за компьютером.
- 16.1.9** Права доступа к настройкам компонентов антивирусного пакета для пользователей должны определяться администратором Системы с возможностью самостоятельной настройки пользователями только в пределах делегированных администратором прав и без применения пароля.
- 16.1.10** Система защиты рабочих станций должна обеспечивать фильтрацию трафика в мгновенных сообщениях Mail.Ru Agent, ICQ, Jabber, QIP, Pidgin и другие, включая антивирусную проверку пересылаемых вложений, а также автоматическое удаление из сообщений ссылок, ведущих на вредоносные и фишинговые сайты.
- 16.1.11** Система защиты рабочих станций должна обеспечивать фильтрацию выдачи результатов поисковых систем Google, Yandex, Yahoo!, Bing, Rambler с показом только безопасных с точки зрения поисковых систем и системы защиты ресурсов.
- 16.1.12** Контроль сетевых подключений на уровне приложений, позволяющий контролировать доступ конкретных программ и процессов к сетевым ресурсам и регистрировать информацию о попытках доступа в журнале приложений.
- 16.1.13** Фильтрация на уровне пакетов позволяющая контролировать доступ к сети Интернет вне зависимости от программ, инициирующих подключение.
- 16.1.14** В Системе должна быть реализована превентивная защита, в дополнение к сигнатурному и эвристическому анализу, состоящая из таких компонентов как:
- 17** защита от вымогателей – позволяющая защитить от троянцев-шифровальщиков;
 - 18** защита от эксплойтов – позволяющая защитить от вредоносных объектов, пытающихся использовать уязвимости в популярных приложениях для проникновения в систему;
 - 19** поведенческий анализ – контролирующий поведение запущенных программ по всем критическим с точки зрения Системы направлениям, таким как: файл HOSTS; целостность запущенных приложений; низкоуровневый доступ к диску; загрузка драйверов; параметры запуска приложений; драйверы мультимедийных устройств; параметры оболочки Winlogon, нотификаторы Winlogon; автозапуск оболочки Windows; ассоциации исполняемых файлов; политики ограничения запуска программ (SRP); плагины Internet Explorer (BHO); автозапуск программ; автозапуск политик; конфигурация безопасного режима; параметры диспетчера сеансов Windows; системные службы.
- 19.1.1** В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
- 19.1.2** Возможность реализации защиты виртуальных рабочих мест с помощью установки виртуальных агентов.
- 19.2 Требования к программным средствам антивирусной защиты рабочих станций и серверов под управлением ОС семейства Linux**
- 19.2.1** Поддержка процессоров следующих архитектур и систем команд:
- 20** Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64);
 - 21** ARM64;
 - 22** IBM POWER (ppc64el).

- 22.1.1** Система, используя актуальную на момент проведения тендера версию ПО, должна обеспечивать защиту рабочих станций и серверов, использующих Samba версий 3.6 - 4.16, или Novell Storage Services (NSS) под управлением операционных систем:
- 23** Linux на основе ядра с версией 2.6.37 и новее, использующая PAM и библиотеку glibc версии 2.13 и новее;
- 24** FreeBSD 11, 12;
- 25** Novell Open Enterprise Server SP2 на базе SUSE Linux Enterprise Server 10 SP3 и новее.
- 25.1.1** Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System).
- 25.1.2** В случае использования версий Samba, отличных от вышеперечисленных, либо Samba для 64-битных платформ семейства Linux должна существовать возможность компиляции модулей интеграции из исходных кодов.
- 25.1.3** Возможность установки из универсального пакета для UNIX-систем, независимого от типа и версии используемой операционной системы, репозитория или пакета рассчитанного на работу с используемым в ОС менеджером пакетов.
- 25.1.4** Возможность установки и обновления Системы как через средства командной строки, так и с помощью графического инсталлятора.
- 25.1.5** Возможность автоматической установки модулей, необходимых для установки необходимых компонентов Системы.
- 25.1.6** Возможность установки компонентов Системы на зараженные вредоносными программами объекты без их предварительного лечения с последующим лечением заданных файловых областей.
- 25.1.7** Поддержка подсистем обеспечения дополнительной безопасности SELinux, систем мандатного управления доступом PARSEC, а также режима замкнутой программной среды (ЗПС).
- 25.1.8** Возможность мониторинга файловой системы с использованием как механизма fanotify, предоставляемого ОС, так и с помощью специального модуля ядра Linux (Linux kernel module).
- 25.1.9** Возможность автоматического распознавания моментов монтирования и отмонтирования новых томов файловой системы (например, на накопителях USB-flash, CD/DVD, массивов RAID и т. п.) и корректировки списка наблюдаемых областей по мере необходимости.
- 25.1.10** Возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства.
- 25.1.11** Возможность управления параметрами проверки составных файлов, таких, как архивы, почтовые файлы, упакованные объекты и прочие контейнеры.
- 25.1.12** В Системе должна быть реализована функция постоянного контроля установленных сетевых соединений с возможностью проверки трафика, передаваемого через защищенные сетевые соединения, использующие протоколы на основе SSL и TLS.
- 25.1.13** В Системе должен быть реализован веб-фильтр с возможностью блокировки ресурсов Интернет по категориям, а также работы в режиме Белого/Черного списков.
- 25.1.14** Система должна поддерживать возможность порождения нескольких одновременно действующих процессов проверки.
- 25.1.15** Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
- 25.1.15.1** поиск и удаление вирусов всех известных типов;

