«ПОДТВЕРЖДАЮ»

Ташкентского городского управления
Палат государственных кадастров
Заместитель начальника
_____А.А.Исламов
«___»_____ 2022 й.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1.	Заказчик	Ташкентского городского управления Палат государственных кадастров (далее по тексту «Заказчик»). Адрес: ,. г.Ташкента район Миробод ул Кичик халка йули дом 9
2.	Исполнитель	Исполнитель в рамках выделенного бюджета может предложить оборудование, с характеристиками, являющимися улучшенными (аналогичные) по отношению к указанным в техническом задании. Для соответствия техническому заданию допускается установка опциональных модулей и устройств имеющихся в линейке производителей оборудования. Исполнитель должен предоставить полностью укомплектованные работоспособные компьютерные техники при необходимости, предложить дополнительные модули, продукты и услуги, по каким-либо причинам не учтенные Покупателем, но обязательные для обеспечения полноты использования запрашиваемой конфигурации. Поставляемое оборудование должно соответствовать международным стандартам, которые должны быть самыми новейшими из выпускаемых соответствующими учреждениями. Вся сопроводительная документация должна быть составлена на русском языке или узбекском языке и передана Заказчику вместе с поставляемым оборудованием.
3.	Страхование	В зависимости от условий поставок
4.	Место поставки	(Адрес: Республика Узбекистан,. г.Ташкента район Миробод ул Кичик халка йули дом 9

9.	Требования к документации	Вместе с отгруженными товарами Исполнитель обязуется направить Заказчику нижеперечисленные документы: - счёт-фактура (инвойс) на сумму общей стоимости отгруженного товара на имя Заказчика; - транспортная накладная, выписанная на имя Покупателя; - упаковочные листы; - сертификат происхождения; - ГТД (грузовую таможенную декларацию) предлагаемое оборудование должно быть официально импортировано в РУз;
10.	Требования к сроку поставки	Максимальный срок поставки товара – 7 банковских дней с момента поступления предоплаты на счет Поставщика. Поставка частями допускается по письменному согласованию Сторон.
11.	Требования к гарантийному обслуживанию (срок, место)	Гарантийный срок для компьютерной техники 36 месяцев после ввода в эксплуатацию или подписания акт приема-передачи. Если в течении гарантийного срока продукция окажется дефектной, неукомплектованной и не будет соответствовать требованиям настоящего технического задания, либо ТУ изготовителя, независимый авторизованный сервис центр обязан устранить дефекты, документировать, а в случае невозможности устранения дефекта заменить продукцию на новую после получения письменного уведомления Заказчика. Все расходы, связанные с устранением дефектов, доукомплектованием и заменой относятся за счёт авторизованного сервис центра. *Условия сервисного обслуживания:* Сервис центр на территории Республики Узбекистан с филиалами и приемными пунктами в регионах Республики Узбекистан. В случае сбоев или неправильного функционирования оборудования или программного обеспечения в течение гарантийного периода, произошедший из-за самой Продукции, Сервис центр гарантирует бесплатную наладку (ремонт) или восстановление оборудования или программного обеспечения в течение пятнадцати (15) дней с даты уведомления со стороны Заказчика. Поставщик гарантирует наступление даты окончания поддержки EOS (end of support/service) аппаратного обеспечения (всех комплектующих) не ранее чем через 5 лет с момента заключения договора поставки аппаратного обеспечения.

		Поддержка аппаратного обеспечения подразумевает доступность сервисного обслуживания всех блоков и компонентов аппаратного обеспечения. Поставщик гарантирует наступление даты окончания приема заказов, производства и поставки отдельных плат и модулей EOM (end of market for expansion) не ранее чем через 5 лет с момента заключения договора поставки аппаратного обеспечения.
12.	Требования к расходам на эксплуатацию	Все транспортные и другие расходы, связанные с заменой дефектного товара и его допоставкой, производятся за счет Поставщика. При возврате товара по рекламации Заказчика и допоставке продукции Поставщик все расходы несет Продавец, а также в маркировку продукции. Поставщик должен предоставить следующую информацию: - по параметрам жизненного цикла закупаемого оборудования с указанием дат окончания поддержки оборудования, окончания приема заказов на поставку ЗИП и комплектующих (отдельных плати модулей) для расширения емкости, о начале продаж данного аппаратного обеспечения в мире; - по методам достижения минимального уровня TCO (Total Cost of Ownership) за счет предлагаемого оборудования (технологического решения), функционала, и т.п. уникальных решений производителя сроком на не менее 5 лет; - об энергопотреблении и энергоэффективности закупаемого оборудования согласно нормативным документам производителя и др. Поставляемые оборудования не должны требовать дополнительных расходов при эксплуатации, кроме расходов электроэнергии и необходимого ремонта.
13.	Порядок сдачи и приема выполненных работ	Поставляемые оборудования не должны требовать дополнительных расходов при эксплуатации, кроме расходов электроэнергии и необходимого ремонта. Приемка поставленного товара осуществляется путем контроля целостности и комплектности поставляемого товара. С целью принятия результатов работ (услуг), Заказчик имеет право создать в установленном порядке Приемочную комиссию. Совместно с предъявлением Приемочной комиссией товаров (работ, услуг), производится сдача разработанного Исполнителем комплекта документации, перечня и требований к оформлению и иными и руководящими документами, действующими на территории