- 25.1.15.2 антивирусного сканирования, заключающегося в полной или выборочной проверке на наличие угроз и проводимого как по команде администратора, так и по расписанию;
- 25.1.15.3 антивирусной проверке «на лету» загружаемых файлов, как на сервер, так и с него;
- 25.1.15.4 автоматического запуска антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
- 25.1.15.5 запуска задач по расписанию и/или сразу после загрузки операционной системы;
- 25.1.15.6 настройки расписания сканирования с указанием параметров запуска.
- 25.1.16 Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, а также действий по отношению к вредоносным объектам различных типов.
- 25.1.17 Сканирующее ядро должно обеспечивать поиск вирусов и других вредоносных объектов в файлах и загрузочных записях дисковых устройств (MBR - Master Boot Record, VBR - Volume Boot Record).
- 25.1.18 Возможность использования для проверки файлов метода потоковой проверки (flow), а также метода проксирования (проxy).
- 25.1.19 Возможность проверки данных, не представленных в виде файлов, полученных через сеть, а также организации распределенной проверки файлов на наличие угроз.
- 25.1.20 Возможность оперативной проверки на наличие угроз файлов, находящихся на локальном устройстве, с которого осуществляется доступ к веб-интерфейсу управления.
- 25.1.21 Возможность проверки на наличие угроз файлов, находящихся на удаленных узлах сети. В качестве таких узлов могут выступать не только рабочие станции и серверы, но и роутеры, ТВ-приставки и прочие «умные» устройства, образующие «Интернет вещей» предоставляющих доступ Secure Shell или Telnet.
- 25.1.22 В состав Системы должен входить SNMP-агент, предназначенный для интеграции с системами мониторинга (Munin, Nagios, Zabbix).
- 25.1.23 Интеграция в систему централизованного управления антивирусной защитой, позволяющая обеспечить управление системой антивирусной защиты «из одной точки» с максимальным удобством для системного администратора.

25.2 Требования к программным средствам антивирусной защиты рабочих станций и серверов macOS

- 25.2.1 Защита устройств под управлением macOS от угроз любого типа: вирусов, руткитов, троянских программ, шпионского и рекламного ПО, хакерских утилит и различных вредоносных объектов, с использованием современных технологий обнаружения и обезвреживания угроз.
- 25.2.2 Защита устройств под управлением следующих версий операционных систем: OS X 10.11 El Capitan / macOS 10.12 Sierra / macOS 10.13 High Sierra / macOS 10.14 Mojave / macOS 10.15 Catalina / macOS 11 Big Sur / macOS 12 Monterey / macOS 13 Ventura / macOS 14 Sonoma.
- 25.2.3 Проверка объектов автозапуска, сменных носителей информации, сетевых и логических дисков, почтовых форматов, файлов и каталогов, включая упакованные и находящиеся в архивах.
- 25.2.4 Мониторинг файловой системы в режиме реального времени, контроль запущенных программ и процессов, с возможностью исключения из проверки отдельных папок и файлов.

- 25.2.5** Мониторинг интернет-трафика в режиме реального времени по протоколам HTTP/HTTPS на содержание угроз, ограничение доступа к nereкомендуемым сайтам, а также к отдельным сайтам и категориям интернет-ресурсов, с возможностью исключения из проверки веб-трафика отдельных сайтов и сетевых соединений для определенных пользователем приложений.
- 25.2.6** Контроль всего входящего и исходящего сетевого трафика, блокировка доступа приложений к сетевым ресурсам согласно выбранному режиму работы и отдельным правилам фильтрации.
- 25.2.7** Защита конфиденциальности с помощью контроля доступа приложений к веб-камерам и микрофонам.
- 25.2.8** Использование системных уведомлений macOS, для отображения сообщений об обнаружении угроз, их обезвреживании или возникновении ошибок в работе компонентов.
- 25.2.9** Возможность подключения к облачным сервисам компании-разработчика для защиты пользователей от инфицированных файлов и посещения нежелательных сайтов.

И.о. начальника службы АСУ:



Котова Е.В.