		Республики Узбекистан. По итогам сдачи приема выполненных работ подписывается двухсторонний акт. Статус и состав приемочной комиссии определяется Заказчиком.
14.	Обязательные требования к Поставщику	• Наличие оригинала соответствующего документа авторизации от производителя/ей на поставку оборудования по данному отбору – в частности, от подразделения производителя, имеющего полномочия осуществлять деятельность непосредственно в стране Заказчика; • Информация о сервисных центрах на территории Республики Узбекистан для обеспечения гарантийного обслуживания с филиалами и приемными пунктами в регионах Республики; • В целях приобретения оригинального лицензионного программного обеспечения, право на поставку всего предлагаемого ПО должно быть подтверждено авторизационным письмом от соответствующего производителя (Dr. Web)
15.	Условия оплаты	Оплата Поставщику за поставляемый Товар будет производиться Покупателем в UZS, прямым банковским переводом на счёт Поставщика следующим образом: Предоплата в размере 30% от общей стоимости поставляемого Товара производится в течение 10 (десяти) банковских дней, с момента вступления заключаемого Договора в силу; Оставшаяся часть оплаты в размере 70% от стоимости Товара, производиться в течение 10 (десяти) банковских дней с даты поставки Товара заключаемого Договора.

		используя слот расширения PCIe. Контроллеры семейства 10 поколения совместимы с аккумуляторами Smart Storage. Аккумуляторы Smart Storage поддерживают одновременно несколько устройств и приобретаются отдельно.
2.1.10.	Сетевой контроллер	Не менее Ethernet 1 Гбит/с 4 порт
2.1.11.	Блоки питания горячей замены	Не менее 2, с мощностью 500 Ватт
2.1.12.	Поддерживаемые операционные системы	Hypervisor, Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES).

Техническая спецификация к ПО

Участники конкурса должны представить авторизационное письмо от производителя Системы, подтверждающее наличие партнерских отношений с компанией-производителем на поставку и поддержку товара. 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. - Наличие локальной службы технической поддержки от производителя в Республике Узбекистан как на русском, так и на узбекских языках. - Программный интерфейс всех антивирусных средств, включая средства управления, должен быть реализован как на русском, так и на узбекских языках. - 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 узбеких языках. - Поставляемый серийный номер должен иметь возможность отложенной активации без ограничения срока. Срок действия лицензионных ключевых файлов на все поставляемые программные продукты должен начинаться с момента активации серийного номера	
Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows	
обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п	Обязательно
обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками	Обязательно
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	Обязательно
обнаружение вирусов внутри контейнеров, не имеющих строгого формата (HTML, MIME)	Обязательно
обнаружение вирусов внутри контейнеров с нечетким значением размера объекта (WISE,	Обязательно

ACTIVE MARK, 7-ZIP, JAR, ASTRUM WIZARD, CHM, BINARYRES и т.д.	
антивирусную проверку файлов и объектов, имеющих формат Smart Install Maker (SIM); DMG, HFS, XAR, Universal Binary (MacOS); SIS (Symbian 9); INNO SETUP (5.3.9 и выше); SETUP FACTORY (линейки 7,8); XENOCODE; TARMA INSTALL (линейка 3); XZ (UNIX); COMPRESS; SQUAHFS; CHILKAT ZIP; пакеты LHA (AWARD BIOS)	Обязательно
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, Setup Factory, Setup Generator Pro, SXA ZIP, Tarma Install, Thunder Setup System, Wise Installation System, Alloy	Обязательно
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	Обязательно
разбор неформатированных почтовых баз и обработка писем с высокой вложенностью (например, переписки с большим количеством ответов и пересылок RE/FW), поддержка формата TNEF	Обязательно
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	Обязательно
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	Обязательно
обнаружение угроз по лицензионным данным (ASPROTECT, PEP и ENIGMA)	Обязательно
обнаружение угроз направленных на 64-разрядные операционные системы, в том числе с помощью специальной 64-битной версии антируткит модуля	Обязательно
обнаружение вредоносных объектов в DEX-файлах (Android)	Обязательно
в целях ускорения проверки архивов и упакованных файлов должно обеспечивать опознание вредоносных программ без запуска распаковщика	Обязательно

Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows	
Система (в том числе с помощью системы централизованного управления), используя актуальную на момент проведения конкурса версию ПО должна обеспечивать защиту серверов под управлением операционных систем: MS Windows Server 2003 SP1 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019	Обязательно
Программные средства Системы должны обеспечивать осуществление антивирусной защиты, включая постоянную защиту от руткит-технологий, наличие резидентного антируткит драйвера.	Обязательно
Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами сервера без их предварительного лечения	Обязательно
С целью противодействия вредоносным программам, запущенным на сервере, для установки должен использоваться защищенный антируткитом инсталлятор (без использования Windows Installer).	Обязательно
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.	Обязательно
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	Обязательно
Компоненты системы должны иметь возможность управления использованием ресурсов сервера 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	Обязательно
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	Обязательно
Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Linux	

Система, используя актуальную на момент проведения конкурса версию ПО должна обеспечивать защиту ресурсов серверов, использующих Samba версий 3.6.0, 4.0.0–4.10.0, и функционирующих под управлением операционных систем	Обязательно
Linux, имеющих версию ядра 2.6.37 и выше, версия glibc 2.13 и выше.	Обязательно
FreeBSD версии 9.x и выше;	Обязательно
Поддержка процессоров следующих архитектур и систем команд: Intel/AMD: 32-бит (IA-32, x86); 64-бит (x86-64, x64, amd64); ARM64;	Обязательно
Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;	Обязательно
Интеграция Системы с Samba должна осуществляться с помощью модуля VFS (Virtual File System	Обязательно
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;	Обязательно
Установка модулей Системы в зависимости от типа используемой операционной системы должна происходить с помощью 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.	Обязательно
Установка и обновление Системы должны быть возможны как через средства командной строки, так и с помощью графического инсталлятора	Обязательно
Система установки системы должна включать возможность автоматической установки модулей, необходимых для установки необходимых компонентов	Обязательно
Компоненты системы должны иметь возможность управления использованием серверных ресурсов при выполнении сканирования файлового пространства	Обязательно
В Системе должна быть реализована возможность мониторинга файловой системы с использованием как механизма fanotify, предоставляемого ОС, так и с помощью специального модуля ядра Linux (Linux kernel module	Обязательно
Должна быть реализована возможность автоматического распознавания моментов монтирования и отмонтирования новых томов файловой системы (например, на накопителях USB-	Обязательно

flash и CD/DVD, массивов RAID и т. п.) и корректировки списока наблюдаемых областей по мере необходимости	
Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы настройки. При этом в случае необходимости внесения изменений, Система должна обеспечивать возможность простого и гибкого изменения настроек администраторами Системы и пользователем в рамках имеющихся у них прав	Обязательно
Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением заданных файловых областей	Обязательно
Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей: поиск и удаление вирусов всех известных типов в файлах; антивирусное сканирование ресурсов сервера, заключающееся в однократной полной или выборочной проверке на наличие угроз и проводимое как по команде администратора, так и по расписанию	Обязательно
антивирусная проверка «на лету» файлов, загружаемых как на сервер, так и с него	Обязательно
помещение найденных зараженных и подозрительных файлов в карантин для дальнейшего анализа	Обязательно
автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС	Обязательно
запуск задач по расписанию и/или сразу после загрузки операционной системы	Обязательно
настройка расписания сканирования с указанием параметров запуска	Обязательно
Управление программой должно осуществляться как с помощью веб-интерфейса, так и непосредственно через конфигурационные файлы. Система управления должна поддерживать возможность настройки параметров антивирусного сканирования с указанием файлов и каталогов, подлежащих антивирусной проверке, и действий по отношению к вредоносным объектам различных типов	Обязательно
Администратор системы должен иметь возможность: определять необходимый уровень анализа, в том числе путем отключения эвристического анализа, ограничения размера файла и глубины проверки; определять типы проверяемых файлов, в том числе с использованием масок;	Обязательно

задавать различные действия по отношению к различным типам вредоносных объектов в случае их обнаружения. управлять детализацией протоколов антивирусной проверки; просматривать результаты антивирусной проверки; просматривать информацию об используемом ключевом файле и его владельце; запускать периодическую проверку в приоритетном или в фоновом режиме; использовать альтернативные языковые файлы; просматривать и изменять настройки компонентов как в табличной форме, так и в текстовом редакторе	
Сканирующее ядро должно обеспечивать поиск вирусов и других вредоносных объектов в файлах и загрузочных записях (MBR — Master Boot Record, VBR — Volume Boot Record) дисковых устройств	Обязательно
Возможность использования для проверки файлов помимо стандартного метода, метода потоковой проверки (flow), а также метода проксирования (proxy	Обязательно
Возможность проверки данных, не представленных в виде файлов в локальной файловой системе, полученных через сеть, а также для организации распределенной проверки файлов на наличие угроз	Обязательно
Возможность оперативной проверки на наличие угроз файлов, находящихся на локальном устройстве, с которого осуществляется доступ к веб-интерфейсу управления	Обязательно
Возможность проверки на наличие угроз файлов, находящиеся 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	Обязательно
В состав Системы должен входить SNMP-агент, предназначенный для интеграции с системами мониторинга (Munin, Nagios, Zabbix)	Обязательно
Интеграция в систему централизованного управления антивирусной защитой, позволяющая обеспечить управление системой антивирусной защиты «из одной точки» с максимальным удобством для системного администратора	Обязательно
Требования к системе управления антивирусной защитой	
Система должна быть построена по клиент-серверной архитектуре с возможностью установки антивирусного сервера централизованного управления не только на серверные ОС MS Windows Server 2008 R2 / 2012 / 2012 R2 / 2016 / 2019, но и на рабочие станции под управлением MS Windows 10 / 8.1 / 8 / 7. Кроме того, должна быть реализована возможность установки сервера централизованного	Обязательно

управления на ОС FreeBSD 10.3 и старше; а также Linux	
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	Обязательно
Аутентификация администраторов должна быть возможна следующими способами: из БД Сервера; с использованием LDAP/AD; с использованием RADIUS; с использованием PAM	Обязательно
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. Система должна иметь возможность	Обязательно
объединения информации от нескольких серверов на одном	Обязательно
распределения защищаемых серверов между серверами управления для получения обновлений в целях снижения общей нагрузки на сеть	Обязательно
обмена статистикой в рамках одной иерархической сети между антивирусными серверами различных версий	Обязательно
контроля отсутствия связанных серверов в расписании антивирусного сервера	Обязательно
построения многоуровневой системы управления с возможностью настройки ролей администраторов и пользователей, а также форм предоставляемой отчетности на каждом уровне	Обязательно
Должна быть реализована возможность запуска мобильного центра управления Системой на операционных системах iOS и Android без использования веб-браузеров	Обязательно
Система управления должна иметь возможность: использования как внешней, так и внутренней СУБД (поставляемой в составе дистрибутива антивирусного сервера). В качестве внешних могут выступать Oracle, PostgreSQL, MySQL, любая СУБД через ODBC-драйвер для операционных систем MS Windows и Linux	Обязательно
замены типа используемой СУБД в ходе работы, после установки серверной части – без	Обязательно

необходимости переустановки серверной части Системы	
управления базой данных средствами системы управления, в том числе возможности очистки базы данных, ее анализа, выполнения произвольных SQL-запросов	Обязательно
в случае интеграции с внешними подсистемами с помощью встроенного Web API, должна иметься возможность аудита действий, произведенных с помощью функций данного Web API	Обязательно
самостоятельного написания обработчиков событий на языке Lua, а также выполнения произвольных Lua-скриптов с помощью средств системы управления	Обязательно
экспорта отчетов в форматы CSV, XML, HTML и PDF	Обязательно
подписки и получения новостей от компании разработчика, в том числе, информирующих об актуальных угрозах в консоли центра управления	Обязательно
наличия множественных путей уведомления пользователей и администраторов путем посылки почтового сообщения, звукового оповещения, всплывающего окна, записи в журнал событий, SNMP-trap	Обязательно
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	Обязательно
ограничения сетевого трафика как при установке агентов, так и при их обновлении	Обязательно
скачивания конфигурационных файлов с настройками подключения антивирусных агентов для ОС семейства UNIX	Обязательно
централизованного обновления антивирусных баз на всех защищенных серверах, в том числе находящихся в режиме off-line, доставки обновлений как по расписанию, так и сразу после их получения	Обязательно
управления ревизиями обновлений продуктов, находящихся в репозитории антивирусного сервера, включая откат обновлений	Обязательно
наличия возможности групповых обновлений; обновлений по защищенному каналу с использованием SSL-сертификатов; организации отложенного обновления	Обязательно
автоматического перехода установленного ПО на более новые версии, в том числе с возможностью выбора обновляемых компонентов	Обязательно
выбора и настройки устанавливаемых компонентов до начала установки антивирусного пакета на клиентские части	Обязательно

чтения полного пакета документации администратора и пользователя непосредственно в консоли центра управления	Обязательно
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 без использования файлов конфигурации типа *.xml	Обязательно
В системе управления должен быть реализован компонент позволяющий проводить сканирование сети с целью обнаружения объектов и определения наличия на них антивирусного агента в режимах поиска в Active Directory, по NetBIOS, по ICMP, по TCP	Обязательно
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	Обязательно
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	Обязательно
Выпуск обновлений вирусных баз производителем Системы не менее 20 раз в сутки независимо от того, рабочий, либо выходной день, что должно подтверждаться созданным Системой отчетом (файлом протокола	Обязательно
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	Обязательно